Australian Prudential Regulation Authority

400 George Street (Level 26)
Sydney NSW 2000

GPO Box 9836
Sydney NSW 2001

T 02 9210 3000
F 02 9210 3411
W www.apra.gov.au

8 May 2014

To: All CEOs of ADIs, general insurers and life companies

Risk management

In January 2014, as part of a package to harmonise and enhance its risk management requirements, APRA released for public consultation a draft cross-industry *Prudential Practice Guide CPG 220 Risk Management* (CPG 220). APRA will in due course release its response to the issues raised in submissions received.

In the interim, however, APRA wishes to clarify its intent in respect of three specific matters that featured in many submissions.

Use of the term 'ensure'

APRA has used the term 'ensure' in prudential standards for several years. A number of submissions have argued that other regulators or courts may not interpret that term consistently with APRA's intention and could, instead, interpret it as requiring that a particular outcome be guaranteed. Submissions argue that this could give rise to legal risks that were not intended by APRA in the drafting of its prudential standards and guidance material. This issue has also been raised by directors in some recent APRA discussions with boards.

To address the concerns that have been raised, APRA proposes to clarify its use of the term by inserting a definition of 'ensure' into each of its general definitions standards (3PS 001, APS 001, GPS 001 and LPS 001). The proposed definition is:

> **Ensure:** when used in relation to a responsibility of the board, means to take all reasonable steps and make all appropriate enquiries so that the board can determine, to the best of its knowledge, that the stated matter has been properly addressed.

This definition is consistent with the approach APRA has taken in its dealings with boards on governance matters. Hence, introducing the definition does not represent a loosening or tightening of the intent of the relevant prudential standards.

Three lines of defence

Submissions raised some concerns about APRA's apparent expectations in relation to the three lines of defence model and, in particular, the distinction between the roles of management and board under that model. APRA's intent is consistent with the desired position of those raising concerns, and it proposes to clarify that in amendments to CPG 220 and, if necessary, to *Prudential Standard CPS 220 Risk Management* (CPS 220). Appropriate amendments will be considered during the finalisation of CPG 220.

Materiality and the risk management declaration

Submissions noted that the risk management declaration in CPS 220 does not contain any reference to materiality. APRA considers that the concept of materiality is appropriate for the Board declaration and proposes to amend the wording accordingly. A revised version of the declaration that reflects this proposed change is attached.

Response

APRA welcomes comments on these proposed refinements, and will consider such comments in finalising its response to submissions on CPG 220. Comments should be provided by 30 May by email to riskmanagement@apra.gov.au and addressed to:

Mr Neil Grummitt
General Manager, Policy Development
Policy, Statistics and International Division
Australian Prudential Regulation Authority
GPO BOX 9836
SYDNEY NSW 2001

Yours sincerely,

Charles Littrell
Executive General Manager
Policy, Statistics and International Division

Attachment A

Risk management declaration

1. For the purposes of paragraph 49 of this Prudential Standard, the Board must provide APRA with a risk management declaration stating that, to the best of its knowledge and having made appropriate enquiries, in all material respects:

   (a) the APRA-regulated institution has in place systems for ensuring compliance with all prudential requirements;

   (b) the systems and resources that are in place for identifying, measuring, evaluating, monitoring, reporting, and controlling or mitigating material risks, and the risk management framework, are appropriate to the institution, having regard to the size, business mix and complexity of the institution and group (where appropriate);

   (c) the risk management and internal control systems in place are operating effectively and are adequate having regard to the risks they are designed to control;

   (d) the institution has a RMS that complies with this Prudential Standard, and the institution has complied with each measure and control described in the RMS;

   (e) where it is a general insurer, the institution's **Reinsurance Management Strategy** complies with *Prudential Standard GPS 230 Reinsurance Management*, for selecting and monitoring reinsurance programs; and

   (f) the institution is satisfied with the efficacy of the processes and systems surrounding the production of financial information at the institution and group (where appropriate).