Governance and Regulation: Has the pendulum swung too far?

John K Morgan – Partner, Allens and Senior Visiting Fellow, University of NSW

13 May 2014

Directors Forum

Finity Consulting
“APRA does not understand the distinct roles of boards and management”

Alan Cameron AO,

at CIFR Workshop: Financial System Inquiry 7 May 2014
The Larger Debate – especially around FSI

- The perimeter of (prudential) regulation
- The methods of regulation – principles, rules, standards, enforcement, supervision, reliance on self regulation etc
- A shift from structure to behaviour (internal culture of the organisation and the culture of the external relationships of the organisation with suppliers, customers, competitors, regulators etc)
- The theory is the internal shall inform and protect the external
- So for today’s discussion
  - Risk Committee and Chief Risk Officer – internal structural changes that impact the structure and delegation of the Board management function
  - Risk culture – regulation of the internal behaviour of institutions
Where is APRA coming from?

- APRA has a single stakeholder mandate in its enabling legislation and the Prudential Acts

  "APRA has a ‘single purpose’ mission to ensure that, under all reasonable circumstances, regulated institutions meet their financial promises to depositors, policyholders and superannuation fund members. We are not distracted from that mission, or conflicted, by … ‘highly politically sensitive issues’ such as consumer protection and anti-money laundering work …”

  John Laker, Chairman of APRA, December 2010

- Main object of *Insurance Act 1973*

  2A(1) *The main object of this Act is to protect the interests of policyholders and prospective policyholders under insurance policies (issued by general insurers and Lloyd’s Underwriters) in ways that are consistent with the continued development of a viable, competitive and innovative insurance industry*
Where is Alan Cameron coming from?

- Management is vested in the board
- Board may delegate powers to a committee, another director (e.g., managing director), an employee or any other person (under general law or s198D)
- Reliance on information or advice is reasonable (not negligent) if made:
  - in good faith,
  - After making an independent assessment of the information or advice, having regard to the director’s knowledge of the corporation and the complexity of its structure and operations
- Independent assessment =
  “no more than that they, having listened to and assessed what their colleagues have to say, must bring their own mind to bear on the issue using such skill and judgment as they may possess” (Southern Resources)
  But base skill required
- No automatic liability for acts or delegates properly made and supervised.
Further legal context of these issues

• The lesson of *Hardie* and *Centro*
  - The board needs to be an intelligent reader of material it is approving
  - Board must have an understanding of the business and that understanding must be brought to the table in its decisions
  - It must have regard to the information it possesses or has learnt
  - It must understand and have regard to the information it is given
  - It needs to be inquiring and sceptical

Here the obligations not unlike the duty in *Centro* to take reasonable steps to comply with or to secure compliance with accounting rules with the added requirement for a board declaration

• The lesson of *Vines* – directors with special expertise will be judged by reference to it

• Also compare positive due diligence requirement in WH&S laws
Possible wider consequences of APRA’s focus on directors’ duties

• The classic duties of care and diligence and to act in good faith in the best interests of the company may be reframed either directly or indirectly by the express provisions of the Prudential Acts, the provisions and focus of the Prudential Standards, the remedies that APRA may apply and the manner of APRA supervision.

  OR (more conservatively)

• The duties may be applied by the courts by reference to the higher expectations that APRA has as to the performance of directors of regulated institutions.

• Distinguish life and superannuation where express statutory change in duty
Impact on management – the particular impact of APRA’s views and CPS 220

- You might say - all companies are subject to regulation, and boards in exercising their duties do so considering regulatory rules
- BUT internal behavioural rules plus supervision and APRA’s powers, start to clash with the traditional conceptions of

  Board duties
  Delegation to management
  Reliance
So what does APRA mean when it says in CPS 220:

- The Board … is ultimately responsible for the institutions risk management framework (para 13)
- … the Board must ensure that … (para 13)
- The board must establish the risk appetite … (para 29)
- The Board must make an annual declaration to APRA on risk management … that must satisfy requirements set out in Attachment A.. (para 49 and 50)

- Compare paras 21 – 27 and other paras which require the regulated institution to maintain a risk management framework that meets specified criteria and do particular things.
That word ‘ensure’! The proposed definition and the terms of the Board CPS 220 declaration.

<table>
<thead>
<tr>
<th>Ensure Definition</th>
<th>Declaration (49-51)</th>
</tr>
</thead>
<tbody>
<tr>
<td>take all reasonable steps</td>
<td></td>
</tr>
<tr>
<td>make all appropriate enquiries</td>
<td>having made appropriate enquiries</td>
</tr>
<tr>
<td>So the board can determine</td>
<td>state</td>
</tr>
<tr>
<td>to the best of its knowledge</td>
<td>to the best of its knowledge</td>
</tr>
<tr>
<td>the stated matter has been properly addressed – sub-paras (a) to (h) in para 13</td>
<td>Sub-paras (a) to (f) of the declaration</td>
</tr>
</tbody>
</table>

- Key words (imagine a court room)
  - Objective,
  - Tested by context and purpose of Standard and legislation
  - Potentially subject to expert evidence of usual (or best) practice
  - The views of APRA important but not necessarily determinative.

- But now imagine the conversation with APRA
### The Board’s role in Para 13 CPS 220

<table>
<thead>
<tr>
<th>Board ‘ensure’ that</th>
<th>Board role</th>
</tr>
</thead>
<tbody>
<tr>
<td>(a) It [i.e. the Board] defines risk appetite and establishes RMS (c/-para 21 and 29)</td>
<td>Personal unless ‘defines’ = ‘approves’</td>
</tr>
<tr>
<td></td>
<td>Seems a more ‘involved’ process required. Should RMS be RMF? What does ‘establish’ mean?</td>
</tr>
<tr>
<td>(b) A sound risk management culture is established and maintained throughout institution</td>
<td>Delegation and reliance – but reporting and inquiry required especially if knowledge of failure</td>
</tr>
<tr>
<td>(c) Senior management take steps necessary to monitor and manage all material risks ...</td>
<td>Delegation and reliance but responsibility below board must sit with senior management – see para 41. again reporting and inquiry if failure.</td>
</tr>
<tr>
<td>(d) Operational structure of the institution facilitates effective risk management</td>
<td>Delegation and reliance but should have oversight of operational structure and how it facilitates risk management</td>
</tr>
</tbody>
</table>
# The Board’s role in Para 13

<table>
<thead>
<tr>
<th>Board ‘ensure’ that:</th>
<th>Board role</th>
</tr>
</thead>
<tbody>
<tr>
<td>(e) Policies and processes are developed … consistent with RMS and established risk appetite</td>
<td>Delegation and reliance but reporting may be important. Board here must “independently” assess</td>
</tr>
<tr>
<td>(f) Sufficient resources are dedicated to risk management</td>
<td>Delegation and reliance. Note the 4 Corners allegations re CBA -1.5 risk officers for 700 planners.</td>
</tr>
<tr>
<td>(g) Uncertainties … recognised, and assumptions relating to models … are well understood</td>
<td>Seems to have a personal element but unclear if this is the board or management</td>
</tr>
<tr>
<td>(h) Appropriate controls are established …, and are understood by, and regularly communicated to, relevant staff.</td>
<td>Delegation and reliance; “independent” assessment</td>
</tr>
</tbody>
</table>
### Risk Management Declaration – an imperfect relationship with Para 13 obligations

<table>
<thead>
<tr>
<th>Declaration</th>
<th>Board role</th>
</tr>
</thead>
<tbody>
<tr>
<td>(a) Institution has in place systems for ensuring compliance with all prudential requirements</td>
<td>Own knowledge and reasonable reliance – literally goes beyond CPS 220; “independent” assessment 13 (a) and (b)</td>
</tr>
<tr>
<td>(b) Systems and resources in place for identifying … material risks, and the RMF are appropriate …</td>
<td>Own knowledge and reasonable reliance; “independent” assessment. 13 (a) to (g) especially (f).</td>
</tr>
<tr>
<td>(c) The risk management and internal control systems … are operating effectively and are adequate …</td>
<td>Own knowledge and reasonable reliance; “independent” assessment 13(h)</td>
</tr>
<tr>
<td>(d) Institution has RMS complying with CPS 220 and has complied with it</td>
<td>Own knowledge and reasonable reliance; “independent” assessment. Para 31 – 32; 13(c)</td>
</tr>
</tbody>
</table>
### Risk management Declaration – an imperfect relationship with Para 13 obligations

<table>
<thead>
<tr>
<th>Declaration</th>
<th>Board role</th>
</tr>
</thead>
<tbody>
<tr>
<td>(e) Reinsurance Management Strategy complies with GPS 230</td>
<td>Own knowledge and reliance; “independent” assessment.</td>
</tr>
<tr>
<td>(f) Institution satisfied with efficacy of processes and systems for production of financial information</td>
<td>Own knowledge and reliance; “independent” assessment.</td>
</tr>
</tbody>
</table>

- Mis-alignment of declaration and paragraph 13 requirements and other parts of CPS 220
- Although core requirements are fairly clear given the importance and possible consequences, the Standard needs to be better constructed
- Potential for regulator (or particular officers in the regulator) to pick and choose between different expressions of principles.
How does board respond to these requirements? Some suggestions.

- Careful mapping of Board obligations
- Setting up delegation framework and minuting it (s251)
- In this context, careful formulation of the role, responsibility and reporting lines of Risk Committee and Chief Risk Officer paramount
- Need for review of operational structure relevant to risk
- Establish/review reporting, and focus carefully on what is reported to the board – enough but not too much – remember Centro! Beware of reliance on advice that just passes question back to the board – Prime Trust.
- But understand that board has a primary role on some key issues – defining risk appetite and establishing RMS
How does board respond to these requirements? Declaration

- Act now to formulate delegations and reporting to satisfy declaration requirements
- Establish appropriate systems of delegation and reporting up to board on each element of declaration
- Review by Risk Committee and CRO which should then report up to the board
- However each board member needs to turn her/his mind and knowledge to each element, ensure understanding and sceptically inquire and challenge responses
Conclusions

• APRA has a narrower focus than the board of a company
• If there is a risk management failure, it wants to hold the board accountable
• The Standard is poorly constructed with overlapping and potentially inconsistent requirements
• To meet the APRA requirements boards
  ▪ Must not just delegate risk management to others
  ▪ Must actively understand the risk management framework
  ▪ Set in place a reporting regime and ‘independently assess’ reports – read, understand and challenge
  ▪ Respond to any failure
Conclusions- the Cameron challenge.

- Alan Cameron has identified the right issue!
- Is he right? In part, as APRA enforces by supervision and persuasion and may prefer the approach that the board takes the fall in a failure.
- The courts may take a more traditional view but are unlikely to have a say.
- At the end of the day APRA seems to be saying that risk management should equate in importance to accounts and financial information.
“... the board plays a critical role in risk governance.”

Allens is an independent partnership operating in alliance with Linklaters LLP.