



# **STAY AHEAD OF THE RISK: RISK GOVERNANCE AND RISK CULTURE**

**IAN LAUGHLIN**



**Member  
Australian Prudential Regulation Authority**

***Institute of Actuaries of Australia, Sydney  
20 May 2013***



**Stay ahead of the risk:**  
**Risk Governance and Risk Culture**

**Ian Laughlin**  
20 May 2013



**Soft skills** ....cluster of personality traits, social graces, communication, language, personal habits, friendliness, and optimism that characterize relationships with other people.

Source: Wikipedia

I want to talk today about risk management matters that are simultaneously both softer and harder than many other aspects of risk management - softer in the sense that they require "soft skills" to get the best outcome; harder in the sense that they are challenging to understand and manage.

Those matters are risk governance and risk culture.

APRA is increasing the attention it gives to both risk governance and risk culture, and in the process further developing our thinking and supervisory practices.

Understanding their importance to APRA is fundamental to staying ahead of the curve in risk management!

First, a bit of history to give context:

### Prudential standards

APRA has always regarded sound risk management as fundamentally important to the prudential management of an institution, in tandem with sound capital management. In

simple terms, risk management helps an institution avoid financial difficulties and capital helps protect customers once a problem has occurred.

For some years, risk management requirements were embedded in various places in our prudential standards.

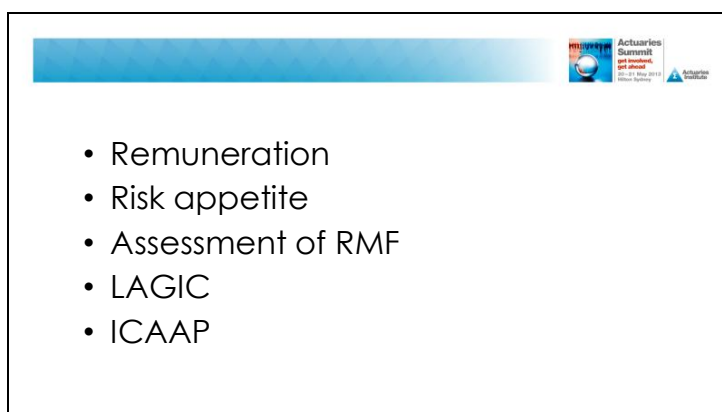
We then started producing dedicated prudential standards for risk management, starting with general insurance in 2002, through to this year with the new superannuation risk management standard, and culminating in the draft consolidated cross-industry standard issued on 9<sup>th</sup> of May, covering ADIs, life insurers and general insurers.

Over time, the prudential standards have become more comprehensive. For example, in the draft just issued, risk governance is given more attention and there are new requirements - in particular for a CRO and board risk committee.

#### Other APRA developments

Our supervision has of course long paid close attention to each institution's risk management, and how well it meets the requirements, and indeed the spirit and intent, of the prudential standards.

We also have sought to lift standards across the industry, as illustrated by the following:



- In 2010, we introduced requirements for a remuneration policy. One of our intentions here was that remuneration arrangements encourage behaviour that supports the institution's long-term financial soundness and its risk management framework. Since then we have provided feedback and guidance to institutions about these policies.
- In recent years we have stressed the importance of a clearly articulated risk appetite statement, which is then embedded in the operations of the business. We have developed and made public our broad approach to the assessment of a risk appetite statement and provided supporting commentary in various speeches. We have engaged boards in discussion on risk appetite and its importance, and we are now seeing a marked improvement in the articulation and use of risk appetite statements.
- For some years, there has been a requirement for the Appointed Actuaries of insurance companies to assess the suitability and adequacy of the risk management framework. In 2012, we reviewed this work and concluded that significant improvements could be made. We worked with the Actuaries Institute and

Appointed Actuaries and we are now finding these assessments are markedly better, and so of much greater value to the insurers and to APRA.

- As you know, our LAGIC capital standards for insurers came into force from the start of this year. Amongst other things, LAGIC introduced more risk-sensitive capital requirements, thus strengthening the link between capital and risk management.
- This is reinforced by the ICAAP, requirements also introduced by LAGIC. The ICAAP must include a description of the arrangements in place to monitor and manage risks and the capital held against those risks. It also must include stress testing and scenario analysis, both important tools for assessing risks.

### Ongoing development

So you can see there has been a pattern of ongoing development of our risk management requirements over the years. I now want to talk about the next phase of that development.

Before I do that, I want to make an important point: Our work on risk governance and risk culture does not mean that we will divert attention from more established areas of risk management, or that we see limited opportunities for improvement in those areas. Rather, we consider that there remains considerable room for improvement in many institutions, and our supervision will reflect that.

### Risk Governance

Let's turn now to risk governance.



**Governance** refers to the actions, processes, traditions and institutions by which authority is exercised and decisions are taken and implemented.

**Risk governance** applies the principles of good governance to the identification, assessment, management and communication of risks

Source: International Risk Governance Council

Many elements of our requirements for the risk management framework contribute to risk governance. For example, board audit and risk committees, the risk management strategy, risk appetite, regular reviews of the effectiveness of the framework and so on. So risk governance is woven through the risk management framework.

In other words, **effective risk governance is a fundamental requirement for high quality risk management.**

The board's role here is particularly important. In a more general sense, an institution's board plays a critical role in its prudential management. The board has specific responsibilities in this respect under the law and through APRA prudential standards. More


importantly, the board sets standards and expectations that have a profound influence on the culture and management of the business, and on the quality of its governance.

This means that the board plays a critical role in *risk* governance.

Because of his or her pervasive influence on the institution, the CEO also plays a fundamentally important role in risk governance.

So while the contribution of others is important, my comments today are going to focus on the board and CEO.

Here are some of the present APRA requirements for boards and CEOs that touch on risk governance:



- Fit and proper
- Composition of board
- Composition of audit, risk committees
- Risk management strategy
- Risk appetite statement
- Declarations by the CEO
- ICAAP and the board's oversight

These might be considered some of the more operational aspects of risk governance, requiring **hard skills**. The real challenge lies in bringing all of this to life, so that risk governance is highly effective. And that also requires **soft skills**.

To help you better understand this, let me hark back to a recent speech by APRA's chairman, John Laker<sup>1</sup> on good governance. He referred then to APRA's PAIRS<sup>2</sup> system for rating risks within an institution and its coverage of risk governance. Here is part of what he had to say:



- Clear direction and leadership, risk appetite, risk strategy and business strategy
- Effective reporting against policies
- Risk appetite embedded
- Promotes culture - integrity and prudent approach
- Strong and independent compliance and IA

<sup>1</sup> Laker, J. *The Importance of Risk Governance*, Australian British Chamber of Commerce, 27 February 2013

<sup>2</sup> PAIRS - *Probability and Impact Rating System* June 2012  
<http://www.apra.gov.au/CrossIndustry/Documents/PAIRS-062012-External-version.pdf>

"To be rated 'low risk' on risk governance, a board would need to demonstrate, *inter alia*, that:

- it is providing clear direction and leadership for the institution, evidenced in a clearly articulated risk appetite statement, risk management strategy and overall business strategy;
- effective reporting, with metrics showing performance against board policies, flows up to it regularly;
- the risk appetite framework is clearly embedded in the institution;
- the board promotes, through both actions and words, an organisational culture that expects integrity and a prudent approach to risk; and
- there is a strong and independent compliance framework and internal audit function.

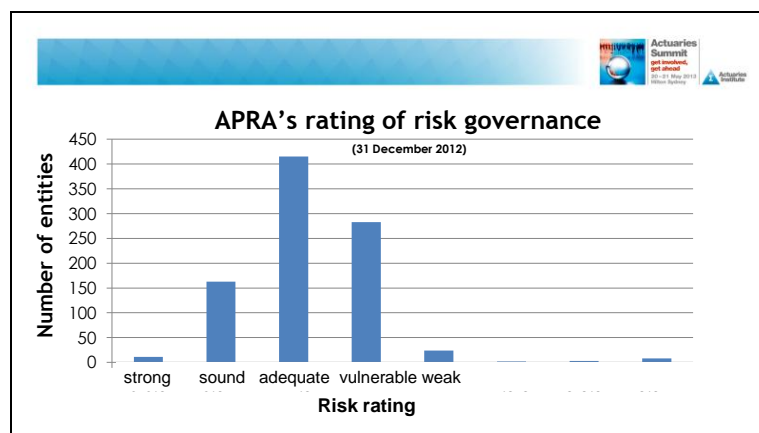
*In this area, our ratings are based very importantly on our on-site reviews, as well as on reviews of board papers and minutes. This 'tyre-kicking' gives insights into the quality and effectiveness of reporting to the board, including from board committees; the level of management oversight and follow-through of issues raised by the board; the escalation of issues from internal audit; and whether compliance issues – bad news and good – are raised in a timely fashion.*

*Our supervisors also review relevant documentation on the risk management framework..... "*

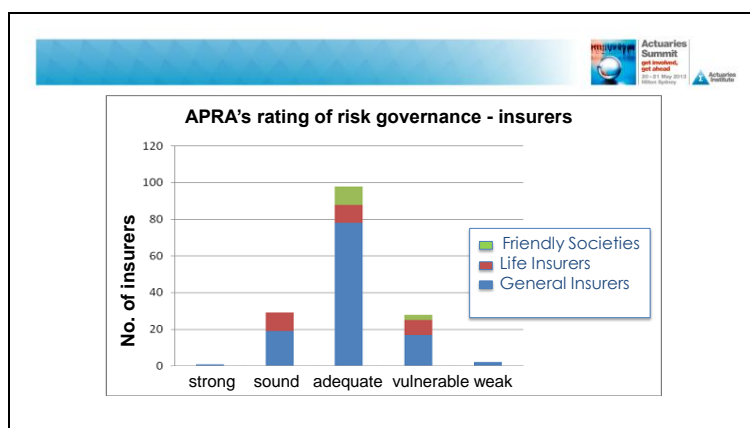
Dr Laker went on to say:

*"What marks out a good board is its activism in embedding a strong risk culture throughout the institution. Behaviours, not structure."*

He then showed the distribution of our ratings for risk governance for all institutions. You can see that a significant proportion was rated vulnerable or weak, and a large number only rated adequate.



A similar, but slightly better picture emerges for insurers alone:



It also is instructive to look at some of the reasons for institutions being rated vulnerable or weak on risk governance. Here are some examples:

- Lack of direction from board
- Risk appetite and tolerances clear
- Board over-reliance on management/actuaries
- Deficiencies in controls, monitoring and reporting
- Risk culture not embedded
- KPIs not aligned with RMF
- Compliance risk management culture
- One person in multiple roles (e.g. AA, CFO, CRO)
- Responsibility for risk management not clear
- Underqualified risk management function


I won't run through this list, but a quick scan of the slide will give you a feel for the sort of issues we encounter. You can see that a number of them represent quite fundamental weaknesses in risk management.

As I have just said, we currently assess risk governance under the PAIRS system and this contributes to the overall risk rating we give to the institution. What we now intend to do is to gradually increase the attention we give to risk governance.

This means that we will be paying more attention to risk governance in our prudential reviews and in our interaction with boards and the CEO. We will be looking to see that the quality of risk governance is being actively assessed, monitored and managed with a clear understanding of its current state and a plan to address any deficiencies.

At the same time, we are proposing (through the consolidated prudential standard issued for consultation on the 9<sup>th</sup> May) to tighten the operational aspects of risk governance. In particular, there will be a need for a board Risk Committee and for a Chief Risk Officer (who must have unfettered access to the board or risk committee).

## Risk Culture




**Culture** ... the predominating attitudes and behaviour that characterize the functioning of a group or organization.

Source: The Free Dictionary

Let's now consider risk culture.

Culture is often described as "the way we do things around here". So a good working definition of risk culture for our purposes is "the way we do risk around here".

For an institution's risk management framework, including its risk governance, to be effective, there must be a strong risk culture which is consistent with the company's espoused values and its risk appetite. Let's break that down a little:



- Risk appetite clear and unambiguous; widely used
- Espoused values clear and consistent with the risk appetite and business strategy
- Values embraced; decisions consistent with values;
- Decision-making clear; consistent with risk appetite and business strategy.

- The risk appetite must be clear and unambiguous; it must be widely used in the management and governance of the institution;
- The institution's espoused values must be clear and consistent with the risk appetite and business strategy (and vice versa);
- The values must be embraced at all levels of the institution, and all significant decisions and actions must be consistent with those values;
- The decision-making process must be clear and consistent across the institution and it should embrace constructive and credible challenge. It also must be completely consistent with the risk appetite and business strategy.



So how on earth can risk culture be assessed by the board (or by APRA)? There isn't a simple answer to this question, but here are some thoughts that might help:

- We know of one regulator<sup>3</sup>, who has engaged a team of psychologists to help with their assessment of an institution's risk culture. I suspect you will be pleased to know that, as interesting as the idea is, we don't intend to go down that path. However, their thinking may be a useful reference for management and board.
- We also are aware of Australian financial institutions<sup>4</sup> engaging external firms to formally assess their risk culture, so clearly there are established assessment services in the market.
- Many institutions already conduct culture surveys of some sort, and some judicious amendments might help specifically assess risk culture.
- Another approach could involve focus groups of staff at various levels and in different parts of the institution - for example to help assess the true level of support for the institution's espoused values.
- Both the risk function and internal audit inevitably would have opportunities in the course of their work to observe the risk culture throughout the business - for example they might see inconsistency with the risk appetite statement or a decision to over-ride policy. They could be required to form views on the risk culture they observe and include commentary in their regular reports.

No doubt there are other techniques that would be effective. The point is that a systematic approach will give far greater insights than would otherwise be obtained. In turn, a better assessment of risk culture will enable it to be more strongly influenced and directed.

### Challenge for APRA

APRA needs to form a view of the quality of an institution's risk governance and its risk culture. We then need to factor this into our supervisory activities, and influence the board and management as required.

To help with this, we plan to enhance our interaction with boards. This will include occasional less formal meetings with chairs of the board and the risk committee, as well as continuing our meetings with the full board. We intend to rely heavily on the board's own assessments of both risk governance and risk culture, and so will be strongly encouraging boards to form firm views and understanding of each. To help the board assessment and to drive necessary change, we intend to pose a series of questions for consideration by the board. Some of these will help address the formal requirement in our prudential standards<sup>5</sup> for assessing the Board's performance relative to its objectives.

---

<sup>3</sup> De Nederlandsche Bank, *Interim report on DNB's supervision of behaviour and culture*, December 2011. <http://www.dnb.nl/en/publications/dnb-publications/other-documents/dnb267601.jsp>

<sup>4</sup> For example, see Australian Financial Review, 4-5 May 2013

<sup>5</sup> See CPS 510 paragraph 35

### For consideration by board



- RA, risk & business strategy – consistent, embedded?
- Values - tone at top/bottom?
- Risk culture – aspiration? Assessment?
- Rem & KPIs support risk culture?
- Decision-making quality & consistency?
- Info complete, accurate & timely?
- Quality of risk governance – assessment?
- CRO & business – balance?
- Risk/return balance – credible challenge?

Let me finish with some examples of what we might ask the board to consider:

- Is the board satisfied that the risk appetite statement, risk management strategy and overall business strategy are clearly articulated, cohesive, understandable and embraced by management? How does the board satisfy itself that they are not just a nicely crafted set of words, but rather are embedded in the decision-making and operations of the business?
- How does the board satisfy itself that the espoused values are truly supported by management and staff at all levels? In other words, is the ‘tone at the bottom’ the same as the ‘tone at the top’? What is the board doing to address any inconsistencies?
- Does the board have a clear view of the risk culture to which it aspires for the institution and how does it assess the prevailing risk culture?
- Do remuneration and KPIs consistently support and drive the desired risk culture?
- How does the board gain a clear understanding of the quality and consistency of decision-making throughout the business and is it satisfied that this is driving an appropriate risk culture? How does the board satisfy itself that decision-making is consistent with risk appetite and business strategy.
- Is the information provided to the board to support its risk governance role comprehensive, complete, accurate and timely?
- How does the board satisfy itself of the quality of the institution’s risk governance? How does the board assess its own performance in this area?
- How does the board satisfy itself that the engagement between the business and the CRO is effective and strikes an appropriate balance?
- Is any unusually profitable part of the business subject to constructive and credible challenge about the risk/return balance?

Finally, even though much of what I have mentioned today involves the board, those in senior management and risk management (and I am sure that includes many in the room today) should ask themselves how they can help the board effectively consider and address the issues raised today.