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

7 October 2014

To: All CEOs of authorised deposit-taking institutions, general insurers and life companies

CPS 220 Risk Management / CPG 220 Risk Management

In January 2014, APRA released its finalised cross-industry *Prudential Standard CPS 220 Risk Management* (**CPS 220**). At the same time, APRA released for consultation with industry draft *Prudential Practice Guide CPG 220 Risk Management* (**CPG 220**). On 8 May 2014, APRA released a letter to industry outlining responses to several key issues raised by submissions in response to the January 2014 consultation; in particular, APRA's use of the term 'ensure' in prudential standards, the three lines of defence model and the concept of materiality for the risk management declaration.

The 8 May 2014 letter noted that APRA's full response to submissions would consider the remaining issues arising from consultation which had not already been addressed. This letter includes that response, as well as responding to submissions on the 8 May 2014 letter itself.

Submissions raised a number of issues which APRA considers would be most appropriately addressed by amending CPS 220. Accordingly, and notwithstanding that CPS 220 was finalised in January, the attachment to this letter outlines further amendments that are proposed.

Regarding the proposals in the 8 May 2014 letter, APRA confirms that it will include a definition of 'ensure' into the definitions standard for each industry and will amend the risk management declaration wording to take account of materiality.

The detail of the response to submissions is included as Attachment A to this letter. CPS 220 includes tracked changes relative to the January 2014 version. CPG 220 is not presented with tracked changes; however, the key changes are described in the Attachment.

APRA welcomes feedback by 4 November 2014 on both CPS 220 and CPG 220. In the case of CPS 220, feedback is only sought regarding whether the proposed refinements give rise to any fundamental concerns. APRA's intention continues to be that CPS 220 and CPG 220 will come into effect on 1 January 2015.

Comments should be provided by email to riskmanagement@apra.gov.au and addressed to:

Mr Pat Brennan
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

Important disclosure notice - publication of submissions

All information in submissions will be made available to the public on the APRA website unless a respondent expressly requests that all or part of the submission is to remain in confidence. Automatically generated confidentiality statements in emails do not suffice for this purpose. Respondents who would like part of their submission to remain in confidence should provide this information marked as confidential in a separate attachment.

Submissions may be the subject of a request for access made under the *Freedom of Information Act1982* (FOIA). APRA will determine such requests, if any, in accordance with the provisions of the FOIA. Information in the submission about any APRA-regulated entity that is not in the public domain and that is identified as confidential will be protected by section 56 of the *Australian Prudential Regulation Authority Act 1998* and will therefore be exempt from production under the FOIA.

Attachment A

1 - Submissions on the 8 May letter to industry

APRA received five letters in response to the 8 May 2014 letter to industry. Submissions were broadly supportive of the proposals in the letter. Some submissions requested that the approach to defining 'ensure' be extended to the superannuation industry. As the superannuation industry was not part of the CPS 220/CPG 220 consultation, this feedback has been noted to be addressed separately at an appropriate time. A range of feedback on CPS 220 and CPG 220, going beyond the issues consulted on in the 8 May 2014 letter was received; that broader feedback is addressed in the later part of this attachment. Two substantive issues specifically related to the definition of ensure were raised:

- One submission recommended that the scope of the proposed definition of ensure be narrowed so that the board was required only to 'make all appropriate enquiries' rather than also including the need to 'take all reasonable steps'. This proposal narrows the scope of the definition significantly, and beyond what APRA expects of a prudently managed institution. For this reason, APRA has not accepted the change.

- Another submission recommended that the definition of 'Board' in each definitions standard be expanded to also include board committees, in order to facilitate delegation by the Board to its committees. APRA accepts that delegation to board committees can be appropriate and this is reflected throughout CPS 220 and CPG 220. APRA's view, therefore, is that this amendment is not necessary and could have unintended consequences given that, by its inclusion in the definitions standard, it would apply to all uses of the term 'Board' across the prudential framework. For these reasons, APRA has not changed the approach outlined in the letter.

One minor clarification to the definition of 'ensure' has been included to make sure that it clearly references only activities consistent with the role of a board.

The May letter proposed the following definition:

'**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.'

The revised definition is:

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

2 – Three lines of defence model and the roles of the board and senior management

The 8 May 2014 letter to industry noted that APRA intended to clarify issues raised with regard to APRA's discussion of the three lines of defence model and, in particular, concerns that APRA's description misconceives the respective roles of the board and senior management. These issues impact both CPS 220 and CPG 220.

APRA response

APRA has clarified the wording of CPS 220 and CPG 220 in a number of places to address these concerns. Specifically:

- *The role of the board in setting risk appetite* - Consistent with the ASX Corporate Governance Principles and Recommendations, the board is responsible for setting the risk appetite of the institution. The board also approves the risk appetite statement. The risk appetite statement is likely to be developed by management for approval by the board and will be implemented and operationalised by management with board oversight. Further detail, including limits for risks, may need to be put in place by management to operationalise the risk appetite statement. In APRA's view, this description is fundamentally consistent with the consultation versions of CPS 220 and CPG 220; however, aspects of the wording have raised industry concern. The revised wording is intended to clarify APRA's original intent in response to the feedback provided.

- *The role of the board in risk culture* – Submissions noted that the board is not able to directly drive the risk culture of an institution and cannot guarantee that a sound risk culture is in place. APRA notes that this concern has, in part, been addressed through the insertion of the definition of 'ensure'. Additional changes have been included to further clarify APRA's expectations regarding risk culture. APRA recognises that thinking on risk culture is evolving and it can be difficult to clearly articulate the risk culture of an institution. That said, APRA does expect that the board form a view of the risk culture in the institution, and the extent to which that culture supports the ability of the institution to operate consistently within its risk appetite, identify any desirable changes to the risk culture and ensure the institution takes steps to address those changes.

- *The role of board committees (and the board) in the three lines of defence*:

    - It has been clarified that the Board Risk Committee and Board Audit Committee assist the board to oversee the operation by management of the risk management framework.

    - Some responses indicated that APRA's description of the role of the Board Risk Committee in relation to the 2nd line of defence and the Board Audit Committee in relation to the 3rd line of defence misconceives the roles of the committees. CPG 220 has been revised to clarify APRA's intentions regarding the roles of each committee.

    - Some submissions commented that the diagrammatic representation of the three lines of defence model in Attachment 1 of draft CPG 220 was misleading as it appeared to show the Board Risk and Board Audit Committees as part of the 2nd and 3rd lines of defence respectively rather than reflecting the role of those committees in assisting the Board as noted above. The diagram has been amended to more clearly reflect APRA's intention.

- Submissions queried the extent of flexibility available to institutions in how they implement the three lines of defence model. The three lines of defence model is widely accepted and used in the industry but its use is not mandatory. CPG 220 has been amended to clarify that the three lines of defence model as described in the CPG is an example, and that alternate models or variations to the three lines-of-defence model may be appropriate to particular institutions where similar outcomes

can be achieved within the requirements of the prudential standards. In particular, the detailed implementation of the model is likely to vary between institutions. In other words, the detailed description of the three lines of defence model in the CPG reflects APRA's view of good practice (which might reasonably be adopted in the absence of sound reasons why an alternative approach is appropriate) rather than a mandatory requirement.

- *The ability of the board to delegate* – the wording of CPG 220 regarding the ability of the board to delegate was the cause of significant confusion. On review, APRA's view is that its expectations in relation to delegation are not substantially different from general corporate law. On that basis, and taking into account amendments to other parts of the CPG to clarify APRA's expectations of boards, the text in question has been removed.

- *The extent of board knowledge of detailed technical and implementation matters* - the standard and CPG have been amended to clarify the extent to which APRA expects boards to be aware of the detail of matters such as the operational structure and the details of risk modelling techniques.

Some submissions requested further detailed guidance for the board on how APRA expects it to meet its responsibilities. APRA considers that the perceived need for detailed board guidance was in large part due to a lack of clarity regarding APRA's expectations of the board in respect of the meaning of 'ensure'. Therefore, the need for detailed guidance on exactly what steps the board should take has been largely addressed through the definition of 'ensure' and the other changes to clarify the respective roles of the board and management outlined in this letter.

3 - Other minor technical matters and clarifications

A range of other minor technical matters and clarifications were suggested in submissions and have been incorporated where appropriate into the attached revised versions of CPS 220 and CPG 220.

APRA response

The more material items, together with APRA's response to each, include:

- Submissions recommended that additional detail be included in CPG 220 in respect of the compliance function. CPG 220 is about risk management and, whilst this embraces the compliance function, APRA wishes to maintain the focus on risk management and has not opted to include further guidance at this time.

- Submissions questioned the ongoing relevance of existing risk management requirements in *Prudential Standard APS 310 Audit and Related Matters*. On 28 August 2014, APRA released a separate letter discussing the consequential changes to other standards as a result of the introduction of CPS 220.

- Submissions requested clarity on the ongoing status of other APRA guidance post CPG 220 implementation – in particular, *Prudential Practice Guide GPG 200 Risk Management* (**GPG 200**), *Prudential Practice Guide LPG 200 Risk Management* (**LPG 200**), *Prudential Practice Guide GPG 230 Operational Risk* (**GPG 230**) and *Prudential Practice Guide LPG 230 Operational Risk* (**LPG 230**). GPG 200 and LPG 200

have been superseded by CPG 220. GPG 230 and LPG 230 address topics that have not been addressed in CPG 220 and so remain relevant.

- Submissions disagreed with the guidance in CPG 220 regarding the signing of the declaration by two directors, specifically that the two directors needed to obtain additional assurance before signing the declaration. Changes have been made to clarify that the two directors sign the declaration on behalf of the whole board, and not in their individual capacity.

- Submissions queried how the timing of the risk management declaration would apply, when a Level 1 institution opted to include its declaration in the declaration of a Level 2 or 3 group, and where the Level 1 institution's balance date differs from that of the head of the group. It has been clarified that, in such cases, the risk management declaration is due at the time the declaration by the head of the group is due.

- Submissions noted that the guidance relating to the notification requirements of paragraph 87 of the consultation version of CPG 220 could be read as suggesting that immaterial changes need to be notified to APRA. The paragraph has been amended to clarify that this is not intended.

- Submissions noted that there may be circumstances where a risk exposure is outside tolerance but, after consideration and evaluation, the institution decides to increase the risk tolerance. The PPG has been amended to take account of this point.