AUSTRALIAN INSTITUTE
of COMPANY DIRECTORS

Level 30
20 Bond Street
Sydney NSW 2000
www.companydirectors.com.au
ABN 11 008 484 197

T: +61 2 8248 6600
F: +61 2 8248 6633
E: contact@companydirectors.com.au

28 March 2014

Mr Neil Grummitt
General Manager, Policy Development
Policy, Research and International
Australian Prudential Regulation Authority
GPO Box 9836
Sydney NSW 2001

By email: riskmanagement@apra.gov.au

Dear Mr Grummitt,

Draft Prudential Practice Guide CPG 220 – Risk Management

The Australian Institute of Company Directors welcomes the opportunity to make this submission with respect to the Australian Prudential Regulation Authority's (APRA) *Draft Prudential Practice Guide CPG 220 – Risk Management* (Draft CPG 220).

The Australian Institute of Company Directors (Company Directors) is the second largest member-based director association worldwide, with individual members from a wide range of corporations: publicly-listed companies, private companies, not-for-profit organisations, charities, and government and semi-government bodies. As the principal professional body representing a diverse membership of directors, we offer world class education services and provide a broad-based director perspective to current director issues in the policy debate.

Increasing risk management standards

As a general principle, it is important that the regulation of risk management arrangements for APRA-regulated entities is not unnecessarily duplicative and that it is considered in the context of existing regulation, such as the provisions of the Corporations Act, which is administered by the Australian Securities and Investments Commission (ASIC) and the ASX Corporate Governance Council's *Corporate Governance Principles and Recommendations* 3rd ed (ASX CGC Principles). We acknowledge that APRA has, over time, taken steps to ensure that the prudential standards that it sets are in line with the Principles. However, the standards set by APRA with respect to risk management under the new *Prudential Standard CPS 220 – Risk Management* (CPS) are, in many instances, a more prescriptive standard than applies to listed companies under the Principles.

Company Directors does not oppose the more vigorous surveillance of companies in the financial sector where APRA reasonably considers such an approach is justified in the circumstances. However, we do oppose the mandating governance and risk management standards and the taking of a "one-size-fits-all" approach to governance and risk management regulation. For this reason, we are of the view that the requirements of CPS 220 and the guidance provided under Draft CPG 220 should be consistent with, and not go beyond, the standards recommended under Principle 7 – Recognise and Manage Risk of the ASX CGC Principles. Before a decision is made to extend risk governance and management standards for APRA-regulated entities beyond those that are set out in the ASX CGC Principles, a full cost-benefits analysis should be undertaken to ensure that the extension is justified and will not unnecessarily increase the regulatory burden for those entities.

While the Draft CPG 220 is intended to provide additional guidance on APRA's expectations for risk management under CPS 220, in our view, it will in fact have the effect of further increasing the standards of risk management governance for APRA-regulated entities and

significantly extends the expectations of what a board should be responsible for with respect to risk management.

In our view, the further increase in risk management standards under the Draft CPG is inappropriate and unjustified. The document should be limited to providing much needed guidance as to how APRA-regulated entities can meet their obligations under the new CPS 220 without adding greater obligations and expectations, particularly on the boards (and possibly the individual directors) of those entities.

Blurring the roles of the board and senior management

One of the most significant ways CPS 220 has increased risk governance standards for APRA-regulated entities beyond what is required under the Principles is the requirement that boards "ensure" the entity's risk management framework is in place and operating effectively (in particular, see paragraph 13 of CPS 220). As raised in a number of submissions made in response to the draft CPS 220, the requirement for the board to "ensure" that the entity fulfils its risk management responsibilities is inappropriate, unreasonable and not practicably achievable. It places too high a burden on the board and blurs the roles and responsibilities of the board with those of senior management. We agree with these submissions and we are disappointed that these concerns were not addressed in the final version of CPS 220.

While it is well-understood that the board is ultimately responsible for deciding the nature and extent of the risks it is prepared to take to meet its objectives (as is reflected in the Commentary to Principle 7 – Recognise and Manage Risk of the ASX CGC Principles), the board will ordinarily delegate the risk management function to management, with the board being responsible for setting the risk appetite for the entity, overseeing the risk management framework and satisfying itself that the framework is sound[1].

Rather than clarifying what APRA's intent was for these requirements for the board to "ensure" it fulfils its duties under CPS 220, Draft CPG 220 actually blurs the roles and responsibilities of the board and of senior management further. For example:

- While recognizing the board's ability to delegate responsibilities, paragraph 9 of Draft CPG 220 expressly states that "this will not absolve the Board from *ensuring* its responsibilities are fulfilled" (emphasis added).
- There are a large number of instances in Draft CPG 220 where the roles and responsibilities of the board and of senior management are conflated (for example, in paragraphs 14, 27, 29, 34, 53, 62 and 68) with no further explanation provided as to how these responsibilities could be divided.
- Paragraph 40 notes that APRA "expects that the Board would be actively engaged in developing and reviewing the risk appetite statement and would be able to demonstrate ownership of the statement".
- Paragraph 54 notes that the risk management function is expected to assist the board in "building risk management capabilities throughout the APRA-regulated institution".
- Where an entity is seeking APRA's approval to put in place an alternative risk management arrangement from those required under CPS 220, the board is "expected to demonstrate to APRA that it has undertaken a process to identify conflicts, has established structural oversight and controls to mitigate additional risk and is satisfied that the risk management framework will ensure these mitigants are adhered to" (paragraph 61).

[1] Principle 7, ASX Corporate Governance Council's *Corporate Governance Principles and Recommendations* 3rd ed (2014)

- Under the "three lines-of-defence risk governance model", the board's delegated committees have been moved from an oversight function to being part of a management function on the second and third lines of defence (Appendix A).

The confusion in the Draft CPG 220 between what the roles and responsibilities of the board are on the one hand, and what the roles and responsibilities of management are on the other hand suggests that APRA's understanding and concept of board oversight is misconceived. APRA seems to see boards as having a hands-on role in company affairs, akin to that of management.

This misunderstanding is often referred to as the "expectation gap" and has been explained as follows:

> "Many people believe that corporate boards and their directors (both executive and non-executive) should be so closely involved in the affairs of the corporation that they can ensure nothing can go wrong. This view is fundamentally flawed, both in law and in practice, and has led to unrealistic expectations about what directors should be doing in areas that are the responsibility of corporate managers. If these expectations were to be met, all directors would have to become, in effect, full time employees of the organisation. This would undermine the non-executive directors' independence of outlook and objectivity which are vital for effective corporate governance."[2]

The role of the board of a company, whether APRA-regulated or otherwise, is one of monitoring, oversight and strategy. The executive, on the other hand, is responsible for the day-to-day operations of the company and for the implementation of strategy set by the board. Unfortunately, this delineation is not well understood by the public, media and is not often reflected in the way the law is applied in Australia or in how APRA sets and applies governance standards. APRA seems to see boards as being involved in the day-to-day minutiae of the business. APRA's requirements under CPS 220 and Draft CPG 220 for the board to "ensure" that the entity fulfils its risk management responsibilities is an unreasonable standard that would require boards to become intimately involved in the risk management systems of the company, rather than taking an oversight role, setting the risk appetite for the entity and satisfying itself that the framework is sound. As overseers of risk management, the board is not in a position to "ensure" the matters that it is required to under CPS 220 and Draft CPG 220 as they are either matters that are outside their purview or they are matters that are not really capable of being determined with the requisite degree of certainty. Any suggestion that this blurring of the roles of the board and of management is good for governance and proper functioning of an organisation is, in our view, confused.

Increasing the compliance burden of boards

By increasing the role and responsibilities of boards with respect to risk management, the effect of CPS 220 and Draft CPG 220 will be to further add to the already heavy regulatory and compliance burden placed on the boards of APRA-regulated companies. Many company directors express dissatisfaction with the amount of time spent by their boards on compliance issues. Board meetings are increasingly dominated by the red tape of regulation and, for companies in the financial sector, APRA's requirements are already the most demanding on their time. APRA's expectations of boards with respect to risk management as detailed in CPS 220 will further compound this issue.

As set out above, the primary role of the board is to monitor and oversee the work of the executive and management. If the regulatory environment continually sets the expectation that directors will consider issues at the same level of detail as management, the value of the board's function is diminished. If the board is too involved in the "doing" of the corporation's

---

[2] Tony Howarth's foreword in Cole S, *Mind the Expectation Gap The Role of A Company Director*, Australian Institute of Company Directors 2012.

activities the board cannot provide the same objectivity and oversight of corporate management. In this way, the increasing compliance burden that the risk standards set under CPS 220 and Draft CPG 220 place on boards will actually add to the company's systemic risk as boards become overwhelmed by the sheer volume of regulation that they are required to comply with, and therefore have less time to focus on the good governance of the company. This, in turn, creates significant risks of a different nature, as boards become distracted from planning for the future growth and development of their companies, which will ultimately be to the detriment of economic prosperity of all Australians.

In APRA's Response to Submissions that was released with the new CPS 220 and the Draft CPG 220, it is noted that the enhancements of APRA's risk management requirements under CPS 220 have been made in response to improvements in global risk management practices following the global financial crisis. It is important to note that Australia has been well-served by the high standards of governance and risk management amongst its financial institutions. This strong governance and risk management culture is evidenced by the fact that Australia did not experience the same level of corporate failures during the global financial crisis as occurred overseas. This was in part due to the diligence and rigour of our regulators, including APRA, and also the high quality of Australia's boards and directors. We should therefore resist following the world-wide trend (most notably the US and the UK) to react to the corporate failures during the global financial crisis through the introduction of new or expanded regulation to address perceived risk management concerns that have not been as significant in Australia.

Company Directors continues to be concerned that, in an environment where regulation and red-tape is increasing, the role of a company director is becoming increasingly onerous and exposed to personal liability. This is having a detrimental impact on board recruitment and retention. By increasing the standards of risk management governance for APRA-regulated entities and significantly extending the expectations of what a board should be responsible for with respect to risk management, CPS 220 and Draft CPG 220 will further compound these issues.

The increased regulatory burden of APRA-regulated entities under CPS 220 and Draft CPG 220 is also contrary to the federal government's current deregulation agenda, which seeks to identify and remove unnecessary and excessive regulation to ease the compliance burden of Australian businesses and improve productivity growth in Australia.

We hope that our comments will be of assistance to APRA. Please do not hesitate to contact Senior Policy Advisor, Gemma Morgan on [redacted] if you would like to discuss.

Yours sincerely,

John H C Colvin
Chief Executive Officer &
Managing Director