30 April 2018

Mr Wayne Byres
Chairman
Australian Prudential Regulation Authority
Level 12, 1 Martin Place
Sydney NSW 2000

Dear Mr Byres

**Prudential Inquiry into the Commonwealth Bank of Australia (CBA) Final Report**

On 28 August 2017, the Australian Prudential Regulation Authority (APRA) announced it would establish a Prudential Inquiry into the CBA. This followed a number of incidents in recent years that have damaged the reputation and public standing of the CBA group.

The purpose of the Prudential Inquiry, contained in the Terms of Reference, was to examine the frameworks and practices in relation to governance, culture and accountability within the CBA group that have contributed to these incidents. The Panel provided its Progress Report on 31 January 2018.

The Panel has now completed its assessment.

In brief, the Panel has identified a number of shortcomings in CBA's governance, culture and accountability frameworks, particularly in dealing with non-financial risks, and has made a series of recommendations designed to strengthen these frameworks. The Panel acknowledges that CBA's efforts to address these shortcomings have gained momentum under its new leadership, but regaining community trust will require, time, hard work and an undistracted risk and customer focus.

We are now pleased to provide you with the Final Report.

Yours sincerely

John Laker AO | Jillian Broadbent AO | Graeme Samuel AC

# PRUDENTIAL INQUIRY INTO THE COMMONWEALTH BANK OF AUSTRALIA

APRIL 2018

# CONTENTS

# EXECUTIVE SUMMARY

Community trust in banks has been badly eroded, globally and in Australia.

Globally, the financial crisis exposed a series of corporate scandals in banks. Governance weaknesses, serious professional misbehaviour, ethical lapses and compliance failures have resulted in substantial financial losses and record fines and penalties. 'Conduct risk' has entered the lexicon of bank Boards and regulators as a clear and present danger.

Banks in Australia were resilient through the crisis but their conduct is far from unblemished. Failings in the provision of financial advice, dubious lending practices, mis-selling of financial products, shortcomings in the setting of benchmark interest rates and compliance breaches have undermined community trust, drip by corrosive drip. Trust is the currency of banks, and improper conduct that undermines confidence or causes harm to customers devalues that currency.

The Commonwealth Bank of Australia (CBA) has acquired the status of a financial icon, built on its history, its continued financial success and its innovation in customer-facing technology. As Australia's largest financial institution, CBA touches a wide range of Australians. Hence, the community holds high expectations for the institution, as does CBA itself. Nonetheless, it too has had a succession of conduct and compliance issues – AUSTRAC's legal action a recent high-profile example – and these expectations have not been met. CBA has 'fallen from grace'.

How can this happen in a bank of CBA's stature and sophistication? This, fundamentally, is the question that the Inquiry Panel has been asked to address.

There is no simple answer, no 'silver bullet' remedy. A complex interplay of organisational and cultural factors has been at work. However, a common refrain has emerged from the Panel's intensive analysis and enquiries over the past six months: CBA's continued financial success dulled the senses of the institution.

This dulling has been particularly apparent, at least until recently, in CBA's management of its non-financial risks (that is, its operational, compliance and conduct risks). These risks were neither clearly understood nor owned, the frameworks for managing them were cumbersome and incomplete, and senior leadership was slow to recognise, and address, emerging threats to CBA's reputation. The consequences of this slowness were not grasped.

The Panel has identified a number of tell-tale markers:

- inadequate oversight and challenge by the Board and its gatekeeper committees of emerging non-financial risks;
- unclear accountabilities, starting with a lack of ownership of key risks at the Executive Committee level;
- weaknesses in how issues, incidents and risks were identified and escalated through the institution and a lack of urgency in their subsequent management and resolution;
- overly complex and bureaucratic decision-making processes that favoured collaboration over timely and effective outcomes and slowed the detection of risk failings;
- an operational risk management framework that worked better on paper than in practice, supported by an immature and under-resourced compliance function; and
- a remuneration framework that, at least until the AUSTRAC action, had little sting for senior managers and above when poor risk or customer outcomes materialised (and, until recently, provided incentives to staff that did not necessarily produce good customer outcomes).

In the environment of continued financial success, two critical voices became harder to hear, leaving

# EXECUTIVE SUMMARY

CBA vulnerable to missteps. One was the 'voice of risk', particularly for non-financial risks. The fact that there had been no large loss-making events in this area (though reputational damage clearly), the heavy emphasis of the risk function on financial risks, and the ineffective operational risk and compliance frameworks, muted that voice. The other was the 'customer voice'. Notwithstanding the customer focus enshrined in CBA's Vision and Values, and its industry-leading customer satisfaction scores, the customer voice (in particular, customer complaints) did not always ring loudly in decision-making forums and product design.

In the Panel's view, cultural factors lie at the heart of these shortcomings. Four broad and interlinked cultural traits stand out.

First, and obviously, a widespread sense of complacency has run through CBA, from the top down. CBA's first ranking on many financial measures created a collective belief within the institution that CBA was well run and inherently conservative on risk, and this bred over-confidence, a lack of appreciation for non-financial risks, and a focus on process rather than outcomes. CBA was desensitised to failings with customers. Delays in (or premature closing of) risk and audit issues and the late delivery of projects were readily tolerated, with limited remuneration or other consequences.

Secondly, CBA has been reactive – rather than proactive and pre-emptive – in dealing with risks. Operational risk and compliance issues tended to receive attention only once they had emerged clearly or reputational consequences began to rear, but that attention did not always guarantee timely and effective resolution. A slow, legalistic and reactive, at times dismissive, culture also characterised many of CBA's dealings with regulators. Taken together, complacency and reactivity led to a sense of 'chronic ease' in CBA, rather than the 'chronic unease' that has proven effective in driving safety cultures in other industries.

Thirdly, CBA became insular. It did not reflect on and learn from experiences and mistakes (its own and others'), including at Board and senior leadership levels. Lessons from previous incidents have not been readily captured or shared across CBA. A lack of intellectual curiosity and critical thinking about the 'bigger picture' and the full depth of risk issues inevitably limited CBA's ability to learn, anticipate and adapt. CBA turned a tin ear to external voices and community expectations about fair treatment.

The fourth cultural trait is the collegial and collaborative working environment at CBA, which places high levels of trust in peers, teams and leaders. Reinforcing this is the significant value placed on the 'good intent' of staff. These are positive elements of a sound culture. However, they have had a downside. Pursuit of consensus has lessened constructive criticism and has led to slower decision-making, lengthier and more complex processes, and a slippage of focus on outcomes. It has also impeded accountability and the individual ownership of risk issues. Trust has not been continually validated through strong metrics, healthy challenge and oversight. Good intent has been too readily used to excuse poor risk outcomes.

The Panel has made a series of specific recommendations designed to strengthen governance, accountability and culture within CBA. They focus on some 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 into CBA's DNA 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.

The Panel has also identified a number of 'better practice' benchmarks that CBA should aspire to meet.

CBA had acknowledged shortcomings ahead of the AUSTRAC action and this Inquiry. Remediation had begun, with a particular focus on upgrading risk management and compliance. These efforts will

need to be substantially enhanced under CBA's new leadership.

CBA's new remediation program is ambitious and on a scale that exceeds previous risk management initiatives. In some areas, it has anticipated the Panel's recommendations; in other areas, however, it remains a blank canvas. To succeed, it will be critical that the program breaks the mould – it cannot succumb to the weight of bureaucracy, unclear accountabilities and porous deadlines that have challenged earlier CBA projects. Milestones must be clear, realistic, and enforced. Senior leaders must take ownership and their remuneration should be linked to successful delivery.

Regaining community trust will require time, hard work and an undistracted risk and customer focus. Many of CBA's working practices and cultural traits are deeply ingrained and must be squarely addressed if the 'reset' of the institution recommended by the Panel is to succeed. The CBA Board must be up to this challenge, and the signs are positive. Significantly, the 'light hand on the tiller' of earlier years has been replaced by a firmer and more visible hand and oversight and challenge has intensified. In the end, however, it will be results that count.

The Report that follows may read as a long catalogue of shortcomings. That would be too narrow a read. The Panel acknowledges the undoubted financial strength and acumen of the CBA, its global standing, and the avowed commitment of staff to servicing customers. CBA needs to translate this financial strength and good intent into better meeting the community's needs and the standards expected of a systemically important bank in Australia. The Report is a road map for this journey.

# 1. INTRODUCTION

## 1.1. Background

On 28 August 2017, the Australian Prudential Regulation Authority (APRA) announced that it would establish a Prudential Inquiry into governance, culture and accountability within the CBA group. The Inquiry's mandate is to identify any shortcomings in the frameworks and practices in these areas and make recommendations as to how such shortcomings should be addressed.

The Inquiry was commissioned against the background of a number of incidents in CBA's recent history that have damaged its reputation and public standing. These incidents have included:

- mis-selling of margin loans to retail customers to invest in financial products recommended by Storm Financial (2008);
- misconduct by financial advisers in Commonwealth Financial Planning, part of CBA's wealth business (2010/11);
- fees for no service in financial advice (2012 to 2015);
- use of an outdated definition of heart attack in insurance products sold by CommInsure (2016);
- anti-money laundering (AML) breaches and AUSTRAC action (2017); and
- mis-selling of credit card insurance (2013 to 2018).

Each of these incidents is, in isolation, concerning. Each has been the subject of considerable public scrutiny. When considered together, they indicate shortcomings in the way CBA has managed its risks and its compliance obligations. Identifying these shortcomings and recommending how they should be promptly and adequately addressed are the key focuses of this Inquiry.

APRA subsequently announced that the Panel to conduct the Inquiry would comprise Jillian Broadbent AO, Dr John Laker AO and Professor Graeme Samuel AC.

The Terms of Reference for the Inquiry are provided in Appendix A. Background on the Panel members is provided in Appendix B.

## 1.2. Scope of the Inquiry

Within the timeframe provided (a little over six months), the Panel could not attempt an extensive audit of CBA's activities. Hence, the Panel was careful to confine the scope of the Inquiry to ensure that its findings are based on recent business practices and prevailing culture, and that its recommendations are timely and relevant.

The Panel has concentrated its analysis and enquiries on developments over the past five years. For much of this period, CBA had a relatively stable Board and senior leadership team and their influence on CBA's evolution can be readily discerned. Renewal is now under way at both these levels. Where issues appear to have more deep-seated roots, this is called out.

In addition, the Panel has not sought to conduct a forensic examination of the incidents listed above. Some are now quite dated and have already been subject to exhaustive review by regulators, Parliamentary inquiries and the courts. Some have required comprehensive remediation and compensation programs. The Panel's approach has been to analyse some more recent high-profile incidents, and other select case studies, for the insights they provide into how CBA's decision-making processes and behaviours have operated in practice. Since it is conducting a Prudential Inquiry, the Panel has limited its review to activities of the bank and those parts of the CBA group in Australia that are subject to APRA's prudential supervision; hence, issues in financial planning and advice are not covered.

The Panel notes that it is not tasked with making specific determinations regarding matters that are

currently the subject of legal proceedings, regulatory actions by other regulators, or customers' individual cases.

Finally, the Panel has not assessed CBA's approach to risk management across the full gamut of risks to which a bank of CBA's scale and business model is exposed. The incidents and other issues examined demonstrate weaknesses in the way CBA has managed its non-financial risks – in particular, operational, compliance and conduct risks – and these risks have received the Panel's attention. If they materialise, these risks can have significant financial consequences, but they are separate risk classes to the financial risks facing banks and require distinct risk management capabilities.

At the very outset, it is important to clarify what non-financial risks are. Drawing on globally accepted definitions, *operational risk* is 'the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events and includes legal risk, but excludes strategic and reputational risk.'[1] *Compliance risk* is 'the risk of legal or regulatory sanctions, material financial loss, or loss to reputation a bank may suffer as a result of its failure to comply with laws, regulations, rules, related self-regulatory organisation standards, and codes of conduct applicable to its banking activities.'[2]

Compliance obligations are broader than strict legal requirements and incorporate standards of integrity and ethical behaviour. For that reason, compliance risk and conduct risk overlap. *Conduct risk* is 'the risk of inappropriate, unethical or unlawful behaviour on the part of an organisation's management or employees.'[3] At its simplest, conduct risk management goes beyond what is strictly allowed under law and regulation ('can we do it?') to consider whether an action is appropriate or ethical ('should we do it?'). The 'can we/should we' distinction is a recurring theme in the Inquiry. Most conduct and reputational issues have a basis in operational risk and compliance weaknesses, but these issues can of course be wider in origin.

## 1.3. The Inquiry's approach

The Panel has focused on identifying the key organisational and cultural factors, or combination of factors, that have contributed to the incidents damaging to community trust in the CBA. In particular, the Panel has sought to understand any dynamic between CBA's continued financial success, its prevailing culture, and any shortcomings in its responsiveness to and management of risk. To this end, the Panel adopted a methodology structured around three core themes that are aligned with the Terms of Reference:

- Governance – the way in which decisions at CBA are made, including how financial objectives, values and strategic priorities impact on decision-making and risk-management, and how decisions, once made, are implemented.
- Accountability – the way in which CBA staff, both individually and collectively, fulfil their responsibilities and the consequences of not doing so.
- Culture – the norms of behaviour for individuals and groups within CBA that determine the collective ability to identify, understand, openly discuss, escalate and act on current and future challenges and risks.

The Inquiry has undertaken a number of different but complementary activities to gather a thorough understanding of CBA's frameworks and practices. These activities included: interviews of Board members, and staff across different levels of seniority, divisions and business units; review and analysis of current risk policies, processes and frameworks across the main areas of interest; a detailed review of CBA's Board, Board Committee and Executive Committee papers and minutes; and relevant reviews from Group Audit and Assurance (hereafter internal audit) and external parties. A CBA staff survey was also conducted to provide a primary source of data about CBA's cultural drivers and its approach to risk management.

[1] Basel Committee on Banking Supervision, *Principles for the Sound Management of Operational Risk*, June 2011.
[2] Basel Committee on Banking Supervision, *Compliance and the compliance function in banks*, April 2005.
[3] Australian Securities and Investments Commission, *Market Supervision Update Issue 57 – Conduct Risk*, March 2015.

In addition, the Panel met with APRA, the Australian Securities and Investments Commission (ASIC), AUSTRAC, the Financial Ombudsman Scheme and other relevant third parties to gain further insights into CBA's frameworks and practices.

To assist the Inquiry, the Panel established an Inquiry Team, which undertook much of the fieldwork, analysis and initial drafting of the Report. The Inquiry Team was made up of staff from:

- APRA, which provided a full-time project team for the duration of the Inquiry incorporating a Secretariat function along with relevant subject matter experts from APRA's supervision and specialist areas; and
- Oliver Wyman, a global management consultancy, which provided specialist input and additional advice about international practices and lessons learned, drawing on its network of global experts. This input was valuable in identifying global 'better practice' benchmarks against which to assess CBA and to shape the Panel's recommendations.

The Panel greatly appreciates the skills, commitment and hard work of the Inquiry Team, under tight time deadlines.

The Panel also wishes to acknowledge CBA's cooperation with the work of the Inquiry.

Appendix C contains a detailed description of the methodology and approach taken by the Inquiry.

## 1.4. Structure of the Report

The Panel's Report, in line with the Terms of Reference, is set out in four main Sections.

Sections A to C provide the Panel's detailed findings, identifying shortcomings in CBA's risk management and compliance functions (the 'what' and 'how') and explaining the cultural and other drivers that may have contributed (the 'why'). The Panel's recommendations to address these shortcomings, taking into account CBA's remediation efforts to this point, are included at relevant parts of these Sections.

Section A analyses CBA's governance frameworks and practices. It evaluates five complementary and reinforcing elements of good governance, divided into five chapters:

- the role of the Board;
- senior leadership oversight;
- risk management and compliance;
- issue identification and escalation; and
- financial objectives and priorities.

Section B analyses CBA's approach to accountability and the extent to which it is reinforced by the way in which staff are incentivised and remunerated. It contains separate chapters on:

- accountability; and
- remuneration.

Section C analyses CBA's culture and leadership.

Section D draws together the Panel's main findings on weaknesses in CBA's governance, accountability and culture, and assesses whether CBA's ongoing and new remediation programs are appropriately focused on these weaknesses. Section D also provides the full listing of the Panel's recommendations.

For ease of reference, the CBA group is described throughout this report as 'CBA' or 'the Group'.

# SECTION A

# GOVERNANCE

# SECTION A: GOVERNANCE

Sound corporate governance is critical to the long-term viability of any company – not least banks, given the crucial role they play in the flow of finance throughout the economy and in safeguarding depositors' funds. In banks, the quality of governance frameworks and practices overlays the management of every risk parameter and instils confidence in the ability of a bank to manage its assets and liabilities prudently. Effective risk governance focuses on the quality, independence and reliability of the internal processes adopted by a bank to manage its risks. It encapsulates not only the role, responsibilities and functioning of the Board in relation to risk governance, but also the adequacy of the internal structures, operational controls and procedures to manage risk throughout the institution.

Ultimately, it is the Board of a bank that is responsible for its prudent risk management. The Board provides direction to senior management by identifying the principal risks facing the bank and by setting its risk appetite. The Board delegates to the Chief Executive Officer (CEO) and senior management primary ownership and responsibility for implementing sound risk management practices and controls in line with the risk appetite. It is management's job to provide leadership and direction to the employees in respect of risk management, and to control the institution's overall risk-taking activities in relation to the agreed appetite for risk. Thereafter, the Board assures itself on an ongoing basis that senior management is responding appropriately to these risks.

In the wake of governance failings and shortcomings in risk behaviour and culture exposed by the global financial crisis, Board effectiveness has come under heightened focus from regulators, globally and in Australia, and from stakeholders.

Organisational and business complexity has necessitated that, over time, banks have in place an array of specialised risk management and control functions. These include credit, market and liquidity risk specialists; operational and IT risk specialists; strategic and enterprise risk specialists; fraud investigators; internal auditors; compliance officers and more. Coordinating the interplay between a banks various risk and control functions and its business units, to ensure that there are no unnecessary overlaps or material gaps in the risk framework, is a vital part of a bank's corporate governance. A lack of role clarity can result in a failure to identify and manage the material risks that a bank faces.

To deal with this complexity, it has become the norm for banks to organise their risk governance structure around the so-called Three Lines of Defence model. While implementation of the model varies from bank to bank, generically this approach is built around three elements:

- First line of defence is the business. The business 'owns' the risk and must ensure that there are controls in place to appropriately manage the risk within the bank's risk appetite.
- Second line of defence is the independent risk management and compliance function. The function develops risk management policies, systems and processes to promote a consistent approach to risk management, and provides independent review and challenge to ensure first line controls are appropriate.
- Third line of defence is the independent audit function (both internal and external). The function provides independent assurance that the risk management framework is adequate and is operating effectively.

All three lines of defence are overseen by the Board, assisted by the following Board-delegated committees:

- Board Risk Committee (BRC), which oversees the implementation and operation of the bank's risk management framework, including monitoring the bank's risk profile relative to its risk appetite and challenging proposals and decisions on all aspects of risk management arising from the bank's activities. The risk management and compliance function provides regular reporting to the BRC to help it discharge its responsibilities.
- Board Audit Committee (BAC), which provides an objective review of the effectiveness of a bank's financial reporting and risk management framework and oversees both the internal and external audit functions. The internal audit function provides regular reporting to the BAC on the effectiveness of the bank's internal control framework.

- Board Remuneration Committee, which oversees the bank's remuneration framework and assists the Board to ensure that the bank's remuneration objectives and the structure of its remuneration arrangements are appropriate.

The Panel has found that, at all levels, the degree of attention and priority afforded to the governance and management of non-financial risks in CBA was not to the standard it would have expected in a domestic systemically important bank. The following five chapters elaborate on this fundamental finding.

The Board, together with its Risk, Audit and Remuneration Committees, demonstrated significant shortcomings in the governance of non-financial risks. For much of the period under review, the Board did not demonstrate rigour of oversight and challenge to CBA management. The tone at the top was unclear. The Board did not have the right balance of both summarised and detailed reporting in these risk areas, and nor did it, until recently, insist on improvement.

At the Executive Committee level, the Panel observed a complacent culture, a lack of accountability for non-financial risk management and lax remuneration practices, which led to almost inevitable attitudinal weakness in relation to emerging risks and customer issues. Overconfidence, bred from financial success, meant that serious gaps in CBA's controls for non-financial risks were overlooked.

CBA's focus on financial risks was not matched by a strong 'risk champion' for operational, compliance and conduct risks. Risk management in these areas was dominated by a 'tick the box', process-driven mentality, which meant that potentially serious non-financial risk issues were not identified early and addressed. CBA's compliance function was under-developed, as was its framework to manage conduct risk.

The treatment of customers is critical for CBA's reputation and public standing. CBA's focus on aggregate customer satisfaction survey results reinforced a 'good news' story that the Board and management were predisposed to hear. Alarm bells from the treatment of aggrieved customers, which should have alerted CBA to serious shortcomings in customer outcomes, did not sound loudly.

These various failings have culminated in a dilution of the 'voice of risk' and the 'customer voice', which did not provide a sufficient counterweight to a strong and mature 'voice of finance' in ensuring sound risk and compliance outcomes.

Under the new Chair, a Board refresh is underway and there are early signs of stronger oversight of non-financial risks. Nonetheless, the following chapters emphasise that there is further work to be done. There is a clear need for CBA to sharpen its governance and management of non-financial risks, lift its capabilities in operational risk and compliance, and significantly strengthen its risk culture.

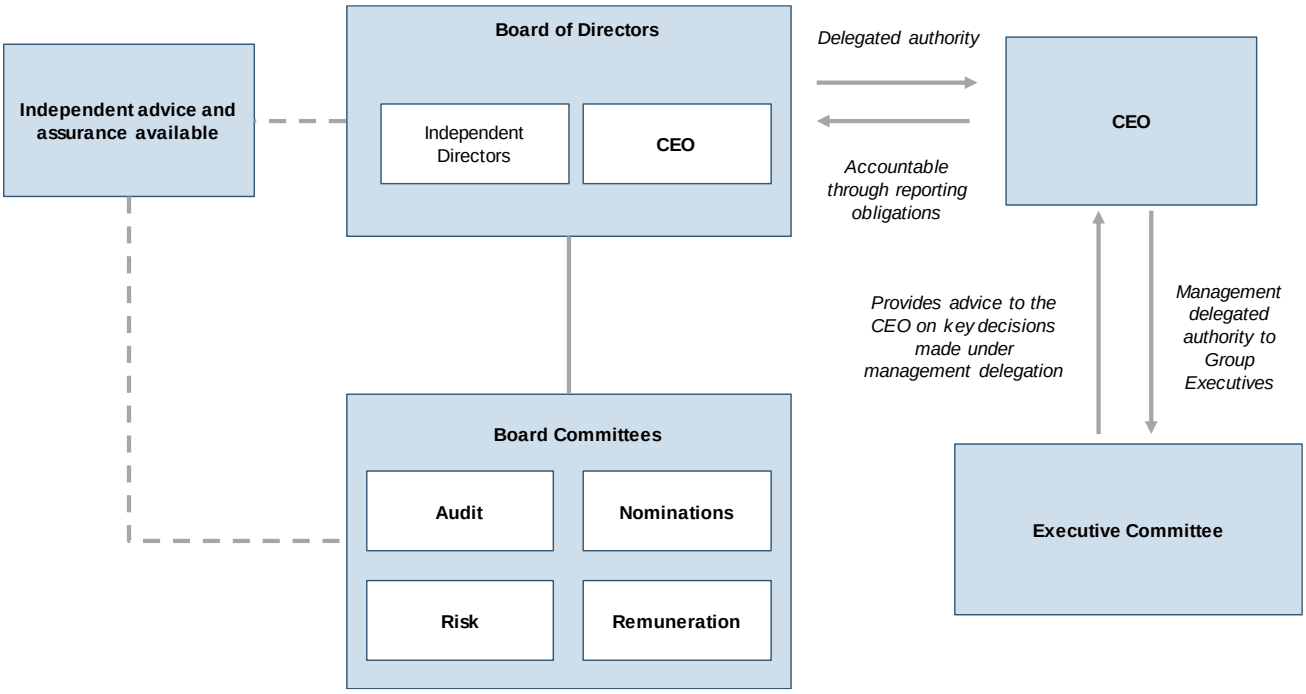
# 2. ROLE OF THE BOARD

## 2.1. Background

The Board of Directors is CBA's most senior governing body. The Board is tasked with setting CBA's strategic objectives, deciding key appointments and overseeing the management and performance of CBA.

CBA's Board has four permanent standing committees: the BAC, the BRC, the Board Remuneration Committee and the Board Nominations Committee,[4] as depicted in Figure 1. In addition, the Board has the power to establish *ad hoc* committees to focus on targeted areas for a specified period of time. The Board has met approximately monthly over the last two years, and its standing committees at least quarterly but in practice around eight to nine times per year. The agendas of the Board and Committee meetings seek to allocate appropriate time to strategic and risk management priorities, including operational, compliance and conduct risks. Senior management seeks advice on the handling of certain issues from Board members while also engaging with them on issues and risks facing CBA.

*Figure 1: Structure of CBA's Board of Directors and standing Board Committees*




Source: CBA

[4] Also referred to as the Board Performance and Renewal Committee.

The Committees of particular relevance to the Inquiry are the BAC, the BRC and the Board Remuneration Committee.

The operation of the BAC is primarily supported by internal audit, CBA's external auditor (PwC) and the finance function, and reporting produced by those functions. Reporting includes a high-level summary of the most significant findings from audit reports issued since the last meeting, and updates from the external auditor. CBA's Executive General Manager (EGM) of Group Audit, as well as PwC, routinely attend Audit Committee meetings, and PwC also attends Risk Committee meetings. On a half-yearly basis, the BAC receives a Thematic Report from internal audit that summarises issues and risk culture. Usually annually, Group Executives and their teams present to the BAC on the control frameworks of their respective businesses.

The Chair of the BAC is also a member of the BRC, notionally providing a vehicle to share information and insights.

The BRC is supported by the Group Risk function (hereafter, Group Risk or the 'risk function' as appropriate), and reporting produced primarily by that team including the CRO (Chief Risk Officer) Report. This incorporates reporting against CBA's Risk Appetite Statement (RAS), which facilitates managing risks by exception, such that the Board can defer to the executive team unless a particular risk exceeds a pre-defined tolerance established in the RAS. The Chair of the BRC is also a member of the BAC and the Board Remuneration Committee, a practice of overlapping membership that is designed to ensure seamless communication between the Committees.

The Board Remuneration Committee is supported by the Human Resources function, with additional support from Group Risk and the Risk and Remuneration Review Committee (a senior management committee), which both provide input into CBA's remuneration processes. This is discussed further in the Remuneration chapter.

In addition to these three standing committees, CBA established a new temporary Financial Crime Review Committee of the Board in 2017 to oversee the Group's response to AML issues and remediation. The Committee is an *ad hoc* committee and represented by a subset of the Board.

## 2.2. Inquiry findings

The Panel acknowledges that the CBA Board and its Committees have, over a number of years, presided over significant financial success and a strong turnaround in aggregate customer satisfaction statistics. The Board steered the Group through the global financial crisis, and has supported a strong strategic agenda including leading customer technology innovation. Nonetheless, shortcomings in the CBA's governance of operational and compliance risks have been highlighted by recent incidents.

The Board and its Committees exhibited a high level of trust and confidence in management driven by recent financial success and a collective belief that CBA is well-intentioned, conservative by nature and customer-centric. The Panel's view is that these factors contributed to a level of complacency and a 'dulling of the senses' within the Board and its Committees to signals that might have otherwise alerted them to a deterioration in the risk profile, and a movement outside of the risk appetite of the Group. These factors are discussed in the Culture and Leadership chapter.

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. This includes the Board or its Committees' treatment of, and sense of urgency surrounding, risk management issues. Importantly, it is also demonstrated through the rigour applied to monitoring and demanding mitigation of key risks and closure of control weaknesses.

CBA's Board has historically deferred to the CEO for internal and external communications to ensure a single consistent voice in terms of strategy, priorities and values. For that reason, the Board did not have a highly visible presence, and the lack of apparent urgency by the Board and its Committees in dealing with non-financial risks may have imparted a tone of inaction to the rest of the organisation. This has likely deprioritised the importance of maintaining rigorous risk management practices in non-financial risks as

compared to the pursuit of financial performance and other risk objectives.

The Panel has identified a number of consistent themes, which are discussed below:

- there was insufficient rigour and urgency by the Board and its Committees around holding management to account in ensuring that risks were mitigated and issues closed in a timely manner;
- gaps in reporting and metrics hampered the effectiveness of the Board and its Committees; and
- a heavy reliance on the authority of key individuals likely weakened the Committee construct and the benefits that it provides.

In addition, the Panel has made overall findings with respect to:

- gaps in communication between Committees despite overlapping membership;
- instances of a lack of candour from management in messaging to the Board and its Committees;
- over-confidence in the effectiveness of the Board and its Committees, and lack of genuine benchmarking; and
- immature oversight of the CBA's risk culture.

Overall, these findings relate largely to the operation of the Board prior to the appointment of the new Chair in 2017. Under the new Chair and refreshed Board, agendas have been enlivened and there has been an increase in urgency, challenge and engagement with the Executive team. Board members interviewed referenced an increasing philosophy of 'don't tell me, show me' to ensure that the trust placed in management teams is verified. In the Panel's view, the new tone being set by the day-to-day actions of the refreshed Board and its Committees, provided it is maintained, will clearly help to address many of the governance issued raised in this Inquiry.

### *2.2.1. Shortcomings in the operation of the Board*

**Insufficient rigour and urgency**

Prior to the appointment of the new Chair in 2017, the Board's agenda was relatively static and not tailored to the issues, risks or focal areas that demanded attention. Face-to-face meetings between the former CEO and Chair were not sufficiently frequent to develop a targeted agenda or to understand the most pressing items on which the next meeting needed to focus.

As part of the standing agenda, the Board reviewed a management update from each Group Executive, as well as a Regulatory and Operational Risk Report. Business unit updates typically focused on strategy and revenue topics. Reports to the Board from its Committees were the final item on the agenda, with the time allotted often being insufficient due to overruns in prior items.

The lack of rigour at Board level was highlighted in an APRA prudential review of CBA's Operational Risk Management Framework in December 2015 that observed several specific control gaps. It was only after this review that the Board increased its attention to long-outstanding issues and began to receive regular reporting on such issues – those raised by APRA and a set of other high-rated issues that had been open since 2013.

One of the challenges facing all Boards is ensuring strong oversight of senior management whilst still preserving an appropriate separation from managerial responsibilities. The Panel accepts that a Board must have a high degree of trust in the executives that it has appointed. However, the degree of trust needs to be continually tested and validated through appropriate metrics and constructive challenge by Directors who collectively must have appropriate levels of expertise and experience.

Interviews with Board Directors and Group Executives, together with the Board's own self-assessment, indicated that there was not sufficient challenge from the Board to Group Executives. The feedback cited a somewhat 'intimidating' environment with a highly intelligent Executive team and a propensity for positive and assuring

messaging from optimistic senior leadership that made constructive challenge more difficult.

Under the new Chair, the level of interaction between the CEO and Chair has increased substantially, and the Board agenda has been recast to ensure a more robust and effective discussion of relevant topics, including the most pressing risk matters. Standard business updates have been abridged, and the time saved has typically been utilised by 'deep dives' into areas of interest, with a recent focus on risk topics.

**Weaknesses in reporting**

The ability of the Board to effectively challenge senior management is influenced by the style of the Chair and the expertise of Directors, but it also relies critically on Boards being provided with comprehensive reporting that clearly highlights matters warranting specific attention. Internationally, there has been considerable focus on the provision of comprehensive and tailored content to Boards to assist with navigating the large quantities of information that are routinely considered by Directors. The Panel has not, until recently, observed similar endeavours at CBA.

The Regulatory and Operational Risk report provided to the Board is dominated by responses to regulatory matters and the top issues being dealt with. However, the report has very limited detail on the risk profile of the organisation, the trajectory of risks or on new and emerging risks. It supports a reactive mindset.

The content of major operational and compliance issues was not always escalated in sufficient detail for the Board to fully understand, discuss and make decisions on these issues. In particular, the Panel noted that neither the Board (nor the BRC) received metrics or analysis on customer complaints. This is discussed in detail in the Issue Identification and Escalation chapter.

The Board has received updates on aggregate losses from operational risk incidents and, of course, has considered specific individual cases receiving regulatory or media attention. However, the Board did not receive alerts on individual incidents or themes that might indicate an underlying or emerging risk or issue that might have reputational consequences. This can be achieved efficiently and effectively through relatively simple threshold reporting, such as that used by the BRC.

CBA now has an initiative to improve Board reporting, with a focus on quality of Board papers and discussions, supported by an extension of time for meetings. As indicated by senior management, this appears to have been driven by more challenge from Board members.

### *2.2.2. Shortcomings in the operation of the BAC*

**Insufficient BAC rigour and urgency**

The Panel acknowledges that the outgoing Chair of the BAC took a diligent approach to his responsibilities. He maintained a close working relationship with both the internal audit teams and the external auditor. He routinely met with them before each BAC meeting and had regular informal communication between meetings; minutes of these meetings and summary reporting were provided to BAC members.

Nonetheless, the BAC itself exhibited a lack of rigour and urgency in holding management to account in addressing and closing out audit issues. This is apparent in the BAC's approach to 'Red' audit reports. Red audit reports encapsulate the highest impact or highest risk weaknesses as identified by the internal audit function.

As outlined in the Issue Identification and Escalation chapter, a significant number of audit issues have had due dates for remediation extended on two or more occasions. Many issues were reopened following further review by internal audit, as the solutions delivered were assessed as ineffective. The BAC was not involved in reviewing or approving extensions of due dates for remediation of audit issues nor was there regular reporting to the BAC that tracked audit issues where the resolution date had been extended one or more times.

The most pertinent example of this shortcoming related to Anti-Money Laundering and Counter-Terrorism Financing (AML-CTF) matters. There were three Red audit reports on this topic, the first in 2013, highlighting a series of repeated issues. The second Red audit report in 2015 noted that

*This issue was raised in our 2013 AML/CTF audit and has not progressed due to a lack of ownership of the Group's AML/CTF processes.*

By September 2016, the third Red audit report on this matter was unambiguous in its messaging to the Chair of the BAC about CBA's failure to close issues in a timely manner and its inability to close issues effectively:

*A large number of AML/CTF issues continue to exist across the Group, with weaknesses identified across Business Unit's (BU's) and Group-wide AML/CTF processes. A number of repeat issues were identified, due to inadequate implementation of action plans. Many of the prior issues remain open, with projects currently underway or due to commence to revisit the AML/CTF operating model and completeness of AML/CTF data flows.*

*… the Group has been slow to address many of the previously identified issues and associated root causes. A number of significant issues from our Audits in 2013 and 2015 remain unaddressed and are either still being remediated… have been reopened due to inadequate remediation… or are yet to be addressed.*

At peer institutions domestically and abroad, Red or critical audit issues are handled with a high level of sensitivity, with first and second line issue owners reporting directly to the BAC to explain the findings and the progress of resolution plans. In many cases, extension of remediation dates must be reviewed by the BAC after Group Executive sign-off, and would usually be accompanied by a face-to-face report to the BAC on reasons for the extension. Repeat Red audit issues are treated with a particularly high level of severity, with issue owners and their relevant executive held to account for failure to close these properly. Importantly, such repeat issues can be evidence of a poor risk culture, low levels of competence or, even worse, an indicator of a business that has closed an issue consciously knowing that it has not properly resolved it.

In the Panel's view, the operation of the BAC at CBA would be characterised as passive by comparison, and not meeting mature practice in this area. The BAC described itself as having a 'light hand on the tiller'. There were three particular shortcomings:

- BAC members were not routinely provided with, nor did they request, copies of Red audit reports. Members were content to rely on a summary of these reports prepared by internal audit, to which the Chair of the BAC and internal auditor spoke;
- owners of issues raised in Red audit reports did not, as a matter of course, appear directly before the BAC. Group Executives and their teams periodically reported to the BAC to discuss their control frameworks, but this was not directly linked to critical audit findings in their business; and
- the BAC did not require timely follow-up of Red audit reports.

Better practice is that audit issue owners in business unit or support functions, rather than internal audit, are primary interfaces to the BAC for a Red audit issue. This creates a strong sense of accountability, while the regular interaction with these functions on their audit issues allows the BAC, and the Board itself, to directly set the tone about the importance of having a sound control environment. Critically, ambiguity of issue ownership can be identified and addressed more quickly, and there is an opportunity to reiterate first line responsibility for ownership of risks (see the Accountability chapter).

The Panel believes that the 'light hand on the tiller' was indicative of the mind-set of 'chronic ease' that had permeated CBA until recently. The BAC did not send a broader signal that Directors were aware, prepared and engaged on emerging non-financial risk matters, and confident to challenge management directly.

In 2017, the BAC introduced a requirement for internal audit to monitor successful closure of audit issues and broaden its coverage of issues to those raised outside of internal audit. However, the BAC and internal audit advised the Panel that they anticipate this will not become a permanent process as capabilities and capacity develop in the second line of defence. The Panel acknowledges the additional rigour introduced and cautions against any return to the *status quo ante*.

**Weaknesses in BAC reporting**

To discharge its governance responsibilities and effectively challenge senior management, the BAC must seek and be provided with clear and concise reporting that highlights the matters requiring the attention of Directors. This information should provide sufficient context to enable Directors to question senior management about the origin and ownership of risk issues, and progress in remediation of risk issues and incidents.

As noted, BAC members were not routinely provided with copies of Red audit reports. Interviews conducted with BAC members and management confirmed that there were few, if any, requests for detailed audit reports by members except the Chair of the BAC. This was well below industry practice.

In addition, the BAC did not receive nor demand metrics showing the closure status of the highest rated audit issues. Standard practice, both internationally and domestically, is that the BAC receives formal metrics and reporting articulating the number of audit reports, the owners, remediation timetables, extensions granted and whether the findings were repeat issues. Audit issues for which remediation timetables are overdue or extended would be highlighted. While summaries are provided, detailed audit reports would be made available.

The BAC has recently made several changes to enhance its operation. The length of committee meetings has been extended to ensure deeper coverage of audit issues. Reporting has also increased, and Directors now receive full Red and significant Amber audit reports.

**BAC reliance on key individuals**

The Panel notes that the BAC relied to a large part on the summary information prepared by internal audit and introduced by the Chair and internal audit to the other members. Globally, diversity in Board makeup and the value of differing perspectives has been critical in promoting healthy challenge. The Panel recognises the high level of engagement by the Chair in managing the BAC processes and his status as an expert in this field. However, the filtering of information through a single Director, combined with an absence of detailed documentation, would not fully utilise the collective experience of Directors or empower them in Committee discussions and in challenging management. It is difficult for the Panel to understand how Directors could provide effective challenge by relying almost entirely on others for their inputs. The Committee's operation, as a consequence, was less effective than it could be.

### *2.2.3. Shortcomings in the operation of the BRC*

**Insufficient BRC rigour and urgency**

The Panel heard through the Inquiry that the BRC had historically paid limited attention to the workings of controls, focusing attention on financial risks with which it was more familiar and that are more amenable to measurement, than on operational, compliance and other non-financial risk types.

A paper dated 5 June 2017 from internal audit to the BAC noted that

> *L2's focus on assurance, in our view, could be enhanced, including their reporting of material control findings to the Risk Committee, in the same way that we report to the Audit Committee.*

As described earlier, the BAC focused on responding to newly identified issues but did not police closure. Its pairing with a BRC that measured mainly financial risks and did not effectively monitor the implications for CBA's risk profile of open control weaknesses, was a significant contributor to CBA's poor track record in managing operational and compliance risks. Inadequate communication between the Committees was another contributing factor (see below). Effectively, monitoring the timely closure of issues affecting risk management was not the primary responsibility of any gatekeeper Committee.

Most global financial institutions, in the light of experience, have developed a sense of 'chronic unease' about the potential threats to their financial and reputational standing from non-financial risks, and their risk culture and risk management frameworks have evolved in line. In contrast, the CBA, led by its BRC, exhibited an inappropriate level of comfort for too long.

More recently, the BRC has made several changes to increase its effectiveness in understanding CBA's non-financial risk profile. Firstly, the BRC's charter has been amended to include an explicit requirement that the BRC 'consider any issues raised by the Group Audit or that affect the appropriateness or effectiveness of the Group's risk management framework or management of risk.' Secondly, the BRC now meets for a longer period, and on a separate day from the BAC, to increase time to discuss matters of concern. Early feedback to the Inquiry has indicated that the level of review and challenge by the BRC has also improved.

**Weaknesses in BRC reporting**

Prior to October 2017, for operational and compliance risks, only aggregate measures of untested or unsatisfactory controls were reported to the BRC as part of Risk Appetite Statement reporting. This limited the BRC's ability to understand risk issues relating to critical control vulnerabilities and provided limited visibility of emerging risks.

Reporting has since improved and deficiencies in key controls are now broken down into seven key themes, including cyber and financial crime, giving the BRC a high-level picture of the overall health of controls in each of these areas. However, the Panel notes that whilst these risk indicators have improved in usefulness, they are still aggregated measures; as such, there is still a risk that a spike in any one important key risk indicator may be diluted within the aggregate reporting for that risk. In addition, last period metrics are reported but there is no medium or long-term trend analysis that would impart to the Board the trajectory of the risk. These shortcomings are outlined further in the Risk Management and Compliance chapter.

Better practice supplements these aggregate measures, with a selection of more precise and bespoke metrics that would indicate emerging risk in specific areas such as AML, cyber or conduct. Better practice BRCs often work directly with relevant divisions to understand how non-financial risks are measured on a day-to-day basis, and to get comfortable that they have the data and reporting to alert them if these specific risks deteriorate. CBA's new Financial Crime Review Committee has done this and it is currently reviewing a selection of key financial crime metrics. This practice needs to be expanded under the BRC to cover other risk types.

Emerging practices globally use technology to enable Directors to 'click through' high-level dashboards to more granular metrics and data to facilitate improved debate, challenge and discussion. As noted above, the balance of information on non-financial risks reaching the Board is not yet satisfactory and the Panel believes further review and enhancement of such information is warranted.

**BRC reliance on key individuals**

Partly as a result of the weaknesses in reporting, the BRC has been heavily reliant on the CRO to determine the risks to be reported to Directors, particularly for operational and compliance risks. For example, up until at least October 2017 regular reporting from the CRO included only 'new major and emerging' issues from each business unit, selected largely at the CRO's discretion. Issue escalation protocols to the BRC are not clearly laid out in CBA policies.

As with the BAC, there was some evidence at the BRC that the reputation of the previous Chair of the BRC and CRO as industry experts with a 'scholarly gravitas' stifled the level of challenge at Committee meetings. There was a high degree of collaboration between these two individuals. In itself, this should be positive. However, the Panel heard that this degree of collaboration led other participants to think that the real meeting had occurred prior to the Committee meeting. This dynamic should have been questioned.

The previous Chair of the BRC and CRO were highly experienced and the respect from other Committee members was not undeserved. However, CBA has acknowledged to the Panel that, with the benefit of hindsight, their strengths were heavily weighted toward financial risk management and they brought less experience to bear in operational risk and compliance matters. This emphasises, again, the benefits to be had from leveraging the collective experience of the full Committee membership, where access to better information and a team of enquiring minds has a higher chance of yielding more effective challenge.

### 2.2.4. Inadequate communication between Board Committees

Despite overlapping Committee memberships, the linkages between Committees of the Board have been inadequate.

The Panel considers that there has been a lack of clarity and delineation in the roles and responsibilities between the BAC, the BRC and the Board Remuneration Committee. This has resulted in gaps in the flow of information between these committees.

In particular, key audit findings highlighting serious gaps in the control environment that were reported to the BAC have not systematically resulted in a formal reassessment of CBA's risk profile and reporting to the BRC against stated risk appetite and tolerances. The existence and ownership of significant control gaps should also be of interest to the Board Remuneration Committee in assessing whether remuneration should be adjusted for senior managers responsible for ensuring a strong control environment. This linkage between Board Committees did not operate effectively.

Two examples illustrate this shortcoming. In August 2015 when the BAC discussed the second Red audit report on AML, there was no formal request or notification to the BRC to consider the implications of the identified control weaknesses for CBA's risk profile. The Board received an update on the topic through a scheduled regulatory report, and subsequently directed the BRC to receive a further update later that year. However, the seriousness of the matter was not reflected in the BRC reporting until November 2016, where Group Risk rated AML-CTF compliance as the top-rated operational risk facing CBA. Interviews with those members of the BRC not overlapping with the BAC indicated that they had no recollection of receiving Red audit reports on this matter, notwithstanding the seriousness of the issues and the significant reputational risk at stake. In such a case, the Panel would have expected to see a formal referral from the BAC to the BRC, provision of the audit report to BRC members, the BRC re-assessing of CBA's risk profile as a result of the findings, and follow-on actions to monitor remediation.

A second example is the APRA-initiated Targeted Review of the *Verification of borrower data used in home loan serviceability assessments*, conducted by PwC and issued in May 2017. This report was qualified on the basis of concerns around the design and/or effectiveness of seven out of ten controls in scope of the review. The BRC was briefed about this matter, but it was not evident that the BAC was. The Panel considers that these weaknesses in a set of the internal controls should have resulted in the BRC requiring management to reassess the inherent risk profile of the mortgage portfolio and report back against the Board's stated credit risk tolerances. There was no evidence that this occurred.

Best practice in Board operations ensures seamless communication between Board committees. Identification of a critical control gap affecting risk management would be formally considered by the BRC, and the BAC may even monitor the matter to ensure that the issues raised have been assessed. Some institutions hold joint and overlapping meetings of their Audit and Risk Committees where relevant audit findings can be discussed. CBA has further work to do to meet best practice in this area. Recent changes in the respective charters of the BAC and BRC referenced earlier are an important step in this direction.

### 2.2.5. Candour of messaging to the Board and its Committees

Given the lack of precision in operational and compliance risk metrics and other limitations in Board reporting, the Board has been highly dependent on a small number of key individuals to filter and curate the information on which they rely to perform their duties.

Evidence reviewed by the Inquiry did not identify a systemic issue in messaging to the Board or its Committees. However, instances were observed where messaging has over-emphasised positive aspects and progress, and de-emphasised more negative elements of risk issues and incidents. Reporting to Boards in this manner can be especially problematic when compounded with insufficient encouragement and quality of challenge or scrutiny by the Board of senior management. In specific incidents reviewed by the Inquiry, there was some evidence of 'good news' messaging. In one instance, the update to the BAC summarised the findings of an external review of CBA's control environment in a particular area, but essentially

relayed only the positive elements of the report. In a second, the gaps in CBA's controls were referenced, but the messaging reassured the BRC that the compliance process was largely working, citing a single example of where the controls had worked as intended. In a third case, interviews suggested that messages to a subsidiary Board were filtered so as to retain management flexibility in dealing with the matter.

Boards globally have tried to compensate for these potential biases by deliberately engaging with specialists and employees at more operational levels in the organisation. This helps them establish the necessary confidence in their organisation's capabilities to manage risk, and to reduce the impact of inevitable management filters that are applied in communicating upward to the Board or its Committees. For example, Board risk committees in Europe and the United States will meet with their AML responsible officer or their cyber security experts to ensure that concerns felt at the 'coal face' in the fight against these key risks are being transparently communicated upward to them. Under CBA's new Chair and refreshed Board, the level of enquiry of staff has intensified, but the Panel suggests this could be taken further.

#### *2.2.6. Over-confidence and lack of benchmarking*

The Panel observed a level of over-confidence in the operations of both the BAC and BRC over much of the period under review.

The Board undertakes an annual assessment of its performance and that of its Directors in response to good governance and the requirements of APRA's *Prudential Standard CPS 510 Governance*. The self-assessments have noted significant strengths of the Board but also highlighted opportunities for improvement. The BAC was identified over successive periods as well-functioning, and recent changes at the BRC to increase its effectiveness have been acknowledged. The Panel's interviews with CBA Directors and senior leadership confirmed the perception that CBA's governance was very effective, and included descriptions of the BAC in particular as 'slick' and 'world class'.

Rigorous benchmarking would have indicated that aspects of CBA's governance practices were, in fact, below mature practice. The generally optimistic tone of the CBA's performance assessments appears reflective of a lack of introspection and constructive challenge, matters which are discussed further in the Culture and Leadership chapter.

As discussed in this chapter, the Board has recently identified a number of areas where the governance practices of CBA can be enhanced in order to deliver better outcomes for stakeholders. Plans have been enacted to address these matters. Many of them accord with the Panel's assessment of where the Board needs to focus its attention to reduce the CBA's vulnerability to further missteps.

#### *2.2.7. Board assessment of risk culture*

The Board is required to form a view on risk culture under *Prudential Standard CPS 220 Risk Management*. The Panel has observed different levels of maturity in the assessment of the risk culture and in the identification of desirable changes. CBA has a sound working definition of risk culture and a framework for ongoing assessment, and there are some robust metrics in place that recognise business unit specific needs. The Panel considers, however, that there is some immaturity in the Board's understanding of the nature of risk culture. This is reflected in some of the language within Board reporting and in the action items that are designed to drive desirable changes to risk culture. Of particular note is the overreliance on the Vision and Values initiative as the primary basis for identifying these changes. This is further explored in the Culture and Leadership chapter.

By way of example, the most recent report to the Board on risk culture in 2017 provides some background information, including previous commentary from external assessments and APRA reviews. However, this commentary has not been clearly translated to ensure appropriate steps are taken to address those issues. This is particularly reflected in the action items, which have focused on frameworks and policies without addressing the issues identified in the external reviews. As discussed later, the Panel believes the Board has some way to go in promoting a mature risk culture in CBA.

# 2. ROLE OF THE BOARD

## Recommendation 1

*The CBA Board maintain its recent heightened visibility, promoting a clear tone at the top in both messaging and action.*

## Recommendation 2

*The processes and practices of the Board and its Audit and Risk Committees be aligned with global better practice for risk management.*

## Recommendation 3

*The Board ensure effective coordination between its Audit, Risk and Remuneration Committees.*

## Recommendation 4

*The BAC increase direct engagement with the business unit and support function owners of significant issues and hold them accountable for timely and effective closure of these issues.*

## Recommendation 5

*The Board ensure it receives adequate non-financial risk information, including early indicators of emerging risks, to support constructive debate and challenge.*

# 3. SENIOR LEADERSHIP OVERSIGHT

## 3.1. Background

CBA has a 'federated' organisational structure. Five business units based on CBA's target customer segments are supported by six central support functions that provide services to the business units. A federated structure is relatively common in the banking industry. Such a structure supports the independence of client-facing business units, provides for bespoke customer or segment-driven strategies, and allows for solutions that are optimised to meet specific needs of the business unit. Under this structure, each business unit implements an independent strategy that is overseen by a Group Executive who is accountable for the unit's performance.

Within CBA, the Executive Committee is the most senior management forum and comprises the Group Executives of business units and central support functions. The Executive Committee's stated purpose is to 'materially enhance customer satisfaction, people engagement, shareholder value and the Group's reputation.' The Executive Committee meets on a weekly basis.

The Executive Committee provides advice in relation to issues, such as CBA's strategic direction and risk appetite, which are within the authority of the Board, CEO or a Group Executive. Under its Charter, the Executive Committee is not a decision-making body. Group Executives have operated with a high degree of empowerment and autonomy in relation to their specific business units, accompanied by expectations of individual accountability for business unit financial and risk outcomes.

From a risk governance perspective, there are also other senior management committees, including:

- the Executive Risk Committee, which meets weekly to oversee credit risk issues. Its mandate includes recommending credit decisions for Board approval outside the delegated authorities of management, monitoring the credit risk profile and approving/endorsing and monitoring compliance with credit risk policies;
- the Asset Liability Committee (ALCO), which meets monthly to oversee market, liquidity and funding risks; and
- the Risk and Remuneration Review Committee, which meets quarterly, or more frequently if required, to advise the Board Remuneration Committee on material risk issues that should be considered in the determination of remuneration outcomes for all staff below Executive level.

Risk management is also specifically considered at the individual business unit level through various committees and forums. Business unit level risk committees form part of the Business Unit Risk Management Governance Framework and advise the relevant Group Executive on material risks and decisions to be made under delegated authorities. Risk forums, which are separate to the senior management committees referred to above, also convene for special projects and *ad hoc* decision making for specific activities.

The Panel does not consider that CBA's federated structure itself raises particular issues. The Panel is mindful, however, that the ongoing success of organisations with similar operational structures is dependent on the relative strength and 'voice' of the risk and other support functions, particularly in relation to those risks, processes and controls that span more than one business unit.

## 3.2. Inquiry findings

In the Panel's view, the Executive Committee was not an effective vehicle for addressing Group-wide risks and issues. Its mandate did not include oversight of the risk profile of the Group, while its dynamics did not encourage a sense of collective accountability for Group risk outcomes or constructive challenge of Committee members.

### 3.2.1. Operation of the Executive Committee

Evidence from interviews with Group Executives confirms the high priority the former CEO placed on vertical empowerment of Executive Committee members to run their own businesses. In and of itself, this can be a good thing. However, when combined with an atmosphere of collegiality and high levels of trust in peers, it resulted in a lack of healthy constructive challenge within the Executive Committee and an inclination for Group Executives not to raise concerns outside their own area, at least until these concerns had risen 'above the waterline' in terms of materiality.

In interviews, Group Executives repeatedly referred to the Executive Committee as an 'advisory panel' to the CEO, which was 'not the same kind of operation as other teams, other ExCo's'. Some stated that the Executive Committee, notwithstanding the collegiate atmosphere, did not function as a cohesive team, to the potential detriment of CBA's broader interests in resolving some long-outstanding issues.

The Executive Committee also tended to view itself through the lens of CBA's strong financial record and the turnaround in aggregate customer satisfaction metrics, with considerable comfort being taken from relative outperformance against peers. The consequences of the resulting complacency are explored in the Culture and Leadership chapter.

These dynamics were reinforced by the formal functioning of the Executive Committee. A review of agendas and papers from its meetings in 2017 did not provide evidence of a genuine focus on the following areas mandated under its Charter:

- agreeing common action where cross-Group coordination was critical to value creation;
- requiring and ensuring an environment of constructive and open challenge;
- sharing information on emerging risks; or
- clarifying and monitoring accountability for delivery of key business outcomes.

In the Panel's view, the Executive Committee did not collectively provide a strong counterbalance to the prevailing views of individual business unit executives, nor did it effectively mobilise the institution when confronted with issues affecting multiple business units. This has invariably contributed to CBA's missteps. The Panel's judgment is based on a number of sources.

Firstly, failings in the AML-CTF control framework did not attract a collective response from the Executive Committee until March 2016, even though material weaknesses in controls across a number of business units had been identified by internal audit much earlier. Several of the business unit Group Executives had themselves identified material concerns with AML-CTF risk management, with some also raising their concerns with Group Risk and/or taking action within their own business units, with varying degrees of effectiveness. Prior to March 2016, discussion on this topic at the Executive Committee was largely limited to endorsement of AML-CTF group funded projects. Successive remediation programs were slow to address the underlying failings in the control framework. The Panel considers that this outcome was, in part, attributable to a lack of collective ownership and understanding of AML-CTF risk at the Executive Committee level.

A broader strategy update to the Board in May 2017 noted the existence of 'too many handoffs between silos and layers, with accountability often not clear enough and agreements hard to reach'. This paper noted that the existence of multiple steering groups and obfuscated decision making had contributed to a number of programs, including one AML program, being disbanded with limited benefits. Executive level oversight of many of these programs did not assist in their delivery and additional layers of unnecessary complexity acted to impede remediation efforts. An Executive Committee clearly focused on and accountable for Group outcomes would have provided appropriate direction and drive in such cases. CBA's Executive Committee did not do so often enough.

Ongoing challenges with data management have been highlighted to the Board as recently as August 2017 noting:

> *We have an incomplete data management framework that is not fully implemented and therefore exposes us to data risk and data quality (DQ) issues. These can adversely impact other risk types, compromise decision making and reporting, and hinder the timeliness and cost*

*of development. Framework design gaps include the absence of clear data risk appetite statements, defined areas of executive accountability, a business and technology aligned data management strategy, and an associated data management improvement support program. There is no defined operating model or responsibility for providing support processes and tools.*

The validity and accuracy of data were also matters identified as areas of concern in the staff survey and focus group interviews conducted for this Inquiry. An executive level Data Governance Committee was originally established to ensure consistent standards of monitoring, governance and controls for data across CBA. However, it has been inactive since late 2016. A renewed focus from Group Executives is clearly required to address this issue.

An IT Risk prudential review by APRA in late 2016 noted numerous issues of concern, including a lack of visibility at the Executive Committee level (and the Board) of the state of health of the IT environment. CBA acknowledged that APRA's findings indicated that it was operating outside of its IT risk appetite. The APRA report recommended enhanced senior level governance and risk reporting for systems resilience, recovery, data storage and integrity, and risk management and culture.

IT user access control weaknesses were identified by external audit as early as 2012 but have not yet been completely resolved, notwithstanding a large investment program. The failure of the Executive Committee to accept ownership and accountability for IT systems used by the business units has been a major contributing factor in CBA's inability to fully mitigate this risk. A stronger voice on the Executive Committee from the risk and enterprise services functions would also have facilitated more timely and effective remediation.

Finally, the Executive Committee took too long to end the mis-selling of credit card insurance. Problems with this product were noted in a 'risk deep-dive' conducted by CBA in 2013 following enquiries from ASIC, and mis-selling was identified by internal audit in 2015. However, the decision to withdraw this product from the market was not announced until March 2018. As the Panel understands it, the delay reflected divergent views from Group Executives about this product, which the Executive Committee, without a decision-making mandate, did not reconcile and resolve.

A well-functioning Executive Committee would generally exhibit a number of characteristics, including:

- operating, with a sense of collective accountability, in the best interests of the institution whilst retaining ownership and individual accountability for individual business units and support functions;
- operating as a 'think tank' to tackle difficult and challenging problems, not primarily as a mechanism to inform others of decisions already made within individual business units;
- all members demonstrating an intricate understanding of the business beyond their individual roles to permit support and challenge across the team;
- providing a culture of constructive challenge and a capacity to test assumptions and beliefs to avoid 'group-think'; and
- encouraging a diversity of thinking styles with topics viewed from different perspectives – a strategic and operational perspective; a task-focused and relationship-focused perspective; and an inside and outside the industry perspective.

The operation of CBA's Executive Committee has fallen well short of this benchmark.

## Recommendation 6

*The CEO ensure that the Executive Committee accepts and embeds collective accountability for management of the Group.*

## Recommendation 7

*The CEO ensure that the Executive Committee:*

- *discusses, understands and takes action to mitigate the impact of risks that span business units;*
- *promotes the voice of support functions as an effective counterbalance to the business units; and*
- *engages in constructive challenge and debate.*

### *3.2.2. Oversight of risk*

CBA's federated structure and the operating model that has been adopted by the Executive Committee place a particular onus on senior level oversight and understanding of risk.

The Charter of the Executive Committee does not provide for it to oversee the aggregate risk profile of the Group across all risk classes. Of the two senior management committees that oversee credit risk (the Executive Risk Committee) and market, liquidity and funding risks (ALCO), the former includes only four Executive Committee members while ALCO includes only the relevant members of the Executive Committee.

Executive Committee members receive a copy of the papers provided to the BRC including the CRO Report; however, these papers are not formally discussed as an agenda item at Executive Committee meetings. In addition, although the EGM Group Audit meets with the CEO on a monthly basis and with each Group Executive on a regular basis, the Executive Committee does not receive regular reports from internal audit and the EGM Group Audit does not attend Executive Committee meetings.

Historically, CBA has not had an Executive-level committee to oversee its operational and compliance risk profile. The Executive Committee has considered operational risk and compliance matters periodically, but these risks were not until recently a regular, formal item on its agenda. Instead, operational risk and compliance matters are considered by the risk committees of individual business units and discussed at a Group level in a monthly update to the CEO, and in monthly meeting between the CEO, CFO, CRO and the Group Head of Operational Risk. Given challenges with data and the ability to aggregate risk information, this narrow approach has limited CBA's ability to form an aggregate view of its operational and compliance risk profile, and to monitor, discuss and analyse emerging operational and compliance risks. In the Panel's view, it has also provided an important but negative signalling effect about the relative importance of operational and compliance risks at CBA.

More recently, senior level oversight of operational and compliance risks has improved. Since October 2017, a formal update on operational and compliance risks, including reporting on CBA's operational and compliance risk profiles, has been included on the Executive Committee's agenda on a quarterly basis. The Panel welcomes this step. However, interviewees have claimed that the quarterly updates are not sufficient, with reporting on operational and compliance risk lacking detail and being largely reactive in nature.

Material provided to the Inquiry by CBA in March 2018 in relation to its Better Risk Outcomes Program (see the Remediation Initiatives chapter) indicates the intention to establish an Operational and Compliance Risk Forum at the Executive Committee level. However, details are scant. In the absence of further information on the charter and scope of this Forum, including why it is positioned as a Forum and not a Committee, the Panel is not able to opine on its likely effectiveness in elevating the institutional profile of operational and compliance risk management at CBA.

In Australia, CBA's peers operate with either a dedicated executive-level risk committee focused on the management of risks faced by the institution as a whole, and/or a specific committee to oversee the institution's non-financial risk profile. Whatever the model chosen, the lesson from CBA's recent missteps is that that the Executive-level oversight of non-financial risks should not be subordinate to financial risks.

Globally, non-financial risk executive committees have become increasingly common, in part a response to major conduct issues that have resulted in material fines and substantial

reputational damage. The establishment of such committees has acted to increase the visibility of operational risk and compliance at senior management and Board level. Better practices in this regard include a mandate that clearly outlines the responsibilities of the committee in relation to operational and compliance risks; inclusion of updates on these risks as regular formal agenda items for committee meetings; active engagement of the committee with the operational risk and compliance functions to stay abreast of developments; and an annual review by the committee of the operational risk and compliance management framework.

## Recommendation 8

*CBA establish an effective Non-Financial Risk Committee at the Group Executive level.*

# 4. RISK MANAGEMENT AND COMPLIANCE

## 4.1. Background

Consistent with APRA's *Prudential Standard CPS 220 Risk Management*, CBA defines its Group risk management framework as 'the totality of systems, structures, policies, processes and people within the Group that identify, measure, evaluate, monitor, report and control or mitigate all internal and external sources of material risk'.

A key element of CBA's risk management framework is its Three Lines of Defence risk governance model, which it refers to internally as the 'Three Lines of Accountability'. Under this model, there are second line of defence (Line 2) teams at Group level and also within business units. Line 2 includes CBA's designated compliance function, which is headed by the EGM, Compliance, who reports to the Group CRO.

CBA's frameworks for managing operational and compliance risk are a subset of its overall risk management framework. The frameworks are documented in two key policies, the Operational Risk Management Framework and the Compliance Risk Management Framework, with detailed implementation guidance outlined in the Operational Risk Management Framework How to Guide. Key elements of the frameworks include CBA's processes for the identification, measurement and management of operational and compliance risks, including:

- the Risk and Control Self-Assessment process, which is a forward-looking assessment of key risks and controls;
- the Controls Assurance Program, which involves periodic testing of the design and operating effectiveness of key controls;
- the Risk in Change process, which involves conducting an assessment to identify and manage variations in CBA's risk profile resulting from material change initiatives such as new or changing products, processes, systems, suppliers and regulation; and
- the Issue and Incident management processes to manage control weaknesses and actual events resulting from weak controls, respectively.

CBA's operational and compliance risk management frameworks are central to its management of conduct risk.

The operational and compliance risk management frameworks are supported by RiskInSite, which is a database system used throughout CBA to record the information generated by the processes mentioned above. This information includes compliance obligations, operational and compliance risks, controls, issues and incidents, and forms the basis for operational and compliance risk reporting. RiskInSite allows responsibility for risk matters to be allocated to individuals and is used to track the status of issues and incidents.

## 4.2. Inquiry findings

The Inquiry has made findings in relation to CBA's implementation of the Three Lines of Defence model, its management of operational and compliance risks, its control environment, its compliance function and its conduct risk profile and strategy.

The findings in relation to the first three areas are particularly significant, and reflect the persistence of issues over time. A key contributing factor has been inadequate management by CBA of an inherent challenge in its federated organisational structure: implementing its Three Lines of Accountability model and Group operational and compliance risk management frameworks in a manner that reflects the specific business model and risk profile of each business unit, while also achieving a degree of consistency across units. Specifically, a number of the findings reflect inadequate mechanisms to manage this challenge, including a lack of:

- clear articulation of minimum standards in the form of Group-wide policies, processes and operating procedures to which all business units must adhere;
- adequate training and guidance to staff who are responsible for implementing Group-wide policies; and
- a clear and enforced process for review and approval of exceptions to Group-wide policies.

#### *4.2.1. The Three Lines of Defence model*

In concept, the Three Lines of Defence is a relatively simple model. However, CBA has not implemented it effectively despite a number of attempts over several years.

In implementing the Three Lines of Defence model, CBA has allowed business units to tailor the model for their purposes rather than adopt a 'one-size-fits-all' approach. While there are benefits in tailoring the model to the nuances of each business unit, the challenges of having multiple models across the Group need to be adequately managed through strong oversight by the Group Risk function. Such challenges include the additional effort required by Group Risk to assess that its minimum standards have been applied, ensuring there are no gaps in roles and responsibilities, and managing risks arising from products and processes that cross business units.

CBA's tailoring of the model across business units has created additional complexity, which has been compounded by a lack of documentation on how the model in each business unit works in practice. CBA has experienced challenges in managing this complexity, particularly in relation to operational and compliance risks.

CBA's attempts to embed the model have only been partially effective. There have been a number of issues. Firstly, as noted in the Accountability chapter, the principle that the first line of defence (Line 1) owns the risk and is primarily and ultimately accountable for appropriate risk management has not been consistently applied. In relation to operational risk and compliance, CBA had identified a lack of Line 1 ownership as an issue in previous years. In its December 2015 Operational Risk prudential review, APRA required CBA to ensure that Line 1 business management had a clear understanding of its operational risk management responsibilities. CBA has acknowledged to the Inquiry that a lack of Line 1 ownership remains an issue.

Secondly, there have been instances of Line 2 performing Line 1's roles:

- in the first half of 2017, CBA identified that in its Home Buying business, Line 2 was performing various activities such as file review, verification and credit decision making that should be performed by Line 1;
- Line 2 has taken ownership of CBA's country risk management systems. In mid-2017, an Executive Committee paper noted that while Line 2 had elected to lead investment in the systems, it was neither the owner of the underlying platforms nor the major beneficiary of the investment. The paper added that, as a result, a key success factor would be the support of the Executive Committee and the relevant two business units; and
- following a review in late 2017 and early 2018 of the operational and compliance risk activities undertaken by Lines 1 and 2 across the Group, CBA identified that in some business units Line 2 was performing activities that would normally be performed by Line 1. This blurs accountabilities and leaves less time and capacity for Line 2 to effectively carry out its key responsibilities of assurance, review and challenge.

The Group-wide review also found significant variability in the resourcing, roles and responsibilities of Line 1 and Line 2 across business units. These findings were not new. Issues identified earlier in relation to operational risk and compliance have included duplication across Line 1 and Line 2, variation in approach and results across teams, Line 2's expertise being misdirected to lower value processing work and lack of specialisation/capability, particularly in respect of control design and testing. The Panel notes its concern at the persistence of these issues.

Thirdly, as evidenced by the findings in the Culture and Leadership chapter, other particular challenges for CBA are that Line 2 has had an inconsistent and sometimes low influence as an independent risk management function across CBA, and that risk management is perceived as a low priority 'administrative task'.

Interviewees confirmed that the operational and compliance risk functions have lacked a strong 'voice of risk'. Contributing factors raised by interviewees included that management of these risks was not being given sufficient priority and that the importance of operational risk had not been communicated adequately by Line 2. A lack of resourcing and capability in CBA's operational and compliance risk management functions, which is discussed below, was also said to have played a role. In its 2015 Operational Risk prudential review report, APRA also noted that it did not see evidence of a strong level of challenge from Group or business unit Line 2 teams.

The Panel has observed two specific issues in relation to the 'voice of risk': the reporting lines of business unit CROs, and the extent of Line 2's involvement in CBA's Risk in Change process.

**Business unit CROs**

CROs within the business units retain a functional ('dotted') reporting line to the relevant Group Executives, in addition to their primary reporting line to the Group CRO. The Panel understands that the rationale for the functional reporting line is to ensure that Line 2 operates as a strong partner to the business by retaining a deep understanding of its operations and being part of relevant governance committees. However, a fundamental principle of the Three Lines of Defence model is that Line 2 staff must be structurally and functionally independent of the business and there must be no conflicts of interest that impede business-aligned Line 2 staff from providing impartial advice and strong challenge to the business. Moreover, the Basel Committee on Banking Supervision's 2015 *Corporate governance principles for banks* provides that:

> *While it is common for risk managers to work closely with individual business units, the risk management function should be sufficiently independent of the business units…Such independence is an essential component of an effective risk management function…*[5]

On balance, CBA needs to ensure that the functional reporting line of business unit CROs to Group Executives does not impede their independence.

**Line 2's involvement in the Risk in Change process**

Key processes such as the new product approval process and Risk and Control Self-Assessment require Line 2 engagement and sign-off. This provides a preventative control for new business, and a detective control that would allow Line 2 to assess risks that may have changed or been introduced in the preceding year. Conversely, CBA's Risk in Change process does not require Line 2 sign-off for initiatives that materially change its risk profile, with the exception of mergers or acquisitions.

The Panel recognises that, given the significant volume of changes undertaken, not all change initiatives can be independently approved by Line 2. However, there do not appear to be adequate mitigants in place to ensure that there is sufficient Line 2 oversight of Risk in Change assessments. Firstly, while Line 2 is accountable for the review and challenge of Risk in Change activities under CBA's operational risk management framework, Line 2 does not adequately fulfil this responsibility across the Group, given it is performing activities that would normally be performed by Line 1 in some business units. Secondly, a bank's culture should foster early and open engagement by the business with Line 2 expert advisors, and encourage Line 1 to seek Line 2's input in the decision-making process, irrespective of whether it is a formal policy requirement. This also does not occur consistently across the Group, given the observations above regarding Line 2's inconsistent influence and risk management being perceived as a low priority.

[5] Basel Committee on Banking Supervision, *Corporate governance principles for banks*, July 2015.

**Remediation initiatives**

As discussed later in this Report, in early 2017 CBA introduced a remediation program, the 'Big Rocks', to improve its risk management. This program included an initiative to enhance the effectiveness of the Three Lines of Defence model. Based on its experience from previous attempts, CBA has adopted a broad financial and non-financial risk focus and principles-based approach in implementing this initiative. To start with, in the first half of 2017 Group-wide principles describing the roles and responsibilities of Lines 1, 2 and 3 ('Three Lines of Accountability principles') were developed, refined through a 'proof of concept' in the Home Buying business and subsequently endorsed by the Executive Committee for application across the Group. Proofs of concept were also undertaken in Wealth Advice and Financial Crimes, with recommendations delivered in February 2018.

The Three Lines of Accountability principles are now being implemented progressively across business units and risk types, with ongoing refinement occurring as needed. As part of the rollout, the risk function in Retail Banking Services (RBS) was restructured in February 2018 to clarify the roles and responsibilities of Lines 1 and 2 in line with the principles. As a result, the risk team supporting RBS, comprising credit, operational and compliance risk staff, has significantly decreased in size as activities and staff have been reallocated from Line 2 to Line 1. The Panel understands that work has commenced within the RBS risk team to build Line 2's capability to fulfil its core responsibilities of providing review, challenge, insights and advice to Line 1. Further proofs of concept have been identified in other business units, with resulting changes expected to occur between July and October 2018.

In February 2018, the Executive Committee endorsed the need for consistency in the roles and responsibilities of the operational and compliance risk functions in the business units, through an accelerated alignment of Line 1 and Line 2 activities with the principles. To achieve this, CBA is undertaking an operational and compliance risk activity realignment project as part of a Group-wide risk remediation program. The project involves Line 2 developing, by 30 April 2018, a detailed template of best practice operational risk and compliance risk activities by line of accountability, and supporting each business unit/support unit to re-align activities and resources across Lines 1 and 2 in accordance with the template. CBA's target completion date for the re-alignment is 30 June 2018. Importantly, CBA has noted that the team structures proposed by the business and support units will be assessed by Group Risk to verify their consistency.

The Panel notes that implementation of the Three Lines of Defence model varies across financial institutions and there is no one 'best practice' model. However, irrespective of the particular model chosen, key principles maintain that business management cannot abrogate its responsibility for risk management, and clear separation of the roles and responsibilities of Line 1 and Line 2 must be upheld.

In embedding its Three Lines of Accountability principles, it will be important for CBA to:

- adequately train staff whose roles change as a result of the implementation of the principles;
- conduct a post-implementation review to confirm that the principles have been effectively embedded. The results of the review should be reported to the Executive Committee and the BRC; and
- require any proposed deviations from the principles to be approved by appropriate staff and to be adequately documented.

## Recommendation 9

*CBA ensure that its Three Lines of Accountability principles are effectively embedded and subject to strict governance. In doing so, CBA must ensure that business units take primary ownership of risk management.*

## Recommendation 10

*CBA ensure that business unit Chief Risk Officers have the necessary independence to provide effective challenge to the business.*

## Recommendation 11

*CBA strengthen its Risk in Change process to ensure that there is effective risk-based oversight from Line 2 across the Group.*

### *4.2.2. Operational and compliance risk management*

In the Panel's view, CBA's management of operational and compliance risks is inadequate and requires significant improvement.

**Operational and compliance risk metrics in the Group Risk Appetite Statement (RAS)**

Until recently, operational and compliance risk metrics in the Group RAS were under-represented relative to metrics for financial risks. The metrics that were included tended to focus on whether risk management processes had been properly executed rather than on CBA's risk profile, were backward looking in nature, and were not sufficiently detailed to provide a meaningful view of CBA's operational and compliance risk profile. The metrics included the proportion of incidents not captured and recorded in RiskInSite within five business days of discovery, annual operational risk losses, and the proportion of controls across the Group that were untested or 'Unsatisfactory'.

In August 2017, more and improved operational and compliance risk metrics were included in the Group RAS as part of an initiative in the 'Big Rocks' program. However, the metrics relating to residual risks and control effectiveness are expressed as aggregates. There is a possibility that crucial risks rated as 'Very High' or controls rated as 'Unsatisfactory' may at an aggregate level be communicated as being within CBA's risk appetite. In the Panel's view, better practice would be to use more granular metrics. The Panel notes, for example, that CBA now monitors and reports to the Board's Financial Crime Review Committee specific metrics that provide a more accurate picture of CBA's financial crime risk profile, such as the number of days it takes to address transaction monitoring alerts.

**CBA's operational and compliance risk policies and frameworks**

CBA has acknowledged to the Inquiry that its operational and compliance risk management policies are documented in a complex manner, making it difficult for Line 1 to implement them effectively. For example, the Operational Risk Management Framework How to Guide is 119 pages long and contains a significant amount of detail on the steps necessary to undertake key operational risk management activities, such as a Risk and Control Self-Assessment and Risk in Change assessment. In addition, interviewees noted that, historically, policies developed by Group Operational Risk had been provided to the business units to implement without sufficient training, with one interviewee noting that new policies were developed and simply 'thrown out there' to be implemented.

As with the Three Lines of Defence model, CBA's policies and frameworks for managing operational and compliance risks have been inconsistently implemented across the Group, given that business units have been allowed significant scope to tailor them to their businesses. This has increased the risk of gaps in the identification, measurement and management of operational and compliance risks, particularly in relation to risks from products and processes that cross business units. APRA's 2015 Operational Risk prudential review report also noted that the variable implementation of the Operational Risk Management Framework across CBA made it difficult to provide a clear picture to the Board and management about whether controls were operating effectively to address key risks.

As part of an initiative in the 'Big Rocks' program, CBA has been simplifying the technical content and form of operational risk and compliance policies. To date, the Operational Risk Management Framework has been reviewed and amended, and immediate priority areas for simplification have been identified. Compliance policies are also being improved by Group Compliance, with a number of policies simplified to date. In addition, accelerated simplification of priority policies has been noted as a deliverable of CBA's operational risk and compliance transformation program.

CBA has also taken a number of steps to improve cohesion between Group operational and compliance risk teams and the business units in designing and implementing policies and frameworks:

- In May 2017, business unit risk teams began reporting to the Group operational and compliance risk functions in addition to the business unit CROs. CBA has noted that this has resulted in the Group functions becoming accountable for the implementation of policies and frameworks as well as their development, and in the Group and business unit risk teams co-designing frameworks;
- a new Group Compliance Policy team is now responsible for engaging with business units to update and implement policies;
- relationship management roles are being established in the Group risk teams to assist business unit risk teams to implement changes within business units; and
- CBA has appointed staff qualified in project management, change management and learning and capability uplift to design and implement change programs. As an example, CBA has noted that the involvement of these staff in the recent rollout of its risk taxonomy (a standardised way of classifying risks, discussed below) assisted in creating a detailed implementation plan to address change management and training requirements.

In addition, CBA is taking steps to promote consistency in the management of operational and compliance risks across the Group. The Executive Committee endorsed the implementation of minimum standards for managing such risks in February 2018. CBA proposes to implement a component of the minimum standards through a phased rollout of simplified operational and compliance risk management frameworks in each of the business and support units. The simplified frameworks are embedded in CBA's Risk Management Implementation (RMI) tool, which was recently designed and rolled out in RBS to enhance Line 1's understanding and management of risk. CBA proposes to pilot the RMI tool in each business and support unit, with the approach for the pilot to be agreed by 30 June 2018.

**CBA's approach to managing operational and compliance risks**

CBA's operational risk and compliance functions have had a heavy procedural bias. This is evidenced by rules-based policies containing very detailed, step-by-step processes that foster a 'form over substance' approach to risk management. It is also evidenced in a significant focus on assessing compliance with policies and procedures. For example, as discussed above, until August 2017 metrics that were included in the Group RAS assessed, among other things, whether or not processes had been executed rather than the bank's risk profile. Specifically, two out of the five operational and compliance risk metrics measured the proportion of incidents not recorded within five business days of discovery in RiskInSite and the number of business days within which significant breaches were notified to regulators.

CBA has acknowledged to the Inquiry a focus on process rather than on mitigating risk. Interviewees noted that the risk function 'couldn't see the forest from the trees' and was 'consumed by process'. This finding is also consistent with the finding in the Culture and Leadership chapter regarding a lack of ownership of outcomes in favour of following process.

CBA's approach to operational and compliance risk has also been focused on reacting to losses and incidents that had already occurred, rather than proactively identifying, measuring and managing risks. As an example, the previous CRO's report to the BRC placed a heavy emphasis on CBA's operational risk loss history and tracking the remediation status of operational risk and compliance incidents with losses greater than $5m. This finding is consistent with the Panel's overall assessment that there have been high levels of

reactivity in CBA's management of operational and compliance risks. It has also been acknowledged by CBA. In 2017, a Board paper outlining the views of Risk Management, Group Audit and Assurance and human resources in relation to CBA's risk culture noted 'risk activity can be focused on reacting to incidents as they arise, rather than proactively addressing potential vulnerabilities'.

**Resourcing and capability of the operational risk and compliance functions**

Effective operational and compliance risk management relies on a risk function that has an adequate number of risk professionals with the right skill sets. CBA has acknowledged that its operational risk and compliance functions are not adequately resourced, with the resourcing gap significantly higher for compliance than for operational risk. CBA has also acknowledged that there is scope to enhance staff capabilities. The issue of staff capability has been a persistent one; APRA recommended in its 2015 Operational Risk prudential review report that CBA review and where necessary enhance Line 2's capabilities at Group and business unit level.

CBA has been recruiting operational risk and compliance staff, in both Group Risk and business units. Recruitment is anticipated to continue until 2019. CBA also intends to upgrade the capability of its staff through an internal capability uplift program and formal capability framework (both in the initial stages of development), as well as through existing talent and succession planning processes.

An Executive Committee paper in late 2017 noted that CBA's capability to standardise the identification, measurement, aggregation and management of risk across the Group required significant enhancement in order to approach best practice. The shortcoming has restricted CBA's ability to analyse the large amount of data in RiskInSite to measure its operational and compliance risk profile. In early 2018, there were around 6,000 risks, 9,000 incidents and 3,000 issues in RiskInSite. As an example of CBA's inability to adequately consider its risk profile from an aggregate, Group-wide perspective, a paper to the BRC in June 2017 (and to the Board Remuneration Committee in August 2017) reacting to APRA's IT Risk prudential review in December 2016 noted: 'Many known issues which had been variously reported at different times but on a specific, disaggregated basis, thus failing to provide an overall view of the IT risk environment'. Limitations in CBA's ability to identify emerging and systemic issues are discussed further in the Issue Identification and Escalation chapter.

In terms of remediation, CBA has recently developed a new operational and compliance risk taxonomy as part of an initiative in the 'Big Rocks' program. There are also initiatives for improving the analytical tools used for operational and compliance risk management, with a rollout of a key tool (Data Analysis Risk Tools (DART)) expected in the first half of 2018. The taxonomy and DART are expected to standardise and enhance the identification, assessment and aggregation of operational and compliance risks across CBA. CBA also expects to progress work on enhancing RiskInSite's user interface to facilitate the use of DART, and on its draft operational and compliance risk controls taxonomy; the target implementation date for the latter is December 2018.

**Line 2's assurance responsibilities**

Resourcing and capability gaps, together with instances of Line 2 performing activities that would normally be performed by Line 1, have contributed to variability in the extent to which Line 2 has fulfilled its core assurance responsibilities across the business units. CBA has acknowledged that Line 2's focus on assurance needs to be substantially enhanced, reinforcing internal audit's view in its June 2017 paper to the BAC, referred to earlier. The enhancement to Line 2's resourcing and capability now under way is essential, particularly given that CBA does not currently use RiskInSite to link compliance obligations to the associated controls but instead relies on the compliance function to manually ensure compliance with those obligations as part of its regular assurance activities.

Gaps in Line 2's assurance activities have contributed to the lack of urgency and comprehensiveness in closing audit issues, discussed later in this Report. The gaps have also contributed to a high percentage of key controls for inherently 'Very High' or 'High' risks being rated as Marginal or Unsatisfactory. CBA's control environment is discussed further below.

CBA has advised the Inquiry that Line 2 is developing more formal and structured assurance plans through an operational risk monitoring register, an integrated operational risk assurance program, a Compliance Monitoring Program and operational and compliance risk 'deep dive' reviews. The Panel understands that the operational risk monitoring register has been established to evidence material instances of challenge or assurance conducted by Line 2 that have not been centrally documented. However, the Panel has not seen the details of the integrated operational risk assurance program.

The Compliance Monitoring Program was established in December 2017 to provide Line 2 business unit teams with a consistent standard and methodology for completing minimum compliance monitoring requirements. The Program also aims to provide the minimum standard for Group Compliance to complete assurance over the business unit compliance monitoring requirements. The Program requires Line 2 business unit teams to complete business activity statements and design and implement annual compliance monitoring plans that need to be effective from 1 July 2018.

Line 2 performed a series of 'deep dive' reviews between June and December 2017 in the areas of financial crime compliance, conduct risk, supplier risk, IT risk, conflicts of interest management and privacy and data protection. The reviews provided an assessment of CBA's capabilities in these areas and recommendations to the Executive Committee and the BRC to improve existing programs and initiate new programs. As an example, the 'deep dive' review of conduct risk resulted in the development and implementation of a Group-wide approach to conduct management (discussed below), whereas previously there had been multiple definitions and approaches to conduct management. The Panel considers 'deep dive' reviews to be an effective method of identifying and addressing operational and compliance risks. Accordingly, the Panel would encourage similar 'deep dive' reviews to be conducted on an ongoing basis across the full range of non-financial risks faced by CBA.

### *4.2.3. CBA's control environment*

In the Panel's view, there is significant scope for improvement in CBA's control environment.

As shown in Figure 2 below, as at December 2017:

- almost 12 per cent of key controls for inherently Very High or High risks were rated as Marginal or Unsatisfactory. This was in excess of CBA's own risk appetite 'trigger' of 10 per cent for this aggregate metric;
- the percentage of key controls for inherently Very High or High risks that were rated as Marginal or Unsatisfactory were in excess of: CBA's risk appetite limit of 20 per cent for two risk themes (Security and Resilience); CBA's risk appetite trigger of 15 per cent for one risk theme (Data); and 10 per cent for the Conduct risk theme; and
- the percentage of residual risks (i.e. inherent risks after the application of controls) rated Very High or High were within CBA's risk appetite.

*Figure 2: Status of key controls*

| Measures by Risk Theme (at 31 December 2017) | Group | Conduct | Security | Data | Disclosure | Errors | Financial Crime | Resilience |
|---|---|---|---|---|---|---|---|---|
| Percentage of key controls for inherently Very High or High risks rated Marginal or Unsatisfactory | 11.7 | 11.7 | 20.2 | 15.4 | 4.0 | 8.6 | 9.0 | 22.8 |
| Percentage of residual risks rated Very High or High | 4.2 | 4.5 | 13.6 | 2.2 | 2.5 | 2.2 | 3.2 | 7.3 |

Source: CBA Executive Committee paper dated 19 February 2018

As discussed in the Role of the Board chapter, the BRC had traditionally paid little attention to controls. An interviewee noted that the Executive Committee also did not have sufficient visibility of thematic control issues and, with the exception of some leaders, controls were not viewed as a priority in CBA. Consistent with CBA's reactive approach to managing operational risk and compliance, the interviewee noted that there was also an assumption within CBA that controls were satisfactory because losses had been low.

## Recommendation 12

*CBA strengthen its management of operational and compliance risk. In doing so, CBA must ensure that:*

- *the Group Risk Appetite Statement includes limits and triggers for more granular operational and compliance risk metrics by risk theme;*
- *minimum standards are clearly articulated in policies and embedded across the Group;*
- *there is a stronger focus on the 'big picture' and identification of emerging risks;*
- *Line 2 effectively fulfils its assurance responsibilities;*
- *the control environment is robust, reflecting effective control design and testing; and*
- *root causes and not merely issues are addressed in a timely and effective manner.*

## Recommendation 13

*CBA build up the capabilities and subject matter expertise of operational and compliance risk staff through training and continued recruitment.*

### *4.2.4. CBA's compliance function*

Until recently, CBA's compliance function had not been given sufficient recognition, stature and authority as a separate risk discipline. CBA has traditionally defined compliance risk as a subset of operational risk and many of CBA's key processes to manage compliance risk are codified as procedural steps in the Operational Risk Management Framework. This is normally effective when the risk is specific and can be managed through a set of controls. However, compliance functions globally have more recently been focused not just on evaluating with business units whether an activity or product is allowed under regulation ('can we?') but, critically, whether they should engage in such an activity or product in the first place ('should we?').

In December 2016, the EGM, Compliance role was elevated to be in line with the EGM, Operational Risk role, with both roles reporting directly to the Group CRO. This is a positive development that is consistent with better practice and will assist in applying much-needed focus and visibility to the management of compliance risk.

At a business unit level, CBA has separated the operational risk and compliance risk functions in only some business units. The separation of the two functions will allow CBA to more extensively develop them as distinct disciplines. Where CBA chooses to maintain coverage of the two disciplines under one manager, this should be on the basis that the individual has a good understanding of both operational risk and compliance or is supported by staff who compensate for any tendency or predisposition of the manager toward one type of risk. The Panel notes that CBA will continue to assess the relevant individuals' capabilities, and has confirmed to the Inquiry that further separation will occur if deemed necessary − for example, as a result of the realignment of operational and compliance risk activities and resources across Lines 1 and 2 in accordance with the Three Lines of Accountability principles.

The Panel notes that a number of banks internationally have elevated the Head of Compliance to membership of the Executive Committee. Short of that, the Basel Committee on Banking Supervision's 2015 *Corporate governance principles for banks* includes guidelines that:

> *The compliance function should directly report to the board, as appropriate… on how the bank is managing its compliance risk… to be effective, the compliance function must have sufficient*

> *authority, stature, independence, resources and access to the board.*[6]

The Basel Committee has also previously noted that it may be useful for the Board or a Board Committee to meet with the Head of Compliance at least annually as this would assist in assessing the extent to which compliance risk is being managed effectively.

## Recommendation 14

*CBA elevate the stature of the compliance function by making the Head of Compliance a member of the Executive Committee and/or the recommended Non-Financial Risk Committee, by making their appointment and removal subject to approval by the Board Risk Committee, and by ensuring that they have direct access to the Board.*

### *4.2.5. Conduct risk*

Conduct risk has been defined by the Australian Securities and Investments Commission as:

> *the risk of inappropriate, unethical or unlawful behaviour on the part of an organisation's management or employees. Such conduct can be caused by deliberate actions or may be inadvertent and caused by inadequacies in an organisation's practices, frameworks or education programs.*[7]

Examples of conduct risks commonly include insider trading, conflicts of interest and mis-selling. However, given the breadth and scope of the definition, conduct risk can arise anywhere there is inappropriate, unethical or unlawful behaviour. Episodes of misconduct can cause serious damage to a bank's reputation and undermine the confidence of customers and other counterparties.

For that reason, conduct risk needs an intense level of scrutiny in a bank.

Until 2017, CBA applied a narrow definition of conduct risk, which focused primarily on risk arising through the design and distribution of CBA's products. CBA's Product Development and Distribution Policy, which governs the approval of new and changed products, was established to, amongst other things, 'ensure products and services are developed and distributed to meet target market and customer needs and interests'. The policy contains various, and generally sound, mechanisms to ensure that both frontline and risk management staff consider and manage conduct risk arising from new and changed products.

In 2017, CBA expanded its concept of conduct risk to more closely align with the ASIC definition, stating that:

> *appropriate conduct is defined by business practices that are fair to our customers, protect the fair and efficient operation of the market and engender confidence in our products and services. Behaviour that does not meet this standard gives rise to conduct risk.*

CBA also established a formal Conduct Risk Strategy designed to manage broader conduct risks other than those arising from product design and distribution. The strategy is designed to embed the 'should we?' question into key decision-making processes, such as CBA's process to decide which projects should be funded.

Documents provided to the Inquiry suggest that, at a high level, the Conduct Risk Strategy should considerably enhance CBA's approach to conduct risk management. In the Panel's view, it is important that CBA's business units be reviewed to understand where they already are exposed to conduct risk and whether such risks are being appropriately managed. It is also important that the BRC and Executive Committee oversee and monitor the effectiveness of the Conduct Risk Strategy.

## Recommendation 15

*CBA review its conduct risk profile in business units, incorporate the findings in its Conduct Risk Strategy and ensure that conduct risk is fully considered in decision-making processes.*

[6] Basel Committee on Banking Supervision, *Corporate governance principles for banks*, July 2015.

[7] Australian Securities and Investments Commission, *Market Supervision Update Issue 57 – Conduct Risk*, March 2015.

# 5. ISSUE IDENTIFICATION AND ESCALATION

## 5.1. Background

Banks face a multitude of issues with potential risk implications. A bank needs to be able to identify these issues early and address them in a timely fashion. This is critical for achieving business objectives and limiting damage from problems that inevitably arise.

Issue management follows the same general pathway at most banks. Firstly, issues must be identified and assessed, and a decision made whether any risks posed will be accepted or mitigated. Issues can either be self-identified from scenario analysis, stress testing or thematic review, or identified via another process, including audit, compliance and regulatory review. Secondly, issues must be escalated to the proper level of the organisation, where actions to mitigate any risk posed are defined and approved. A process must be put in place to track progress in remediating the issue, culminating in completion of each appropriate action and closure of the issue. Banks will also have mechanisms in place to review and analyse individual risks. These will be used to determine root causes, trends, or patterns that may indicate larger systemic issues.

CBA has frameworks for issue identification, escalation and resolution, originating from staff (including in the business units, in the Group Risk function, and in internal audit), whistleblowers, customers and regulators. Weaknesses observed in the implementation of these frameworks give a background and context to how serious missteps have occurred in the recent past. Many, though not all, of the core problems with which CBA has struggled are industry-wide problems, but failures in issue management exacerbated their consequences at CBA.

In the Panel's view, strengthening CBA's issue management capabilities is critical.

**Staff**

CBA defines a 'risk' as an uncertainty on the achievement of objectives. Staff may raise an 'incident' or 'issue' related to one or more risks that follows a prescribed process for recording, rating, escalation and resolution. An 'incident' is an event causing unexpected outcomes from business processes, for example an event that causes CBA a financial loss. An 'issue' is a control weakness or gap that exposes CBA to potential losses, reputational damage or breach of regulation. All incidents and issues are required to be logged within five days of identification in RiskInSite, CBA's operational risk system of record.

Once recorded, incidents are rated based on impact to the business by way of financial loss, reputational damage or breach of regulation. Incidents must be escalated to predetermined levels of business unit management and Group Risk staff based on their severity. Senior management oversight of incidents is set according to escalation triggers. Incidents causing a loss of over $1 million are reported to the CRO and the Executive Committee. The Board is updated on aggregate losses from operational risk incidents. It has also considered specific incidents that have resulted in very high losses, regulatory focus, or media attention.

'Issues', once identified, are rated according to the likelihood an incident will occur in the next 12 months and the potential impact of the incident. Issues are then escalated to business unit management and Group Risk according to their rating. Group Risk may challenge how the business unit has rated an issue in some circumstances. Business unit risk forums are another escalation point for business unit management and risk staff to discuss incidents and issues. Issues may be escalated to the BRC through the CRO's Report, although issue escalation protocols to the BRC are not clearly set out in CBA policies. The Executive Committee does not receive reporting on issues from each business unit but rather focuses on the process of issue management. In addition, the CEO

has bilateral discussions with each Group Executive monthly, during which issues are discussed.

Group Risk reviews action plans for issues rated 'Medium' or higher. To close an issue, sign-off is required from the issue owner (the person accountable for the issue) and the issue manager (the person who manages due date extensions and rating change requests in RiskInSite). Group Risk is responsible for reviewing the closure of issues rated 'High' and 'Very High', as well as a sample of lower-rated issues. CBA policy does not specify how Group Risk is required to verify issue closure.

Issues raised by internal audit are treated similarly. Internal audit and the relevant business unit will agree on action items to remediate any problems identified during an audit, after which they follow the same issue ownership and management guidelines described above. Internal audit historically has been required to validate the closure of all 'High' and 'Very High' rated audit issues, and a sample of medium and lower-rated issues on a six-monthly basis. Recent proposed changes to internal audit's responsibilities will broaden its mandate for issue monitoring and validation.

**Whistleblowers**

CBA has in the recent past suffered damage to its reputation due to whistleblowers making their concerns public. In 2016, the Australian Bankers' Association (ABA), together with banks including CBA, undertook a program of work aimed at making bank staff confident they may report inappropriate behaviour without fear of adverse consequences. This initiative was prompted by a number of reviews, such as the Senate Economics References Committee, that identified deficiencies in Australia's corporate whistleblower practices. In December 2016, the ABA published guiding principles for improving protections for whistleblowers.

As part of the program, CBA enhanced its existing whistleblower framework. This included an update to the single policy that governs how matters of concern raised by whistleblowers are dealt with across the Group, and assignment of responsibility for managing whistleblower concerns to specific functions and individuals across CBA.

The Board approved the whistleblower policy in March 2017 and updated it in June 2017. The policy is consistent with the ABA's guiding principles. The policy is publicly available and applies to both current and former employees of CBA.

The Inquiry reviewed some individual whistleblower cases to determine whether policies were followed and whether complaints were properly handled. In each of the cases reviewed, policy was adhered to and there was no impropriety in the handling of the complaint.

However, the Panel found there is room to improve the confidence of staff more generally in CBA's whistleblower framework. The staff survey conducted for the Inquiry asked staff to respond to the following:

> *If I reported misconduct or other risk issues through a confidential channel, I am confident I would be protected*

The degree of confidence with this comment declined in proportion to the seniority of the staff responding. Some 95 per cent of those at EGM level agreed with the comment, declining to 68 per cent of middle management. On this basis, there is still work to be done to achieve the original goal of making staff confident that any report of inappropriate behaviour comes without adverse consequences.

**Customers**

CBA defines a complaint as 'an expression of dissatisfaction relating to the Group's products, services, activities or the complaints handling process itself where a response or resolution is explicitly or implicitly expected.' Regulatory guidance advises the recording of all complaints unresolved after five days from notification, and some types of complaints that are resolved within five days.[8] CBA has implemented a system designed to capture all complaints regardless of when they are resolved. This has created a

[8] Australian Securities and Investments Commission, *Regulatory Guide 165 Licensing: Internal and external dispute resolution*, July 2015.

high volume of complaints data available to CBA to interrogate.

Three main parties are involved in handling customer complaints: frontline staff in the relevant business unit, Group Customer Relations (GCR) and the Customer Advocate team. Most complaints are resolved by business unit frontline staff. GCR responds to more complex complaints referred by frontline staff or senior management, or matters of concern raised by customers directly to them. The Customer Advocate responds to complaints referred from GCR or appealed by the customer. The Customer Advocate is also tasked with promoting fair customer outcomes and resolving the root cause of customer complaints.

Information and metrics regarding customer satisfaction and customer complaints are provided to the Executive Committee. This customer complaint information includes number of and trend in customer complaints by business unit, information on resolution times, and some high-level information regarding themes in customer complaints. Information regarding overall customer satisfaction, but not customer complaints, is provided to the Board. Business unit staff are required to record 'issues' and 'incidents' as they relate to customers in RiskInSite.

**Regulators**

CBA is supervised across its activities by both domestic and overseas regulators. CBA has a policy that details its contact, procedures and reporting requirements with regulators. This policy is monitored for compliance by the Group Compliance team, which reports to the CRO.

CBA categorises contacts with regulators into routine contact for non-contentious operational or administrative matters, and non-routine contact for contentious or unanticipated matters. Business unit compliance teams are required to notify Group Compliance of most types of non-routine contact.

Business units must also maintain accurate and auditable records of their contact with regulators. All matters should be recorded in RiskInSite within five business days. According to policy, any regulator report or correspondence that is deemed contentious or raises material concerns must be reported to the BRC by Group Compliance.

## 5.2. Inquiry findings

The Panel has found shortcomings in CBA's handing of issues escalated from staff, customers and regulators. CBA has difficulty identifying broad, systemic issues in its businesses, including by linking sources of risk data across the institution and through analysis of customer complaints. In addition, CBA has had difficulty resolving identified issues as a result of organisational complacency, low senior-level oversight, and weak project execution capabilities.

CBA prides itself on success with customers, which has been viewed in terms of short-term, aggregate satisfaction metrics. Reporting to the Board on these metrics alone has obscured visibility of complaints from customers with extreme negative experiences. Nor has this reporting given impetus to fully analysing the complaints data available to CBA.

The Panel also heard that CBA has interacted with regulators in a legalistic and defensive manner, inhibiting the development of constructive engagement with regulators.

### *5.2.1. Issues escalated from staff*

The majority of issues in CBA are raised by staff across the three lines of defence. CBA has exhibited weaknesses in issue management, most notably in issue resolution. As a result, the consequences of recent missteps have been more severe than otherwise.

CBA has historically faced difficulties in the three phases of issue management: issue identification, escalation, and resolution:

- issue identification has improved in recent years but there are weaknesses in CBA's ability to identify large potential issues from across multiple areas and sources of information;
- issue escalation is also improving, but there are critical issues that do not rise to the senior leadership of the organisation;
- issue resolution has been a significant problem for CBA, which has often approached the process of fixing problems without adequate urgency or thoroughness.

# 5. ISSUE IDENTIFICATION AND ESCALATION

When taken together, CBA has fostered an unsatisfactory environment that has tolerated inadequate and tardy resolution of issues, and inconsistent execution of risk and compliance projects.

Shortcomings in the CBA's Board, Board Committees and Executive Committee oversight over operational and compliance risk issues are discussed in the Role of the Board and Senior Leadership Oversight chapters. Details, causes and implications of CBA's other weaknesses in issue management are discussed below, as are CBA's efforts to improve its capabilities in this area.

**Limited systemic issue identification across CBA**

The capability of CBA's business unit and risk staff to identify issues has increased in recent years. A 2016 internal audit thematic report showed a 24 per cent rise in total issues identified during that year. Commentary from internal audit noted that this was primarily due to business unit staff increasingly identifying and logging risk issues. The probable cause of this behaviour was the emphasis on raising issues by the former CEO and the associated SpeakUP campaign across the organisation (discussed in the Culture and Leadership chapter).

While there has been an improvement in frontline issue identification, there has been continued weakness in identifying larger emerging and systemic issues with a major potential impact on CBA. Interviewees told the Inquiry that the increase in issues identified by the business units has been driven by increased logging of symptoms of the same set of key issue areas. CBA has processes to identify emerging and systemic issues from these symptoms, but weaknesses are evident in CBA's ability to assess these issues, particularly across multiple business units or by aggregating information from multiple sources.

The processes for emerging risk identification include an emerging risk radar updated by the CRO. However, the definitions of likelihood and impact of emerging risks are not well developed compared to peers. This has been noted in third-party reviews of CBA's risk management capabilities.

Contributing to this weakness is that RiskInSite does not allow for easy amalgamation of risks across business units. CBA's business units historically used different risk taxonomies. Those different taxonomies meant that Group Risk needed to manually check for systemic issues that may have been applicable across multiple areas of the organisation. As discussed in the Risk Management and Compliance chapter, a common risk taxonomy that can be used to aggregate and better manage group-wide risks across business units has recently been developed by CBA.

Many global banks have structured, formalised systemic issue identification processes to join risk information from different sources, for example systemic issue analysis of customer complaint data and linking this to issues raised by staff or from other sources. The Group operational risk or compliance functions are often best positioned to perform these types of analysis, particularly analyses across different sources of data. Consistent with Recommendation 12 in the Risk Management and Compliance chapter, CBA should foster an operational risk and compliance environment with stronger staff focus on the 'big picture' and identification of emerging risks from different sources of information and across business units.

**Weakness in remediating issues**

CBA's most significant weakness in issue management has been issue resolution. This includes both the identification of appropriate remediation actions for an issue and ensuring that these actions are carried out in a timely manner with the rigour required to mitigate risks.

*Remediation of audit issues*

CBA's internal audit function discovered many of the most serious conduct and compliance issues faced by CBA. Low levels of senior oversight contributed to a lack of urgency in closing these issues. Specifically, internal audit raised many significant issues to the BAC. The BAC followed up on progress against some issues (particularly where regulators expressed concern) and reviewed the control environment of each business unit on an annual basis, but its tracking and monitoring of audit

issues was not systematic and below peer standards.

This lack of follow-up has led to a build-up of issues across CBA, which in turn has slowed issue resolution times. A June 2017 internal audit thematic report noted a 44 per cent increase in material issues over the 11 months leading to the report and that this volume of risk issues was 'manifesting in staff pressure.' This had resulted in an increase in resolution times for 'Very High' and 'High' issues from 200 to 275 days over the three years leading up to the report.

Data on issue closure at CBA shows a lack of urgency in closing issues. As of October 2017, more than 25 per cent of open 'Very High' or 'High'-rated audit issues, related to audit reports from the past five years that contained an unsatisfactory rating for control environment or management awareness and action, have had their resolution date extended twice or more. Of these open issues, 39 per cent had remained open for more than two years.

Lack of oversight of issue closure has also impacted on the thoroughness of issue management at CBA. Internal audit's review of issues closed found that, in the first half of 2016, 12 per cent of audit issues closed by business units were closed without the risks being wholly mitigated; this decreased to eight per cent in the second half of 2016. An internal audit report on progress in remediating AML control weaknesses in December 2014 showed that of five issues, four had been closed without fully addressing the risks. Internal audit also noted in 2017 that there was potential for 'inappropriate risk acceptance in the organisation'. That is, business units might be willing to accept higher levels of risk without appropriate controls, which they might not have the capacity or willingness to create within allotted timeframes.

As noted earlier, the BAC extended responsibilities for internal audit in late 2017. These included independent monitoring of the resolution of the Group's significant issues, reporting to the BAC on a quarterly basis and regular follow-ups on management progress against significant audit reports. While these are welcome changes, the Panel notes that they were made only after recent high-profile missteps.

Lengthy resolution times, frequent delays in closing issues, lack of rigour in issue closure, potential higher tolerance for accepting risks, and slowness in enhancing internal audit's role in issue monitoring, evidence an organisational complacency with respect to management of audit and other issues.

*Board attention to long-outstanding issues*

Board oversight of issues that have been outstanding for long periods, and pressure to resolve such issues, is an important element of the tone at the top. Overall, the CBA Board's attention to long-outstanding issues was historically low and increased significantly only after APRA's December 2015 Operational Risk prudential review. In that review, APRA stated that CBA's Operational Risk Management Framework was 'not effectively identifying, escalating, and addressing significant operational risks.'

In addition to this observation, the APRA review highlighted several specific and significant control gaps that had remained open at CBA for a lengthy period of time. APRA required CBA to report to its Board and to APRA regarding these control gaps and any other gaps that had not previously been escalated to the Board or senior leadership, or did not have a clear owner. CBA was initially reluctant to accept the broader observation around its issue management capabilities, stating in its response:

> *We recognise that more work needs to be done to further embed the Operational Risk Management Framework (ORMF), and we are committed to achieving this outcome. Specifically, we accept your concerns that we are yet to close off issues in areas related to data quality, stability of 3LoD approaches and rogue trading controls … Whilst we accept that in respect of the above issues (among some others) the ORMF has not worked effectively we do not agree with the broader conclusion that the ORMF is not effectively identifying, escalating and addressing significant operational risks.*

The Board now receives regular reporting on long-outstanding issues. Initially, the report mainly

covered areas of concern to regulators. It now includes details of issues that have been open for over two years and have been extended twice or more. However, some issues identified as part of APRA's December 2015 review remain open. The longest outstanding issue, relating to data quality, has a closure date of December 2019, at which time it will have been open for over six years. Reporting to the Board and Executive Committee does not provide an assessment of the ongoing residual risk to the organisation during the period of remediation.

The Panel acknowledges that there will always be issues that require long-term projects to solve. In these cases, trade-offs need to be made between implementing short-term tactical solutions to reduce the immediate risk and building more comprehensive solutions. In considering these trade-offs, CBA must recognise that while short-term solutions reduce risk quickly, they are not a substitute for long-term solutions and should not be treated as such. Further, having too many tactical solutions in place at once creates complexity, which becomes a risk in itself.

*Remediation of issues raised by staff*

A recurring theme from focus groups and some interviewees was that, during the former CEO's leadership, there was a heavy emphasis on finding and escalating issues, but substantially less focus on resolving them. Frontline staff members frequently and increasingly raised issues. However, discussion at senior levels, and accompanying remediation actions, often had to be prompted by scrutiny from internal audit, the media, a regulator or another external party. The BAC minutes observed that, historically, management frequently had prior awareness of control environment issues identified by internal audit, external audit, or the regulator, but that scrutiny from one of these bodies was required as a 'trigger' for remedial action to begin. A number of recent high-profile issues at CBA, such as the media coverage over CommInsure, the AUSTRAC legal proceedings, and mis-selling of credit card insurance, stemmed from issues that were, to varying extent, known to management but were not effectively prioritised and addressed until media or regulatory attention forced further remediation efforts.

One case study the Panel explored during the Inquiry highlighted this problem. In this case study, management became aware of control gaps in a particular business unit in December 2011. However, the issues were not acted upon until after APRA imposed a requirement for CBA to address them in December 2012. An external firm highlighted the same weaknesses in April 2013. CBA put a project in place to address these gaps from May 2013 until January 2015, when the project was ended; this was despite an interim report from internal audit stating there was insufficient evidence for closure of some underlying control issues. The project was resumed only after internal audit issued a Red audit report on the same set of control issues in October 2015. In this case, both the creation and the resumption of remediation actions required a Line 3 or external trigger despite prior management awareness of control issues. The Board and APRA further elevated scrutiny of these control issues to ensure they were being addressed and closed. Closure was confirmed in a report dated March 2018.

This reactive aspect of the culture at CBA has not been helped by a process-based approach to risk management. CBA's RiskInSite system functions as a system of record, but it lacks high quality data inputs, advanced analytics, or tracking of risk mitigation. This promotes an approach that focuses on completing lists of assigned actions rather than ensuring underlying risks are mitigated. Improvements scheduled to RiskInSite are noted in the Risk Management and Compliance chapter.

*Project execution capabilities*

CBA has self-identified a poor capability for executing risk projects. An internal CBA self-assessment of project execution capabilities noted that cross-business communication for project purposes was weak and that review and oversight of progress on long projects was insufficient. Evidence of this was particularly acute in 2014/15. CBA increased its total funding pool for total Group projects from around $850 million to $1.2 billion in that year, but this pool was reduced the following year when CBA determined it did not have the capacity to complete the increased volume of projects. The inability to increase the capacity for project execution is a symptom of the complexity that CBA has layered upon itself. In interviews, the

Panel heard there is a perception amongst CBA staff that project execution capability is poor.

Weak risk project execution capabilities mean that efforts to resolve issues sometimes fail altogether and are subsumed by new attempts to fix the same problems. This cycle of project creation can give the false impression of constant progress.

*Better practices*

Better practices employ several tools to ensure the effective remediation of issues. The underlying principles are clear. The Board and Executive Committee must oversight and regularly follow-up on progress against major control gaps. Management should answer directly to the Executive Committee and the Board or one of its Committees for significant delays in remediating major issues. While this has occurred in some instances at CBA, it has not been done systematically at the Executive Committee or Board levels, as this Report has noted.

In addition to senior level oversight, good practice in issue resolution includes:

- clear protocols for recording action items, including responsible persons and due dates;
- procedures for follow-up, escalation, and oversight of items, including extensions or delays to completion of remediation actions;
- procedures for recording and approving closure of action items;
- assurance that closed items are completed effectively and that completion has fully addressed the underlying issue; and
- procedures for enforcing accountability for addressing issues. These consequences can apply to an individual (e.g. through remuneration) or collective (e.g. imposing a capital penalty on businesses that do not appropriately remediate major issues).

## Recommendation 16

*The Executive Committee and Board improve their processes for monitoring issues raised by internal audit, regulators and other sources, and end any organisational tolerance for untimely or ineffective resolution of significant and outstanding matters of concern.*

### *5.2.2. Issues escalated from customers*

In recent years, a number of CBA customer complaints have found their way into the public domain and have cast CBA in a poor light. As noted throughout this Report, there is a paradox here. CBA staff believe in and speak of the customer as their number one focus. And the message from the top is that the customer cannot be treated poorly.

In the Panel's view, some of the weaknesses in addressing issues raised by customers stem from the distinction between customer satisfaction and the treatment of customer complaints. In particular, the Panel has found:

- there has been too much focus on short-term, aggregate customer satisfaction metrics and not enough focus on resolving the tail of extreme examples of poor customer experience; and
- identification of systemic issues from customer complaints has been weak.

**Excessive focus on short-term, aggregate view of customer satisfaction**

Despite the public focus on treatment of customers by banks and other financial institutions, the Panel specifically noted that the CBA Board did not receive any metrics or analysis on customer complaints. Nor was there evidence of Board or Committee-level review of any systemic risks that these customer complaints might highlight. Customer complaints are a key risk indicator for conduct issues and are part of the BRC's remit at many institutions.

CBA has traditionally defined success in customer service through the Roy Morgan customer

satisfaction score,[9] and that has now switched to use of the Net Promoter Score.[10] CBA takes pride in having retained first place among major Australian banks on the Roy Morgan metric since July 2015, having formerly been fourth. Reporting to the Board on aggregate customer satisfaction continues to emphasise CBA's ranking relative to its peers. However, reporting does not emphasise the serious customer complaints that may be a small portion of overall complaints but may nonetheless represent a large number of customers with an extremely negative experience. These complaints may pose reputational or other risks to CBA.

Reporting to the Executive Committee does not emphasise severe customer complaints. This information is important of itself and needs to be analysed to judge whether it has implications for a larger number of customers, or may impact on the reputation of CBA. Specifically, the Executive Committee does not discuss individual complaints as a group, nor does CBA have a process for proactively escalating risks arising from severe individual complaints to the Executive Committee.

At present, the Executive Committee receives reporting with some information on the 'top' emerging issues from customer complaints. However, only two issues are selected each month, and a robust process has not been in place to determine how these are selected.

Board materials reviewed by the Inquiry did not include any discussion of customer complaints, systemic issues from these complaints, or risks arising from severe individual complaints; aggregate customer satisfaction scores are mentioned as part of management updates from each business unit to the Board.

Customers want a bank that is trustworthy, ethical, strong, and secure. Achieving these qualities requires attention to vulnerable customers and individual, serious complaints, in addition to aggregate customer satisfaction scores. The Panel agrees with the sentiment expressed in an interview that CBA is only as good as its attention to the most exposed.

CBA is seeking to improve handling of sensitive complaints as part of its Complaints Management Strategy, introduced in mid-2017. The strategy includes new 'sensitivity guidelines' that prompt escalation to a high-priority complaints team. This may help CBA address the most severe complaints for dissatisfied customers more promptly. Planned training for staff on customer care and customer vulnerability may also help to resolve complaints from customers in difficult situations.

The Complaints Management Strategy also includes strengthening and clarifying the role of the Customer Advocate team. This team is responsible for handling complex customer complaints and actively advocating for the customer in regular business processes. Its recent efforts include identifying CBA's most vulnerable customers and ensuring that customer-facing staff are equipped to appropriately handle the concerns of these customers.

Another recent effort by the Customer Advocate team has been to develop a new Group-wide policy for business units conducting customer remediation projects. It is intended that staff will be able to use this policy to identify if an incident or systemic issue requires a formal remediation project, and how best to conduct such remediation in a fair and efficient manner. The policy is accompanied by reference guides, which support each step in the remediation framework and provide practical guidance on how best to proceed with remediation efforts. The Panel welcomes these efforts, which should assist CBA in promoting customer care and giving appropriate attention to exposed customers. If they are to succeed, however, senior level attention and oversight will be essential. In better practice peer organisations, topics discussed by the Executive Committee and Board include:

- trends observed in customer complaints (both volume and topic);
- sophisticated customer metrics, including, for example, sentiment across social media platforms;

[9] Based on a Roy Morgan survey that asks how happy customers are with the service/company.

[10] The Net Promoter Score measures the willingness of customers to recommend a company's products or services to others. It is used as a proxy for gauging the customer's overall satisfaction with a company's product or service and the customer's loyalty to the brand.

- systemic issues observed in customer complaints that could result in regulatory breach or group-wide reputational damage; and
- individual material customer complaints that may result in adverse regulatory or reputational damage. Reporting includes the complaint, its cause and the remediation plan. There is also regular reporting on whether remediation actions have been closed and on whether deadlines have been extended or delayed.

## Recommendation 17

*CBA report on customer complaints to the Board and Executive Committee in line with better practice peer organisations.*

**Weak proactive identification and remediation of systemic customer issues**

Traditionally, the Group Customer Relations team was responsible for identifying systemic issues emerging from customer complaints. The large volume of information on customer complaints available to CBA was not fully utitilised in its analysis. A July 2015 Board paper stated that only 3.4 per cent of all complaints were reviewed to find systemic issues. Internal audit assessed that this may cause CBA to miss significant insights in systemic issue analysis. In particular customer complaints were not generally tied to other sources of data to identify systemic issues.

A July 2017 Executive Committee paper noted that only one full-time equivalent (FTE) was dedicated to identifying systemic issues and that this resourcing needed to be improved. The paper also identified that the capability for root cause analysis of customer complaints more broadly was immature. The cause of this immaturity was identified as a lack of clear governance, manual processes and lack of staff incentives related to resolving root causes of complaints. CBA has transferred the responsibility for identifying systemic issues emerging from customer complaints to the Customer Advocate to resolve these problems. The Customer Advocate now has a team of 5.5 FTE for this role.

A project is currently underway to enhance the systemic issues process within the Customer Advocate team. A new case management system is under development to support the systemic issues function to run efficiently and with appropriate risk management. It includes a single system interface to document issues, manage workflow and record decision making and outcomes. Enhancements also include data-driven identification of potential systemic issues using complaints data. The project, if implemented properly, should facilitate better systemic issue identification from customer complaints. The Customer Advocate also intends to improve its reporting across CBA, including the referral of potential issues to business units for investigation.

In better practice peers, banks perform systemic issue identification on the full set of customer complaints received and link this to other sources of data to investigate operational and compliance risk issues. Banks have in recent years increased investments in data and analytics to analyse complaints data, for example by product, business line or geography. CBA's Complaints Management Strategy calls for improvements in both resourcing and technology for systemic issue identification from customer complaints. The Panel views this as a positive step.

## Recommendation 18

*CBA prioritise investment in the identification of systemic issues from customer complaints.*

### *5.2.3. Issues escalated from regulators*

The Panel has met with the domestic agencies APRA, ASIC and AUSTRAC, as well as with the Financial Ombudsman Service Australia.

The regulatory agencies found CBA defensive, and at times perfunctory, in its attitude to matters raised by them. The Panel also heard concerns about CBA's lack of proactive engagement on these matters.

The Panel heard that CBA's 'default response' to being challenged was a legalistic and defensive

posture, compared to a more open approach taken by some of its peers. The Panel heard of occasions where CBA would insist on hearing why it was legally required to take action before it would do so. This adversarial approach appeared to put strict legal interpretation above risk or customer outcomes. Observations were also made on the difficulty of obtaining cooperation on matters where the Group Legal department had already provided a response. A more cooperative and less legalistic response would only be provided if the matter was escalated to CBA's senior management.

The Panel noted a theme from interviews suggesting slowness or disinterest in responding to regulatory concerns. This included difficulties in prioritising concerns that were raised on a pre-emptive basis, and frequent delays in complying with regulatory requests. The Panel heard of positive messaging put on risk issues, including an emphasis on the relative advantages CBA claimed it had compared to peers, and the downplaying of risks where no loss had yet been experienced.

Interviewees also noted that some regulatory concerns raised had been met with a response that the concerns were already known and considered not as important as other priorities, which would receive more urgent attention. This approach can be juxtaposed with instances where CBA staff sought requirements from the regulator in order to prioritise funding for remediation programs.

The Panel also heard evidence that CBA was less proactive and slower to comply with regulators compared to some peers. This was demonstrated by CBA's inclination to wait for the regulator to make initial contact following the emergence of an issue, or to rely on regulators sharing information rather than approaching other regulators with an interest in an issue. Interviewees interpreted this as a reluctance to proactively volunteer information on matters of regulatory concern. Frequent delays in compliance with regulatory requests pointed to a lack of capability in handling, or the de-prioritisation of, such requests.

In the Panel's view, CBA's new leadership team must strengthen its engagement with regulators. Better practice peers build positive working relationships with their regulators in solving risk and customer-related issues rather than view regulators as forces to be opposed on a strictly legal basis. Constructive engagement with regulators will be an essential element in addressing CBA's reactive culture.

### Recommendation 19

*CBA strengthen its dialogue and engagement with regulators.*

# 6. FINANCIAL OBJECTIVES AND PRIORITISATION

## 6.1. Background

Banks are naturally focused on financial objectives. Financially strong and profitable banks, participating within a competitive market for financial services, are the foundation for a stable, efficient and competitive financial system. Financial strength enables banks to meet the interests of customers, employees and shareholders and, as the global financial crisis has highlighted, is a pre-condition for economic growth.

Critically, however, banks must strike the right balance between short and long-term objectives and appropriately navigate the tension between the potentially competing interests of different stakeholders.

In a large organisation such as CBA, trade-off decisions are made every day at all levels. When making such decisions, a balance is required between, on the one hand, financial discipline and shareholder value considerations (the 'voice of finance') and, on the other, considerations of risk management, including aspects of a conduct and reputational nature (the 'voice of risk'), and of good customer outcomes (the 'customer voice'). Importantly, these latter considerations include the 'should we?' reflection in decisions CBA makes, especially with regard to customers.

Previous chapters have highlighted shortcomings in the governance, management and mitigation of non-financial risks and customer complaints. Collectively, these shortcomings contributed to a weak and inconsistent 'voice of risk' and 'customer voice' in CBA. By contrast, the 'voice of finance' has been strong and mature. In the Panel's view, this imbalance – especially when combined with cultural traits of complacency, reactivity and self-perceived but incomplete customer focus – has been a significant factor in the dynamics of CBA's decision making.

A symptom of this imbalance was captured in thematic commentary from internal audit to the BAC in December 2015:

> *We continue to see repeat issues in our audits… despite issues being signed off as complete. This can be the result of insufficient oversight by leaders, limited technical skills amongst those individuals involved in the fix, and fixes not designed in a sustainable way. System changes can also result in controls being disturbed and requiring reassessment. We appreciate that, in the current challenging business environment, risk issues can at times be deprioritised behind income generating priorities.*

## 6.2. Inquiry findings

The Panel observed imbalance between the 'voice of finance' on the one hand, and the 'voice of risk' and the 'customer voice' on the other, in two areas:

- CBA's investment prioritisation process (IPP) in design and practice has generally only addressed risk, compliance and resilience issues on a reactive basis once these become 'high rated' issues; and
- trade-off decisions in which financial objectives were implicitly prioritised over the 'customer voice'.

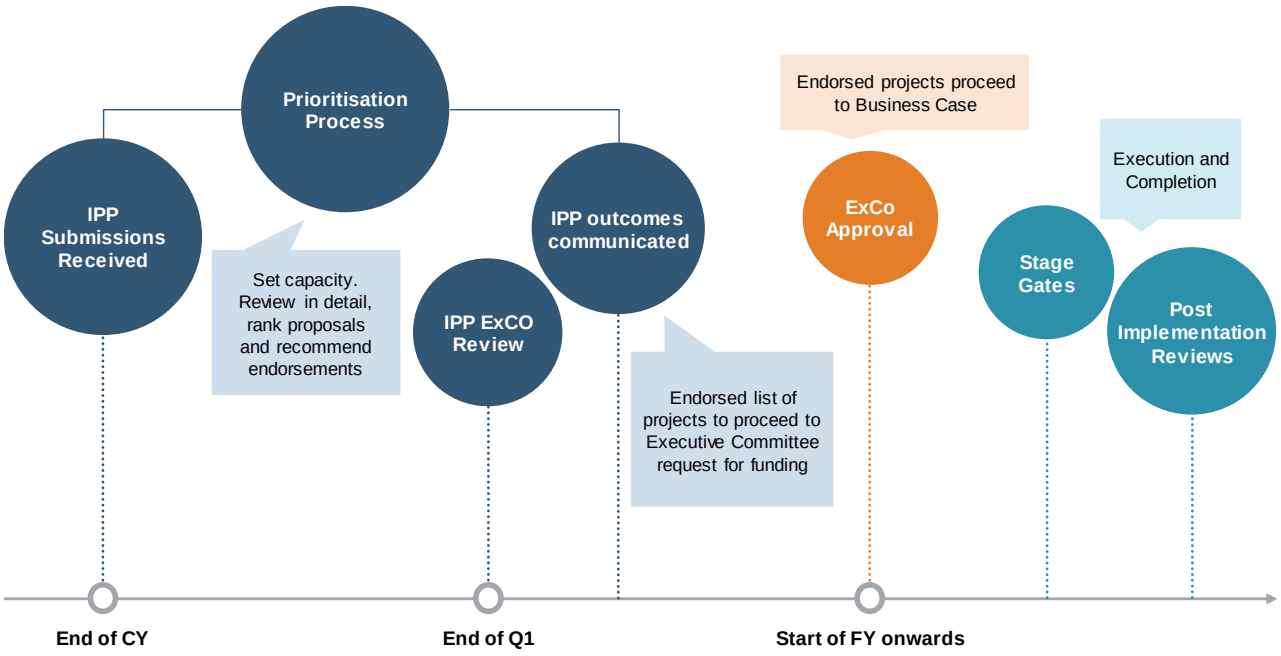
### *6.2.1. Investment prioritisation*

**Investment prioritisation process**

CBA's financial objectives and priorities are defined at the highest level through the setting of Annual Business Plans and the IPP. Both of these processes are informed by and embedded within the CBA Group's broader strategic planning cycle, in which the Board and Executive Committee define and agree long-term strategic priorities and focus areas, which flow into top-level financial planning and investment decisions.

CBA's IPP is an established process to review, select and approve Group-level projects. The IPP captures projects for which investment expenditure is anticipated to be greater than $10 million (for business units). Projects submitted to the IPP are subject to risk assessment by the CRO of the sponsoring business unit or support unit and are also designated a category of investment (see below). Submissions are subject to an intense evaluation process before endorsement by the Executive Committee and advised to the Board (see Figure 3 below).

*Figure 3: CBA's Investment Prioritisation Process*




Source: CBA

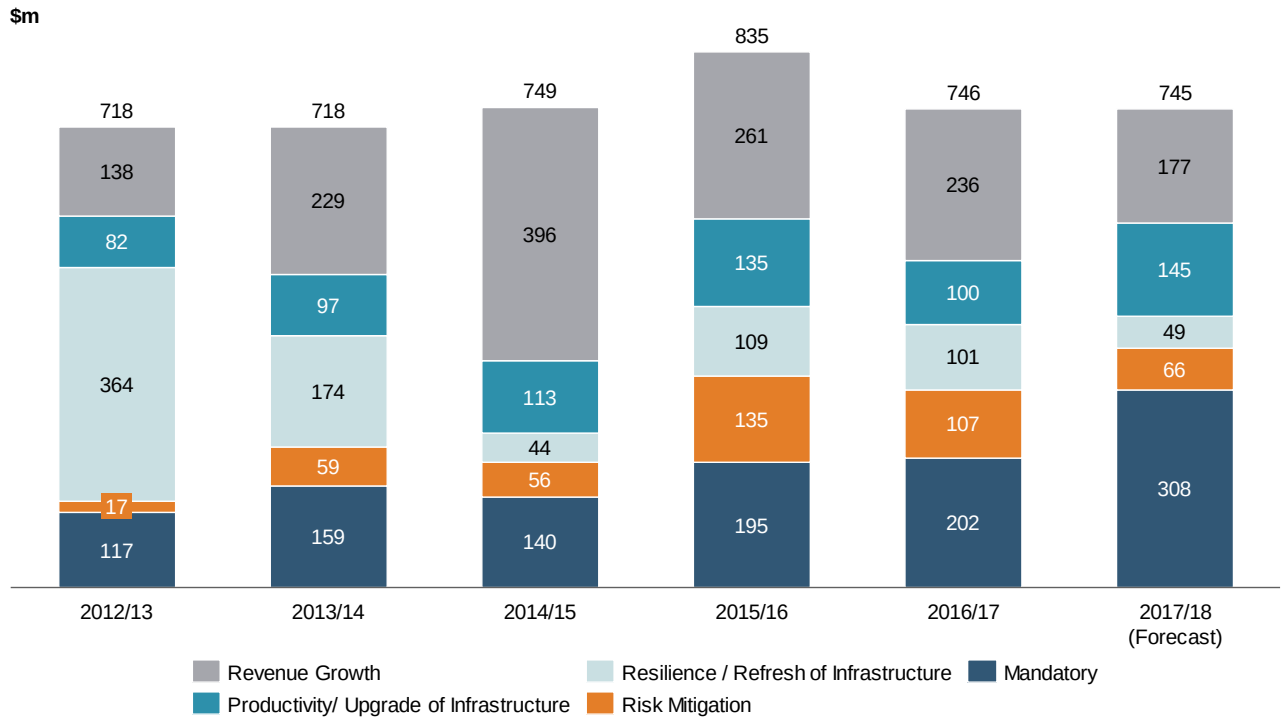
In parallel with the above Group-wide process, business units are allocated funding for their own projects that cost less than $10 million. Historically, this has not applied to support functions such as risk and finance, which have had to seek funding through the IPP even for proposals of less than $10 million. Projects proposed by Group Risk needed to be sponsored by the CRO as well as discussed with the CFO prior to review and approval by the Executive Committee.

For Group Risk, this process has changed recently, with a funding budget being granted for 2017/18 and 2018/19 to allow it to invest in strategic risk IT infrastructure.

**Adequate investment in response to 'high rated' issues**

The Panel noted that CBA invests substantially each year in risk and compliance projects, and as part of strategic growth initiatives. CBA typically has around 60 such group-level investment projects in train at any given time. As shown in Figure 4 below, investment in 'Mandatory' and 'Risk Mitigation' projects has broadly been increasing since 2012/13, within a largely flat total investment budget.

*Figure 4: Group-level gross investment spend*




Note: business unit level investment expenditure not captured.
Source: CBA

Further, proposals to address identified 'high rated' risk and compliance issues have invariably been endorsed by the Executive Committee, including on occasion as a direct result of the former CEO intervening to ensure adequate investment for the long-term. In an email to the Executive Committee, the former CEO noted:

> *I recognise that we have here a challenging trade-off between mitigating inherent risk, and the opportunity cost of the resources required for that mitigation. In our resource constrained environment, that is tough. We rightly have confidence in the strong culture we have built here, which is a strong defence against abuse. But it is not perfect…*
>
> *With that in mind, I will be advising the Risk Committee of the Board next week that: – [the relevant CBA executive] will coordinate a long term, Group-wide approach to remedying the control weaknesses… I recognise that none of us feel that this is among the highest near-term value initiatives we could undertake within the Group. But it is critical to long-term value. We need a systematic and determined way of going about this….*

**Limited scope for proactive investment in risk and compliance before 'high rated' issues arise**

However, CBA's IPP framework provides for priority investment in risk and compliance projects only on a reactive basis after these become 'high rated' issues. In general, no structural provision is made for investment in the portfolio of 'medium rated' issues before they become 'high rated' in order to proactively move to better practice.

The reason for this lies in the approval criteria for investment proposals. IPP submissions are categorised as 'Maintenance' or 'Growth' proposals. Maintenance includes 'Mandatory' (i.e. to meet compliance obligations), 'Risk Mitigation' and 'Infrastructure Resilience' proposals. Maintenance proposals are endorsed as a first priority ahead of Growth proposals, but only once stringent criteria are met. Mandatory proposals are endorsed 'only if the relevant regulations require implementation to commence immediately' and Risk Mitigation proposals are endorsed only for 'proposals addressing issues with a high probability and high impact'. Infrastructure Resilience proposals are only endorsed for 'systems requiring immediate refresh'. It is possible for proposals not meeting these criteria to be addressed through business unit level funding, although business unit level financial targets and related remuneration incentives would discourage this in practice.

In practice, the most common way for issues to become identified as 'high rated' is adverse findings being raised by internal audit, external audit or APRA. One interview observed – in relation to business-unit rather than group-level investment expenditure – that APRA's prudential letters and supervisory requirements were critically important as 'ammunition' without which funding approval would not have been obtained.

CBA's IPP practices appear robust but are characterised by a dominant 'voice of finance'. Strong rigour is applied to test the value, scope, timing and necessity of proposed projects. By contrast, there is not the same degree of systematic rigour in ensuring sufficient investment in risk and compliance. The risk function is a key stakeholder in the process, but its role has been less visible, intrusive and influential. Sponsors of risk and compliance projects are effectively required to jump multiple hurdles to have projects approved. Some select examples follow.

Firstly, the great majority of testing and questioning documented in the IPP has been directed towards financial discipline. For example, some questions raised by Investment Development, the team in Group Finance evaluating initial submissions, are set out below. These included inappropriate focus in relation to compliance projects as to whether fines had been levied historically.

> *How urgent is this? Why do we need to do this now? What is the impact if this is delayed by 6/12/18 months?*
>
> *Are there opportunities to minimize spend required in FY17?*
>
> *Can these issues be resolved through ad hoc and tactical remediation on specific problems?*
>
> *Any fines levied historically?*

Secondly, no comprehensive written risk assessment was submitted to the Executive Committee as part of the IPP proposal when seeking endorsement of a project, with the Executive Committee being provided with only a short one-paragraph description.

Thirdly, no risk assessment has historically been performed if a project was rejected or deferred. Outside of the annual risk assessment processes, there has been no tracking of the operational risk of not doing a project, nor has there been a process to understand the cumulative impact of the risk through time. As a result, the impact of rejection or delay of a risk mitigation project on CBA's risk profile has not been measured or monitored.

Finally, once a Maintenance proposal is endorsed, there have been no formal mechanisms to ensure timely development of a business case and timely execution of the actual program. While atypical, a small number of Maintenance proposals were observed to be endorsed but not subsequently progressed until some years later. Examples of this were CBA's country risk management project (relating to improved monitoring of credit risk exposures by country) and AML resilience (relating to controls to reconcile data across key systems).

An illustrative comment from the staff survey notes:

> *I am strongly of the view that Investment in Risk priorities and risk infrastructure are viewed as a 'grudge purchase' by finance and BU's. The only lens we seem to apply on Risk (and other) investment spend is an ROI or productivity lens. Sometimes the finance team have to accept that there is a necessary mandatory 'Stay in Business' capex or opex associated with risk infrastructure, frameworks and oversight and that will never achieve an ROI or productivity outcome but it will keep our doors open. Finance's seat at the table has been too dominant and we have often experienced… cutting back on risk investment spend or prioritisation to achieve financial outcomes.*

Outside the IPP, the Inquiry has observed a degree of implicit filtering of justifiable smaller scale risk and compliance projects at lower levels of the organisation.

An overall observation from the focus groups was that there was a tendency not to ask for investment in risk management solutions because of a general view that nothing will be done (not necessarily due to unwillingness to fund, but because everyone was too busy to implement, and nothing has been done about issues in the past). Related to this, there was a relative acceptance (or lack of agitation) regarding lack of investment in a range of systems that would allow better control and proactive risk management.

**The 'CRO backlog'**

A symptom and consequence of the IPP addressing risk, compliance and resilience issues on a reactive basis is the 'CRO backlog'. This backlog is essentially a list of risk and compliance projects considered to be of value but that had not been funded or progressed. The list was finalised during 2017 under the new Group Risk leadership team. As at late 2017, the CRO backlog comprised 27 items, including several described as 'must have'. These various items were initially raised for consideration in the period from December 2014 to September 2017.

Examples of highest priority items included: enhanced reporting and analysis of commercial property exposures against underwriting standards (as a result of elevated standards following APRA's industry-wide Commercial Property prudential review); and introduction of a group-wide system for managing conflicts of interest.

An incidental issue highlighted by the CRO backlog is that Line 2 had in practice become responsible for risk and compliance projects not pursued by Line 1 owners. Reflecting this, the CRO backlog allocated each item to a Line 2 EGM, but no Line 1-accountable individual was noted for any of these items.

**Further examples illustrating CBA's approach to investment trade-off decisions**

Two examples from 2015 illustrate CBA's approach to investment trade-off decisions at the margin. They confirm the Panel's conclusion that CBA invests adequately in relation to 'high rated' risk, compliance and resilience projects, but does not proactively invest in risk and compliance before such issues arise.

1. Control Remediation Review

In 2015, the former CEO requested that the risk and internal audit functions provide the Executive Committee and the Board with an independent view on whether there were any significant risk exposures that required further funding as part of the 2015/16 budget setting process.

The headline conclusion of the paper was that

> *the Group is already significantly focused on risk remediation. Key risk exposures escalated for senior management attention have been prioritised and are heavily invested in and therefore, receiving significant focus in the Business Units… No specific additional initiatives are, in Lines 2 and 3's view, critical in the current environment.*

The paper went on to note 'certain areas that could be considered by senior management to provide the Group with greater comfort or governance over a number of the Group's top ten risk areas or control concerns.' These areas were data management, supplier risk, conduct risk, manual controls and end-to-end controls, and AML-CTF. Most notably, commentary in the Board paper relating to conduct risk stated that as at that time:

> *Only 3.4% of the 885,849 customer complaints logged in the past 12 months were reviewed by Group Customer Relations for systemic issues. Approximately 250 potential issues were however identified from this analysis. This suggests an opportunity for the Group to more rapidly evaluate and respond to customer feedback received through complaints.*

In relation to manual controls it was observed:

> *A significant proportion (>80%) of key controls in RiskInSite are classified as manual in nature. International financial industry manual control benchmarks… suggest that leading practice is below 60%... Further to the high volume of manual controls, there is a general view that issues may be arising due to a lack of an end to end controls design view across the Group. Recent events… reinforce this view.*

The associated Board minutes record, in summary, that the Board noted the outcomes of the review and management's recommendation that no change was required to the Group's 2015/16 budget as a result. In the Panel's view, this was an opportunity missed to drive improved risk management.

2. Project re-sequencing

Around August 2015, in response to a substantial increase in group-funded projects and an associated deterioration in project execution, Group Finance developed scenarios for deferring or restricting expenditure for as many projects as possible, for Executive Committee consideration. For Mandatory (e.g. compliance) projects, the key criteria utilised was that projects would be deferred to the extent they related to 'proposals without near term fixed deadlines, or have deadlines likely to move'.

The Executive Committee ultimately endorsed a pushing back of around eight per cent of planned investment spending in 2015/16 to subsequent financial years. In practical terms, this meant that eight Maintenance and 13 Growth projects were deferred, typically for three to six months or to the next financial year.

This example illustrates CBA's appetite at the margin to push back Maintenance (and Growth) projects in response to reduced project execution efficiency and to achieve short-term financial objectives.

**Challenges associated with increasing investment expenditure**

The Panel accepts that there are constraints on CBA's ability to rapidly increase group-wide investment. The key constraints emphasised by CBA are senior management and subject matter expert bandwidth to effectively oversee complex Group-wide projects, and limited windows to safely implement IT system changes. In light of these constraints, improvement in this area is not as straightforward as simply increasing yearly investment expenditure. CBA did increase group-wide investment significantly in 2015/16 but, as noted, this led to a deterioration in project execution efficiency. Moreover, the stringent criteria applied to Mandatory (i.e. compliance) projects are not without merit, as they mitigate the risk that late-stage

changes to legislative or other regulatory requirements will result in thrown away costs.

Nonetheless, the Panel believes that CBA needs, over time, to more pre-emptively invest in risk, compliance and resilience projects rather than wait until they develop into 'high rated' issues. This may involve some combination of higher investment, scaling back of Growth proposals and/or redirection of management attention, at least for an interim remediation period.

Once issues have become 'high rated', their time-critical nature creates elevated pressure for more tactical and bespoke solutions, adding to the build-up of organisational complexity. Reflecting this, a March 2016 Board Paper from Enterprises Services observed:

> *The complexity of our IT ecosystem is caused by the deep interconnection of IT systems, proliferation of technologies, rate of change, and multitude of IT providers. This complexity is a gradual and inadvertent bi-product of the mass digitisation of our staff and customer experiences in real-time, our multi-channel strategy (driving the interconnection of our systems) and technical debt associated with project delivery which frequently does not account for necessary maintenance or deprecation of legacy systems…*
>
> *Historically investment in new equipment and features have been favoured over the maintenance of existing systems. This has led to an underinvestment in support capabilities both in projects and in strategic investment requests.*

Further, CBA's approach to investing in 'Infrastructure Resilience' proposals (i.e. only for systems requiring immediate refresh) may have contributed to instances in recent years in which CBA has failed to provide advertised benefits to customers.

**Recent improvements**

More recently, CBA has made a number of enhancements to its IPP process:

- funding for Group Risk to invest in Risk IT infrastructure for 2017/18 and 2018/19 has been pre-approved. Related to this, Group Risk has introduced elevated governance arrangements to track and co-ordinate management of the 'CRO Backlog';
- Group Customer Advocacy now reviews each IPP proposal to test alignment with, among other things, CBA's Vision and Values and customer outcomes;
- below the IPP level, additional governance forums have been introduced for business units and enterprise services to agree on business unit funding for small-scale resilience projects; and
- CBA has introduced the 'Platform Model', which in summary is a new operating model for engagement between business units and enterprise services, along groups of platforms with common capabilities. The objectives of the Platform Model include clarifying joint accountability, providing for more stable funding, and elevating the transparency and visibility of trade-off decisions.

These enhancements are a positive step. The first three are essentially tactical improvements that respond to limitations in the IPP. In the Panel's assessment, structural change is required to the way CBA makes investment trade-off decisions at the margin, to adopt a more pre-emptive approach and to elevate the relative 'voice of risk'.

## Recommendation 20

*CBA take in its investment prioritisation processes a more pre-emptive approach to investment decisions in risk management, compliance and resilience areas prior to these becoming 'high rated' issues.*

### *6.2.2. Decision-making in response to customer objectives*

As this Report has emphasised, banking at its most basic level is predicated on community trust. The fastest way for banks to erode such trust is to fail to 'do the right thing' by their customers. This is particularly the case given banks are increasingly judged not by reference to the sum total of customer interactions, but rather by reference to the fairness of outcomes for their most exposed customers.

The Panel noted two examples of trade-off decisions being made in which financial objectives were implicitly prioritised over the 'customer voice'. In each case, CBA was aware of the potential for poor customer outcomes but only took appropriate action in response to regulatory or external scrutiny. The 'can we?' question won out over the 'should we?' question. In the event, the compensation that was paid to aggrieved customers in these two incidents was relatively small compared to the reputational damage CBA suffered.

**Consumer Credit Insurance**

The Panel analysed the drivers that led to CBA systematically selling consumer credit insurance (CCI) to customers for which the product was unsuitable.

CCI has been packaged together with various loan products and operates to repay the loan balance if the borrower becomes sick, injured or involuntarily unemployed. However, a customer who is unemployed when purchasing CCI will typically be unlikely to claim under the policy because they do not meet the employment criteria.

An internal RBS 'deep dive' report from May 2013 drew attention to the risks associated with inappropriate CCI product design and sales practices. The paper noted the potential for these risks to 'lead to customer complaints' and if 'not addressed appropriately there is the potential for customer and reputational impact'.

An internal audit report of April 2015 subsequently identified:

> *Approximately 64,000 customers who were unemployed at the time of a Credit Card application were sold [Credit Card Plus (CCP)] insurance. Sales staff are not required to disclose to the customer that involuntary unemployment or temporary/permanent disablement benefits cannot be claimed if their situation remains unchanged.*
>
> *… these sales practices may not have resulted in a fair outcome for the customer. CommInsure Management will analyse data, understand customer impacts and implement changes to CCP product design and sales processes as required.*

The response to this internal audit finding developed over time. The initial response, in May 2015, for sales via branch and telephone, was to ask the customer if they were employed. However, for online sales, the response was only to include the following 'fine print' in the Product Disclosure Statement:

> *If you are working less than 20 hours a week or if your employment is seasonal in nature then Credit Card Plus may not be appropriate for you as you will not be able to claim for the monthly benefit.*

Based on these and miscellaneous other changes, the BAC was advised that the audit issue was closed in February 2016. In August 2017, ASIC announced that CBA would refund 65,000 customers over $10m in aggregate, and introduce additional checks into its online sales processes. CBA announced that it would cease selling its CCI product in March 2018.

In the Panel's assessment, CBA's response for online sales channels was inadequate. It reflected a failure to effectively address the root cause of an issue even after it was identified by internal audit and escalated to Executive Committee level. In interviews with the Panel, it was acknowledged, at Group Executive level, that a key factor in the delayed response was the Executive Committee's reluctance, without a decision-making mandate, to achieve consensus between two business units (one that issued the product and one that distributed it) with strongly held but divergent views.

**Delay in updating CommInsure's heart attack definition**

The definition of 'heart attack' used by CommInsure, CBA's insurance subsidiary, in its retail advice life insurance products came under intense media scrutiny in 2016. CommInsure had been aware of medical developments and early market movements towards updated heart attack definitions in 2012, but its definition was not updated at that point. In 2014, although a significant portion of the market had adopted a universal standard definition, CommInsure again chose not to update its definition at the time of a product review. Instead, it took steps to clarify the name of its heart attack benefit at this point, describing the benefit as 'heart attack of specified severity'.

The heart attack definition was one component of a complex product, which had presented CommInsure with profitability challenges. The Panel observed that decision-makers in the lead-up to the 2014 decision placed significant weight on financial considerations, including their interpretation of desired profit outcomes and the availability of reinsurance support. Although representatives of CommInsure's risk teams provided input to the product review process, financial considerations prevailed over broader risk implications, including potential customer outcomes, in this decision. Interviews with CommInsure Directors and senior executives conducted for the Inquiry confirmed that the 2014 decision was taken through a commercial lens and the 'should we?' question was not addressed. CommInsure has accepted this was a misjudgement.

In 2015, CommInsure decided to update its heart attack definition from October 2016, with no backdating. However, in March 2016, faced with media scrutiny, the planned changes were accelerated and backdated to May 2014. Subsequently, faced with regulatory scrutiny, the backdating was taken further to October 2012. A review of the evolution of the relevant Product Management Policy shows that customer advocacy was introduced as an explicit consideration as part of the process from 2016.

**Recommendations**

The key recent enhancement relating to customers is the elevation of the Group Customer Advocacy function, as outlined in the Issue Identification and Escalation chapter. The following recommendation builds on that development.

## Recommendation 21

*CBA leadership champion the 'should we?' question in all interactions with customers and key decisions relating to customers.*

# SECTION B

# ACCOUNTABILITY

# SECTION B: ACCOUNTABILITY

In banks and other financial institutions, accountability is closely linked with governance, risk management and culture. Accountability will not resolve issues in these areas but, when embedded, clear accountability will strengthen their effectiveness.

Accountability is built on frameworks that provide for clarity of ownership for responsibilities and obligations, and proportionate consequences when adverse risk management, compliance and customer outcomes occur. In particular, business lines, risk management and compliance, internal audit and other control functions should have clearly delineated responsibilities in regard to the identification, monitoring and management of risk. Effective accountability mechanisms will encourage the prompt identification and escalation of new and emerging risk issues, and will have clear consequences for not doing so.

A bank's accountability framework seeks to ensure that individuals fully understand, agree and readily accept their responsibilities as appropriate to their role, see objectives as attainable to achieve desired outcomes, and are prepared to accept the consequences of achieving (or not) those outcomes. The accountability framework can then be leveraged as the foundation for establishing collective accountability and providing clarity of end-to-end ownership. The standards of accountability to which a bank adheres are a key indicator of its organisational culture.

Within CBA, the vertical lines of accountability that travel down business lines are generally well understood. The Panel's assessment, however, is that collective accountability across business lines has been poor. As a result, accountability in CBA has been, at best, opaque. This has led to an inadequate sense of ownership of risk, most acutely for activities that span the Group. Specifically, the Panel noted an absence of accountability arising from an inability to identify who was accountable when things have gone wrong. In this regard, CBA's actions in relation to accountability sit in stark contrast to the high standards set by the Board in its Group Delegation of Authorities Policy.

Accountability is one of CBA's five core values. To further embed accountability, CBA intends to drive cultural change through the Accountability Change Program (discussed in the Culture and Leadership chapter). This program seeks to provide greater clarity on personal accountability for risk management through detailed mapping of accountability to roles, and to build a culture of active identification and mitigation of risks through training on 'softer' skill development and mindsets.

Remuneration outcomes are one of the best levers to hold individuals accountable for the proper discharge of their responsibilities. Through remuneration frameworks, banks can set policies and procedures that seek to incentivise positive risk behaviours by linking remuneration with risk and compliance outcomes. Remuneration signals the behaviours that an organisation values and celebrates. When it comes to driving a bank's culture – its desired behaviours and actions – how it rewards its people is critical.

CBA's application of its remuneration policies did little to reinforce accountability and effective risk management across the group. Until recently, the CBA Board had not held senior leaders to account for adverse risk and compliance outcomes that have occurred on their watch. A willingness to excuse poor risk outcomes with limited consequence for executive remuneration has undermined the usefulness of variable remuneration schemes as a tool for promoting prudent risk-taking behaviours and fostered a culture of entitlement over one of genuine accountability.

# 7. ACCOUNTABILITY

## 7.1. Background

At its simplest, accountability means being answerable for actions, decisions and outcomes within one's area of control and influence.

In an organisational context, it is important to distinguish between the concepts of 'responsibility' and 'accountability'. Whereas individuals can be held *responsible* for the actions that they personally undertake, in institutions individuals are held *accountable* for the actions, decisions and outcomes that take place within their area of control and influence, *irrespective* of whether they themselves were personally involved in taking those actions or decisions. Understanding this distinction, and following through on it in practice, is fundamental to effective corporate governance.

Accountability can be delivered through formal frameworks and culture. Formal frameworks refer to structures and systems designed to provide a means by which responsibilities are assigned to individuals or groups, and outcomes are assessed in a fair and transparent manner. Examples commonly used include delegated authorities, formal policies, role statements, performance benchmarks and assessments, management information systems and internal controls. These frameworks drive the behaviour of employees in large institutions by sending signals to employees, customers and external parties on what an institution values and how it serves its clients.

Frameworks without the right culture are unlikely to be effective. Staff at all levels have responsibility for their tasks. However, the cornerstone of culture is the actions and behaviours of the CEO and the Group Executives, and the standard to which they are held by the Board. An embedded culture and framework for accountability starts with leadership and cascades down through an institution. It requires a clear understanding of roles and responsibilities, appropriate skills and resources and mechanisms for monitoring outcomes, and it can play a positive role in highlighting good behaviours.

Internationally, prudential regulators have long recognised that maintaining high standards of accountability is a key attribute of a financial institution's corporate governance.[11] In Australia, the Government has recently enacted the Banking Executive Accountability Regime (BEAR),[12] which strengthens APRA's powers in assessing the transparency and accountability of decision-making processes within authorised deposit-taking institutions (ADIs). The regime will require an ADI to notify APRA of accountable persons with defined areas of responsibility and obligations, and authorises APRA to disqualify individuals who breach the required standards. Importantly, each ADI must maintain 'accountability maps' setting out who is accountable for key risks.

The importance that CBA places on accountability is evidenced by its inclusion as one of the Group's five core values. In elaborating its values, CBA makes clear that being accountable means that all staff: 'understand and deliver what is expected of me'; 'take ownership and follow up'; and 'acknowledge mistakes, escalate them quickly and learn from them'. In addition, team leaders are expected to 'set clear expectations of each person and the team'.

CBA has formal frameworks to define accountability across the Group, including role statements and delegated authorities, which are embedded through a values assessment in an individual's performance

[11] See Basel Committee on Banking Supervision, *Enhancing corporate governance for banking organisations*, February 2006; Financial Stability Board, *Guidance on Supervisory Interaction with Financial Institutions on Risk Culture – A Framework for Assessing Risk Culture*, April 2014.

[12] BEAR comes into effect from 1 July 2018 for large ADIs, which are required to have all accountable persons registered by 1 October 2018.

review. Importantly, for the purposes of this Inquiry, the CBA Board's Group Delegation of Authorities Policy:

- delegates broad operational authority to the CEO and clearly specifies that 'the CEO is still accountable for the authority sub-delegated';
- defines the limits of delegated authority and states that failure to comply 'will be inconsistent with the value of Accountability and/or expected risk behaviours. Failure to comply by an employee may result in action including loss of performance payments and termination of employment'; and
- specifies that 'accountability cannot be delegated but responsibility can. The delegation of authorities does not mean the person or entity who has made the delegation is no longer held accountable. The delegator is accountable for the delegate's actions even though they have delegated responsibility to them.'

## 7.2. Inquiry findings

A lack of accountability is a common theme underlying several of the issues observed in this Inquiry. This contributed to: an inability to identify who is accountable when things have gone wrong; inadequate remuneration outcomes for adverse risk and compliance outcomes; weak issue escalation, management and closure; insufficient Executive Committee oversight; and inadequate business unit supervision of functions performed elsewhere in the Group.

In the Panel's view, CBA has a poor track record in relation to accountability. The level of accountability observed falls a long way short of the standard set by its own delegations policy. The Panel has found that a lack of accountability has been a characteristic of CBA for some time and has been a significant driver of recent missteps. This has manifested itself in a number of ways, highlighted throughout this Report, such as a tolerance for 'excuses' used across the Group to explain away poor risk and compliance outcomes.

Clarity of accountability, with unclear roles and responsibilities, has been identified in a number of external reports. PwC's 2015/16 report on controls noted 'there is ambiguity of ultimate accountability'. Weak accountability was also identified in this Inquiry through the staff survey and emerged as a theme in interviews of CBA leaders, with common responses such as 'if you ask what accountability means you get different answers.'

There are a number of drivers behind CBA's struggles with accountability:

- a cultural 'mentality of trust' and 'over-consulting', manifested in a lack of constructive challenge throughout the senior management levels and at the Board, and in bureaucracy diluting accountability (highlighted in the Culture and Leadership chapter);
- a federated organisational structure that required but did not have clear roles and responsibilities for issues that spanned business units and a lack of collective and end-to-end accountability (Senior Leadership Oversight chapter);
- limited appetite for consequence management (Remuneration chapter); and
- limited reporting on issue closure (Issue Identification and Escalation chapter).

The first three of these drivers are further explored below. An illustration of the lack of clear ownership of risk systems is also provided.

### *7.2.1. Trust and over-consulting*

Minutes from management committees often discussed ambiguity or lack of accountability as a root cause for poor risk management and compliance outcomes. For example, an Executive Committee meeting in July 2017 in relation to a discussion around risk culture highlighted that 'There is some evidence of a tendency to 'over consult' as it is not clear which forum has decision-making rights. This can slow decision-making and inappropriately spread accountability for outcomes.'

### *7.2.2. Consequences of the federated organisational structure*

Under CBA's federated organisational structure, Group Executives were empowered for their respective business units. However, there was confusion about accountability for risks and issues across business units, and a lack of consensus and clear vision of accountability at the Executive Committee level.

This issue is not unique to CBA or the Australian financial industry. The US OCC's risk management guidelines[13] caution on the risks created by a federated structure:

> *As the OCC observed during the financial crisis, it can be challenging to instill a sense of 'risk ownership' in a front line unit when multiple organizational units are responsible for the risks associated with the front line unit's activities. Banks whose business leaders viewed themselves as accountable for the risks created through their activities fared better in the crisis than banks where accountability for risks were shared among multiple organizational units. The OCC cautions covered banks that rely on such a structure to be diligent in reinforcing the front line unit's accountability for the risks it creates.*

The Executive Committee Charter attempts to address this risk through one of its five primary activities, which is clarifying accountability where overlap might exist across the group. However, considerably less time has been spent in this area than in the other primary activities, as evidenced by the structure and agendas of the 2017 Executive Committee meetings. This has contributed to the sense of collective complacency.

As explained in the Senior Leadership Oversight chapter, the Executive Committee was an 'advisory panel' to the CEO and did not always operate as a cohesive team. As a consequence, it failed to promote collective accountability for the overall Group, as evidenced by numerous examples in this Report. Interviews conducted with Group Executives reflected a lack of consensus and clear vision of accountability at the Executive Committee level regarding the nature and scope of Group Executive accountability.

**Accountability failings in AML-CTF compliance**

One example of how a lack of collective accountability translated into inaction at the Executive Committee was highlighted in an interview with a Group Executive in relation to accountability for AML-CTF. The interviewee advised that the project to achieve compliance was run by the Group Operational Risk function (Line 2) and that accountability for achieving compliance was with that team. However, attributing to the second line the failure of the Group to achieve compliance on this project was contrary to the principle that the first line owns the risks emerging from their business units under CBA's Three Lines of Accountability model.

A lack of collective accountability by senior leadership was a primary factor in CBA's inability to effectively manage its AML-CTF compliance obligations. Several business unit Group Executives had, over the period from 2014 through 2016, material concerns with AML-CTF risk management weaknesses pertaining to their specific business units. Internal audit completed three Red audit reports in relation to CBA's compliance with AML-CTF requirements. The common theme across these audit reports and in the evidence submitted to the Panel was that for AML-CTF compliance, CBA had:

- unclear end-to-end ownership and governance;
- no end-to-end assurance; and
- lack of awareness of the roles and responsibilities of Line 1 and Line 2.

A lack of accountability was highlighted in an email in which a CBA senior executive was quoted in relation to AML, '…I just don't think [person] feels that [they were] ...accountable for AML for [business unit] all those years.' To which the response was: '[they weren't]…that has been your accountability, under advice from Risk.'

In June 2017, shortly prior to commencement of the AUSTRAC proceedings, a paper presented to the Executive Committee on the 'Program of Action' defining the remediation program for Financial Crimes, explicitly clarified the nature of business unit ownership, stating:

> *The success of the program will require active ownership of financial crime risk management by the BUs according to the 3LoA. For Line 1 BU leaders, this means that: …BUs are accountable for the risk that is generated by the products and*

[13] Office of the Comptroller of the Currency, *Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches; Integration of Regulations*, September 2014.

*services they offer, even if some risk management activity is delegated to other functions… We anticipate that for some BUs, where knowledge of Financial Crime requires enhancement, and/or has previously been delegated to Risk Management personnel, this will constitute a significant change that will need to be led by the Group Executive.*

### 7.2.3. Limited appetite to apply consequence management

The lack of individual and collective accountability was also evident in the deliberations of CBA's Group Risk and Remuneration Review Committee (RRRC), which is the highest management level committee responsible for considering whether bonuses should be reduced for risk and other matters. The deliberations highlighted three examples of the poor track record of accountability at CBA, particularly as it related to senior leaders.

**Complexity 'excuse' used to diffuse accountability**

The first example highlights how complexity has been used as an excuse for diffusing accountability, and how risks spanning multiple business units have historically presented CBA with a significant accountability problem. The September 2017 RRRC minutes record:

*The Group RRRC noted that the recommendation following the root cause analysis for [the project] was that no one person or team could be held accountable due to the inherent end to end complexity in [the relevant] processes and the legacy that has built up over time. …The Group RRRC decided that complexity can no longer be an acceptable explanation for lack of accountability. Given that many of the Group's processes are considered complex with multiple areas involved, numerous hand offs and no one silo being responsible for the overall process, the Group would end up having no one accountable for risk matters for many key processes… Going forward, it is recommended that individuals be held accountable for simplifying known complexities.*

The inadequate focus on the role and capacity of CBA senior leaders to drive systematic improvement over time is evident. This problem was noted but was not effectively resolved.

**Unclear roles and responsibilities used to diffuse accountability**

The second example highlights that CBA senior leaders were not held accountable for resolving unclear roles and responsibilities at lower levels of the organisation. This is evident from the decision taken at the November 2016 RRRC meeting relating to the failure to submit transaction threshold reports to AUSTRAC.

*The discussion at the RBS RRRC noted that it was difficult to ascertain who in RBS and ES was responsible given the length of time that had passed, the lack of available documentation and poor governance. The accountable executives (ES and ATM/IDMs) responsible for IDM design, technical configuration and rollout have since left the Group. There is limited information available on the decisions made at the time in terms of how the control was implemented and operates…*

*STATUS: On the basis of the response received to questions, it is proposed that going forward specific focus is given to reinforcing obligations of individual and collective accountability.*

Undue focus was placed on allocating blame to specific individuals responsible for specific tasks, without appropriate focus on overarching accountability of CBA senior leaders. The CBA Board has subsequently addressed this with its decision to hold the CEO and Group Executives collectively accountable for the AUSTRAC issue.

**First line accountability not consistently applied**

The third example highlights that ultimate first line accountability was not consistently applied. In response to an adverse risk outcome, a CBA senior leader sought in August 2016 to attribute accountability only to Line 2 rather than accepting first line accountability, stating:

*There are many contributing factors and contributors to the situation. I find it difficult to 'punish' people for a red audit when audit is one of our lines of defence and no actual incident has occurred. I strongly encourage you to reconsider*

> *this as a topic for this specific forum! The one person who should be held accountable is the person who was meant to implement this appropriately for the Board and that is [a senior individual within Line 2]…*

This approach is inconsistent with CBA's Three Lines of Accountability model. The Accountability Principles discussed below outline that accountability for adverse risk or compliance outcomes should sit with first line staff, with the second line accountable for the oversight and challenge of the first line.

**Accountability in action**

The Panel was advised of a positive example of collective accountability at CBA, at its New Zealand subsidiary Auckland Savings Bank (ASB), where accountability for risk was linked to remuneration outcomes. Following an adverse risk management outcome, the relevant GM had their bonus cut to zero, with remuneration impacts also applied to a number of people who had the capacity to detect the issue earlier. There were remuneration consequences for the ASB leadership team, including the CRO, CFO and CEO reflecting their accountability for oversight. This is a good example of how the Accountability Principles (later in this chapter) could work in practice to drive better risk management and compliance outcomes in the long-term interests of CBA and its stakeholders.

### *7.2.4. Lack of accountability for risk systems*

In recent years, a lack of clear ownership of key credit risk systems has impacted on the oversight of and timely investment in these systems. Identification and resolution of these gaps has been overly dependent on internal audit, APRA and in one case CEO direction. Three examples draw this out:

- Collateral Management System;
- Credit Risk Limit System; and
- country risk management systems.

**Collateral Management System**

CBA's Collateral Management System (CMS) was introduced in 2006 to provide a single source for bank-wide recording of collateral (e.g. mortgages and other security documents). As a result, users of CMS span business unit and Group functions in both first and second line roles.

In mid-2014, APRA recommended that CBA undertake an audit of CMS, as this had not been done recently. Internal audit's subsequent Red audit report of December 2014 concluded that 'the current application and usage of CMS is not effective in providing the Bank with a single source of truth for collateral management'. The two key drivers were a lack of governance and ownership and limited system functionality. In relation to governance, the audit report stated:

> *From a governance perspective, since its implementation in 2006, a business owner has not been identified. As a result, there has been limited management oversight of the integrity of information in CMS.*

Over the course of 2015, CBA conducted diagnostic work and completed a detailed business case to upgrade CMS to provide a single, accurate and complete bank-wide collateral record. Critically, however, during this period there was still a lack of internal agreement on the owner(s) of CMS. The method of resolving this issue was that the dispute was put to the Executive Committee, where the CEO nominated two EGMs as jointly accountable for CMS. Following clarification of governance arrangements and ownership, CBA upgraded CMS over the course of 2016 and early 2017.

CBA did not have a clear business owner for a core credit management tool. Moreover, this gap was not identified and addressed within the business unit, until it was raised by internal audit and APRA and escalated to the CEO. A similar lack of ownership was evident more recently with respect to other credit risk related systems.

**Credit Risk Limit System**

CBA's Credit Risk Limit System (CRLS) is the key system used to monitor and manage credit exposures relating to derivatives. In September 2017, internal audit concluded its Red audit report regarding the CRLS. The key 'high rated' audit findings included that:

> *There is no single owner or Accountable Executive for Derivatives Counterparty Credit Risk….*
> *Governance for managing known issues is inadequate…*
> *Ownership for CRLS is unclear and it is not a fit for purpose system for credit risk management…*

The report also noted that, prior to the response to the audit:

> *There has been no accountable Risk Executive for counterparty credit risk from derivatives. Leadership is required to resolve the multiple process issues noted in this audit and to play a lead role in the solution to the weak IT infrastructure.*

Whilst CBA took steps to address the specific issues identified in this audit report, the lack of a system owner persisted. The Inquiry was advised in interviews that the 'orphaned' status of CRLS was the result of a lack of clarity in relation to accountability and of the federated structure in dealing with issues that span multiple business units.

**Country risk management systems**

In relation to country risk, the absence of Line 1 ownership meant that the Line 2 was required to sponsor the project to improve CBA's ability to effectively manage its overseas exposures (see Risk Management and Compliance chapter).

These different examples, in the Panel's view, highlight that CBA's weaknesses in accountability have been broad and deep-seated. Improving accountability will help to address real and perceived complexity in CBA's operations. Such action will remove the excuses used to explain away poor risk and compliance outcomes, while greater transparency will result in clearer roles and responsibilities, a better alignment between risk and reward and more constructive challenge leading to more robust decision-making.

CBA has identified that further investment is required to improve the understanding of accountability across the Group and has a number of initiatives underway. These include staff training to reinforce the value of accountability, and remediation work on the Three Lines of Defence model (see the Remediation Initiatives chapter) to reinforce accountability for risk.

CBA has also begun to address shortcomings through a focus on end-to-end accountability for product owners, known as the Risk Management Implementation (RMI) program. This requires the accountable senior leaders to map where tasks are performed, and to ensure that controls are in place to mitigate the risks associated with those products or services. The Better Risk Outcomes Program discussed later in this Report will see RMI extended to cover the whole of CBA. The Panel sees RMI as a positive step towards addressing the lack of accountability and ensuring that the first line of defence understands and owns the risks within its business.

## 7.3. Accountability Principles

The Panel sought to answer the question of what is better practice in relation to accountability. As noted earlier, regulatory responses to the global financial crisis have focused on addressing the lack of individual accountability of senior leaders. However, articulating better practice has been more challenging.

Executives who demonstrate accountability will ensure effective supervision of delegated activities, enable appropriate funding and resourcing, proactively respond to material risk issues to ensure they do not persist without effective resolution, and exhibit leadership behaviours receptive to 'bad news'.

A key to embedding a sound risk culture is for leaders to role model appropriate risk behaviours. As noted in the Risk Management and Compliance chapter, CBA has yet to embed its Three Lines of Accountability model and establish a clear understanding of, and accountability for, the respective role of each of the three lines in effectively mitigating risk.

The Panel believes that the Accountability Principles set out below, which have been developed for this Inquiry, represent a good starting point for CBA by placing the onus for individual and collective accountability on the CEO and Group Executives.

# 7. ACCOUNTABILITY

*Figure 5: Accountability Principles*

**Accountability for the CEO**

(a) The CEO has delegated authority from the Board and is accountable for the overall management of the Group.

(b) The CEO in turn delegates authority to the Group Executives for the effective execution of operational activities.

(c) The CEO retains accountability for any delegation of the Board's authority, and is responsible for the Group Executives executing on their individual and collective accountabilities.

**Individual Accountability of Group Executives**

(a) Business unit Group Executives are ultimately accountable (with the CEO) for the products and services that their respective business units offer to customers.

(b) Business unit Group Executives are accountable for risk management outcomes, compliance obligations and adverse customer outcomes on an end-to-end basis. This requires that they have appropriate oversight of, and are satisfied with, the overall soundness of governance arrangements, policies and processes, people, systems, and tools and controls in meeting the institution's risk expectations/appetite and delivering an appropriate outcome. Where this is not the case, they should consider the risks involved in continuing the relevant business activity or offering the relevant product or service.

(c) Accountability of business unit Group Executives is not diminished by the location where particular functions are performed within the group (e.g. delegated activities) nor by the extent of Line 2 or Line 3 involvement or challenge.

(d) Group Executives must consistently exhibit leadership behaviours that create an environment that encourages staff to raise issues of concern.

(e) Group Executives must escalate issues of concern to the CEO/Board and ensure follow-up of material issues and effective resolution of root causes.

(f) Group Executives are responsible for cascading the above principles to lower level staff (modified with regard to their more specific roles).

**Collective Accountability for Group Executives**

All Group Executives are collectively responsible for identifying, escalating to the CEO/Board and mobilising resources within the Group to address systematic issues of concern.

In summary, the Panel considers that the implementation of CBA's formal frameworks to drive accountability have fallen short. CBA has not articulated a comprehensive vision of individual and collective accountability for CBA senior leaders. As a result, the Group's inadequate application of accountability has inevitably made it more prone to risk and misconduct issues and incidents.

## Recommendation 22

*CBA, building upon the foundation established by BEAR, incorporate the Accountability Principles set out in in this Report.*

# 8. REMUNERATION

## 8.1. Background

Remuneration practices at financial institutions globally came under a harsh spotlight during the global financial crisis, as they were exposed as promoting behaviours and outcomes that were inconsistent with sound risk management and the best interests of customers.

In response, in 2009 the Financial Stability Board (FSB) released its *Principles for Sound Compensation Practices* and accompanying Implementation Standards,[14] designed to achieve a clearer alignment between remuneration practices and prudent risk-taking. The FSB Principles represented a 'circuit breaker' that sought to realign executive remuneration systems with prudent risk management and long-term financial sustainability.

In 2009/10, APRA gave effect to the FSB's *Principles* through amendments to its prudential standards on governance and the introduction of *Prudential Practice Guide PPG 511 Remuneration*. These establish minimum requirements and better practice expectations in relation to the design, governance and implementation of remuneration policies.

Since the crisis, a growing number of misconduct cases globally have raised prudential concerns over weaknesses in governance, risk management and remuneration practices in dealing with conduct risk. These episodes prompted the FSB to issue, in March 2018, *Supplementary Guidance to the FSB's Principles and Standards on Sound Compensation Practices*. This guidance sets out eight recommendations on better practices in relation to the promotion of ethical behaviours and good conduct, and elaborates on how compensation practices and tools can be used to that end. The Panel supports these recommendations and believes that CBA should adopt them within its remuneration framework and practices.

During 2017, APRA reviewed remuneration policies and practices across a sample of large APRA-regulated entities to gauge how their stated remuneration frameworks and policies were translated into outcomes for senior executives ('APRA's benchmarking exercise'). An information paper on this was published by APRA in April 2018.[15]

**Industry initiatives**

Conduct issues abroad have clearly had their echo in Australia. There have been a number of incidents in banking and in financial services more generally that reflected behaviours that were not in the best interests of customers. Remuneration and incentive structures appeared to be a significant driver of these behaviours.

In 2016, the Australian Bankers' Association commissioned an independent review (the Retail Banking Remuneration Review) into remuneration practices in retail banking in Australia. The Report from this review (the Sedgwick Report, after its author),[16] released in April 2017, highlighted numerous weaknesses in banks' remuneration systems that carry with them 'an unacceptable risk of promoting behaviour that is inconsistent with the interests of customers', and identified an urgent need for banks to address unsound remuneration practices. In particular, the Sedgwick Report called for:

- the removal of all bonuses linked directly to sales volumes and sales targets;
- eligibility for bonuses to be assessed against a range of factors (i.e. a 'balanced scorecard') including customer outcomes;

[14] Financial Stability Board, *Principles for Sound Compensation Practices*, September 2009.
[15] Australian Prudential Regulation Authority, *Remuneration practices at large financial institutions*, April 2018.
[16] Stephen Sedgwick, *Retail Banking Remuneration Review*, April 2017.

- the adoption of genuinely customer-centric performance measures which look to customer outcomes, not simply loyalty or satisfaction surveys;
- behavioural and ethical 'gateways' to determine access to bonuses; and
- a rebalancing of the size of variable pay relative to fixed pay.

CBA has committed to adopting all recommendations from the Sedgwick Report on sales commissions and product-based payments in retail-focused businesses by June 2018. The Panel welcomes CBA's response. Given that commitment, and the detailed analysis of incentive structures in retail banking in the Sedgwick Report, the Inquiry has not revisited this issue.

## 8.2. CBA's remuneration framework

In line with banking industry practice, CBA has established a formal remuneration framework with a strong link to values, and to risk and compliance outcomes. The framework sets a number of financial and non-financial hurdles for determining variable remuneration, and allows for manager discretion in applying adjustments based on values and risk outcomes. Importantly, variable remuneration can be adjusted downwards in response to incidents involving poor conduct, inadequate risk management or failure to adhere to CBA's values. For members of the Executive Committee, discretion is exercised by the Board.

Total remuneration is split between three core components:

- a fixed component, which is the salary paid to all permanent employees;
- short-term variable remuneration (STVR), which is individual performance-based remuneration that can be awarded to specific staff to reflect their contribution to a number of objectives, including financial, strategic and people management objectives; and
- long-term variable remuneration (LTVR), for which the Executive Committee[17] is eligible, reflecting the influence this group in particular has on long-term outcomes.

Total remuneration for Executive Committee members is broadly made up of one-third each of fixed salary, STVR and LTVR. Weightings differ across institutions, but CBA's weighting of Executive Committee remuneration components is broadly in line with domestic and international peers. Variable remuneration is intended to incentivise CBA's senior leaders to achieve short-term objectives and align their behaviour and decision-making with long-term objectives.

A significant proportion of the Group's employees (24,185 individuals or 47 per cent in 2017) are eligible for STVR. Executive Committee members can receive STVR of between zero and 150 per cent of their fixed remuneration for performance outcomes ranging from 'Below Expectations' to 'Above Expectations'. The structure of EGM and GM level STVR is similar. Employees below GM level also have annual discretionary STVR awards.

For Executive Committee STVR, a deferral period of two years applies (see Figure 6 below).[18] Half of the STVR is deferred as equity and awarded ('vesting') annually in two equal instalments. Deferral provides CBA with an opportunity to cancel variable remuneration should decisions made in the current year impact adversely on the Group in future years. Payment in the form of equity aims to encourage behaviour in the interests of shareholders.

For Executive Committee members, LTVR is up to a maximum of 150 per cent of fixed remuneration (from 2017/18). The LTVR vesting in a given year is based on performance over the previous four years. The current year's LTVR will only be awarded if the performance hurdles over the next four-year period are achieved. Similar to STVR, this is designed to incentivise senior leaders to act in the interests of shareholders, while allowing CBA to withhold

[17] Together with certain employees in Colonial First State Global Asset Management (CFSGAM).

[18] Excluding the CEO and Group Executives, all EGMs and GMs, and all employees with an STVR award of $150,000 or greater, defer one-third of the STVR into equity that vests in three equal tranches over three years.

remuneration if an issue is identified today that is the result of poor prior-year decisions.

CBA has a number of oversight processes in place to govern the remuneration process. The Board Remuneration Committee is the key body responsible for remuneration across CBA. It works with the BRC and management's RRRC to review and consider risk and reputational matters in determining variable remuneration outcomes and vesting of deferred awards for the CEO, Group Executives and any other employees whose activities may materially impact the financial soundness of the Group.

The RRRC is chaired by the CRO and is comprised of risk, finance and HR executives. It meets quarterly to review and make recommendations on risk adjustment of remuneration outcomes as a result of any material risk breaches. Significant losses (>$5m) or near misses (>$25m) are reviewed and investigated by the RRRC to determine whether individual employees contributed to the risk incidents, and whether formal consequences should be imposed. Any risk or performance issues that may impact on the awarding of current year STVR or the vesting of deferred awards are reported to the Board Remuneration Committee by the RRRC, along with any recommendations for the reduction of any deferred awards.

From 2017/18, CBA has also introduced business unit-specific RRRCs to broaden the scope of risk issues monitored by the RRRC, establish greater consideration of risk insights across the Group, and deliver more robust and consistent individual employee consequence outcomes, including at senior levels.

CBA's remuneration framework provides for the withholding of variable remuneration that has been earned but not paid (known as 'malus'), but there are no formal mechanisms to retrieve payments that have been earned and actually paid (known as 'clawback'). Although clawback has been introduced in overseas banking jurisdictions, CBA noted in interviews that it believes putting a clawback policy into practice would be problematic.

Every six months, the Board Remuneration Committee, with input from the BRC, considers whether to apply malus to the unvested short or long-term remuneration for Executive Committee members based on risk considerations. This process is supported by commentary from the Group CRO in order for the Board Remuneration Committee to make an informed decision.

During 2015/16, the Board Remuneration Committee undertook a review of remuneration arrangements for Executive Committee members. The objective was to ensure executive remuneration drove a strong focus on improving long-term performance. Based on this review, the Board sought shareholder approval for the following changes at the 2016 AGM, which predominantly focused on planned changes to the 'balanced scorecard' used to assess performance:

- inclusion of an assessment of leadership and Vision and Values in short-term scorecards; and
- inclusion in long-term scorecards of a new 'people and community' metric, with a 25 per cent weighting, which would measure long-term progress and achievement in diversity and inclusion, sustainability, and culture. Relative total shareholder return (TSR) and customer satisfaction performance measures would be weighted at 50 per cent and 25 per cent, respectively.

These recommendations were rejected in a 'first strike' on the remuneration report. Shareholders cited a number of concerns:

- the remuneration framework was complex and lacked transparency (an 'opaque application of Board discretion' in their words);
- executive remuneration outcomes were out of line with CBA's performance and shareholder experience;
- STVR in particular did not adequately reflect executive accountability or the consequences of risk and reputational issues;
- non-financial measures were too highly weighted, with insufficient clarity on how objective and stretching performance hurdles would be set;
- there was duplication of measures across the STVR and LTVR plans;
- the methodology used to determine the shares allocated under the LTVR was problematic; and

- the proposed 'people and community' metric was seen to lack transparency and be overly reliant on Board discretion to determine vesting outcomes.

CBA responded by updating the remuneration framework in 2017 (see Figure 6) through:

- increased weighting for objective financial metrics in STVR. For example, the weighting of the CEO's performance measures was increased from 40 per cent to 60 per cent;
- deferral of STVR over two years and paid as equity;
- a heightened focus on risk and reputational matters; and
- consideration of non-financial risk in LTVR to balance shareholder and broader community outcomes.

The changes were approved by shareholders at the 2017 AGM, significantly increasing the degree to which key performance indicators (KPIs) are market based and therefore more transparent to external parties. The changes addressed investor concerns by reducing Board discretion through increased use of quantitative measures for KPI scorecards (e.g. quantitative assessments increased from 45 per cent to 75 per cent of the CEO's scorecard), and enhanced performance, risk and remuneration review and consequence guidelines.

A crucial element in assessing the effectiveness of the remuneration framework is how CBA determines and adjusts variable remuneration. The Group uses three processes:

- KPI performance management;
- Group values; and
- the risk gate opener.

*Figure 6: Summary of changes to the remuneration framework*

| | Up until 2016/17 | As of 2017/18 |
|---|---|---|
| **STVR** | | |
| **Weighting to financial measures** | CEO – 40%<br>Business unit Group Executives[1] – 45%<br>Support function Group Executives – 25%<br>CRO – 25% | CEO – 60%<br>Business unit Group Executives[1] – 60%<br>Support function Group Executives – 40%<br>CRO – 30% |
| **Deferral** | 50% of STVR deferred as cash for one year | 50% of STVR deferred over two years with 50% vesting as equity each year |
| **LTVR** | | |
| **Allocation approach** | Fair value, opportunity of 100% of fixed remuneration | Fair value, opportunity of 150% of fixed remuneration |
| **Performance measure** | Relative TSR[2] – 75%<br>Relative customer satisfaction – 25% | Relative TSR[2] – 75%<br>Trust and Reputation Measure – 12.5%<br>Employee Engagement Measure – 12.5% |

Notes:

1. Group Executive for International Financial Services had a lower weighting of 40%
2. Acts as a financial gateway in that CBA's TSR over the performance period must be positive

Source: CBA Board Remuneration Committee, 4 June 2017

**KPI performance measurement**

Employees covered by STVR plans are subject to a performance measurement framework evaluated against a range of KPIs. In addition, EGM level and above are subject to a more rigorous 'balanced scorecard' covering objectives including shareholder value, customer satisfaction, leadership, community, strategic initiatives and business performance.

Assessment against KPIs determines whether individual staff members have met their objectives, and the extent to which they may qualify for STVR. CBA intends to change the measurement of customer outcomes in KPI scorecards from Customer Satisfaction to Customer Net Promoter Score (NPS) as the primary measure, effective as of 2017/18 for most retail-focused business units. This change aims not only to highlight the proportion of customers who are very satisfied, but also to encourage reductions in the number of dissatisfied and neutral customers.

The Panel notes that performance measured against KPIs or a balanced scorecard is consistent with domestic and international practice. The wide range of variables used for assessment appears reasonable and aligned with what would be expected for CBA. However, consistent with findings in APRA's benchmarking exercise, the Panel notes that the conditions that allow LTVR to vest are based on performance measures with no explicit link to long-term financial soundness.

Recent changes to the remuneration framework are summarised in Figure 6 above.

The Panel would caution that the increase in the weighting of financial objectives for Group Executive KPIs in 2017/18, with more quantitative measures used to assess executive performance, could increase the risk that financial considerations might unduly influence behaviour if the additional processes outlined below to assess and adjust for Group values and risk are not operating effectively.

**Group values**

In 2017, CBA introduced an additional component to the remuneration process, where an individual's demonstration of the CBA's declared values is assessed and included in performance results. The values component includes assessment against CBA's values of integrity, accountability, collaboration, excellence and service and produces one of three results: 'inconsistently applied', 'consistently applied' and 'exceptionally applied'. As with other elements of the remuneration framework, performance against these values are self-assessed in the first instance, with managerial input following. In 2017, the values assessment affected the remuneration of four per cent of staff negatively ('inconsistently applied'), and 16 per cent positively ('exceptionally applied').

**Risk gate opener**

Some financial institutions incorporate risk objectives within balanced scorecards, while others like CBA have chosen to adopt an overlaying adjustment (termed the 'risk gate opener') to the remuneration result. There are advantages and disadvantages with both methodologies. The key to embedding risk issues in remuneration outcomes is in the implementation.

In 2015, CBA introduced the risk gate opener, which allows performance-based remuneration to be reduced as a result of poor risk outcomes. It applies to all staff eligible for STVR. It works in one direction only; it does not reward sound risk management through increased remuneration.

All eligible employees have a standalone risk assessment with three potential outcomes:

- staff who are assessed to have fully met requirements will not have their remuneration adjusted ('fully met');
- staff who are assessed to have partially met requirements may receive reductions in remuneration on a discretionary basis ('partially met'); and
- staff who are assessed to have not met requirements will receive no STVR for that year, mandated by policy ('not met').

# 8. REMUNERATION

CBA's approach of adjusting remuneration for poor risk outcomes separately, rather than as a component of overall performance, provides significant flexibility over the size of adjustments. Adjustments under this process can be up to the full value of STVR.

Generally, the risk assessment starts with a self-assessment by the individual. This is then reviewed by the responsible manager, who needs to undertake appropriate due diligence. For risk events not considered by the RRRC, managers must determine the risk assessment as part of the performance review and provide supporting commentary where the assessment is less than 'fully met'

For employees with deferred awards, other than the Executive Committee and those employees defined by CBA as material risk takers, risk and compliance are monitored by the Group CRO and the risk function, and relevant information is passed on to the RRRC for assessment. In addition, for EGMs, risk adjustments are approved by the business unit Group Executive, supported by the business unit CRO, having sought input from the Group Risk teams such as Operational Risk and Compliance. The CEO reviews all remuneration outcomes for EGMs and Group Executives, including the degree of risk gate adjustments.

The risk assessment aims to provide structured guidance for a robust application of the risk gate opener, as detailed in Figure 7 below.

*Figure 7: CBA's risk assessment framework*

| | |
|---|---|
| **Behaviour** | • Did the employee demonstrate they have a good understanding of risk associated with their role and responsibilities?<br>• Did the employee identify and escalate issues quickly and follow up to resolve?<br>• Did the employee take all the necessary steps to understand and meet customer needs?<br>• Did the employee behave in line with the Group and business unit risk appetite at all times and in accordance with BU policy and procedures |
| **Severity** | • What impact did the employee's risk behaviour have on customers, colleagues, and the Group's reputation?<br>• Was there evidence of repeated failures, even though there was not bad intent?<br>• Was deliberate disregard demonstrated in the employee's behaviour?<br>• Was the employee aware of the policies and procedures that applied to their role? |

Source: CBA

## 8.3. Inquiry findings

The Panel has observed significant weaknesses in the implementation and broader oversight of the remuneration process in CBA, particularly in adjusting remuneration as a result of poor risk and customer outcomes. At the highest level, the CBA Board has not until recently held the CEO and Group Executives to account by exercising its discretion to materially reduce remuneration outcomes in response to adverse risk management, compliance and customer outcomes. The remuneration outcomes of the CEO and Group Executives can be summarised as follows:

- prior to 2016/17, it was extremely rare for the CEO and Group Executives to have remuneration reduced on risk grounds. The Board Remuneration Committee's review of CEO and Group Executive remuneration was based on extremely brief commentary from management, with a narrow focus on realised financial and reputational impacts;
- in 2015/16, for example, the reputational damage from the CommInsure issue (discussed earlier) resulted in only a relatively modest remuneration adjustment for the CEO[19] and impacts on some lower level staff;
- in early August 2017, prior to the announcement of the AUSTRAC proceedings, the Board Remuneration Committee had proposed to make relatively moderate adjustments to STVR for the CEO and Group Executives for 2016/17. This was despite having assessed this group as 'partially met' from a risk perspective and the Board Remuneration Committee (supported by the BRC and CRO) having sufficient information about weaknesses in the AML-CTF control framework to apply a more material risk adjustment. The Board Remuneration Committee proposed that STVR outcomes for the CEO and Group Executives be reduced by 10 per cent reflecting collective accountability for long-outstanding risk issues. In addition, the Board proposed further reductions of between 10 per cent and 25 per cent for the CEO and Group Executives for specific issues such as AML-CTF control weaknesses, wealth management business control weaknesses, enterprise services control weaknesses and issues identified by internal audit. These risk adjustments would have reduced STVR for the CEO to around 85 per cent of fixed remuneration; and
- following the AUSTRAC announcement, the CBA Board announced that the 2016/17 STVR for the CEO and Group Executives would be reduced to zero, a reflection of 'the collective accountability of the Executives for the overall reputation of the Group and risk matters'.

The 2016/17 remuneration outcome for the CEO and Group Executives represents a significant shift, setting a precedent for *collective accountability* at the most senior levels of the CBA. The rigour of the Board's actions, if maintained, make it much more likely that collective accountability will be enforced through CBA. However, the Panel believes that a risk-based review of the performance of each Executive Committee member is important for risk issues that address areas of *individual accountability*.

In the Panel's view, the remuneration outcomes are symptomatic of significant weaknesses in the implementation and broader oversight of the remuneration process in CBA, which have undermined the promotion of greater accountability. These weaknesses have been:

- inadequate Board oversight and challenge;
- ineffective application of the remuneration framework; and
- gaps in the remuneration framework.

### *8.3.1. Inadequate Board oversight and challenge*

The Accountability chapter highlighted the challenges CBA has faced in relation to accountability. The Panel believes that the CBA Board were too tolerant of accountability being diffused, excused or simply unable to be determined. This tolerance cascaded down through senior leadership of CBA and resulted in the

[19] Based on a self-assessment against the reputation metric in the KPI scorecard rather than as a result of the application of the risk gate opener.

ineffective application of the remuneration framework. CBA noted in executive interviews that it was reluctant to apply remuneration adjustments if there was no evidence of malfeasance given that, in general, 'CBA staff are of good intent'. Good intent has been too readily used to excuse poor risk outcomes.

**CEO and Group Executive remuneration**

In the case of the CEO and Group Executives, the remuneration framework has not been applied rigorously. The Panel has found that the Board provided inadequate oversight and challenge of remuneration outcomes and, as a result, has been reactive rather than pre-emptive when applying risk adjustments to variable remuneration. Until recently, the Board Remuneration Committee appeared reluctant to adjust variable remuneration for the CEO and Group Executives. As noted above, this was particularly evident in relation to the media and investor reaction to the AUSTRAC legal action.

In addition to its reactive approach, there was no evidence in CBA's documentation that the Board Remuneration Committee had considered making risk adjustments to the relevant years' deferred remuneration for events such as AML-CTF (that is, applying a malus policy). Instead, with very limited exception, CBA has a preference to deal with risk issues in the current year's performance assessment. The absence of a clear malus policy for deferred remuneration undermines the effective application of the remuneration framework.

The Board Remuneration Committee has relied heavily on performance assessments for individual executives provided by the CEO, and advice provided by the Group CRO and management's RRRC. There also appears to have been little appetite to improve decision-making on remuneration outcomes through requests to the BRC or the BAC for confirmation or an independent view of the appropriateness of risk management outcomes for individuals under scrutiny.

The Panel's review of the Board Remuneration Committee papers and minutes suggests that CBA did not undertake a detailed assessment of each Executive's performance. There was no comprehensive assessment of the effectiveness of risk management within each Executive's area of responsibility. Prior to 2016/17, the risk assessment was largely guided by the Executive's self-assessment. The commentary from the Group CRO did not provide an assessment, resulting in the Board Remuneration Committee approving variable remuneration outcomes for the CEO and Group Executives largely based on generalised attestations from the CEO and the Group CRO.

From 2016/17, CBA has piloted a new process to subject the Executive Committee to a more consistent and structured risk assessment through the adoption of a detailed risk scorecard, which aggregates various inputs. The risk scorecard was extended to the EGM level in 2017/18, with the potential for a further roll out to GMs in due course. The risk scorecard will add more rigour to the remuneration process, but its application to the CEO and Group Executives' STVR in 2016/17 was overtaken by the AML-CTF events.

CBA's remuneration framework notes that, in providing advice, the Group CRO is to consider risk culture, risk appetite, controls, incidents and issues under the Executive's accountability. However, despite an improvement observed in the quality of the CRO's risk assessment for the 2016/17 performance period, the CRO's paper to the Board Remuneration Committee had little in the way of a formal assessment to form the basis for individual executive remuneration decisions. The paper highlights incidents at a high level but does not provide a risk assessment or recommended actions for the Board Remuneration Committee.

The lack of documentation results in limited transparency of decision-making, which constrains the effective governance over decisions and the oversight required by APRA's prudential framework. Without a documented assessment, a 'herding' of Executive variable remuneration outcomes can result, with outcomes being more closely tied to the overall financial performance of the CBA rather than to individual performance and risk outcomes. The result is that Group Executives have generally received the same or very similar outcomes regardless of the risk assessment for each individual.

CBA's practices in this area are not dissimilar to the weaknesses identified by APRA in its benchmarking exercise. APRA noted instances of poor quality, incomplete or inadequate documentation provided to the Board Remuneration Committee, hindering

the Committee's ability to review and independently assess the remuneration outcomes of individuals.

**Lack of Board guidance**

The Board Remuneration Committee has not provided clear guidance on its expectations of how managers should appropriately exercise their discretion when considering a reduction to remuneration for poor risk outcomes. The only risk outcome where an adjustment to remuneration is mandated by policy is a 'not met' risk assessment, which will automatically result in a zero STVR outcome. As a result, risk adjustments have been applied infrequently, inconsistently and with only limited consequences for poor risk outcomes. As discussed below, the risk gate opener has been ineffective in promoting strong accountability and risk discipline.

In the Panel's view, the Board needs to set clearer expectations through comprehensive guidance on how reductions to STVR and LTVR should be determined, as part of a move towards better practice. This will allow management to apply the framework in line with Board expectations, ensuring that the process is applied clearly and consistently across business units and support functions so that the consequences for poor risk outcomes are well understood and applied even-handedly.

CBA proposes to improve its current guidance in this area. CBA is also considering the introduction of a mandated minimum downward adjustment for STVR (e.g. ten per cent) for a 'partially met' rating. A mandated minimum adjustment is a step towards better use of the risk gate opener. In the Panel's view, however, there needs to be a more comprehensive set of criteria in the guidance to achieve better remuneration outcomes.

Some financial institutions globally have instituted prescriptive rules for measurable risk symptoms, especially for conduct, that as a matter of policy must be taken into account in human resource processes such as promotion and remuneration. CBA's introduction of the risk scorecard for senior executives, including a detailed analysis of risk issues and incidents, is a step in this direction but its effectiveness remains to be seen.

Better practice is for banks to have a database or 'library' of consequence management options to assist in learning from previous incidents and to set clear expectations for both positive and negative risk outcomes for remuneration. Such a database would provide CBA with the opportunity to reflect on issues and incidents, apply learnings more broadly, and reinforce positive risk management messaging. It would also assist CBA from a cultural perspective (see Culture and Leadership chapter) to move from a 'safe to raise issues' environment to one of constructive challenge and learning.

**Governance of the remuneration framework**

Following the shareholder strike, the profile of the Board Remuneration Committee has increased. It now holds longer and more frequent meetings, providing a greater opportunity for rigorous review and challenge of the remuneration process and outcomes. Better practice would include risk and internal audit executives presenting a comprehensive assessment to the Board Remuneration Committee, six-monthly or annually, on issues that could impact on executive remuneration outcomes. In addition, for 'significant financial institutions, the size of the variable compensation pool and its allocation within the entity should take into account the full range of current and potential risks.'[20]

Better practice is for effective coordination between the BRC and the Board Remuneration Committee[21] to assist in an integrated approach to remuneration, and that 'subdued or negative financial performance of the entity should generally lead to a considerable contraction of the entity's total variable remuneration, taking into account both current compensation and reductions in payouts of amounts previously earned, including through malus and clawback arrangements.'[22] In this vein, APRA's benchmarking exercise observed that some institutions hold joint meetings between the Board Remuneration Committee and the BRC to focus on

[20] Australian Prudential Regulation Authority, *Prudential Practice Guide PPG 511 Remuneration*, November 2009.
[21] Ibid.
[22] Ibid.

the appropriateness of risk ratings and remuneration outcomes for Executive Committee members, risk and finance staff and material risk-takers.More broadly, under APRA's *Prudential Practice Guide PPG 511 Remuneration*, the Board Remuneration Committee is 'expected to identify material deviations of remuneration outcomes from the intent of its policy'.[23] CBA has not followed this guidance, which reflects global better practice. The Panel found no evidence that the Board received or had requested quantitative data to assess the effectiveness of the application of the remuneration framework.

As part of its review of remuneration practices, the Panel requested data to test the effectiveness of the risk gate opener. CBA was unable to provide some of this data and, in some instances, was only able to do so for the most recent financial year. The data that was made available confirms that there have been material deviations of remuneration outcomes from the intent of the remuneration framework. However, the Panel's review of Board Remuneration Committee documentation and minutes indicate that it did not receive quantitative data that could have alerted it to this problem. The Panel's assessment of the effectiveness of the application of the risk gate opener is covered below.

Global better practice is that a Board Remuneration Committee is well informed to ensure it has the visibility, knowledge and expertise to challenge the executive remuneration process and its outcomes, and to ensure it makes appropriate remuneration adjustments in discharging its responsibilities. Senior management needs to support the Board Remuneration Committee by providing a clear and comprehensive set of information ahead of meetings to allow for sufficient review of issues that could impact executive remuneration outcomes. At a minimum, the Panel believes that the Board Remuneration Committee should require reporting to:

- allow the Board to assess the effectiveness of the framework across the Group, and the appropriateness of the outcomes being generated including the application of the risk gate opener as well as other aspects of the framework;
- inform the Board of differences in the scale of risk reductions across business and support units, and provide assurance that these differences are justified;
- assist in the review and update of guidance to management on the appropriate reduction in variable remuneration for staff that partially meet risk requirements to strengthen the link between risk-conscious behaviour of employees, consequence management and remuneration outcomes across the Group; and
- inform the Board of the systemic or analytical link between employee sanctions executed such as a formal warning, and the remuneration outcomes that are generated so that there is tangible accountability for poor outcomes.

The Panel believes that CBA has fallen short of global better practice in this area. The Board Remuneration Committee has not been provided with sufficient information to perform its duties and therefore could not effectively challenge remuneration outcomes and make appropriate adjustments to variable remuneration. The Panel believes that further actions are required to strengthen the link between risk-conscious behaviour of employees, consequence management and remuneration.

## Recommendation 23

*The CBA Board exercise stronger governance to ensure the effective application of the remuneration framework. In particular, the Board assess remuneration outcomes for Group Executives to reflect individual and collective accountability for material adverse risk management and compliance outcomes. In turn, Group Executives cascade accountability throughout the Group on a consistent basis.*

[23] Australian Prudential Regulation Authority, *Prudential Practice Guide PPG 511 Remuneration*, November 2009.

## Recommendation 24

*To support the effective oversight of the remuneration framework:*

- *the Board require a comprehensive risk assessment from the CRO to assist it in determining appropriate risk adjustments for poor risk behaviours and outcomes for the CEO and Group Executives;*
- *the Board require comprehensive analytics and reporting from management, including the assessment of Group values and the use of the risk gate opener; and*
- *the BRC actively support the Board Remuneration Committee in ensuring that risk outcomes are reflected in executive remuneration outcomes.*

### 8.3.2. Ineffective application of the remuneration framework

As noted earlier, CBA's remuneration framework provides the opportunity, through the risk gate opener, to adjust remuneration to account for risk behaviours and associated outcomes. Since other opportunities to enforce accountability appear to have been limited, the importance of ensuring this process is effective is critical.

The Panel has observed a widespread reluctance to adjust remuneration for poor risk and compliance outcomes. Where risk adjustments have been made, they have not been consistently applied, particularly at the senior management level, and have not been of sufficient magnitude to incentivise positive risk and compliance behaviours. The reluctance to adjust remuneration has undermined the effectiveness of the remuneration framework. Relatively large numbers of employees have received 'partially met' risk assessments but no associated reduction in their remuneration. In 2015/16, 738 employees received a 'partially met' risk assessment outcome, but 457 of these employees (62 per cent) had no risk reduction applied to their remuneration. There was still a high number of staff (382 employees, representing 27 per cent) in the same position in 2016/17 (refer to Figure 8 below).

The weak application of the risk gate opener reinforces the weaknesses identified earlier in CBA's application of the Three Lines of Defence model. The staff survey results showed that the application of penalties was weaker when competing priorities, such as hitting financial targets, were introduced. For example, although more than 90 per cent of surveyed CBA staff agreed with the statement 'My performance objectives encourage me to manage risk effectively', only around half agreed with the statement 'People in this organisation are penalised if they take unacceptable risks, even if their actions end up making a sale or saving the organisation money'. One employee commented: 'the risk culture is generally good… but it comes under pressure at times when short-term ROE targets are at conflict with long-term risk management'.

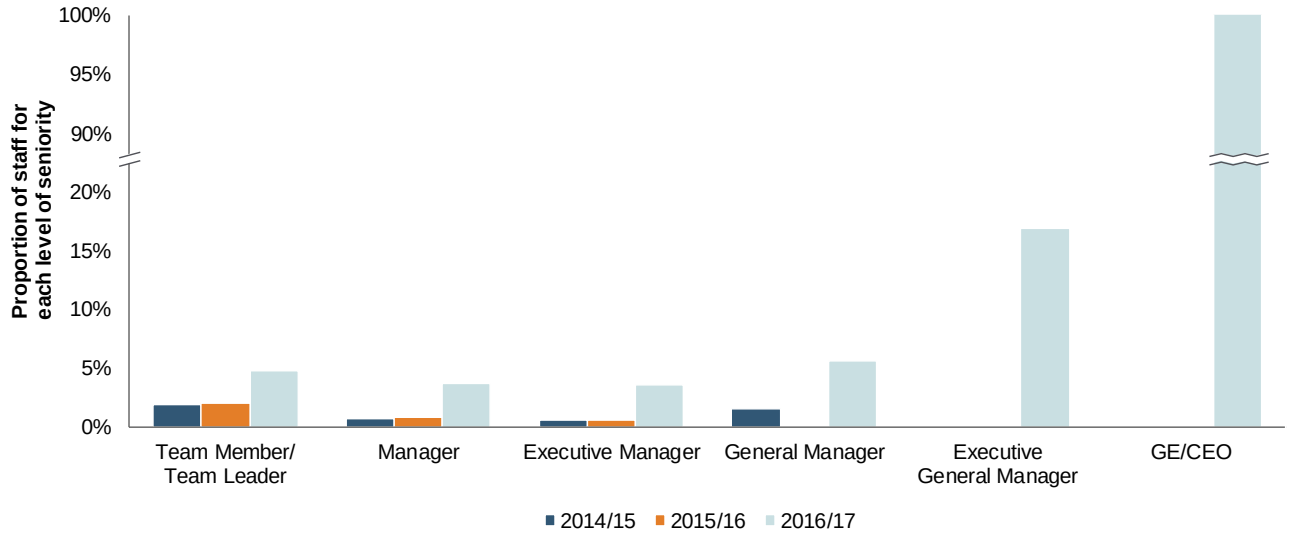
The Panel acknowledges that there may be mitigating circumstances in some cases where the risk gate is not applied, and other disciplinary procedures may be available. However, the scale of employees facing no remuneration consequences for failing to fully meet risk requirements undermines the credibility of the risk gate opener process and impedes CBA's accountability objectives.

More generally, given CBA's business mix and the lack of volatility in earnings for most business units, variable remuneration for many staff has been a relatively constant figure. In the Panel's view, this creates the very real danger that variable remuneration takes on the character of an entitlement to share in the continued financial success of the CBA, rather than a genuine 'at risk' component that is intended to drive positive individual performance and imposes clear consequences for poor risk outcomes.

This danger may have been magnified by a second weakness with the risk gate opener, namely, its inconsistent application for senior staff at GM level and above compared to staff below GM level. The most extreme example is that, as the CBA was receiving multiple sources of evidence of weakened controls from internal audits and from APRA and other independent external reviews, there were no risk adjustments in 2015/16 applied to staff at GM level and above who were assessed as having only 'partially met' the risk gate opener (refer to Figure 8).

# 8. REMUNERATION

*Figure 8: Risk gate application – staff receiving risk reductions by seniority*




Source: CBA

The Panel observed a marked improvement in the use of the risk gate opener in 2016/17. A total of 1,027 staff received a risk reduction in that year, compared to 281 staff in 2015/16, and the proportion was more evenly spread across seniority levels. This corrected the skew away from senior management level employees observed in earlier years (refer to Figure 8). The improvement may have been driven by media scrutiny of the CEO and Group Executive remuneration outcomes following AUSTRAC's legal action, and by those divisions where risk issues had become more prominent as a result of the evidence on weakened controls.

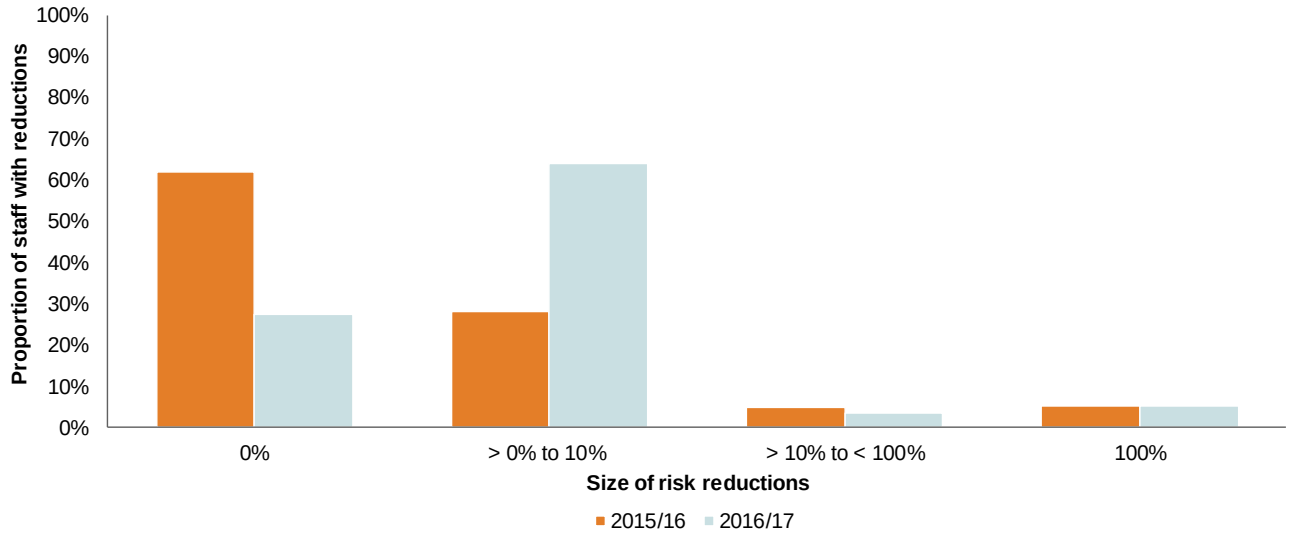
Despite the improved use of the risk gate opener in 2016/17, the Panel observed a disparity in its application and in remuneration outcomes across divisions. Areas with higher application of risk adjustments largely appear to be those reacting to external factors. For example, the significant increase in the application of the risk gate opener in enterprise services staff may have been a response to the October 2016 APRA IT Risk prudential review letter to the CBA Board. In it, APRA noted weakness in the areas of resiliency, recovery, data storage, and risk management and culture.

The APRA letter raised IT risk issues in an integrated manner for the first time. A Board Remuneration Committee paper of August 2017 noted the: 'Many known issues which had been variously reported at different times but on a specific, disaggregated basis, thus failing to provide an overall view of the IT risk environment'. The Board responded by proposing a 25 per cent STVR risk reduction for the Group Executive, Enterprise Services and the Chief Information Officer, and the data indicated that this was cascaded through the division.

When the risk gate opener was applied, the Panel observed that the size of the adjustments to remuneration would have been unlikely to influence the risk/reward trade-off for employees. Most risk reductions were no more than 10 per cent of variable remuneration for the staff concerned, although there were a small number of reductions of up to 100 per cent. For example, of the 281 staff who received a risk reduction in 2015/16, 207 received a risk adjustment of 10 per cent or below. Adjustments of a small size are unlikely to alter or strongly influence prioritisation of risk mitigation, especially for senior leadership who typically receive (and expect to receive) STVR at 100 per cent or more of their fixed remuneration. The range of outcomes for 2015/16 and 2016/17 is illustrated in Figure 9.

# 8. REMUNERATION

*Figure 9: Impact of risk gate opener reductions – size of risk reductions*




Note: For staff assessed as 'partially met' or 'not met'

Source: CBA

The Panel notes that CBA is proposing to enhance its risk assessment guidance to reflect the minimum operational and compliance risk indicators that should be included in all employee risk assessments, confirming how specific risk indicators should be measured (e.g. overdue mandatory learning, misconduct, etc.). This guidance is intended for use by employees for self and leader assessment and incorporated into remuneration discussions to ensure consistency.

CBA is also proposing to improve the capability of managers to undertake risk assessments, aligned with its Accountability Change program, by rolling out training modules focusing on accountability and ownership, managing risk, accountability-focused performance review conversations and assessment, and reviewing KPIs aligned to accountability within an updated scorecard.

Global better practice is for performance to be measured in an objective, independent manner with a clear set of criteria to which staff are to have regard when applying risk assessment processes like the risk gate opener. Remuneration assessments and outcomes should be consistently applied throughout the institution and there should be a process to ensure that the same behaviours across the institution are treated in the same way. Better practice focuses on the cultural importance of quality risk assessments at the middle of the organisation so that the day-to-day decisions affecting the organisation are aligned to those being made at higher levels. The Panel believes that the application of the risk gate opener sets a relatively low bar for risk management, only penalising clear instances of non-compliance. There is more CBA needs to do to address this weakness.

APRA's benchmarking exercise highlighted that downward adjustments to the remuneration of individual executives is rare, whereas employees at lower levels receive downward adjustments more regularly. This is consistent with CBA's practices. While use of a risk modifier such as a risk gate opener is considered to be global better practice, CBA's application has been deficient. As a result, CBA's remuneration practices have been at the lower end of that practice.

## Recommendation 25

*In support of the effective application of the remuneration framework:*

- *the CBA Board provide clear guidance to management on the Board's expectations in determining an appropriate level of risk adjustment for good and poor risk behaviours and outcomes;*
- *the risk function assist in the application of the risk gate opener in the Group through applying more rigour in challenging outliers, observed inconsistencies and absolute levels of risk reductions; and*
- *CBA, with due regard for confidentiality concerns, communicate the impact of both good and poor risk outcomes on remuneration across the Group to reinforce the link between accountability and consequence.*

### *8.3.3. Gaps in the remuneration framework*

Though the key weaknesses in CBA's remuneration framework discussed in this chapter relate mainly to governance and implementation issues, the Panel has concluded that there are a number of improvements that can be made to the remuneration framework itself to clarify and improve its effectiveness. These improvements relate particularly to policy relating to variable remuneration, and to the application of malus and clawback.

The Panel notes that the weighting given to financial measures in the CRO's scorecard is materially lower than that of the CEO and business unit Group Executives, following the remuneration changes in 2016/17. This is in line with better practice identified in APRA's benchmarking exercise. However, the CRO's target fixed and variable remuneration mix is not materially different to that of the business unit Group Executives. Industry practice for CRO remuneration arrangements varies, with CROs at some other banks having a quite different target remuneration mix than their executive colleagues, typically with a higher weighting on fixed remuneration aimed at safeguarding the independence of this critical function.

CBA's remuneration framework lacks an upside for sound risk management. The risk gate opener is a downward adjustment and there is no explicit encouragement or reward for strong risk management. Emerging global practice includes an upside potential to reward good risk management. There are also some examples globally of an upside being applied in a team environment to encourage stronger risk outcomes. However, this approach is still in its infancy. CBA's remuneration framework also provides no basis for collective risk adjustments, positive or negative, as a means of demonstrating collective accountability across a team, business unit or division as a result of significant risk events. The collective adjustment to the remuneration of the CEO and Group Executives in response to commencement of the AUSTRAC proceedings has been a one-off to this point. One recent significant change to the remuneration framework from 2016/17 onwards has been the change to the deferral of STVR, now taken as equity over two years for the CEO and Group Executives. This change has elevated CBA to the lower end of good practice, although practice varies across jurisdictions; up to 60 per cent of STVR is deferred over two to five years in some jurisdictions and up to seven years in others. CBA plans to make changes to adapt to the implementation of the Banking Executive Accountability Regime (BEAR), including potential adjustments to mandatory deferral requirements and the scope of roles covered.

Global better practice is for remuneration frameworks and supporting guidance documents to include clear guidance on when and to what degree malus and clawback are used, and how they should be applied to short-term as well as long-term variable remuneration. It is more common in some overseas jurisdictions, for example, to include the use of clawback in remuneration frameworks under local regulatory requirements. However, there have only been a handful of successful examples of current or former senior executives being held accountable for past risk and compliance failings by requiring the return of variable remuneration already paid.

Clawback is not a feature of remuneration frameworks in financial institutions in Australia but this tool, were it designed to be readily exercised, would help to drive behaviours that avoid unsound risk management and strengthen accountability for senior management and other material risk-takers. The FSB Supplementary Guidance sets out eight

recommendations, one of which includes clawback as a tool for how remuneration can be used to promote ethical behaviours and good conduct. The Panel believes that as part of adopting these recommendations, clawback could be a particularly effective tool for cases of serious misconduct.

## Recommendation 26

*CBA review and update its remuneration framework and practices to include:*

- *the potential for an upside for sound risk management and collective risk adjustments to promote collective accountability;*
- *specific management guidance on the application of malus to both STVR and LTVR; and*
- *the adoption of the FSB supplementary guidance on sound compensation practices, including the potential for clawback in the case of serious misconduct.*

# SECTION C

# CULTURE

# SECTION C: CULTURE

Even though all banks – especially large ones like CBA – require an extensive network of formal rules and procedures through which to monitor and manage their risks, these formal mechanisms are of themselves insufficient in ensuring sound risk management. Ultimately, no Risk Appetite Statement, limit structure or risk management system can anticipate or respond to every situation effectively. Alongside the formal rules, banks must also pay attention to the way these rules are interpreted and practiced – that is, 'the way things are done around here.' These practices form part of the cultural norms of a bank.

Culture has a marked impact on a bank's standing and reputation in the community. Culture can be thought of as a system of shared values and norms that shape behaviours and mindsets within an institution. Once established, the culture can be difficult to shift. Desired cultural norms require constant reinforcement, both in words and in deeds. Statements of values are important in setting expectations but their impact is *sotto voce*. How an institution encourages and rewards its staff, for instance, can speak more loudly in reflecting the attitudes and behaviours that it truly values.

As was evident in the aftermath of the global financial crisis, a bank's risk culture can have a profound effect upon its long-term success or failure. In many global institutions, a multitude of poor risk practices had been allowed to flourish, despite well-established principles of prudent risk-taking. Notwithstanding the range of regulatory reforms introduced in response to the crisis, a series of scandals has continued to shine a light on ethical shortcomings and weaknesses in banks' cultures.

Against this backdrop, the Inquiry has devoted considerable attention to understanding CBA's prevailing culture, recognising the multi-faceted and complex nature of culture in an institution. In the process, the Panel uncovered clear weaknesses in CBA's culture. The most striking was a pervasive sense of 'chronic ease'. There has been a widespread tendency towards complacency and reactivity (as opposed to proactivity and pre-emption) manifesting in multiple ways.

Connected and contributing to this 'chronic ease' were weaknesses created by the lack of skills in the operational risk and compliance functions, failure of leadership to 'walk the talk' regarding risk, lack of introspection and reflection, insufficient levels of challenge, and an historic difference in stature between the risk function and business units. These behaviours tend to reinforce and impact on each other.

At the same time, the Panel acknowledges that there are positive aspects of CBA's culture. For example, CBA has moved from being an internally competitive (or even combative) institution to being much more collegial and collaborative in recent years, driven by the tone at the top. The desire to be more values-led and customer-oriented is evident.

CBA needs to resolve the current weaknesses in its culture and continue to promote the positive elements. In doing so, the Panel would encourage CBA to deepen learning capabilities across the institution, bolster efforts to embed empowerment and sufficient challenge, and tackle the more difficult steps to fully become a values-led institution.

Whilst the Panel acknowledges CBA's recent efforts, it must emphasise that, as many financial institutions are finding out, culture change is a multi-year journey. Given various recent incidents, coupled with increased public and regulatory scrutiny, CBA is now poised at an important juncture in this journey. The Panel believes CBA needs to demonstrate committed and purposeful action in moving towards a sound risk culture.

# 9. CULTURE AND LEADERSHIP

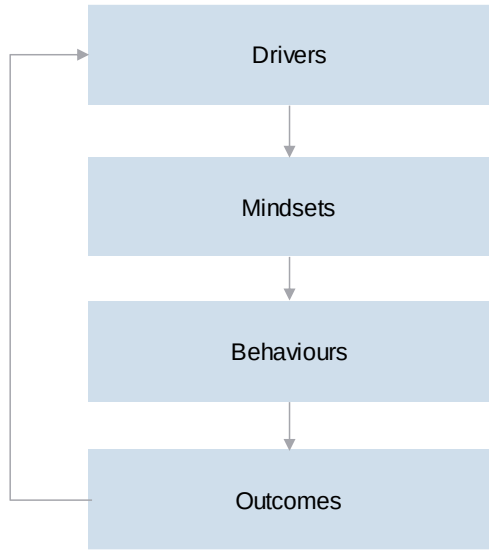
## 9.1. Background

Understanding an institution's culture can be challenging. Organisational culture is rarely homogeneous and can be opaque to external observers. Typically, an institution's culture will consist of many layers: some aspects will be common across the whole organisation whereas others will exist as 'sub-cultures' within individual teams, departments, and peer groups. Culture can also be viewed through various lenses – such as the customer culture, the innovative culture or the risk culture.

Risk culture refers to the norms of behaviour for individuals and groups that shape the ability to identify, understand, openly discuss, escalate and act on an institution's current and future challenges and risks. It is not separate to organisational culture but reflects the influence of organisational culture on how risks are managed.

Key elements of organisational culture are depicted in Figure 10 below.

*Figure 10: A simple schematic of how culture works*




*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.

*Mindsets* 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.' The Inquiry has focused in particular on the impact of shared mindsets and behavioural norms as they bear on risk management at CBA.

**What does sound risk culture look like?**

A sound risk culture is one that is consistent with the organisation's risk appetite or strategy and is appropriately embedded across different parts of the business. There is no single best practice for sound risk culture but there are, in principle, some

common elements. They include a clear tone at the top and role modelling of good risk behaviours by leaders, constructive challenge from a range of perspectives, timely and transparent information flows without fear of blame, and a consistent approach to risk management through the economic cycle. These elements consistently support effective risk management, promote sound risk-taking, improve risk awareness and support appropriate behaviours and judgments about risk-taking within a strong risk governance framework. A sound risk culture is evident through appropriate rewarding of individuals and groups for taking the right risks in an informed manner and penalising those who act otherwise. It also ensures that activities beyond the institution's risk appetite are recognised, assessed, escalated and addressed in a timely manner.

**Risk culture requires constant attention**

The maintenance of a sound risk culture is an ongoing task. There will always be internal and external factors that influence it, as well as the natural human biases and institutional drift that may over time erode it.

In approaching this issue, the Panel found it instructive to understand the lessons from other industries, such as oil and gas, nuclear and aviation, in which a culture of safety is paramount. These industries have undergone a common evolution path, typically taking in excess of 10 years. In the first phase, institutions aimed to reach 'goal zero', to demonstrate that safety was taken seriously at both a personal level and an institutional level (through standards, measurement, processes, policies and operating model). However, institutions realised that this was not enough; incidents were still occurring (and not just freak occurrences). This led to the second phase, where initiatives were undertaken to build a culture of 'chronic unease'. Institutions focused on developing authentic leadership, 'walking the talk' and building open and trusting cultures, to embed a continual concern for safety into the DNA of the organisation. As this became embedded, institutions reached a third stage and began to focus on the bigger topic of 'do I care?' addressing all aspects of risk from physical safety to wellbeing and health with a moral dimension.

Overall, the financial services sector globally lags best practice and the Panel sees CBA as no exception. In particular, as will be discussed below, the Panel believes that CBA is still embedding 'goal zero' and has not yet reached a state of 'chronic unease'. On the contrary, the Panel observed a sense of widespread complacency in CBA.

## 9.2. Inquiry findings

In analysing the multiple data and information sources reviewed by the Inquiry, the Panel has identified nine cultural themes that have inhibited sound risk management in CBA. These are:

- widespread complacency;
- reactivity rather than pre-emption regarding risk;
- uneven influence of the risk function;
- not fully 'walking the talk' when it comes to risk management;
- less tendency towards reflection, introspection and learning (from mistakes);
- collegial, high trust environment, leading to some over-confidence and over-collaboration;
- striving to balance empowerment with challenge, although not well executed;
- aiming to be a values-led institution, but an over-reliance on good intent; and
- self-perceived, but incomplete, focus on the customer.

For each of these themes, the behavioural norm and/or shared mindset is explained and the key drivers that have contributed to or reinforced the norm or mindset are described. In many cases, there is no simple one-to-one mapping of behavioural norm and driver, as the drivers may impact on more than one norm; the cultural drivers are also mutually reinforcing.

### *9.2.1. Widespread complacency*

The Panel found that there has been a prevalent culture of complacency in CBA, particularly with respect to addressing risk management shortcomings. Complacency has manifested itself in four interconnected ways, which has led to an overall 'dulling of the senses' where sound risk management is concerned.

Firstly, complacency is exhibited in the willingness of staff to accept less than optimal outcomes and attribute them to various factors over which they have no control, whether they are internal or external to CBA (externalisation). This complacent attitude was seen at the top of the institution. In interviews with Group Executives, frequent explanations for poor outcomes were given along the lines of 'we did the best we could', and that observed challenges faced by CBA were due to shifts in social expectations, rising regulatory demands and unbalanced political and media scrutiny. One Group Executive viewed this type of complacency as an industry-wide issue, stating that 'there has been slow industry reform compared to shifts in community, political and media expectations.'

Complacency in the form of externalising responsibility has also been present more widely across CBA, with staff regularly referring to perceived complexity, bureaucracy and scale of CBA. Common refrains of 'it's big and complicated', or 'it's not always easy' were often given during focus group discussions. These provide a seemingly socially acceptable (at least within CBA) explanation for the implementation of sub-optimal solutions, for mistakes being made or for issues not being addressed in a timely manner. Staff also used these refrains to rationalise and accept perceived inaction on the part of leaders. These behaviours are coupled with expressions of frustration and a sense of 'learned helplessness', as reported in the survey. In particular, risk issues were often seen to remain unresolved by staff, reinforcing a sense of helplessness.

Another impact of externalisation of responsibility has been that once a view is entrenched, it can then be used as justification for unrelated issues. For example, there was significant negative media coverage over allegations of misconduct in CommInsure's handling of claims and product management. Subsequent investigations concluded that many of the allegations were not substantiated by evidence (although, as discussed in the Financial Objectives and Prioritisation chapter, there were failings in this area). This has led to a perception that media coverage is inherently 'unfair', inclining staff to not listen and give excuses, and further reinforcing a complacent mindset.

This externalisation is a self-reinforcing process; as the collective beliefs are repeated, they gain more plausibility within the organisation. Another aspect of this process is the effect of continued favourable operating conditions. Australia has enjoyed uninterrupted economic growth for 27 years, an operating environment of sustained buoyancy for banks. Within that, CBA has been particularly successful relative to its Australian peers on financial and customer satisfaction measures, further amplifying a level of optimism and self-satisfaction. CBA has not been subject to the stresses that confronted major global banks during the crisis, and its recent Executive team has had very limited experience of operating in downturns. As one interviewed Group Executive noted: 'we fell into the trap, we've had it so good for 10 years, through the GFC, our ROE [return on equity].'

Secondly, complacency has manifested itself through repeated behaviours around avoidance of ownership of outcomes in favour of following a process. People focus on what they have to do; that is, they follow an often narrowly defined process or mandate, rather than seek to deliver the ultimate outcome or goal. This appears as a habitual pattern of behaviour and mindset throughout CBA.

At the senior level, this lack of ownership of outcomes is related particularly to the lack of collective ownership of risk management. The Executive Committee has acted as an 'advisory panel' to the CEO, which reinforced 'vertical' empowerment over collective responsibility for Group outcomes. With individual leaders focusing on accountability in their own areas, the drive for Group-wide interest and challenge was reduced. This dynamic is detailed in the Governance and Accountability Sections.

The lack of ownership of outcomes in favour of following process filtered down into the Group, with staff reporting a 'box-ticking' attitude to risk management. In the staff survey, a significant proportion of respondents agreed with the statement: 'people are a lot more focused on risk management processes than outcomes in this organisation.' Comments included, 'there is a tick-box approach rather than one of understanding the true broader risks' and 'we don't empower bankers to utilise their risk judgment to ultimately achieve the best risk outcomes.'

Thirdly, complacency has manifested itself in the ineffective use of remuneration mechanisms. As emphasised in the Remuneration chapter, remuneration mechanisms (including use of the risk gate opener) have not been applied effectively, especially in the context of risk management failings over the past few years. From a cultural standpoint, this gives rise to a reinforcing loop of poor ownership and risk behaviours.

Lastly, complacency can be seen in the collective mindset of risk conservatism, driven by how CBA sets financial risk management parameters. This perception of institution-wide conservatism has contributed to a sense of complacency through the belief that 'we are ok'. This was seen in focus groups with middle managers and in interviews with the Executive Committee. As one interviewee noted:

> *We are generally a conservative bunch, we always look for the cons, we are prudent and very cognisant of risk in everything that we do. We review our risk appetite and then decide.*

In short, the multiple examples of complacency throughout CBA could be described as a repetitive cycle of inertia. A sound risk management culture requires a sense of 'chronic unease', with staff at all levels continuously looking out for current and emerging risks and improving the business. Instead, the Panel detected a sense of inertia leading to weaknesses in risk management and, ultimately, complacency.

### *9.2.2. Reactivity rather than pre-emption regarding risk*

The Panel found that, rather than being proactive and pre-emptive, CBA has been highly reactive in dealing with operational and compliance risks. Reactivity is strongly related to complacency and it has shown itself in a number of ways. Staff have generally been good at reacting to and flagging issues once they have arisen but, commonly, the follow through to issue resolution has been lacking. A reactive approach to operational risk and compliance issues has been apparent at senior levels. Lastly, there has been a slow and reactive approach to regulatory interaction.

CBA staff are increasingly logging issues in the RiskInSite system, encouraged by the SpeakUP campaign which began in 2014. Survey respondents indicated that 'staff are encouraged to speak up and report without a culture of blame.' This was also a strong theme emerging from focus groups. One member said, 'I feel it is safe to speak up, it is okay to raise issues.' Another said that 'I think we've done a lot of work on that.'

However, the attention given to raising issues does not flow through to timely and effective issue resolution in CBA. As discussed throughout this Report, CBA's issue escalation mechanisms have tended to be reactive, process-based and often ineffective, and resolution has been prolonged. Many issues have been improperly risk accepted, had their resolution deadline repeatedly extended or marked as resolved but later reopened. Staff have also found the high volume of issues in RiskInSite 'overwhelming' to deal with. In the staff survey, relatively few respondents supported the statement, 'in my experience, people in this organisation are good at dealing with issues before they become a major problem.' Similarly, in focus groups, there were frequent comments along the lines of 'people are aware that something is an issue, identify it, but the point of doing something can take a long time.'

One of the drivers of good issue flagging yet poor issue resolution has been the relative emphasis given to the former through the extensive Vision and Values initiative led by the previous CEO, which included the SpeakUP campaign. This initiative has a number of components, including formal communications, trainings, workshops and business unit-specific cultural assessments. However, the initiative from the top to create psychological safety in raising issues was not accompanied by equal focus or embedding of issue resolution. This has led to blind spots in related areas of risk management essential to strong issue resolution.

Reactivity has also been apparent in the senior leadership team's approach to managing operational and compliance risk. Interviews with Group Executives confirmed the perception that the 'waterline' for escalation of operational and compliance items to the Executive Committee was too high to ensure effective oversight. This has inhibited the ability to identify emerging risks. One Executive Committee member stated, 'we need to restructure the content (that goes to the Executive Committee) so that we get real time, emerging

issues.' A reactive approach was also seen at the Board level, where the information escalated failed to effectively highlight broader factors related to risk, reputation and the customer. These elements are described further in the Governance Section of this Report.

Finally, as noted in the Issue Identification and Escalation chapter, CBA has been less proactive with regulators and slower to comply with regulatory requests, compared to some of its peers. This behaviour has been indicative of a reactive leadership culture.

Complacent and reactive behaviours have exacerbated ongoing operational and compliance risk issues in CBA. Furthermore, the normalisation of behaviours, such as raising issues without an expectation of resolution, has been understood as 'just how CBA does things', and this has strongly shaped the way staff understand the risk culture of their workplace.

### *9.2.3. Uneven influence of the risk function*

The risk function has had an uneven (that is, an inconsistent and sometimes weak) influence across CBA. This has been partly driven by the natural organisational divide between business units that generate revenues and support functions. The risk function has faced more obstacles than the business units in carrying out its mandate. Moreover, the credibility, authority and respect of the risk function has been inconsistent across CBA, and at times weak.

The Inquiry has identified examples of the risk function facing more obstacles than business units in carrying out its mandate. More than half of the Executive Committee members interviewed acknowledged that they had experienced or witnessed behavioural challenges in translating risk decisions into business operations. As one Group Executive said, 'we all agree that the business units own the risk, but what does that mean in practice? There isn't yet unanimous agreement.' One of the main drivers of this behavioural characteristic at Executive Committee level is the empowerment of business units without the accompanying empowerment of strong support functions. The Financial Objectives and Prioritisation chapter has also noted that the 'voice of risk' has been less effective than the 'voice of finance' in relation to investment prioritisation, in part due to the capability and resourcing challenges facing the risk function.

The Inquiry has also found that the credibility of the risk function with business units has been inconsistent across CBA. In the staff survey, relatively few people agreed with the statement 'within this organisation, staff in the risk and compliance functions have equal influence to those in other areas of the business.' In some areas, the risk function was perceived more as an inhibitor than a necessary partner.

One of the main drivers of the inconsistent influence of the risk function has been the amount of bureaucracy built up in CBA, resulting in risk management being perceived as a low priority 'administrative task'. In focus groups, there was a common view among participants that 'Line 2 adds a huge amount of bureaucracy.' In the staff survey, relatively high numbers of staff agreed with the statements, 'The time required to complete many risk-related processes exceeds the value they add.' In addition, over 100 respondents expressed the sentiment that risk management activities are 'onerous', 'complex', 'time consuming', and 'really achieves very little other than as a form filling exercise.' The risk function was also described as focusing on policy writing and correctness of frameworks over implementation and engagement with the business. Furthermore, the operational risk and compliance frameworks enforced in the past had helped foster the perception of the risk function as process-focused and onerous, due to the behaviours it encouraged. Whilst these issues are now subject to extensive remediation programs, they remain part of the mindset affecting the relationship between the risk function and the rest of CBA.

Another driver of the inconsistent influence has been the low and varied capability levels in the risk function, particularly in operational risk and compliance. Focus group participants shared low confidence in the risk function, pointing to the 'deficiency in the capability of practitioners'. This led to views such as, 'Risk is seen to be an administrative, rather than strategic, function in the business… the old handbrake, slowing down the speed.' Overall, this mindset has driven behaviours that reflect a lack of urgency, awareness and maturity around operational risk and compliance.

In an organisation with sound risk culture, the risk function acts, and is seen by the business to act, with a strong voice. The function would also be appropriately resourced and empowered. At CBA, the drivers described above have instead contributed to the uneven and sometimes weak influence of the risk function. The Panel believes that these behaviours and mindsets have had a negative influence on CBA's risk culture, hindering the necessary respect for, and relationship with, the risk function.

### *9.2.4. Not fully 'walking the talk' when it comes to risk management*

When it comes to risk management, the Panel found that CBA is not yet fully 'walking the talk'. Whilst staff perceive that expected behaviours, roles and communications regarding risk are clear, and self-report high risk awareness, the Panel observed poor execution of risk management practices and behaviours. Ultimately, there has been a significant gap between perceptions and practices regarding risk management at CBA.

On the one hand, there are reported high levels of perceived clarity around roles and communications. Over 90 per cent of respondents to the staff survey agreed with the statement 'My risk management responsibilities are clearly communicated to me.' Internal audit findings on risk culture have also consistently reported high risk awareness across CBA. This awareness has been partly driven by the SpeakUp campaign, described above.

On the other hand, the self-reported risk awareness has not been consistently translated into action, and good risk management practices have not been well embedded. At the top, as this Inquiry has found, the Board has not applied sufficient rigour in holding management to account for the mitigation and closure of risks and issues. At the Executive Committee level, there has been insufficient consideration of operational and compliance risk, particularly with regard to emerging risk issues. The lack of 'walking the talk' by leadership is evident further down CBA. According to the staff survey, while staff generally agreed with the statement 'leaders at all levels of this organisation communicate consistent risk-related messages,' far fewer agreed with the statements 'I believe senior leaders in this organisation mean what they say' or 'senior leaders in this organisation set an example of how to do things the right way.'

Various examples of not 'walking the talk' on risk management have been provided in this Report. The Three Lines of Defence model has not been implemented well, resulting in blurred responsibilities and lack of ownership. In most of the focus groups, participants also recognised limited reward and recognition of proactive, sound risk management practices. This has driven a distortion in prioritisation and decision making as good risk behaviours are not reinforced structurally. At the same time, remuneration adjustments have not been applied consistently and transparently. Focus group participants said 'it's not transparent if people are getting penalised.' As noted above, the 'voice of risk' has also not been prominent in investment prioritisation. One staff member commented:

> *sometimes strategy is a word used, but too often it becomes tactical change that needs to be reviewed short to medium term rather than…actually investing in the long term outcomes.*

The most prominent driver of 'walking the talk' is leading by example. Notwithstanding the positive example set by the previous CEO in promoting the Vision and Values initiative, the Inquiry found that CBA's leaders have not all consistently practiced what they preached. Although it is difficult to achieve perfect alignment between words and action, the gap at CBA signalled that following this 'walk', rather than the 'talk', was acceptable. Specifically, leaders have been observed to communicate the importance of values, but not necessarily act accordingly themselves. A 2014 report by the Ethics Centre to the CBA noted that CBA referred to their values 'when it [was] convenient.' In the same vein, over 350 respondents in the staff survey expressed a negative view of leadership, often alluding to not 'walking the talk'. For example:

> *Whilst leaders espouse the values, there are clear examples of leaders' behavioural indiscretions which have had a blind eye turned to them.*

CBA has sought to address this shortcoming through its Our Commitments initiative launched in

early 2017. Our Commitments is an updated form of the Statement of Professional Practice, and sets out expectations for behaviour with eight key commitments. Staff are asked to decide an action by asking: 'can I do it, and should I do it.' However, this initiative to begin the 'living of the Vision and Values' is yet to gain traction within CBA. It is difficult to answer the question, 'should I do it?' when leaders are not seen to adequately 'walk the talk'. Whilst the initiative is a well-formed attempt to make the values practical, the Panel believes it is too early to form a view on its effectiveness.

A sound risk culture would require all leaders and employees to role model appropriate risk behaviours and action (not just awareness), supported by practices that are well embedded in the organisation. In the Panel's view, CBA's role modelling in this area needs to improve.

#### *9.2.5. Less tendency towards reflection, introspection and learning*

The Panel has found that reflection, introspection and learning from experiences and mistakes have not been regularly integrated into day-to-day work patterns of staff across CBA. A focus on the immediacy of day-to-day issues has limited the ability to develop a strong feedback loop to learn from mistakes; as a consequence, CBA staff have been at risk of missing the bigger picture or the full breadth and depth of issues. In addition, learnings across business units have not been translated in a meaningful way.

CBA has not set aside the requisite space, time and permission for quality reflection, introspection and learning. There is little evidence to suggest that reflection is a skill that is widely valued in practice. In fact, there appears to be a genuine lack of appreciation for its importance. This behavioural characteristic has been observed at the top of CBA. With respect to the various incidents under review, only a few Board members and leaders interviewed mentioned without prompting taking time to personally reflect on these; those who did, often did so after the Inquiry had begun, and pointed to a 'lack of questioning', 'not seeing the wood for the trees', and 'insufficient time to consider issues.'

A low capacity to self-reflect has also been observed more broadly across CBA. Employees commented on working in an environment in which institutional outcomes are not absorbed for lessons learned, with 'not enough [management focus] on the learnings from negative outcomes which are a normal part of business.' Examples include previously logged issues not being socialised with frontline staff for learning, and remuneration outcomes not being recorded for ongoing referral, consistency and learning.

Related to this has been an over-focus on the immediacy of the day-to-day. Across CBA there appears to have been a mindset, and practice, of honing in on current issues and challenges, whether they are internal (organisational) or external (regulatory, technology, etc). Over-focusing on the day-to-day was particularly apparent at CBA's senior levels. Within the tightly curated, fast-paced Executive Committee meetings, which have emphasised accuracy, structure and sharpness, insufficient time appeared to be given to longer-term thinking and exploration. One Executive Committee member told the Panel that for 'important topics… there is not the time and space to get under the issues and get them all surfaced.' Another example of missing the bigger picture was the inadequate attention given to identifying systemic and emerging risk issues, as discussed in the Issue Identification and Escalation chapter.

Executive Committee meetings tended to focus on intellectual debate and speed, rather than on reflection. Executive Committee members commonly described the 'socratic' questioning style set by the previous CEO leading to some 'decisions being driven by the best debater rather than the person with the most robust position.' One Executive Committee member also commented that: 'we were not as intellectually curious as we should have been.'

This tone at the top has flowed down to CBA more broadly. The tendency within middle management has been to 'rectify quickly and move on', rather than embed lessons and instigate behavioural and mindset changes. Survey respondents stated that: 'we don't take the time to understand why something went wrong before putting a fix in place' and 'we need to get better at learning from mistakes, we have been too busy to do this effectively.' Another respondent noted that they 'rarely have time to think about what the optimal process should be, or what themes should be drawn out, or the implications of what [they are]

doing.' Limited reflection and learning coupled with the focus on the day-to-day has also led to missing the bigger picture or full depth of risk issues, both current and emerging.

In the Panel's judgment, CBA has not applied sufficient levels of foresight, curiosity, critical thinking and questioning. In interviews, leaders commented that they would devote attention to the symptoms of broader risk management issues without questioning the overall capability of the relevant business, which was a key driver in ensuing outcomes.

Finally, CBA has not been able to properly translate and apply learnings from one business more widely across the Group. This was referred to a number of times in interviews and survey responses, including in relation to recent incidents. A key structural driver of this characteristic is CBA's federated structure, which has led to Group-wide risk issues in the past being under-addressed, without clearly assigned owners, until they resulted in live incidents. This has created difficulties in Group-wide communication. Comments received by the Inquiry were that the operating model 'makes it challenging for a business unit to see the end-to-end view of risks across the value chain', and 'inhibits the ability to truly understand potential risk impacts on downstream and upstream activities.' In the staff survey there was relatively low agreement with the statement 'people in this organisation communicate a lot with others outside their business unit in order to make better decisions.' One respondent said:

> *Each BU seems to look after their own department, instead of CBA as a whole organisation. If any risk doesn't directly impact their BU, very little will be done.*

In summary, CBA has not succeeded in building a strong risk culture where learning, reflection and self-challenge are present. Ultimately, CBA has been missing out on a strong feedback loop, or reinforced 'risk memory' (a muscle to be constantly exercised), which allows the institution to learn from previous mistakes and, crucially, to adapt.

#### *9.2.6. Collegial, high trust environment leading to some over-confidence and over-collaboration*

The working environment at CBA is largely collegial, with high levels of trust in peers, teams and leaders. However, the Panel observes that this strength has been somewhat exaggerated, leading to some over-collaboration in CBA and over-confidence in abilities.

The levels of collegiality, collaboration and trust within CBA have reportedly increased over the past few years. The common perception at senior levels was that, under leadership predating 2011, a culture of internal competition and a 'very combative environment' was fostered, leading to entrenched silos. The collective desire to move beyond this, reinforced by a new tone from the previous CEO, has reshaped the culture to one that now values collegiality, collaboration and trust. One Group Executive said: 'we really trust in team spirit… we rely on the team.' This was reinforced in interviews and focus groups by the common refrain of 'things have changed', implicitly for the better.

The desire to move away from a past combative culture has led to some over-compensation in pursuit of collaboration. The result has been pockets of excessive consultation or consensus-driven activity, leading to slower decision making, lengthier processes and slippage of focus on outcomes. Referred to multiple times particularly by risk function staff, this type of behaviour has been at the expense of constructive challenge and cross-examination across the three lines of defence.

Furthermore, a collegial environment has led to over-confidence (and sometimes misplaced confidence) in the abilities and decisions of people in CBA, including its leaders. Examples of over-confidence included many instances of internal communications expressing confidence in projects that ultimately delivered late and either over budget or without all benefits realised. Similarly, CEO all-staff emails consistently focused on topics such as success in customer satisfaction or financials, community engagement or pride in values, and rarely emphasised the importance of risk management or continuous learning.

Over-confidence has been driven by a focus on IQ (narrowly defined technical know-how) and 'good intentions.' This was also a key finding of the 2014 Ethics Centre report, which stated: 'collectively, the unofficial (but operational) values convey CBA as an IQ-focused organisation.' Because of this, there has been a reliance on raw intellect over comprehensive analyses of data on risk issues. This was especially prevalent at senior levels, where some leaders (Executive Committee and Board level) have highlighted that they faced challenges in admitting a lack of understanding of issues. Contributing to this was the decision by the previous CEO to appoint Group Executives who 'have not yet peaked in their careers' and had limited exposure to potential downsides. The impact has ultimately meant less focus on a broader leadership repertoire of skills and traits, such as reflection, humility, learning and adaptive capacity, and practical experience of managing throughout cycles.

A strong risk culture should be appropriately collaborative, in which processes are also simple and efficient in order to understand and manage risks, and staff are open to constructive criticism and are self-questioning. At CBA, over-consultation has made the institution more complex and bureaucratic, and prevented it from quickly responding to risk issues, while over-confidence has likely reinforced the sense of complacency and chronic ease.

### *9.2.7. Striving to balance empowerment with challenge, although not well executed*

One of the objectives of the previous CEO was to empower Group Executives and encourage challenge. This was well intentioned, but was not always well executed in practice. The empowerment of leaders led to underdevelopment of collective accountability. And despite challenge being mandated in the Executive Committee Charter, this was not practiced in sufficient measure and often prompted a defensive response.

In the Panel's view, the focus on empowerment of individuals was not balanced with a corresponding focus on collective accountability. Leaders were empowered to make decisions that affected the performance and future of their specific business area, and to own the outcomes of those decisions. During Executive Committee interviews, several examples were provided indicating the previous CEO generally favoured the views of business unit heads above those of other leaders. The focus on empowerment meant that CBA did not demonstrate behaviours that promote shared responsibility for the sound management of the Group. These behaviours also signalled that raising concerns at the Executive Committee may not be productive.

The Panel also found that there have been insufficient levels of challenge at CBA. The previous CEO had encouraged an environment of openness and challenge, alongside his SpeakUP initiative, with many Executive Committee members referring positively to this in interviews. One noted that the previous CEO 'likes to have that challenge and encourages an open discussion by the management team.' Yet in spite of this encouragement, evidence shows a reluctance to challenge across CBA, including at the Executive Committee and Board level. Group Executives were less likely to raise concerns outside their own area, especially if previous attempts to raise issues were seen to be unfruitful. An attitude of 'relationship at all costs' has been referred to in a number of interviews, with any significant challenge interpreted as a lack of collaboration. The Board's strong confidence and trust in senior management's 'high IQ' and their ability to 'take care of all things' meant that the Board also did not challenge management strongly, or hold them to account over longer time frames. In this way, the encouragement to challenge at CBA has been more nominal than real.

In examples where challenge has occurred, it has been met with defensiveness, indicative of a lack of appreciation and understanding on how to receive, interpret and learn from challenge. In the staff survey conducted for the Inquiry, relatively high numbers of staff agreed with the statement 'in my experience, people in this organisation often get defensive when their views are challenged by colleagues.' The survey results on this question had the starkest contrast to CBA's internal survey results for a similar question. A number of survey respondents named senior individuals who had been particularly non-receptive to feedback or challenge. This overt defensiveness by leaders creates a symbol of what is appropriate behaviour (that is, don't challenge, don't ask too many questions) for the rest of the organisation and has had a clear impact on the mindset of staff.

Organisations with a significant degree of risk maturity are able to balance individual empowerment and accountability, with collective responsibility and rigorous challenge. In the Panel's view, CBA has fostered a culture of empowerment, but with weak collective accountability and ineffective challenge. This is another repetitive cycle, which has created challenges for openness, transparency and the ability to freely express views at CBA, and has reinforced the sense of chronic ease.

### *9.2.8. Aiming to be a values-led institution, but an over-reliance on good intent*

CBA has striven to be a values-led, ethical institution, the bedrock of which has been a conscious program of work initiated by the previous CEO. In the Panel's view, however, the focus on good intent has led CBA, at times, to incorrectly frame risk concerns and create blind spots in terms of risk management.

The Panel acknowledges the steps that CBA has been taking to become a values-led organisation. The most significant is the Vision and Values initiative, launched in 2013 in partnership with The Ethics Centre. Since then, there has been significant work and ongoing communications around the vision ('to excel at securing and enhancing the financial wellbeing of people, businesses, and communities') and the corporate values (Integrity, Accountability, Collaboration, Excellence, and Service). Within this program, a number of smaller initiatives were launched, including the SpeakUP program and ongoing monitoring and incorporation of values into key formal mechanisms (training, recruitment and performance frameworks). The development of the Conduct Risk Strategy in 2017 has also provided a risk framework for ethical behaviour. The Panel recognises that this work has had an impact on CBA's culture. However, neither the vision nor the set of values are well embedded within CBA, evident throughout the data collected by the Inquiry.

One informal aspect of the values in the collective consciousness of CBA is 'good intent.' Institution-wide, employees appear to place high value on good intent, and tend to characterise their habits and practices in reference to it. In Executive Committee interviews, nearly 80 per cent of senior leaders referenced operating with good intent, particularly in the context of this Inquiry, making comments such as 'there was no bad intent.' This is similarly observable at lower levels of CBA, with one representative focus group participant stating: '99.95 per cent of the time, the intention is right.'

Whilst being values-led is a positive cultural attribute, the focus on operating with good intent and personally 'doing the right thing' at CBA has created blind spots where risk management outcomes have been concerned. Specifically, framing strong risk management as a matter of good intent overshadows the focus on capability and consequences, including addressing process and system weaknesses. One person stated: 'if you make a mistake, it's ok, because everybody makes mistakes, so long as there was no malintent,' and another said: 'if everyone has good intent, you won't get punished.' The narrow framing of these processes as a matter of intent has meant that staff can become insensitive to risk concerns and the need for a more holistic approach to risk management.

An institution exercising sound risk management practices may be motivated by values but will remain diligent in identifying and responding to emerging risks. CBA's efforts to be a values-led institution are a positive element of its culture, but have created a danger of over-reliance on good intent over risk management. In the Panel's view, this has likely contributed to weaknesses in CBA's risk capability and to the sense of complacency.

### *9.2.9. Self-perceived, but incomplete, focus on the customer*

CBA perceives itself to have strong customer orientation. Whilst this is well intended, it is also incomplete. At all levels of the institution, there is noticeable pride in customer service and customer satisfaction, but there has been less focus on identification of systemic issues from customer complaints.

CBA has been number one out of the four major banks in Australia for customer satisfaction for the past five years, according to Roy Morgan benchmarking. Culturally, CBA staff express pride in this achievement at all levels of the institution. For example, regular CEO weekly emails called out customer satisfaction score performance every

month over the course of 2017. One senior leader shared that:

> *We've got the highest ever customer experience and Net Promoter Score (NPS). In all these forums, it's the only thing that will generate spontaneous applause… it's a huge source of pride everywhere.*

A push to embed customer service within CBA's values has been a deliberate focus of both of the previous two CEOs. This has been enshrined in the publicly stated goal that CBA be first in customer satisfaction and inclusion of 'service' as one of CBA's five corporate values.

Although CBA has drawn comfort from strong customer satisfaction metrics, which reflect an aggregated view of customer sentiment, it has missed the tail where customer issues reside. As discussed in the Issue Identification and Escalation chapter, the most serious customer complaints, though only a small percentage of CBA's customer base, have not been promptly and effectively addressed. Nor has CBA devoted sufficient attention to identifying systemic issues or applying a long-term mindset.

Focus groups and survey participants expressed views that CBA has developed bespoke, manual, 'band-aid' technology and process fixes in the name of serving the customer, rather than investing in long-term solutions. This is essentially treating the symptom rather than addressing the cause, and may introduce risk issues down the track. Examples given on data integrity and legacy systems were particularly salient. One focus group member stated:

> *Leadership underinvests in tools and systems that would improve the management of risk. A lot of investments that have been done are customer-facing.*

In summary, CBA has historically taken comfort in being customer-oriented but this focus has been incomplete. For a mature culture, a more complete orientation would be required at all levels of CBA, including holistic consideration of dissatisfied customers consistent with sound long-term risk and customer outcomes.

## 9.3. Recommendations

The Panel acknowledges that CBA is taking steps to improve its culture (including as it relates to risk culture). The most significant step is the Vision and Values initiative, which also embraces SpeakUP, Our Commitments and ongoing monitoring of risk culture. This work has had a positive impact on CBA's culture but continued effort is required to build upon this foundation. In addition, the Accountability Change Program, launched in late 2017, will further embed accountability and nurture a culture of identifying and mitigating risks. The Panel also acknowledges that CBA's new remediation program, BROP, is aimed at improving CBA's culture.

In the Panel's view, however, more must be done to ensure that CBA has a robust and healthy risk culture. CBA will need to take a holistic approach that includes targeted steps to remediate the cultural weaknesses outlined in this chapter. These steps will need to be aligned with the requirements of the Board and management to form a view on risk culture under Prudential Standard CPS 220 Risk Management.

CBA will need to regularly monitor changes to its risk culture, demonstrating what has changed. The onus falls squarely on CBA itself. As the Group of Thirty *Banking Conduct and Culture* report of July 2015 stated, 'Supervisors and regulators cannot determine culture.'[24]

Culture change is a multi-year journey that will require sustained effort and attention from CBA leaders at all levels. The four recommendations are necessary next steps in that journey. They cover areas in which all leaders can continually develop and improve, and demonstrate their willingness to accept personal responsibility for driving cultural change. Aligned with regulatory requirements and expectations, CBA needs to continually monitor its progress in assessing risk culture and to meeting these recommendations.

[24] Group of Thirty, *Banking Conduct and Culture: A Call for Sustained and Comprehensive Reform*, July 2015.

# 9. CULTURE AND LEADERSHIP

The first two recommendations require senior leaders to take personal responsibility for cascading the tone at the top, in a way that is authentic and consistent with each individual leader's style. This extends to the Board and aligns with Recommendation 1 relating to the heightened visibility of the Board. Focusing on being authentic is vital in closing the gap between the 'talk' and the 'walk' and achieving effective 'echo from the bottom.'

The third recommendation addresses the requirement that a sound risk culture have an effective working relationship between the business units and the risk function, characterised by respect for their separate responsibilities and open communication. Openly identifying and working through impediments to this relationship, related to structures or capability and, importantly, rooted in behaviours and mindsets, are key to enhancing it. In similar situations, positive outcomes can come through initiatives such as secondment of business unit staff to the risk function, and vice versa.

In the fourth recommendation, CBA should articulate the positive behaviours (for example questioning, adaptability) that actively reinforce its values and address negative behaviours (for example complacency, reactivity) which contribute to the gap between intent and action.

While considerable effort has been put into communications and initiatives that promote ethical behavior, CBA needs to recognise that being ethical in all types of behaviour, including risk management, is evidenced in actions, not ideals. Ensuring that the values are personally demonstrable, especially in dealing with customers, will contribute to the maturing of CBA's culture.

## Recommendation 27

*Senior leaders reinforce key behaviours of increasing self-reflection, giving and receiving constructive challenge and dealing with conflict effectively.*

## Recommendation 28

*CBA ensure that its senior leaders are capable of cascading the desired tone at the top in a personal and authentic manner.*

## Recommendation 29

*The divide between business units and the risk function be bridged through effective working relationships at all levels.*

## Recommendation 30

*The Vision and Values initiative focus on staff personally living ethical values, with due consideration of CBA's Conduct Risk Strategy, to close the gap between good intent and actions.*

# SECTION D

# REMEDIATION INITIATIVES AND PANEL RECOMMENDATIONS

# SECTION D: SECTION D: REMEDIATION INITIATIVES AND PANEL RECOMMENDATIONS

Since the global financial crisis, banks globally have been required to fundamentally enhance their frameworks and practices for managing both financial and non-financial risks.

At many institutions, this has required large transformation or remediation programs aimed at enhancing the governance, culture and accountability around risk management as well as developing the practical tools, processes and capabilities required to manage risks. Initially, given the nature of the crisis, these programs were focused on financial risk but they quickly evolved to include non-financial risk. This shift reflected the series of corporate scandals in global banks involving misconduct, financial crime and other areas of non-financial risk, and the resulting increased regulatory attention in this area.

Banks in Australia are also spending significantly on risk management and compliance efforts after a series of high-profile failings. Resource commitments are not expected to decline significantly in the near term, and in many cases are likely to increase.

CBA is intensifying its risk remediation efforts. Its latest program must deliver. The Panel has articulated a series of shortcomings at CBA across the three primary areas of focus − governance, accountability and culture – that these efforts must address.

Each of these shortcomings, taken on its own, would not necessarily account for the types of incidents or issues that CBA has experienced in recent years. However, in the Panel's view, it is the collective weakness across these areas, and the lack of any one obvious pillar of strength, that has contributed to an operating environment in which such missteps could occur in a bank of CBA's standing.

Ahead of the Inquiry, CBA introduced its 'Big Rocks' program and other initiatives designed to strengthen its risk management capabilities. If delivered successfully, these initiatives would address some of the findings in this Report.

A new program, the 'Better Risk Outcomes Program' (BROP), is intended to substantially extend and enhance this work. It will subsume many of the initiatives already underway, including the 'Big Rocks' program. To drive a consistent approach to managing risk, all risk remediation activity will be centralised in one overall program, governed by the Board and led by the CEO.

The new program is complex and ambitious in scope, and prioritisation will be essential. Its final structure and many areas targeted for remediation or improvement are not yet clearly defined. For this reason, the Panel cannot readily assess CBA's ability to deliver the desired outcomes in a timely and effective manner.

Under the new Chair, a series of improvements has also been initiated to improve the effectiveness of the Board and its Committees.

CBA's track record in delivering improved risk outcomes, particularly in operational and compliance risk, does not impress. As highlighted in this Report, CBA has faced significant issues in execution including project extensions, recurrence of issues and weaknesses in issue closure. CBA will need to lift its game in program delivery for risk initiatives. Critically, CBA must avoid its tendency to layer on bureaucracy and yet more theoretical frameworks, and drive real improvement in its day-to-day risk management activities.

Notwithstanding CBA's efforts to date and the ambitions of its new remediation program, the Panel considers that there is more to do to ensure that the shortcomings identified in this Report are being addressed. The Panel has made a series of recommendations through the Report that address key levers to promote change in CBA. For convenience, these recommendations are listed in the final chapter.

# 10. REMEDIATION INITIATIVES

## 10.1. Background

**The need for remediation**

Through the preceding chapters, the Panel has articulated a series of weaknesses at CBA across the three primary areas of focus: governance, accountability and culture.

These weaknesses include:

- inadequate oversight and challenge by the Board and its gatekeeper committees of emerging non-financial risks;
- an over-confidence in the operation of the Board and its committees, and a lack of benchmarking to assess effectiveness;
- unclear accountabilities, starting with a lack of ownership of key risks at the Executive Committee level;
- weaknesses in how issues, incidents and risks were identified and escalated through the institution and a lack of urgency in their subsequent management and resolution;
- inadequate reporting of customer complaints to the Executive Committee and the Board;
- overly complex and bureaucratic decision-making processes that favoured collaboration over timely and effective outcomes and slowed the detection of risk failings;
- an operational risk management framework that worked better on paper than in practice, supported by an immature and under-resourced compliance function;
- an emphasis on process rather than outcomes in operational risk and compliance; and
- a remuneration framework that, at least until the AUSTRAC action, had little sting for senior managers and above when poor risk or customer outcomes materialised (and, until recently, provided incentives to staff that did not necessarily produce good customer outcomes).

Shortcomings developed in a culture at CBA that was both complacent and reactive in the oversight and management of non-financial risks.

In his meeting with the CBA Board in December 2015, APRA's Chair characterised CBA as 'bureaucratic and arrogant', elaborating that 'arrogance' referred to the complacency that can develop within an institution after a long period of success.

**Success factors for risk remediation**

Despite a considerable financial commitment to improving risk and compliance outcomes, banks globally have had varying degrees of success, and embedding further improvement in risk management and compliance capabilities remains a necessary priority for many. Typically, remediation programs that fail, do so not for want of design but for want of execution. Outlined below are a number of core attributes that have made some remediation efforts in the industry more successful than others.

Given the cross-organisation nature of risk transformation and remediation, successful programs are often overseen at both Board and Executive Committee level to ensure adequate engagement of all relevant parties, to foster a sense of urgency and to maintain focus and momentum. For banks mobilising changes that span multiple business units, first line Executive sponsorship, or at least joint sponsorship with support functions, typically leads to a higher likelihood of success and more integrated outcomes. This helps to ensure that solutions are not just frameworks articulated on paper, but turn into effective day-to-day practices. In addition, secondment of talent out of business lines or other non-risk roles and into the remediation programs injects capability, credibility and interconnectedness to the rest of the business.

As with any large program, having clear objectives, detailed project planning, comprehensive resource plans, and clear accountability are non-negotiable prerequisites. Without these, it is impossible for

senior executives who are responsible for monitoring the health of the program to differentiate between a program that will deliver on time and with the right outcome, and one that simply has momentum. In addition, banks that successfully deliver large risk remediation programs are able to ensure that these projects have committed, multi-year budgets, with funding allocated outside of regular annual cycles where required.

For very large, complex and particularly lengthy programs, standard practice is to engage internal audit or an outside function to conduct assurance on the initiative itself. This independently assesses the program management's health and capabilities, and the likelihood that the program will achieve its stated objectives in the timeframes required and the budget allowed. It allows the Executive team and the sponsors to take remedial action and correct the course of the program at an earlier stage where necessary.

Furthermore, many programs rely on a small group of senior executives or subject matter experts whose capacity can be easily stretched across many workstreams and deliverables. Successful programs sequence initiatives and/or source the right quantum of skillset to avoid bottlenecks and ensure that key individuals can give adequate attention to the elements that require their input.

Finally, culture plays a major role in the successful embedding of better risk outcomes as part of large programs. In many cases, effective risk management can be impeded by behaviours and shared mindsets that can render the risk management framework ineffective. Remediation initiatives should be mindful of such factors, and ensure that structural changes go hand-in-hand with the necessary cultural changes. As discussed in the Culture and Leadership chapter, messaging from senior leadership is particularly important for achieving cultural change but so, too, is senior leadership demonstrating commitment to the objectives through their actions and decisions.

## 10.2. CBA's remediation initiatives

**Board effectiveness**

Under the new Chair and in response to the self-assessments of its performance, the Board has taken a number of actions designed to improve its effectiveness. As discussed in the Role of the Board chapter, these include:

- extended Board and Committee meetings, to provide more time on strategic issues and to facilitate more effective challenge of management;
- a refreshed and more focused Board agenda with greater time allowed for 'deep dives' on priority matters, including risk items;
- a review of reporting to the Board and Committees to improve the quality of information provided;
- reporting by Committees to the Board at relevant points during the meeting rather than rushed at the end;
- amended charters to ensure stronger communication between Committees and clarity of roles and responsibilities; and
- measures to strengthen the BAC's oversight of audit issue closure.

In addition, ongoing Board renewal has seen the retirement of a number of long-standing Directors.

**'Big Rocks' program**

Following the change of CRO in July 2016, Group Risk initiated a remediation program targeting improvements in risk management. The 'Big Rocks' program was designed to make CBA's risk function more responsive to business needs, to simplify policies and processes and improve focus on underlying risk management responsibilities. By mid-2017, the program contained nine initiatives ('Big Rocks'), including:

- review of and improvements to risk appetite frameworks at the Group and business unit levels, including more specific risk appetite

metrics for operational and compliance risk and corresponding reporting to the Board;

- efforts to simplify and improve risk policies and processes with an overall goal to create a set of risk policies that are easier for business units to implement. These began with operational and compliance risk policies, and were expanded to include credit risk;
- improvements in the operating model for and capabilities of the operational and compliance risk functions: This included several 'Big Rock' initiatives with different aims:
  - an operating model initiative with several workstreams relating to ways of working within the risk function;
  - an initiative to clarify the roles of the first and second lines of defence;
  - an initiative called 'RiskConnect' to broaden and deepen the capabilities of risk professionals through rotations, training and the establishment of a new portal related to the capabilities of risk management professionals; and
  - an effort to streamline and standardise CBA's method of interacting with regulators;
- a Risk Technology Strategy initiative that will create a risk IT platform for future improvements to CBA's risk technology infrastructure and further seeks to develop an improved risk architecture for the business. Specific improvements are also planned to various technologies in current use, including the RiskInSite system; and
- a model risk management initiative aimed at improving policies and practices governing the use of models of various risk types throughout the business.

In addition to the 'Big Rocks', CBA developed other targeted initiatives during 2017 that focused on enhancing its approach to risk management. These included changes to governance and reporting to the Board and Executive Committee, new approaches to project management within the risk management and enterprise services functions, a program to improve issue and action closure, cultural work on CBA's Vision and Values, and changes to the remuneration framework intended to improve accountability for sound risk management.

Additionally, there were remediation efforts in specific risk disciplines, such as the Financial Crime 'Program of Action' (described further below), and a range of initiatives conducted by the Customer Advocate team to enhance the way that customers are served.

As of early 2018, these initiatives were at various stages of completion. Some are undergoing transition into business-as-usual practices, while others have yet to receive investment approval.

The Panel's review of 'Big Rocks' and other 2017 initiatives indicate that they are sound in scope and ambition, and if delivered effectively would address some of the findings in this Report. For example, the improvements in the Risk Appetite Statement have been positive, although some further improvements are recommended in the Risk Management and Compliance chapter. However, as discussed later in this chapter, the Panel has reservations about CBA's delivery capability for the bulk of work remaining.

**The Program of Action**

To address concerns raised by the AUSTRAC action, a new financial crime capability upgrade was introduced in August 2017 as an organisational priority. This program has over 100 FTE staff allocated to it, and was temporarily spearheaded by an EGM from RBS to provide it with additional leadership and sponsorship. CBA transitioned this program to a new EGM of Financial Crime Compliance in March 2018. The approach has three core elements:

- immediate actions to strengthen specific areas of financial crime compliance;
- capturing all applicable global compliance obligations and assessing current operations to identify any further actions required; and
- designing the future operating model for financial crime compliance.

In line with the Terms of Reference, this Inquiry has not made observations about this program.

# 10. REMEDIATION INITIATIVES

**CBA's Better Risk Outcomes Program**

In March 2018, toward the end of this Inquiry, CBA notified the Panel of its intention to substantially expand and elevate its remediation work in the management of risk. The new BROP is intended to extend and enhance CBA's remediation of ongoing issues, in particular with respect to operational and compliance risk.

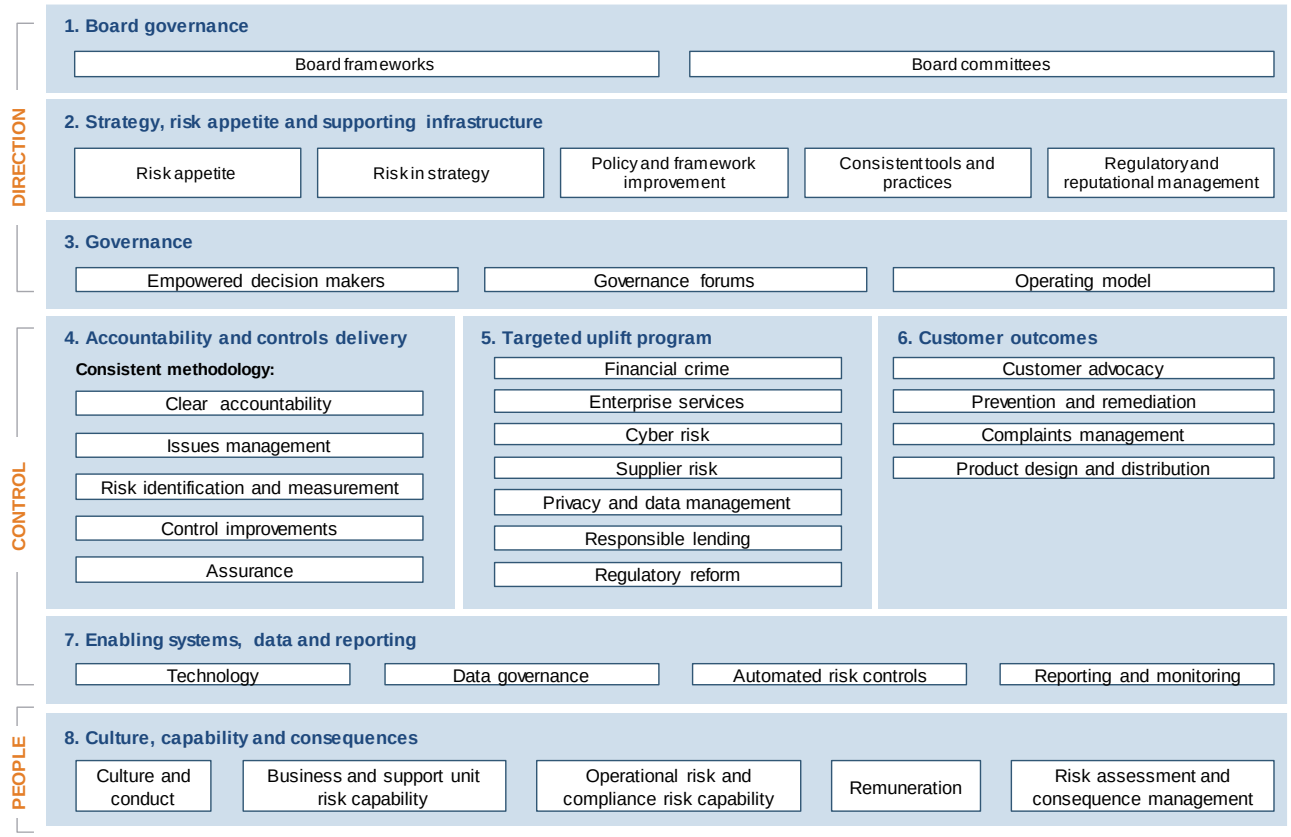
BROP aims to centralise all risk remediation activity for these risk disciplines into one overall program, governed from the top of CBA, with the objective of driving a consistent approach to managing risk. The program is owned by the CEO.

An overview of the program was presented to the Inquiry team in late March by the new CEO and the CRO. The program's final structure and many areas targeted for remediation or improvement are not yet clearly defined. Hence, the Panel's view of the program outlined below is based on the limited information available to date.

BROP is extensive and broadly mirrors the key components that would be expected of a program designed to substantially re-engineer a risk management framework. This program is set out in Figure 11. Effectively, the program is planning or anticipates changes across all key elements of the risk management framework spanning Board governance, risk management, management oversight, accountability, controls, customer, technology, and people and culture.

As of the date of this Report, the full Program still requires Board endorsement, funding allocation and key leadership appointments, including the overall BROP leader. CBA's initial assessment is that the program will encompass the work of approximately 800 full-time equivalent roles across eight work streams, overseen by a small team of senior leaders

*Figure 11: Better Risk Outcomes Program initiatives*




Source: CBA

## 10.3. Inquiry findings

The Panel welcomes the steps taken by CBA to improve the governance and effectiveness of risk management and compliance. The Board is taking a clear and more visible leadership role, that, given the scale of challenges facing CBA, will need sustained energy and focus.

The Panel views the increased ambition of BROP as appropriate given the range of shortcomings in the management of non-financial risks it has identified. At the same time, however, the Panel strongly recommends that CBA maintain the momentum of existing priority risk programs and avoid using the existence of a new and broader structure to extend pre-committed delivery timetables without adequate justification.

The Panel would also emphasise that the increased attention from the Board and the new CEO will be critical in overcoming the cultural traits of complacency and reactivity highlighted in this Report. Through the course of the Inquiry, it has become apparent to the Panel that CBA was largely aware of its challenges but it was not until 2017, in the face of external pressures, that it developed momentum to address them.

In addition to direct oversight by the Board and the CEO, there are other positive elements in BROP that the Panel believes will improve the ability of CBA to deliver on outcomes, if the Program is implemented as proposed. These include:

- an enhanced program team targeted to be put in place over the next three months;
- a focus on end-to-end accountability with business units taking ownership for risk outcomes, rather than just deferring to Group Risk;
- a focus on delivering risk management outcomes as opposed to a more superficial achievement of milestones or deliverables that do not address underlying issues;
- a more holistic view of the multiple initiatives underway, with the aim of designing and integrating these as a collective rather than focusing on delivery of individual and piecemeal changes; and
- an ambition to source more diverse talent to provide expertise and capability that CBA may not have currently.

Given the relative immaturity of the new program, the Panel cannot readily assess CBA's ability to deliver the desired outcomes in a timely and successful manner. For the same reason, the Panel is not able to confirm that the scope and anticipated outcomes of BROP will fully address the findings and associated recommendations in this Report.

Some key challenges lie ahead for CBA that are both a reflection of BROP but also CBA's track record in delivering risk remediation programs.

The program is ambitious, with some 35 different initiatives. This poses logistical challenges with governance and oversight, as well as staffing, given the number of appropriately skilled resources needed to achieve such a broad and deep outcome. CBA identified 'limited organisational bandwidth' as a potential threat to the success of the 'Big Rocks' program, and this risk will increase with the extension of that program to BROP. In the Panel's view, if CBA is to be able to focus on and deliver against these ambitions, it must consciously put on hold other priorities so as to free up organisational capacity and senior management bandwidth.

Ensuring that each of the initiatives works together in a holistic manner will require a significant amount of effort, expertise and knowledge of Group operating models to mitigate the risk that, whilst individual frameworks are solid in concept, collectively they do not achieve the better risk outcomes anticipated by BROP. The Panel has observed that some previous initiatives have looked positive on paper but that CBA has struggled to embed them.

A number of BROP initiatives are yet to be fully defined. These may be 'placeholders' to accommodate potential changes recommended by this Inquiry or identified through other efforts underway to assess CBA's capabilities. Either way, the initiatives need to be articulated fully, adequately funded and resourced, and incorporated into the overall risk management fabric being delivered by the other initiatives. For example, BROP anticipates a culture initiative, but limited

details have been provided on what this important workstream will achieve and how it will be executed.

CBA's track record in delivering against major risk initiatives has been a chequered one. For example, CBA commenced its work on the Three Lines of Defence model as early as 2010, and BROP includes further work on this model nearly a decade later. CBA's efforts to close out AML issues have run over many years, involving a number of programs and new initiatives to address previously closed issues. One of the most recent efforts was evaluated in a post-implementation review as not having fully delivered the expected benefits despite a slight cost overrun. Separately, an external review of CBA's key controls noted that many required further actions to close out issues from prior years, some raised as early as 2010. These shortcomings have been discussed in earlier chapters.

Many workstreams or initiatives within BROP will require skilled operational and compliance risk staff. CBA has identified a shortage of employees with the relevant skills and capacity at present and has highlighted the need to recruit additional operational and compliance risk expertise. CBA is likely to face challenges sourcing talent given the scarcity of, and competition for, such resources in the market. CBA has historically been reliant on significant external support to deliver its programs. However, the Panel has concerns that continued extensive use of external resources could dilute accountability if not paired with clear senior management ownership that provides essential continuity.

In many cases, program documentation for many of CBA's remediation programs that would evidence a strong, well-run initiative was not provided to the Panel upon request. These include detailed project plans, risk and issue registers, and budgets. Whilst there may be observable traction in some cases, the lack of detailed planning and milestones makes it difficult for those overseeing or auditing the program to assess whether it is genuinely on track, or simply moving in an overall positive direction. Lack of such project discipline would also contribute to the types of delays to key risk programs observed in this Inquiry.

## 10.4. Recommendations

The Panel has outlined a series of actions that it believes will assist CBA in executing the BROP program successfully.

### Recommendation 31

*CBA senior leadership have 'skin in the game' and adequate time commitment to perform program director or oversight roles, rather than relying on external parties to provide leadership.*

### Recommendation 32

*There is clear accountability for program delivery and remuneration consequences for unsuccessful outcomes.*

### Recommendation 33

*CBA determine the programs or initiatives that may need to be deferred to create organisational capacity to deliver the BROP and its associated initiatives.*

### Recommendation 34

*CBA develop and demand rigorous project disciplines and subject them to independent review.*

### Recommendation 35

*CBA design, evaluate and implement BROP in an end-to-end manner that ensures formal frameworks are effectively embedded into day-to-day operations.*

# 11. PANEL RECOMMENDATIONS

In the preceding chapter, the Panel has summarised CBA's remediation plans and has made specific recommendations on how CBA might enhance its ability to deliver on its plans.

This chapter brings all the Panel's recommendations together. Viewed overall, the recommendations focus on five key levers to promote change in CBA:

- more rigorous Board and Executive Committee level 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 into CBA's DNA of the 'should we?' question in relation to all dealings with and decisions on customers; and
- cultural change to support enhanced risk identification and remediation, moving the dial from reactive and complacent to empowered, challenging and striving for best practice.

A number of these recommendations reinforce and set the bar for initiatives that are underway. Other recommendations provide signposts for additional work that CBA must undertake to strengthen governance, culture and accountability.

To better inform its deliberations and in particular its recommendations, the Panel obtained advice on the range of risk management practices globally. This articulated a view of mature practices for the areas that the Panel evaluated, which have been taken into account in informing these recommendations.

## Section A: Governance

### *Role of the Board*

1. *The CBA Board maintain its recent heightened visibility, promoting a clear tone at the top in both messaging and action.*
2. *The processes and practices of the Board and its Audit and Risk Committees be aligned with global better practice for risk management.*
3. *The Board ensure effective coordination between its Audit, Risk and Remuneration Committees.*
4. *The BAC increase direct engagement with the business unit and support function owners of significant issues and hold them accountable for timely and effective closure of these issues.*
5. *The Board ensure it receives adequate non-financial risk information, including early indicators of emerging risks, to support constructive debate and challenge.*

### *Senior Leadership Oversight*

6. *The CEO ensure that the Executive Committee accepts and embeds collective accountability for management of the Group.*
7. *The CEO ensure that the Executive Committee:*
   - *discusses, understands and takes action to mitigate the impact of risks that span business units;*
   - *promotes the voice of support functions as an effective counterbalance to the business units; and*
   - *engages in constructive challenge and debate.*
8. *CBA establish an effective Non-Financial Risk Committee at the Group Executive level.*

### *Risk Management and Compliance*

9. *CBA ensure that its Three Lines of Accountability principles are effectively embedded and subject to strict governance. In doing so, CBA must ensure that business units take primary ownership of risk management.*
10. *CBA ensure that business unit Chief Risk Officers have the necessary independence to provide effective challenge to the business.*
11. *CBA strengthen its Risk in Change process to ensure that there is effective risk-based oversight from Line 2 across the Group.*
12. *CBA strengthen its management of operational and compliance risk. In doing so, CBA must ensure that:*
    - *the Group Risk Appetite Statement includes limits and triggers for more granular operational and compliance risk metrics by risk theme;*
    - *minimum standards are clearly articulated in policies and embedded across the Group;*
    - *there is a stronger focus on the 'big picture' and identification of emerging risks;*
    - *Line 2 effectively fulfils its assurance responsibilities;*
    - *the control environment is robust, reflecting effective control design and testing; and*
    - *root causes and not merely issues are addressed in a timely and effective manner.*
13. *CBA build up the capabilities and subject matter expertise of operational and compliance risk staff through training and continued recruitment.*
14. *CBA elevate the stature of the compliance function by making the Head of Compliance a member of the Executive Committee and/or the recommended Non-Financial Risk Committee, by making their appointment and removal subject to approval by the Board Risk Committee, and by ensuring that they have direct access to the Board.*
15. *CBA review its conduct risk profile in business units, incorporate the findings in its Conduct Risk Strategy and ensure that conduct risk is fully considered in decision-making processes.*

### *Issue Identification and Escalation*

16. *The Executive Committee and Board improve their processes for monitoring issues raised by internal audit, regulators and other sources, and end any organisational tolerance for untimely or ineffective resolution of significant and outstanding matters of concern.*
17. *CBA report on customer complaints to the Board and Executive Committee in line with better practice peer organisations.*
18. *CBA prioritise investment in the identification of systemic issues from customer complaints.*
19. *CBA strengthen its dialogue and engagement with regulators.*

### *Financial Objectives and Prioritisation*

20. *CBA take in its investment prioritisation processes a more pre-emptive approach to investment decisions in risk management, compliance and resilience areas prior to these becoming 'high rated' issues.*
21. *CBA leadership champion the 'should we?' question in all interactions with customers and key decisions relating to customers.*

## Section B: Accountability

### *Accountability*

22. *CBA, building upon the foundation established by BEAR, incorporate the Accountability Principles set out in in this Report.*

### *Remuneration*

23. *The CBA Board exercise stronger governance to ensure the effective application of the remuneration framework. In particular, the Board assess remuneration outcomes for Group Executives to reflect individual and collective accountability for material adverse risk management and compliance outcomes. In turn, Group Executives cascade accountability throughout the Group on a consistent basis.*
24. *To support the effective oversight of the remuneration framework:*
    - *the Board require a comprehensive risk assessment from the CRO to assist it in*

*determining appropriate risk adjustments for poor risk behaviours and outcomes for the CEO and Group Executives;*

- *the Board require comprehensive analytics and reporting from management, including the assessment of Group values and the use of the risk gate opener; and*
- *the BRC actively support the Board Remuneration Committee in ensuring that risk outcomes are reflected in executive remuneration outcomes.*

25. *In support of the effective application of the remuneration framework:*
    - *the CBA Board provide clear guidance to management on the Board's expectations in determining an appropriate level of risk adjustment for good and poor risk behaviours and outcomes;*
    - *the risk function assist in the application of the risk gate opener in the Group through applying more rigour in challenging outliers, observed inconsistencies and absolute levels of risk reductions; and*
    - *CBA, with due regard for confidentiality concerns, communicate the impact of both good and poor risk outcomes on remuneration across the Group to reinforce the link between accountability and consequence.*
26. *CBA review and update its remuneration framework and practices to include:*
    - *the potential for an upside for sound risk management and collective risk adjustments to promote collective accountability;*
    - *specific management guidance on the application of malus to both STVR and LTVR; and*
    - *the adoption of the FSB supplementary guidance on sound compensation practices, including the potential for clawback in the case of serious misconduct.*

## Section C: Culture

### *Culture and Leadership*

27. *Senior leaders reinforce key behaviours of increasing self-reflection, giving and receiving constructive challenge and dealing with conflict effectively.*
28. *CBA ensure that its senior leaders are capable of cascading the desired tone at the top in a personal and authentic manner.*
29. *The divide between business units and the risk function be bridged through effective working relationships at all levels.*
30. *The Vision and Values initiative focus on staff personally living ethical values, with due consideration of CBA's Conduct Risk Strategy, to close the gap between good intent and actions.*

## Section D: Remediation Initiatives and Recommendations

### *Remediation Initiatives*

31. *CBA senior leadership have 'skin in the game' and adequate time commitment to perform program director or oversight roles, rather than relying on external parties to provide leadership.*
32. *There is clear accountability for program delivery and remuneration consequences for unsuccessful outcomes.*
33. *CBA determine the programs or initiatives that may need to be deferred to create organisational capacity to deliver the BROP and its associated initiatives.*
34. *CBA develop and demand rigorous project disciplines and subject them to independent review.*
35. *CBA design, evaluate and implement BROP in an end-to-end manner, that ensures formal frameworks are effectively embedded into day-to-day operations.*

# APPENDIX A.
# APRA Prudential Inquiry into CBA: Terms of Reference

The purpose of the Prudential Inquiry is to examine the frameworks and practices in relation to governance, culture and accountability within the CBA group, so as:

1. to identify, in light of a number of incidents in recent years that have damaged the reputation and public standing of the CBA group, any core organisational and cultural drivers within CBA that have contributed to these incidents.
2. to assess, at a minimum, whether any of the following areas, or their implementation, are conflicting with sound risk management and compliance outcomes:
    a. the group's organisational structure, governance framework, and culture;
    b. the group's framework for delegating risk management and compliance responsibilities;
    c. the group's financial objectives;
    d. the group's remuneration frameworks;
    e. the group's accountability framework; and
    f. the group's framework for identification, escalation and addressing matters of concern raised by CBA staff, regulators or customers.
3. to consider, where CBA has initiatives underway to enhance the areas reviewed under (1) and (2) above, whether these initiatives will be sufficient to respond to any shortcomings identified and, if not, to recommend what other initiatives or remedial actions need to be undertaken.
4. to recommend, to the extent that there are other shortcomings or deficiencies identified under (1) and (2) above that are not already being addressed by CBA, how such issues should be rectified.

The Prudential Inquiry should not make specific determinations regarding matters currently the subject of legal proceedings, other regulatory reviews or investigations by regulators other than APRA, or customers' individual cases.

# APPENDIX B.
# Panel Membership

The Panel established to conduct the Prudential Inquiry is comprised of:

**Jillian Broadbent, AO**

Ms Jillian Broadbent, after an extensive career with Bankers Trust Australia, has served as a non-executive director on a number of publicly listed companies. She is Chancellor of the University of Wollongong, currently sits on the Boards of Woolworths and Swiss Re and was formerly Chair of the Clean Energy Finance Corporation and a member of the Board of the Reserve Bank of Australia. Ms Broadbent was made an Officer of the Order of Australia in 2003 for services to economic and financial development in Australia.

**Dr John Laker, AO**

Dr John Laker is Chair of the Banking and Finance Oath, and formerly Chair of APRA over an 11-year period until 2014. He is a member of the Council of the University of Technology Sydney and of the External Advisory Panel of ASIC. He lectures at the University of Sydney and undertakes advisory work for the International Monetary Fund and the Basel Committee. Dr Laker was appointed an Officer of the Order of Australia in 2008 for his services to financial regulation.

**Professor Graeme Samuel, AC**

Professor Graeme Samuel is a Professorial Fellow in Monash University's Business School and School of Public Health and Preventative Medicine. He was previously Chair of the Australian Competition and Consumer Commission, Associate Member of the Australian Communications and President of the National Competition Council. In 2010, he was made a Companion of the Order of Australia for services to public administration through contributions in economic reform and competition law.

# APPENDIX C.
# Activities Undertaken by the Inquiry

The Inquiry has undertaken a number of different but complementary activities to gain a thorough understanding of the current practices and frameworks at CBA.

In summary, these activities included:

- in-person interviews of:
  - current and former CBA Board Directors and relevant Group Executives;
  - senior management, including Executive General Managers and General Managers;
- an assessment of the CBA culture;
- document reviews of:
  - policies, processes and frameworks;
  - reports, Committee papers and minutes; and
  - prior independent reviews from internal audit and external parties, such as consultants;
- case studies;
- 'better practice' benchmarking; and
- meetings with relevant third parties.

CBA has provided its full cooperation with the work of the Inquiry, facilitating access to employees, providing requested documents, arranging requested interviews and enabling the focus groups and the staff survey.

**Interviews**

Over 90 interviews with current and former CBA Board Directors and staff were conducted as part of the Inquiry, capturing a broad range of staff levels and functions. These interviews included:

- one-on-one interviews conducted by the Panel with 15 current and former CBA Board Directors, CEOs and Group Executives, including the current and/or recent chairs of the Board's Risk, Audit and Remuneration Committees; and
- interviews by the Inquiry team with over 75 senior CBA employees, current and former. The level of seniority included Group Executives, Executive General Managers and General Managers. All three lines of defence were represented.

**Culture assessment**

To assess the risk culture of CBA, primary data collected by the Inquiry team was combined with various sources of secondary information. Resulting cultural findings are based on comparisons and contrasts across these data sources, forming a holistic view of risk culture at CBA. The three primary data sources were:

1. A staff survey of the Group Executive team and the top five layers of the institution.
2. Culture interviews with 11 Executive Committee members.
3. Focus groups with Executive Managers (around 110 participants across multiple business units and functions).

An online staff survey was sent to nearly 10,000 staff, from Group Executives down to staff reporting to a Manager. Around 6,000 responses were received. The survey contained 61 questions, to which participants responded on a 5-point scale, ranging from 'strongly agree' to 'strongly disagree' with a 'neutral' option. There were also two optional free-text questions regarding leadership and risk culture, with around 1,500 responses each. The survey was designed to assess cultural drivers by providing insights into any behavioural norms that may prevent risks being identified and mitigated and the perceptions of staff surrounding various aspects of risk management.

Eleven interviews were held by the Inquiry team with Executive Committee members, with the resulting data anonymised. These interviews

# APPENDIX C.
# ACTIVITIES UNDERTAKEN BY THE INQUIRY

focused on the behavioural norms within the Executive Committee that influence the effective management of risk. The interviews used an inductive, qualitative inquiry methodology, focusing on issues such as team dynamics, decision-making norms, leadership style, conflict management, learning and skill development, communication patterns, risk appetite, emotion management and shared beliefs and values.

Eleven focus groups were held with around 110 Executive Managers, chosen at random from various business areas within CBA including Risk, Retail Banking Services (RBS), Institutional Banking and Markets (IB&M), Business and Private Banking (B&PB) and Enterprise Services (ES). These focus groups, each lasting 90 minutes, were designed as structured workshops conducted on a confidential basis, and discussed topics such as leadership, team dynamics, cross-business-unit dynamics, issue escalation, culture and values, remuneration structures and risk management.

In addition, the Inquiry team reviewed other relevant sources of data, including:

- fact-finding interviews undertaken by the Panel and Inquiry team with 15 current and former CBA Board Directors, CEOs and Group Executives, and over 75 senior leaders of CBA;
- quantitative analysis of Executive Committee meeting data;
- thematic analysis of weekly CEO all-staff updates in 2017;
- broader institutional engagement surveys;
- internal Audit Risk Culture reviews; and
- data and information collected from other Inquiry assessment streams.

**Document review**

Over 10,000 documents requested of and voluntarily produced by CBA were reviewed as part of the Inquiry. Documents included framework documents such as policies and procedures, Board and Board committee papers, executive committee papers, audit reports, project documentation, internal staff communications, human resources data, and emails and correspondence.

**Case studies**

The Panel reviewed more recent incidents that have occurred at CBA and that were considered relevant to the Inquiry. This review provided additional insights into how CBA's decision-making processes and behaviours have operated in practice. However, the Panel did not conduct a forensic examination or audit, and did not form a view about any allegations surrounding these incidents.

**'Better practice' benchmarking**

With support from Oliver Wyman's global expert network, global experience and industry benchmarks were analysed to help form views about 'better practice' and emerging industry trends. The global experts shared their experiences dealing with other financial institutions that have suffered damage to their reputation and have undertaken remediation programs in response.

**Meetings with relevant third parties**

The Panel met with APRA, the Australian Securities and Investments Commission (ASIC), Australian Transaction Reports and Analysis Centre (AUSTRAC), the Financial Ombudsman Service (FOS), and other relevant third parties to gain further insights into CBA's frameworks and practices.

**Inquiry Team**

The Inquiry team was made up of the following (current and former) staff from APRA and staff from Oliver Wyman.

APRA: Steve Bisson, James Douglas, Steve Blinco, Jamshed Khambatta, Ron Vidal, Christopher Sheehan, Elpitha Stavropoulos, Mike Cornwell, Elizabeth Arzadon, Tamara Scicluna, Sigrid Neumueller, Janna Garcia, Anna Adamou.

Oliver Wyman: Edward Emanuel, Ibon Garcia, Chris Evans, Matt Tottenham, Jasmine Fowdh, Lynnette Lin, supported by a team of nine consultants.

# APPENDIX C.
# ACTIVITIES UNDERTAKEN BY THE INQUIRY

Specialist workshops and international practice expertise from Oliver Wyman: Sir Hector Sants (London), Davide Taliente (London), Graeme Jeffrey (London), Allen Meyer (New York), Kevan Jones (London), Peter Reynolds (Hong Kong), Christian Pedersen (Singapore), Til Schuermann (New York), Michelle Daisley (London), Martin Andersson (Stockholm).

Editorial assistance: David Lewis.