INSURANCE COUNCIL OF AUSTRALIA

Mr Neil Grummitt
General Manager, Policy Development
Australian Prudential Regulation Authority
GPO Box 9836
SYDNEY NSW 2001
By email: riskmanagement@apra.gov.au

28 March 2014

Dear Mr Grummitt

DRAFT PRUDENTIAL PRACTICE GUIDE CPG 220 - RISK MANAGEMENT

The Insurance Council of Australia (Insurance Council) welcomes the opportunity to comment on the Draft Prudential Practice Guide CPG 220 – Risk Management (Draft CPG). The Insurance Council continues to support APRA's commitment to improve risk management practices across general insurers with the intention to enhance protection for Australian policyholders.

We consider, however, that the Draft CPG has several shortcomings that need to be addressed. This submission raises concern with Directors' obligations stemming from the repeated use of the word "ensure" in Prudential Standards, which we consider should be replaced throughout with "reasonable steps be taken". The submission also argues that APRA's interpretation of the "three lines of defence risk governance model" should be amended, moving Board committees out of the actual lines of defence and placing them firmly in a position of oversight (with consequent revisions to the diagram in Appendix A of the Draft CPG). The Insurance Council strongly believes that the Board should not be required to perform management tasks and that the Prudential Practice Guide should be quite clear on that point.

There are a number of specific requests and suggestions for clarification contained in the Attachment.

The use of "reasonable steps" instead of "ensure"

The Insurance Council maintains the view, as explained in its letter of 20 May 2013 on GPS 110, CPG 110 and its submission of 10 July 2013 on CPS 220 that Boards will not generally be in a position to "ensure" that the matters set out in paragraph 13 of CPS 220 are met. The standard required by the plain English definition of the word, which means "to make sure or certain", is unachievable for non-executive directors (NEDs).

The Insurance Council notes APRA recognition of the issue in its Response to Submissions document dated 31 January 2014, where it states that submissions such as the Insurance Council's "appear to reflect a lack of understanding about what APRA means by the word ensure". However, it is important to note that APRA's intended meaning may have far reaching consequences in a situation where issues arise as to board members' compliance. The word "ensure" has a plain English definition that could be applied in the event of a dispute concerning a member's compliance with paragraph 13 of CPS 220.

The Insurance Council's view is that APRA should not use the word "ensure" in Prudential Standards unless it truly intends to impose a strict requirement on Boards to "to make sure or certain" that a thing is done. Such a requirement should not be imposed on a Board (particularly NEDs) without careful consideration as to board members' practical ability to comply. It is submitted that that would be limited to very rare instances, if at all.

In all other cases, the standard imposed on board members should be consistent with the normally accepted duties of directors, for instance to "take reasonable steps" that something is done (for example, section 344(1) of the Corporations Act as discussed in the Centro case). The Insurance Council submits that this is also more consistent with APRA's responsibilities as a prudential regulator. It is far better to impose on directors a standard that they can meet and which represents APRA's expectations than one with which it may be impossible to comply.

Instead of replacing the word "ensure" in CPS 220, as proposed by the Insurance Council in its submissions, APRA has included some commentary in its Response to Submissions document on its expectations of Boards (page 11) and in the Draft CPG. Most significantly, paragraph 12 of the Draft CPG says:

> "In determining whether the Board has met its responsibilities, APRA will assess the steps taken by the Board to ensure, to the best of its knowledge and having made appropriate enquiries, it meets its responsibilities."

In this paragraph, APRA does not state what standard of "steps" will be required to satisfy it. The Insurance Council considers that this gap needs to be addressed. The standard that directors are expected to meet should be transparent. It should not be left unclear, with APRA having discretion as to interpretation. The Insurance Council submits that the appropriate standard to be applied to the "steps" to be taken by directors is the concept of "reasonable steps", which is well founded in Australian law and should be applied in this case.

The same issue arises where the word "ensure" is used in other Prudential Standards. Examples include:

- paragraph 6 of GPS 110 regarding capital adequacy;
- the Objectives section of GPS 230 regarding the reinsurance management framework;
- paragraphs 21 and 32 of CPS 231 regarding outsourcing risks;
- paragraphs 15 and 19 of CPS 232 regarding business continuity management; and
- paragraphs 16, 21, 44, 84 and 85 of CPS 510 regarding Board expertise, the adequacy of policies and audit plans.

Given that APRA has decided to clarify, as it has done in the Draft CPG, what it means by the word "ensure", the Insurance Council submits that it should also do the same in relation to the other Prudential Standards provisions which require Boards to "ensure" things be done. To do otherwise would lead to different interpretations of the word in different places.

The Insurance Council holds the strong view that this should not be done through retention of the word "ensure" in the Prudential Standards with clarification in numerous Practice Guides relating to those references (i.e. as it has proposed doing in relation to CPS 220). Such an approach would be both inefficient, as APRA would be repeating the same explanation in each Practice Guide, and also ineffective as a Practice Guide is guidance only.

Instead, it is submitted that APRA should replace the word "ensure" in each Prudential Standard with the intended meaning (i.e. "take reasonable steps" to meet the obligation). An alternative would be to include a definition of "ensure" in the Definitions Prudential Standard GPS 001 so that it appropriately defines all uses of the word in the Prudential Standards. However, this is not preferred given the difference between APRA's definition and the plain English definition of the word that is likely to result in confusion.

Board Committees should be moved out of the three lines of defence risk governance model.

Paragraph 6 of the Draft CPG includes:

> "The second line-of-defence comprises the specialist risk management function and responsible Board Risk Committee(s) (BRCs) that are functionally independent from the first line-of-defence".

Similarly, paragraph 7 of the Draft CPG includes:

> "The third line-of-defence comprises the independent assurance function and Board Audit Committee, each of whom provides independent assurance to the Board".

The Insurance Council is extremely concerned that the inclusion of the BRC in the second line-of-defence, and the Board Audit Committee in the third line-of-defence, effectively requires NEDs to take a management role. Whilst the diagram in Appendix A shows their roles as "oversight", it also inappropriately includes them as part of the second lines. The Insurance Council considers that this approach by APRA is not appropriate and that the role of the Board and its committees is one of oversight and not as part of management.

In order for NEDs to remain independent of the operations, the final CPG 220 should distinguish between the roles of management and the NEDs. In particular, the final CPG 220 should state the NEDs' role is to guide and monitor management. This is supported by the Draft CPG referring to oversight in its paragraphs 2, 4, 6(d), 24(d), 28, 29, 61(e) and Appendix A, point 10. See also paragraphs 13(c) and 32(d) of CPS 220.

If you have any questions or comments in relation to our submission, please contact John Anning, the Insurance Council's General Manager Policy, Regulation Directorate, on tel: or email:

Yours sincerely

Robert Whelan
Executive Director & CEO

INSURANCE COUNCIL OF AUSTRALIA

ATTACHMENT

REQUESTS FOR CLARIFICATION OF POINTS IN THE DRAFT CPG

Paragraph 9 states delegation *"will"* not absolve the Board. We consider that *"will"* should be replaced with *"may"*. This would allow consistency with sections 189 and 190 of the Corporations Act 2001 (see Justice Santow's comments in ASIC v Adler and 4 others involving HIH Insurance [2002] NSWSC 171 at paragraph 372, points 10 to 12).

Paragraph 43 mentions the Board should understand the limitations and assumptions relating to any models. This level of detail should only be required of the Board Risk Committee.

Paragraphs 70 to 73 should be revised to clarify around what constitutes a Risk Management Information System (MIS). Standard 25(g) in CPS 220 requires "a management information system (MIS) that is adequate, both under normal circumstances and in periods of stress, for measuring, assessing and reporting on all material risks across the institution".

The Draft CPG provides guidance on the MIS in paragraphs 70 to 73, however it is unclear what is defined as a Management Information System (MIS). That is, does an MIS include the policies, processes, procedures and a computer system or is an MIS solely a computer-based system? If APRA defines MIS as solely a computer-based system, the impact will require all organisations to either develop or purchase a computer-based system. This will be at substantial cost and also will not be effective considering that risk-based information comes from a variety of sources and cannot practicably be housed in the one system.

Paragraphs 75 and 76 should be revised to clarify the term "elements'" of the risk management framework (RMF). Standard 45 in CPS 220 states that the RMF must be "subject to review by internal and/or external audit at least annually …".

In paragraphs 75 and 76 of the Draft CPG, APRA provides guidance on the annual review process stating that it will "accept annual reviews that explore particular elements of the risk management framework in depth and on a rotational basis" and provides an example "if an institution's risk management framework has six material elements, it may choose to review two of these every year".

It is unclear in the guidance how APRA defines "elements" of the risk management framework, for example whether they are to be risk categories or any sub process (such as training, reporting, and risk identification) of the RMF. The implication of this lack of clarity is that some organisations may commission independent reviews of two risk categories per year (e.g. Health & Safety and Credit Risk), while others will focus on two processes (e.g. Culture and Risk Assessment).

Paragraph 78 states *"APRA expects the comprehensive review to include a comparison of the institution's current practice against better practice".* The Insurance Council does not agree with the use of the phrase *"against better practice"*. We believe that institutions should use practices most appropriate to their operations and that there should not be a presumption that "better practice" exists. We therefore suggest this wording be replaced with

the phrase “other market practices”, which reflects an open mind as to what others are doing without the presumption that change is effectively required given that non-adoption of “better practice” must be justified.

Paragraph 84 states that *“.... APRA expects that the two directors ... who sign the [risk management] declaration would have obtained reasonable assurance and, if necessary, independent advice on the matters upon which they have made the decision.”*

The final CPG 220 should make it clear that such reasonable assurance comes from management and any independent advice is from an external party. As set out in Attachment A to CPS 220 effective from 1 January 2015, the risk management declaration is to the best of the Board’s knowledge and having made appropriate enquiries.

In this regard, APRA’s comments on page 11 of its Response to Submissions document are relevant. The Insurance Council considers that APRA should include some additional examples in paragraph 11 of the draft CPG to outline how it would consider the Board to have met the “knowledge and ... enquiries” approach.

Further, a Board makes a resolution or declaration on behalf of all members even though one or two members sign on behalf of the Board. The requirement in paragraph 84 for the two designated signatories to obtain additional assurance appears to put a higher duty of care on these two persons over and above that of the other directors. The Insurance Council requests that APRA clarify that that the two signatories do not carry a higher duty of care compared to other directors who also approve the declaration.