INFORMATION PAPER

Risk culture

October 2016

Disclaimer and Copyright

Contents

Introduction

The 2008 financial crisis revealed major shortcomings in the way the global financial sector managed risk. This was not solely an issue of poor risk measurement, or weaknesses in internal control structures. It also reflected deficiencies in institutions' *attitudes* towards risk. In combination, a poor risk culture and weak risk management (the former often being the root cause of the latter) led to unbalanced and ill-considered risk-taking, to significant losses and, in some cases, to institutional failures. The impact on the financial stability of affected countries was significant.

Although APRA-regulated institutions avoided the worst of the financial crisis, Australia has not been without its own examples of poor risk culture. The failure of HIH Insurance in 2001, for example, highlighted the central role that a weak organisational culture, and a dismissive attitude to risk management, had in the demise of the insurer. Similarly, foreign currency trading losses at a major bank in 2004 identified the link between the risk culture of its trading area and the scant regard given by the business to the underlying risk and management risk limits.

More recently, APRA highlighted the emergence of increased risk-taking within the life insurance industry with respect to the underwriting and pricing of, in particular, group insurance business. At its heart, this stemmed from a focus on growth without, in a number of institutions, adequate regard to the risks that came with it. Similarly, in the past few years, APRA observed that sound market practices for the origination of residential mortgage loans had, in some instances, been sacrificed to considerations of preserving market share and growth.

Unlike the earlier episodes highlighted above, which affected individual institutions, the more recent issues in group risk insurance and mortgage lending have manifested in a deterioration in general industry practices. There is nothing wrong with an institution or an industry pursuing a higher risk strategy, provided it does so consciously, and with appropriate risk management capabilities and financial capacity. In some of these cases, though, hindsight and supervisory scrutiny would suggest that the decision was not a conscious one: considerations of risk were not always front of mind in a highly competitive environment.

It is also interesting to juxtapose these recent experiences with the assertion made by most institutions that they believe they have a good, if not strong, risk culture; to the extent there are deficiencies in the industry, most institutions consider they exist within their peers. And where there have been specific problems identified within their own businesses, 'bad apples' are typically seen as the cause. Yet in the case of mortgage lending standards, for example, there were few lenders who could claim their risk culture was sufficient to prevent them succumbing to the weak practices that eroded industry standards.

Unfortunately, a poor risk culture can persist for some time without detection, or immediate damage. Typically, it will be when a poor risk culture is combined with adverse market conditions and/or other stresses that there is greater potential for a build-up of unbalanced and ill-considered decisions to result in significantly adverse, and potentially crippling, financial outcomes. Good times will often mask poor practices. In an Australian context,

where the domestic economy has enjoyed 25 years without a serious recession, this should sound a clear note of caution against complacency.

APRA's supervisory approach

Much of the attention on global regulatory responses to the GFC has focussed on strengthening the balance sheet of financial institutions. While these measures help to strengthen the resilience of financial institutions, they do not address the risks of poor behaviours and/or attitudes to risk by the decision-makers within an institution. Tackling risk culture is, to a large degree, the final frontier in the post-crisis response, and was the catalyst for the publication of the Financial Stability Board's (FSB's) *Guidance on Supervisory Interaction with Financial Institutions on Risk Culture* in 2014.[1]

APRA aims to ensure that risk-taking in financial institutions is conducted within reasonable bounds and that risks are clearly identified and well-managed. Consistent with this objective, APRA has traditionally placed a strong emphasis on robust frameworks for the governance and risk management in regulated institutions. Within this, broad observations of behaviour and culture have influenced APRA's supervisory assessment of governance and risk management for some time.

Building on the lessons of the GFC, APRA's focus on risk culture intensified in 2013 when it commenced a review of how the prudential framework established the roles and responsibilities for risk management within financial institutions. This review recognised that the traditional focus of supervisors on governance, risk management and internal controls would likely be inadequate if insufficient attention was given to risk culture. The result was *Prudential Standard CPS 220 Risk Management* (CPS 220)[2], which came into force in January 2015. Among other things, it introduced a new requirement for each Board of APRA-regulated authorised deposit-taking institutions (ADIs) and insurers to ensure that it:

'*...forms a view of the risk culture in the institution, and the extent to which that culture supports the ability of the institution to operate consistently within its risk appetite, identifies any desirable changes to risk culture and ensures the institution takes steps to address those changes'*.

Leading up to, as well as since, the introduction of CPS 220, APRA has observed a much stronger focus on risk culture by the Boards of regulated institutions. This is a welcome development. All involved would acknowledge, however, that given the nuances and complexities involved, there is more to do to fully understand their institution's risk culture. Most institutions are still grappling with how best to clearly articulate what type of risk culture they aspire to, identify any specific weaknesses in their current risk culture, and how they most effectively address those weaknesses. It is therefore critical that this attention on risk culture be sustained.

Ultimately, a sound risk culture across the industry is not something that can be regulated into existence. It requires persistence by those tasked with the stewardship of financial institutions – primarily the Chief Executives and their senior executive teams, with support

[1] Financial Stability Board 2014, *Guidance on Supervisory Interaction with Financial Institutions on Risk Culture: a Framework for Assessing Risk Culture* <http://www.fsb.org/2014/04/140407/

[2] APRA 2015, *Prudential Standard CPS 220 Risk Management* <http://www.apra.gov.au/CrossIndustry/Documents/Prudential-Standard-CPS-220-Risk-Management-January-2015.pdf>

and oversight by Boards of Directors - to ensure that the industry operates within a risk-taking framework that appropriately balances risk and reward, and seeks to operate in a manner that is sustainable over the long run.

That said, APRA can support and reinforce this work. Having drawn greater attention to the issue, APRA will continue to identify and encourage better practices across the industry, and – through enhancing its own supervisory skills and practices in this area - be active in seeking out indicators of a poor risk culture which have the potential to adversely impact on the stakeholders that APRA seeks to protect: depositors, policyholders and superannuation fund members.

To aid this endeavour, this information paper on risk culture provides:

- an overview of developments in the identification and supervision of risk culture;
- observations on current industry practices; and
- an outline of APRA's supervisory priorities.

The paper will hopefully prove useful to APRA-regulated institutions as they continue their efforts to understand and manage their own risk cultures. This is far from an easy task, but nonetheless it is critically important for the industry's long-run health.

Chapter 1 – An increased focus on risk culture

Failings within the global financial sector revealed by the GFC contributed to significant losses and, in some cases, institutional failures in a significant number of jurisdictions. Although there were a range of factors that contributed to those failings, in a number of cases it has become clear that behavioural influences impeded the balanced and considered management of risk.

Some of the undesirable behaviours which have been highlighted through various national and international reviews and inquiries into the causes and costs of the GFC include:

- pursuing short-term financial interests, including personal interests, with little or no consideration of customer interests;
- observing the letter of relevant law and regulation, while contravening the spirit of those laws and regulations;
- treating risk management processes and/or controls as inconveniences which can be disregarded when expedient to do so;
- poorly defining management accountabilities for risks;
- failing to reward good risk management and/or apply consequences for poor management of risks;
- senior executives and/or directors failing to take timely actions to mitigate significant risks;
- concealing problems, rather than resolving the underlying causes of the problems; and
- failing to challenge the status quo and consider alternative viewpoints, resulting in a false sense of security and risk blind spots.

In most instances, institutions were to some extent aware of these undesirable behaviours (whether they were prevalent across the institution or just within a smaller group). They had not, however, fully appreciated the potential adverse impacts of these behaviours on the institution's attitude towards risk-taking and risk management, or understood what factors were driving them. This failure to appreciate the importance of their risk culture to long-term organisational success was a key failing that the GFC brought to light.

Defining risk culture

Risk culture can be thought of as the impact of organisational culture on risk management. A definition of organisational culture that is often cited is:

'...a system of shared values (that define what is important) and norms that define appropriate attitudes and behaviours for organisational members (how to feel and behave)'.[3]

Risk culture is the application of this concept to the way an organisation takes and manages risk. Risk culture is therefore not separate to organisational culture, but reflects the

[3] O'Reilly, C. A. and J. A. Chatman 1996, *'Culture as social control: corporations, culture and commitment.'* Research in Organizational Behavior Vol 18: pp 157-200

influence of organisational culture on how risks are managed. One of the more widely accepted definitions of risk culture is:

'the norms and traditions of behaviour of individuals and of groups within an organisation that determine the way in which they identify, understand, discuss, and act on the risks the organisation confronts and the risks it takes'.[4]

The norms and traditions as they relate to risk culture are formed through shared experiences within an organisation or market over time. Therefore, the drivers of risk culture, how it forms within an organisation, how it can be influenced and changed, are multifaceted. This definition of risk culture also acknowledges the potential for the existence of various sets of shared norms and behaviours within a single organisation. This adds additional complexity to the task of understanding risk culture, since it necessitates consideration of how varying norms and behaviours within parts of an organisation interact with each other and impact the way in which the organisation as a whole perceives and manages risks.

Importantly, this definition recognises that all organisations have a risk culture, regardless of whether this is actively considered or managed.

Risk culture and corporate governance

The Basel Committee on Banking Supervision defines corporate governance as:

'a set of relationships between a company's management, its board, its shareholders and other stakeholders which provides the structure through which the objectives of the company are set, and the means of attaining those objectives and monitoring performance. It helps define the way authority and responsibility are allocated and how corporate decisions are made'.[5]

An organisation's risk culture is influenced by both formal elements (such as governance and risk management frameworks and structures), as well as informal elements (such as expectations and behavioural norms). Formal governance structures provide an important framework through which appropriate behaviours can be encouraged and supported (and through which poor behaviours can be detected and acted upon).

Ideally, both formal and informal elements of an organisation's risk culture will be mutually reinforcing. For instance, an organisation demonstrating day-to-day adherence to organisational values, effectively balancing risk and reward, and reporting both good news and bad, enhances the effectiveness of its formal governance structures. However, the converse is also true. That is, poor behaviours and expectations undermine the effectiveness of formal governance structures. Therefore, the informal aspects, although more difficult to observe and assess, are an equally important influence on risk culture.

[4] This definition is contained within the International Institute of Finance report 2009, *Reform in the Financial Services Industry: Strengthening Practices for a More Stable System;* and is also referenced in the Financial Stability Board's 2014 *Guidance on Supervisory Interaction with Financial Institutions on Risk Culture: A Framework for Assessing Risk Culture*. For other views on risk culture refer to Power M., S. Ashby and T. Palermo, London School of Economics and Political Science 2013, *Risk Culture in Financial Organisations* and Group of Thirty 2015, *Banking Conduct and Culture – a Call for Sustained and Comprehensive Reform.*

[5] Basel Committee on Banking Supervision Guidelines 2015, *Corporate Governance Principles for Banks* <http://www.bis.org/bcbs/publ/d328.pdf>

Risk culture and conduct risk

There are a range of definitions of conduct risk, with conduct regulators tending to focus on risks associated with customer outcomes (for both consumers and businesses) and market integrity. The International Organisation of Securities Commissions (IOSCO) Research Department refers to harmful conduct as:

'...a broad term that refers to conduct (not necessarily illegal conduct) by a firm or an individual market participant that could (1) harm the interest of investors; (2) jeopardize fair, efficient, and transparent markets; or (3) lead to potential systemic risk (or any combination of these)'.[6]

In the Australian context, one of the responsibilities of the Australian Securities and Investments Commission (ASIC) is to regulate the conduct of financial services companies. ASIC has defined conduct risk as:

'the risk of inappropriate, unethical or unlawful behaviour on the part of an organisation's management or employees'.[7]

Therefore, while conduct and prudential regulators both have a legitimate interest in cultures within financial institutions, their interest stems from different underlying objectives. ASIC's focus on culture is from the perspective of its mandate as a conduct regulator, and ensuring fair outcomes for customers and investors. ASIC is primarily interested in culture because it is a driver of conduct in the firms that make up its regulated population. APRA's focus on risk culture reflects its prudential mandate - that as a result of undesirable behaviours and attitudes towards risk-taking and risk management, the viability of an APRA-regulated financial institution itself might be threatened, and this may in turn jeopardise both the institution's financial obligations to depositors, policyholders or fund members, and financial stability.

Given this common area of interest, conduct and prudential regulators need to work collaboratively on risk culture-related matters. For example, to the extent that a prudential regulator's assessment of a poor risk culture could help identify the potential for poor customer outcomes, this may provide useful insights for the conduct regulator's surveillance. Similarly, where the conduct regulator identifies behaviour that produces poor customer outcomes, this can provide useful insights for the prudential regulator as to the organisation's broader attitude to risk. In this way, the work of the two agencies, while pursuing their respective mandates, can be mutually supporting.

Regulatory developments

The international regulatory framework has been significantly strengthened since the GFC. In addition to higher capital and liquidity requirements, there has been much more attention given to governance, remuneration, risk appetite, and risk culture. This activity reflects an

[6] International Organisation of Securities Commissions Research Department 2016, *Securities Markets Risk Outlook – 2016* <http://www.iosco.org/library/pubdocs/pdf/IOSCOPD527.pdf>

[7] Australian Securities and Investments Commission 2016, presentation, *ASIC Investment Banks Conduct Risk Review.*

evolution in the manner in which prudential regulators are evaluating the effectiveness of governance structures and risk management frameworks of regulated institutions.

Governance requirements have long been a foundation of global prudential regulatory requirements[8]. These requirements were designed to support the prudent management of financial institutions by, amongst other things, supporting the effective operation of Boards and facilitating independent oversight of management.

Recognising the contribution of remuneration practices at large financial institutions to imprudent risk-taking leading up to the GFC, this topic has also received increased attention within the international regulatory community. One of the first responses to the GFC was the issuance by the FSB of its *Principles for Sound Compensation Practices* in 2009[9]. These Principles sought to align remuneration with prudent risk-taking, and align employee incentives with long-term profitability.

Regulatory requirements and supervision approaches also recognised the need to understand the structures institutions use to define the acceptable bounds for risk-taking. This resulted in a greater focus on the need to establish clearly articulated risk appetite frameworks[10]. Regulatory requirements for risk appetite frameworks focus on structures and approaches for communicating, understanding, assessing and monitoring the types and levels of risk across regulated institutions, and on how well this is embedded in day-to-day operations.

Although greater balance sheet strength and stronger governance, remuneration and risk appetite frameworks have increased the resilience of the financial system, they provide only a partial remedy to failings uncovered by the GFC.

The heightened attention to risk culture by prudential regulators reflects the significant contribution lax behaviours and attitudes towards risk made to the GFC. It is also a recognition that financial metrics, organisational structures and risk management frameworks are necessary but not sufficient to deliver the standard of risk management that is expected of prudentially-regulated financial institutions.

No prudential regulator has sought to prescribe an appropriate risk culture. Rather, the focus has been on understanding the extent to which the risk culture of individual institutions supports their formal governance structures and facilitates the balanced consideration and management of risk. To assist in this task, in 2014 the FSB issued *Guidance on Supervisory Interaction with Financial Institutions on Risk Culture* for supervisors, which highlighted the following indicators of risk culture:[11]

- tone from the top;
- accountability;

[8] For example see Basel Committee on Banking Supervision 1999, *Enhancing Corporate Governance for Banking Organisations* <https://www.bis.org/publ/bcbs56.htm>

[9] Financial Stability Board 2009, *Principles for Sound Compensation Practices Implementation Standards* <http://www.fsb.org/wp-content/uploads/r_090925c.pdf?page_moved=1>

[10] For example see Financial Stability Board 2013, *Principles for An Effective Risk Appetite Framework* <http://www.fsb.org/2013/11/r_131118/>

[11] Financial Stability Board 2014, *Guidance on Supervisory Interaction with Financial Institutions on Risk Culture: a Framework for Assessing Risk Culture* <http://www.fsb.org/2014/04/140407/>

- communication and challenge; and
- incentives.

This Guidance acknowledges, however, that there are many factors that influence risk culture, and that these indicators should not be viewed as an exhaustive list; rather, they provide a good high-level starting point from which risk culture can begin to be assessed.

Approaches of prudential regulators to risk culture

There have been a range of approaches adopted by prudential regulators to address risk culture, and it remains an evolving area of supervisory practice. Most of the regulatory responses can be grouped into the three broad categories outlined below, although across jurisdictions there is considerable variation in regulatory intensity and focus across these categories.

Public advocacy and education

Globally, many financial sector regulators have sought to draw attention to failings in risk culture within the financial sector, and publicly challenged the industry to do better.[12]

In the Netherlands, for example, DeNederlandsche Bank (DNB) has supplemented its public statements with guidance for industry on approaches for assessing culture, as well as publishing its observations from assessments of culture in individual institutions.[13]

The focus of other regulators' guidance has typically centred on specific indicators of risk culture such as board effectiveness, remuneration or market conduct. The goal has been to provide senior executives and directors with a clear message that the industry needs to respond to the shortcomings that have been identified, while at the same time providing helpful information and guidance that allows them to more quickly adopt better practice.

Increasing regulatory expectations

Many regulators have introduced new, or stronger, expectations in relation to risk culture. In most instances, this has involved establishing general expectations or approaches that should be used, rather than seeking to prescribe a target risk culture.

The Hong Kong Monetary Authority, for example, requires that the Board and senior management of a regulated institution *'…create a strong corporate and risk management culture and ensure that the authorised institution's risk appetite is well enshrined within the culture'*[14]. Other countries that have established specific risk culture regulatory expectations include the USA, UK, the Netherlands, and Singapore.

[12] Examples of such speeches can be found at: <https://www.newyorkfed.org/governance-and-culture-reform>

[13] For example refer to DeNederlandsche Bank 2015, *Behaviour and Culture in the Dutch Financial Sector* <http://www.dnb.nl/en/binaries/DNB%20brochure%20gedrag%20en%20cultuur%202015%20ENG_tcm47-326577.pdf?2016082504>

[14] Hong Kong Monetary Authority 2010, *Supervisory Policy Manual, General Risk Management Controls*, Section 2.1 <http://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/IC-1.pdf>

Several regulators have introduced additional expectations in areas they consider to be strong drivers of risk culture, such as remuneration. FSB member jurisdictions have, for example, implemented in some manner the 2009 *Principles for Sound Compensation Practices*.

Some regulators have also focussed attention on management accountability and how this influences risk culture. For example, in the UK the Prudential Regulation Authority (PRA) and the Financial Conduct Authority (FCA) noted that:

'...the behaviour and culture within banks played a major role in the 2008-09 financial crisis and in conduct scandals such as Payment Protection Insurance (PPI) mis-selling and the attempted manipulation of LIBOR. However, under the statutory and regulatory framework in place at the time, individual accountability was often unclear or confused. This undermined public trust in both the banking system and in the regulatory response'.[15]

In response to this concern, the UK authorities introduced the Senior Managers Regime earlier this year, which requires institutions to more clearly specify the individual responsibilities of senior managers. One of the Regime's aims is:

'...to encourage individuals to take greater responsibility for their actions, (which) will make it easier for both firms and regulators to hold individuals to account."[16]

More proactive approach to assessing risk culture

Consistent with the FSB's *Guidance on Supervisory Interaction with Financial Institutions on Risk Culture,* there has also been a move by prudential supervisors to place greater emphasis on specifically assessing risk culture, and considering how risk culture affects the safety and soundness of institutions.

Given the relatively recent focus on risk culture, most prudential supervisors have yet to publicly state how they assess risk culture, with the exception of the PRA in the UK and DNB in the Netherlands. The PRA has published details of some of what it considers to be potential indicators of a poor culture, and has stated that it assesses culture as part of normal ongoing supervisory activities.[17]

DNB has gone further than other supervisors by establishing a dedicated team which comprises experts from a range of (for a supervisor, non-traditional) backgrounds, including organisational and social psychology, to review institutions' culture[18]. DNB's approach focuses its assessment of culture on behaviours observed in specific areas. These include decision-making, leadership, communication and group dynamics. Some elements of DNB's methodology include, for example, conducting one-on-one interviews with directors and management as well as observing the operation of board and executive meetings.

[15] Financial Conduct Authority July 2014, Consultation Paper FCA CP14/13PRA CP14/14, *Strengthening Accountability in Banking: a New Regulatory Framework for Individuals* < http://www.fca.org.uk/your-fca/documents/consultation-papers/cp14-13>

[16] Ibid.

[17] Prudential Regulation Authority June 2014, *Statement of Policy: The use of PRA Powers to Address Serious Failings in the Culture of Firms* <http://www.bankofengland.co.uk/pra/Documents/publications/policy/2014/powersculture.pdf>

[18] DeNederlandsche Bank November 2015, Speech, Wijnand Nuijts, Mirea Raaijmakers, *Supervising Culture and Behaviour at Financial Institutions: The Experience of DeNederlandsche Bank*.

Developments in APRA's regulatory and supervisory approach

APRA's approach to the regulation and supervision of the related subjects of governance, remuneration, risk appetite and risk culture since the GFC has been broadly consistent with the international developments outlined above, and has drawn on the full range of approaches utilised elsewhere.

Regulatory initiatives have centred on revisions to *Prudential Standard CPS 510 Governance* (CPS 510)[19], and the introduction of CPS 220. These changes strengthened a number of existing requirements, and introduced a number of new ones. For example, APRA introduced:

- specific remuneration requirements in 2010 for ADIs and insurers, and (via a separate prudential standard) in 2012 for superannuation entities;
- a formal requirement for Boards to approve their institution's risk appetite statement from 2013 for superannuation entities, and 2015 for ADIs and life and general insurers; and
- the requirement for Boards to form a view on risk culture in 2015 for ADIs and insurers.

These regulatory changes have sought to embed the manner in which APRA's supervisory focus has evolved over time.

In 2015, APRA also established a small, central team to coordinate work and provide a centre of expertise on the related issues of governance, culture and remuneration. This team leads the development of APRA's thinking, design of supervisory practices, and coordination of industry engagement on these highly inter-related topics.

To date, APRA's work has largely been exploratory, and heavily focussed on assessing institutions' approaches to implementing the risk culture requirements of CPS 220. This has primarily occurred within the context of APRA's normal prudential review activity, but has been supplemented with useful workshops with senior industry participants, as well as engagement with interested consultants and academics. Chapter 3 outlines APRA's future priorities in the area of risk culture.

[19] APRA 2015, *Prudential Standard CPS 510 Governance*, <http://www.apra.gov.au/CrossIndustry/Documents/Final-Prudential-Standard-CPS-510-Governance-(January-2014).pdf>

Chapter 2 – APRA's observations on risk culture

In late 2015, APRA commenced an information gathering exercise in relation to industry practices with respect to risk culture. This exercise included discussions with a significant number of APRA-regulated institutions across the ADI, insurance and superannuation sectors. APRA also held three roundtables with directors to explore how Boards approach and view their role in relation to risk culture. In addition, APRA met individually with a number of directors of regulated institutions to discuss institution-specific deliberations on risk culture.

APRA also met with external practitioners, including consultants and academics, as well as with foreign regulators.

This chapter summarises the common observations and issues that participants raised during these discussions. The observations primarily emphasised the challenges involved in better understanding:

- the prevailing risk culture within an institution; and
- the ways that it can be influenced.

Approaches to risk culture

A common theme of the discussions was that approaches to understand and manage risk culture are at a relatively early stage of development: most APRA-regulated institutions' efforts to date have been focussed on the initial task of understanding and assessing the *current state* of risk culture. The catalyst of this effort was generally attributed to the introduction of CPS 220 and efforts by APRA-regulated institutions to meet the new requirements, although many institutions were endeavouring to understand and assess their risk culture to deliver broader business benefits rather than simply fulfil a regulatory compliance obligation.

All institutions viewed risk culture as a sub-set of organisational culture. Although similar definitions of risk culture have been adopted by institutions, consultants and regulators, institutions noted that a key challenge is ensuring that there is consistent understanding of the drivers of risk culture.

The early stage of industry's risk culture development also reflects the need within institutions to more deeply understand the complexities of risk culture and behavioural drivers. This was viewed by some participants as a key step to 'operationalise' risk culture within an institution and to facilitate meaningful action.

Defining risk culture

Some examples of how institutions have defined risk culture are set out below.

'…the norms and traditions of behaviour for individuals and of groups within an organisation that determine the way in which they identify, understand, discuss and act on the risks an organisation confronts and takes.'

'…reflects the underlying mindset….it lies at the heart of how… staff think and behave. Culture shapes and influences attitudes and behaviours…. and how to deal with dilemmas when they come up. It is about doing the right thing, with good outcomes…'

'…is employees understanding and living 'do the right thing'. It's about taking the right risk, with the right controls for the right return.'

'the system of values and norms of behaviour that shapes the decisions and actions of staff. It determines the collective ability…to: identify, understand, openly discuss and act on both current and future risks to the organisation; operate consistently within the risk appetite; and ultimately achieve the strategic goals and objectives of the organisation.'

Variance in approaches

The approaches to understanding and assessing risk culture varied by institutional size, business mix and complexity. Approaches were also influenced by institutions' areas of focus and triggers for considering risk culture. In some cases, risk culture efforts formed part of a broader program of work on organisational culture. In other cases the focus on risk culture was a specific program of work.

There was variation in the degree to which risk culture programs concentrated on specific business units or the institution as a whole. Larger institutions noted that size and complexity introduced additional challenges, particularly regarding the greater prevalence of sub-cultures. In these instances efforts were segmented, often by geography or business unit.

Target state

CPS 220 requires that a Board not only forms a view of risk culture but also:

'…identifies desirable changes to the risk culture and ensures the institution takes steps to address those changes'.

To identify desirable changes and progress, some institutions that were further advanced highlighted the need to define and work towards a target or aspirational state. While recognising that culture is dynamic, it was noted that an aspirational state was useful to guide and prioritise culture-specific initiatives. Less work has been undertaken by industry to define a target state of risk culture.

Role of the risk function

For the majority of institutions, risk culture-specific work was being undertaken within the risk function (i.e. the second line of defence in the 'three lines of defence' risk management and assurance model)[20]. For institutions that were further advanced in implementing risk culture programs, greater emphasis was given to the clarity of responsibilities between first line and second line of defence functions. In their view, it was necessary that frontline business units were the ultimate owners of both risk and risk culture.

Leadership

All institutions were clear on the central role of leadership in shaping and driving both organisational and risk culture. The role of leadership also features prominently in academic literature. The FSB's *Guidance on Supervisory Interaction with Financial Institutions on Risk Culture* refers to this as *'tone from the top'*.

Senior executives

Senior executives were almost universally acknowledged as one of the most powerful influences on risk culture. In particular, institutions saw the role of Chief Executive as pivotal in shaping the institution's risk culture.

The significance of the Chief Executive and senior executive roles was attributed to the direct and highly visible nature of the interactions between them and employees. Senior executives were seen as having an immediate and tangible impact on behaviours both through communication (what they said) and role modelling (what they did). Institutions noted the direct impacts on behaviour and risk culture where there were disconnects – both real and perceived – between stated values and actual behaviours. Employees were seen to be particularly aware of instances of *'do as I say, not as I do'*.

Boards

In their engagement with APRA, directors acknowledged the importance of the Board's role in supporting management to establish a sound risk culture. External practitioners also highlighted the influence Boards can have in shaping risk culture within an institution. For instance, directors are able to influence risk culture through their oversight and governance role, their interactions with senior executives and employees, and their influence in senior executive appointments. How the directors' involvement in these issues are perceived provides strong behavioural signals for staff. In this way, directors contribute an important element of *'tone from the top'*. To be effective, it is critical that the (implicit and explicit) messages from directors about what behaviours are important are consistent with those emanating from senior executives.

[20] APRA January 2015, *Prudential Practice Guide CPG 220 – Risk Management*, Appendix A <http://www.apra.gov.au/CrossIndustry/Documents/Prudential-Practice-Guide-CPG-220-Risk-Management-January-2015.pdf>

Assessing senior executive and Board behaviours

Institutions used a number of methods to assess the behaviours of individuals in leadership positions. Two examples were the use of 360 degree feedback mechanisms and, in a similar vein, Board performance reviews.

It was unclear from discussions, however, whether assessments such as these were systematically being incorporated into work that institutions were undertaking to understand the current state of their risk culture. These reviews can provide valuable insights into behaviours and attitudes that can be brought together to provide insight into cultural interplays and group dynamics at the leadership team level – both for senior executives and Boards.

Purpose and values

What an institution really values and sees as important will be evidenced by the behaviours of its staff. Institutions that had attempted to get a deeper understanding of their risk culture indicated that clarity and a shared understanding of organisational purpose and values were central to driving cultural and behavioural outcomes.

For this reason, these institutions, and a number of consultants, felt strongly that there needs to be clear alignment between organisational purpose, stated values and actual behaviours. Institutions acknowledged that this was a challenge, as there could at times be some misalignment between stated values and perceived values (as demonstrated by behaviours). In particular, culture was often referenced as a critical element in framing how decisions are made when there are 'competing tensions', 'moments of truth' or 'dilemmas'. Decision-making in these circumstances, and what gets priority, is framed by behaviour and culture. Most institutions had organisation-wide values, but acknowledged practical difficulties in making these meaningful as behavioural drivers. Institutions that were actively seeking to refine and embed cultural change reiterated that organisational purpose and values needed to be a key reference point ingrained in all decision-making.

Using organisational purpose and values to frame behavioural expectations

In an attempt to provide greater clarity, some institutions have introduced behaviour guides that are used to provide examples of values in practice. A number of the guides that APRA reviewed provided specific examples of decisions and dilemmas. Institutions are also starting to incorporate behavioural assessments in performance management processes. This is designed to capture 'how' performance is achieved and not just 'what' is delivered. In the more sophisticated cases, performance review processes include upside potential for behavioural elements.

Assessment, metrics and insight

A wide range of tools are being used to gain insights into the current state of organisational and risk culture.

In discussing these tools, a common challenge regularly identified in discussions with APRA was the way in which the information gleaned from various tools could be brought together, or 'triangulated', to provide meaningful insights into risk culture. Challenges were also noted in identifying predictive, or leading, indicators of behaviour and risk culture. Between institutions, the level and sophistication of assessment tools varied considerably.

Despite the recognised challenge in gaining insight into risk culture, institutions consistently asserted to APRA that their risk cultures were broadly 'good' or 'strong'. Institutions did, however, acknowledge that risk culture was an issue within their industry. This view that any problems lay elsewhere suggests the need for a deeper analysis and understanding of risk culture across the entire financial sector.

Surveys

Most institutions employ staff surveys. These may be internally or externally facilitated. Different survey approaches for risk culture are used, and include:

- drawing on findings from staff engagement surveys to provide risk culture insights;
- including risk-specific questions in engagement surveys; and/or
- conducting risk culture specific surveys.

Most institutions deploy surveys due to ease of use and applicability across an entire organisation. However, institutions also highlighted some limitations of survey-based approaches. For example, where a survey was specific to risk management, or risk culture, some noted that this could subtly trigger risk-aware responses and that individuals were 'primed' to respond accordingly; as a result, survey responses and results may not reflect actual behaviour.

Survey design was seen as critical in generating valid and reliable results. Responses to surveys were noted as being influenced by individuals' perceptions. A common example given was the design of questions and whether these asked the individual to comment on their own behaviours or their perception of the behaviours of those around them. A number of institutions noted that most people have a positive view of their own behaviour and that survey responses reflect this; respondents are more likely to be open-minded when commenting on those around them. In summary, staff often judge themselves based on their intent, but judge others based on observed impact.

Similarly, where managerial performance metrics included responses to survey outcomes (such as employee engagement), some institutions noted that this could result in undue influence being exercised on responses. Though this approach may produce results that align to performance metrics, it may not be conducive to generating an accurate reflection of staff views, and therefore could undermine the value of surveys.

Survey fatigue was another issue raised. Some institutions noted that the frequency of issuing surveys to staff, including those not related to risk culture, could result in less

considered responses being received. These institutions aim to coordinate the timing of all surveys as a way to mitigate the risk that they are not taken seriously.

Surveys were often supplemented with focus groups and interviews. These were designed to explore identified issues in greater detail and to understand underlying root causes of behaviours and perceptions. Focus groups and interviews were also used to a greater extent in institutions that emphasised face-to-face interaction as a means of understanding behaviour and culture.

Reporting and dashboards

As with surveys, many institutions are attempting to develop or refine management reports that can be used to provide a snapshot of the current state of risk culture. Reports and dashboards primarily leverage existing data, with a wide variety of metrics in use for this purpose. Some typical examples include breaches of risk limits, trends in risk reporting, whistleblower reports, compliance breaches, loss events, exit interviews, code of conduct breaches, employee communications, completion of training programs, response to audit issues and number/type of complaints.

Reports and dashboards observed by APRA generally varied in accordance with the sophistication of institutions' understanding of, and approach to, risk culture. Where institutions were looking to refine risk culture, metrics were aligned to known points of cultural influence. In those institutions where reporting on risk culture was relatively new, metrics were based more on the current state of risk culture.

Institutions raised a number of challenges around developing reports and dashboards that accurately summarise the state of risk culture. Some of these challenges include:

- accuracy and accessibility of underlying data;
- aggregation of data across tools, functions and business units;
- determining the appropriate frequency of reporting on changes in risk culture;
- ability to identify leading indicators of risk culture; and
- identifying meaningful measures of behaviour.

Institutions that were further advanced in developing risk culture reports are combining risk and human resources data to gain additional insights into risk culture. Examples of such data sets include code of conduct warnings, untaken leave, limit breaches, and significant budget outperformance. The sources of such information often sit across different information systems, and institutions highlighted the challenges this creates in bringing the information together in a simple, timely and effective manner.

Reporting data and insights

One institution has been reviewing risk and human resources data to consider how these can be combined and used as a leading indicator. It is observing this data over an extended period of time to determine whether any risk events or breaches could have been predicted. The institution is considering how to apply these combined data points in a forward-looking manner.

Reviews and assurance

The ability to reliably assess risk culture was viewed by some institutions as requiring specialist skills. These institutions felt there were limits within existing resources, and therefore are increasingly engaging independent parties to undertake risk culture reviews. In pursuing these engagements, some institutions are looking beyond traditional financial skill sets to employ a more cross-functional, multi-disciplinary approach to risk culture.

The common types of review and assurance work observed by APRA are set out below.

Internal audit

There is increasing consideration being given to how risk culture can be incorporated in internal audits – both as a stand-alone review and as a component of all reviews. Internal audit teams were seen as having good exposure across all aspects of an institution, and as a good mechanism by which consistent and continuous assessments can be made. As a result, some organisations have begun programs in which internal audits include a report on cultural aspects of the business unit being reviewed.

However, the potential lack of specialist behavioural assessment skills was raised as an issue by a number of institutions as a challenge that is yet to be satisfactorily addressed.

Internal audit

One institution has established a team within its Internal Audit unit that is responsible for assessing risk culture. The team consists of organisational psychologists and behavioural scientists who undertake a range of risk culture assessment activities. This includes in-depth reviews of risk culture as a complement to traditional internal audit activities. The team has assisted with developing tools that allow business units to self-assess risk culture through identifying positive and negative behaviours. The team also provides risk culture training.

External providers

A number of institutions indicated they had used external providers to assist with developing risk culture frameworks, or to review the risk culture of a specific function or business unit. In engaging external providers, the main objective was to leverage specialist skill sets.

A number of external providers deploy social science disciplines, notably organisational psychology, within risk culture review work. This includes developing models in which academic theory and research from both social sciences and behavioural economics is deployed to provide insight into risk culture. In some cases, a combination of surveys and interviews generate insights into behaviours at an individual and social level. Qualitative and quantitative data points are then applied in the various providers' proprietary models to form views about how staff will behave when faced with risk decisions.

Reviews of supporting frameworks and governance structures

Some institutions have undertaken work to assess whether purpose and values are central to the way they operate. In these cases, institutions indicated they had reviewed core documentation (some had engaged external support for this activity), including their strategy,

risk appetite, policies and procedures to determine whether the values that these implied were aligned to their organisation's stated purpose and values. Some of these reviews found some degree of misalignment in specific areas. This has often led to institutions revising policies and practices to better align with organisational purpose and values.

Review of alignment to organisational purpose and values

One institution (with assistance from an external firm) undertook a review of its policies and structures to determine where these embodied, or where they undermined, its stated values.

One of the core tenets supporting the institution's purpose is that there is a focus on deepening the relationship with existing customers in preference to acquiring new customers. The review found that pricing for a particular product was mis-aligned to the institution's purpose, favouring new customers over existing ones. As a result, changes were made to supporting frameworks to ensure organisational purpose and values were a central reference point in how the institution made its decisions. Product pricing and approval processes were adjusted to ensure that existing customers were always entitled to the best rates on that specific product. This was viewed as a key mechanism for strengthening organisational culture and guiding behaviour consistent with organisational objectives.

Informal approaches

Some institutions highlighted that, notwithstanding the increasing sophistication associated with the more systematic risk assessment tools outlined above, they continued to place a degree of reliance on insights from informal interactions with staff across the organisation. It was readily acknowledged that this observational approach is clearly subjective. Both directors and senior executives, however, considered that these interactions are an important complementary mechanism to form views on the state of both organisational and risk culture.

Risk maturity

The size, scope and complexity of institutions that APRA regulates varies widely, and this results in differing levels of sophistication and maturity of risk management frameworks. This can influence both the state of risk culture within an organisation, and the attention it receives.

The maturity of risk management within institutions, and clarity of responsibilities across the three lines of defence model, were viewed as important influences on risk culture by many institutions. These relate both to staff capability to understand risk issues, and the degree to which risk management frameworks are genuinely embedded in day-to-day operations.

In a number of institutions where the risk management framework was less sophisticated, efforts were concentrated on embedding the risk management framework across all operations. Risk culture considerations in these cases appeared to be less developed.

Some differences across industries were also apparent with, in general, ADIs and insurers appearing further advanced in their approaches to understanding and managing risk culture than superannuation entities. This reflects, at least in part, that the risk culture requirements for ADIs and insurers set out in CPS 220 are stronger than those currently applicable in *Prudential Standard SPS 220 Risk Management*[21], which applies to superannuation entities, as well as the different operating models within the industries. Over time, however, APRA expects to align its expectations in relation to risk culture to all regulated sectors.

Risk appetite

Risk appetite was identified as a foundational element of a sound risk culture in the FSB's *Guidance on Supervisory Interaction with Financial Institutions on Risk Culture*. Using risk appetite statements as a tool to support conversations about risk within business units was considered by institutions as an important indicator of risk culture. Many institutions are currently considering both the extent to which risk appetite is used by leadership to drive effective risk management, and as a core component of the risk management framework.

Risk appetite and risk culture

One institution has revised its risk appetite statement to capture the key tenets of its approach to risk culture. This includes expression of the interaction between purpose, values, behaviours and risk management. Articulated values and behavioural expectations are set out in the risk appetite statement, to which qualitative statements of risk appetite are aligned. Bringing these elements together was viewed as being a key mechanism for aligning risk decisions with behavioural expectations.

[21] APRA July 2013, *Prudential Standard SPS 220 Risk Management* <http://www.apra.gov.au/Super/PrudentialFramework/Documents/Final-SPS-220-Risk-Management-July-2013.pdf>

Chapter 3 – APRA's supervisory priorities

APRA's overarching objective is for regulated institutions to establish and maintain sound risk cultures that are aligned with their organisational objectives, values and risk appetite. Doing so will reduce the potential for undesirable behaviours to jeopardise institutions' financial well-being.

Experience indicates that institutions often fail to identify deficiencies in their risk culture until after suffering a major loss. In the Australian context of an extremely long period of economic expansion and generally sound prudential outcomes, it is sensible to observe and learn from the travails of others. There are a number of useful lessons available from the North Atlantic experience during, and following, the GFC. One such lesson for APRA is that there is an important role for prudential supervision to encourage a strong focus on risk culture within regulated institutions. Based on recent discussions, the vast majority of the regulated financial sector supports that proposition.

Institutions possessing a clear view of the risk culture they desire, and an understanding of the extent to which their current risk culture differs from this target state, will be better placed to create and maintain sound risk cultures. But creating and maintaining a desired risk culture represents a material challenge and requires on-going care and attention. Understanding and accepting these challenges will help institutions to proactively reduce the risks that arise from a poor risk culture, and reinforce investments in risk governance, risk management and balance sheet strength that have occurred since the GFC.

That is not to say that a sound risk culture can prevent all undesirable behaviour, or all material losses. But a sound risk culture can, all else being equal, reduce both the frequency and impact of behaviour-driven losses. A sound risk culture will also contribute to increased public trust in financial institutions and the financial sector more broadly.

Each individual institution has its own risk culture, and each risk culture should ideally reflect the fact that each institution has its own business objective and values. APRA therefore has no intent to try to impose a common risk culture across prudentially-regulated entities, or prescribe the specific characteristics of a 'good' risk culture. It is likely, however, that APRA will over time identify practices and approaches that are associated with (or undermine) a sound risk culture, and will share these observations with regulated institutions and other relevant stakeholders.

Consistent with this principles-based approach, APRA's focus will be on the supervision of institutions' risk culture, rather than the regulation of risk culture. In particular, APRA will continue to develop and evolve its supervisory approach with a view to strengthening its capacity to more systematically assess a regulated institution's risk culture. When needed, APRA will apply greater supervisory focus to institutions that are either unwilling or unable to address behaviours which are inconsistent with prudent risk management practices.

In the medium term, it may be appropriate to refine the regulatory framework, including both prudential standards and guidance material, in relation to risk culture. At the present point in time, however, no specific changes to regulatory requirements beyond the general alignment of prudential requirements across regulated sectors are planned.

The current state of the art, both in Australia and internationally, in relation to assessing risk culture continues to evolve, and has not yet reached the point where widespread expertise on risk culture is readily available. Given the increased attention being given to the issue, however, it is likely that such expertise will develop over time. APRA's own supervisory expectations of risk culture will also evolve. To expedite APRA's own expertise on risk culture, in 2015 APRA established a dedicated Governance, Culture and Remuneration risk specialist team. This small team will work with APRA's supervisors to drive the development of APRA's thinking, supervisory practices and industry engagement on these important issues.

Specific areas of APRA focus

Continue to encourage APRA-regulated institutions to focus on risk culture

APRA's initiatives that will help maintain the prominence of risk culture within regulated institutions include:

- engaging with the broader APRA-regulated financial sector – through, for example, speeches and publications such as this one – to reinforce the need for continued focus on risk culture and, where needed, highlighting any areas of concern;
- providing information and guidance to industry, where appropriate, on approaches that can be used to assess and strengthen risk cultures;
- bilateral discussions with institutions' senior executives and directors to highlight and seek remediation for any specific concerns that are identified through routine supervision activities; and
- conducting pilot on-site reviews at individual institutions focussing specifically on risk culture.

A more anticipatory supervisory approach to risk culture

Although APRA already considers risk culture as part of its ongoing supervisory activities, APRA intends to refine and sharpen its approach to assessing risk culture. Conducting pilot risk culture reviews will form a key component of this work.

APRA expects that this more intensive review will enable it to better anticipate potential risk issues, and strengthen its forward-looking supervisory approach. For example, where a regulated institution is found to have indicators of a poor risk culture, supervisory attention will correspondingly increase. As with APRA's more general approach to supervision, which focusses on the prevention of problems before they materialise, the goal of these risk culture reviews will be to promote prompt corrective action to any shortcomings identified, or establish mitigating actions. In doing so, the potential for loss from unbalanced and ill-considered risk decisions is reduced, potentially adverse outcomes for depositors, policyholders and superannuation fund members can be avoided, and (in the extreme case) threats to financial stability are eliminated.

Reviewing industry remuneration practices

The remuneration requirements contained in CPS 510 were introduced in 2010 for ADIs and insurers. Requirements for superannuation were introduced in *Prudential Standard SPS 510 Governance*[22] in 2012. The fundamental principle underlying these requirements is that performance-based components of remuneration must be designed to encourage behaviour that supports:

- the regulated institution's long-term financial soundness; and
- the risk management framework of the institution.

Remuneration frameworks, and the outcomes they produce, are therefore important barometers and influencers of risk culture.

APRA intends to conduct a stocktake of current industry remuneration practices to gauge how well existing requirements are being implemented, and how they are interacting with the risk cultures of regulated institutions. This will include reviewing the remuneration arrangements and outcomes for some senior executives, risk and control staff, and material risk-takers at a sample of institutions.

APRA will also use this opportunity to compare its remuneration requirements with more recent international regulatory developments and supervisory practices.

This work will commence in 2016 and will continue into 2017. APRA will engage with industry participants, as well as relevant industry experts, throughout this period as it formulates its views.

[22] APRA November 2012, *Prudential Standard SPS 510 Governance*, <http://www.apra.gov.au/Super/PrudentialFramework/Documents/Final-SPS-510-Governance-November-2012.pdf>

APRA