



# Discussion Paper

## Harmonising cross-industry risk management requirements


9 May 2013

## Disclaimer and copyright

While APRA endeavours to ensure the quality of this publication, it does not accept any responsibility for the accuracy, completeness or currency of the material included in this publication and will not be liable for any loss or damage arising out of any use of, or reliance on, this publication.

© Australian Prudential Regulation Authority (APRA)

This work is licensed under the Creative Commons Attribution 3.0 Australia Licence (CCBY 3.0).

 This licence allows you to copy, distribute and adapt this work, provided you attribute the work and do not suggest that APRA endorses you or your work. To view a full copy of the terms of this licence, visit [www.creativecommons.org/licenses/by/3.0/au/](http://www.creativecommons.org/licenses/by/3.0/au/).

## Preamble

APRA is committed to harmonising and consolidating its prudential standards across APRA-regulated industries, where appropriate. Consolidated prudential standards are now in place for outsourcing, business continuity management, governance, and fitness and propriety. This discussion paper describes APRA's proposal to harmonise and enhance its current risk management prudential requirements in a consolidated cross-industry prudential standard, *Prudential Standard CPS 220 Risk Management* (CPS 220), that would apply to authorised deposit-taking institutions (ADIs), general insurers and life insurers, and Level 2 and Level 3 groups. CPS 220 will not apply to the superannuation industry. Instead, RSE licensees must comply with the superannuation-specific risk management prudential standard due to commence on 1 July 2013.

Draft CPS 220 largely reflects the existing risk management prudential standards in the general and life insurance industries. There is no specific risk management prudential standard for ADIs but some risk management requirements are included in a number of ADI prudential standards. As well as harmonising existing requirements, APRA has added requirements to reflect its heightened expectations for risk management.

APRA is also proposing enhancements to *Prudential Standard CPS 510 Governance* (CPS 510) to ensure risk management governance principles are aligned with the draft CPS 220.

APRA expects to finalise the proposed CPS 220, updated CPS 510 and a prudential practice guide prior to their implementation date of 1 January 2014.

Written submissions on this package should be sent to [riskmanagement@apra.gov.au](mailto:riskmanagement@apra.gov.au) by 5 July 2013 and addressed to:

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

## 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 Act 1982* (FOIA). APRA will determine such requests, if any, in accordance with the provisions of the FOIA. Information in the submission about any APRA-regulated institution 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.

# Contents

<b>Glossary</b>	<b>5</b>
<b>Executive Summary</b>	<b>6</b>
<b>Chapter 1 – Introduction</b>	<b>7</b>
1.1 Harmonisation	7
1.2 Enhancements	7
1.3 Industry-specific requirements	7
1.4 Timetable	8
1.5 Structure of this paper	8
<b>Chapter 2 – Harmonising existing risk management requirements</b>	<b>9</b>
2.1 Harmonisation	9
2.2 General insurer requirements	9
2.3 APRA-regulated institutions that are part of a group	9
2.4 APRA-regulated institutions that are the Head of a Level 2 group	10
<b>Chapter 3 – Enhancing risk management requirements</b>	<b>11</b>
<b>Risk Management (CPS 220)</b>	<b>11</b>
3.1 Board oversight of risk management	11
3.3 Management information systems	11
3.4 Risk management function and the Chief Risk Officer	11
3.5 Consistency between business objectives and risk management framework	11
<b>Governance (CPS 510)</b>	<b>12</b>
3.6 Board Risk Committee	12
3.7 Board Audit Committee	12
<b>APRA-regulated institutions that are the Head of a group</b>	<b>12</b>
<b>Chapter 4 – Cost-benefit analysis information</b>	<b>13</b>

## Glossary

ADI	An authorised deposit-taking institution under the <i>Banking Act 1959</i> (Banking Act)
Authorised NOHC	A non-operating holding company authorised under the Banking Act or the <i>Insurance Act 1973</i> (Insurance Act) or registered under the <i>Life Insurance Act 1995</i> (Life Insurance Act)
APRA	Australian Prudential Regulation Authority
APRA-regulated institution	An ADI, extended licensed entity (ELE), general insurer, life insurer, RSE licensee or authorised NOHC
General insurer	A general insurer authorised under the Insurance Act
GPS 220	<i>Prudential Standard GPS 220 Risk Management</i>
Insurer	A general insurer or a life insurer
Level 1 institution	An individual operating company authorised to undertake activities within a single APRA-regulated industry (ADIs, general insurers, life insurers and RSE licensees)
Level 2 group	A consolidated group within a single APRA-regulated industry, headed by an ADI, general insurer or authorised non-operating holding company
Level 3 group	A conglomerate group containing an APRA-regulated institution with operations across more than one APRA-regulated industry and/or including material non-APRA-regulated activities
Life insurer	A life company, including a friendly society, registered under the Life Insurance Act
LPS 220	<i>Prudential Standard LPS 220 Risk Management</i>
Non-APRA-regulated institution	An institution other than an APRA-regulated institution
RSE licensee	A registrable superannuation entity licensee as defined in the <i>Superannuation Industry (Supervision) Act 1993</i>

## Executive summary

This discussion paper sets out APRA's proposed approach to harmonising, consolidating and enhancing a number of risk management requirements set out in existing prudential standards that apply to ADIs, general insurers, life insurers ('insurers') and authorised NOHCs. In many areas, the requirements that apply across these industries are essentially identical.

APRA has already consolidated a number of its 'behavioural' prudential standards, relating to outsourcing, business continuity management, governance, and fitness and propriety. These prudential standards apply equally to ADIs, insurers and authorised NOHCs. APRA proposes to continue this process of harmonisation with a consolidated prudential standard, *Prudential Standard CPS 220 Risk Management* (CPS 220), which would apply as well to conglomerate (Level 3) groups. The standard will not apply to the APRA-regulated superannuation industry.

The proposed CPS 220 consolidates APRA's existing risk management requirements for insurers and will replace some ADI risk management requirements that are currently included in a number of ADI prudential standards. Following finalisation of the draft CPS 220, APRA will revoke *Prudential Standard GPS 220 Risk Management* (GPS 220) and *Prudential Standard LPS 220 Risk Management* (LPS 220). In addition, draft CPS 220 proposes a number of enhancements to APRA's existing prudential requirements to reflect and make more explicit its heightened expectations in this area. In some respects the enhancements will underpin the improvements that have been made in risk management practices, locally and globally, in response to lessons learned in the global financial crisis.

APRA is also proposing to amend *Prudential Standard CPS 510 Governance* (CPS 510) to ensure that governance requirements related to risk management are aligned with those in CPS 220.

The most important of APRA's proposed risk management enhancements are:

- the requirement that institutions have a Board Risk Committee that provides the Board with objective non-executive oversight of the implementation and on-going operation of the institution's risk

management framework. APRA is proposing that this Committee must operate under a different charter than the Board Audit Committee, although APRA's composition requirements will not prohibit the same people sitting on both committees. This requirement will be located in the amended CPS 510; and

- the requirement that institutions designate a Chief Risk Officer (CRO) who is involved in, and provides effective challenge to, activities and decisions that may materially affect the risk profile of the institution. The CRO must be independent and have no responsibilities that may conflict with his or her risk management role (i.e. no 'dual-hatting'). In particular, APRA is proposing that the CRO cannot be the Chief Executive Officer, Chief Financial Officer, the Appointed Actuary or the Head of Internal Audit.

APRA will maintain its principles-based approach to the application of its risk management requirements and will, where appropriate, consider exemptions for smaller institutions that can demonstrate they meet, in substance, the principles underlying the requirements.

APRA's intention is to release CPS 220 and CPS 510 in final form in the second half of 2013, after reviewing submissions. The new risk management requirements are intended to become effective from 1 January 2014.

# Chapter 1 – Introduction

## 1.1 Harmonisation

Since its establishment as an integrated prudential regulator in 1998, APRA has where appropriate sought to take a consistent, harmonised approach to the setting of prudential requirements for APRA-regulated institutions, irrespective of the industry in which the institutions operate. In this way, like risks are treated in a like manner. Harmonisation creates a common language and also simplifies compliance, particularly for groups that operate across regulated industries.

In September 2011, APRA released consolidated prudential standards on outsourcing, business continuity management, governance, and fitness and propriety. These prudential standards apply to the ADI, general and life insurance industries, recognising that, on behavioural matters, the risks facing regulated institutions in each of these industries are very similar. The standards were originally issued as industry-specific prudential standards but at different times, reflecting the different stages of development of APRA's regulatory requirements for each industry. Accordingly, although the substance of each prudential standard was the same across the industries, there were a number of minor differences in the requirements. These differences were harmonised in the consolidated prudential standards.

APRA now proposes to harmonise the current industry-specific risk management requirements by issuing draft CPS 220<sup>1</sup>. This new consolidated prudential standard is intended to replace the existing requirements for ADIs and insurers at Level 1, and extend these requirements to Level 2<sup>2</sup> and Level 3 groups. It will also replace some Level 1 and Level 2 ADI risk management requirements that are currently included in a number of ADI prudential standards.

The consolidated prudential standard will ensure harmonised prudential requirements apply across the ADI and insurance industries except, as discussed below, where there are specific reasons for

maintaining an industry-specific approach. Further, for Level 2 and Level 3 groups, the harmonisation of prudential requirements will support the oversight and management of group-wide risks, including material risks from non-APRA-regulated institutions within the group. Relevant guidance material will also be harmonised on a cross-industry basis.

In the superannuation industry, RSE licensees will not be subject to CPS 220 but will operate under the superannuation-specific risk management prudential standard due to commence on 1 July 2013.

## 1.2 Enhancements

Draft CPS 220 proposes a number of enhancements to APRA's existing risk management requirements to reflect and make more explicit its heightened expectations in this area. In some respects, the enhancements will underpin the improvements that have been made in risk management practices, locally and globally, in response to lessons learned in the global financial crisis. The crisis exposed serious shortcomings in the governance and risk management of major global financial institutions which are being addressed by institutions and prudential supervisors<sup>3</sup>.

APRA also proposes to make amendments to CPS 510 to ensure that governance requirements related to risk management are aligned with CPS 220.

## 1.3 Industry-specific requirements

In some areas, industry-specific requirements for risk management remain necessary and/or appropriate, particularly where there are underlying differences in the legislative framework applying to an industry. In such areas, the industry-specific requirements will be preserved in CPS 220 but clearly expressed as being applicable only to that industry or industries. Importantly, draft CPS 220 does not prescribe the manner in which a particular risk must be dealt with, other than as required under other prudential standards; this is similar to the approach

1 APRA proposes that CPS 220 will supersede *Prudential Standard GPS 220 Risk Management* (GPS 220) and *Prudential Standard LPS 220 Risk Management* (LPS 220).

2 Level 2 general insurers are currently subject to group-wide risk management requirements; hence, the extension will be to Level 2 ADIs and Level 2 NOHCs.

3 Governance lessons from the crisis and subsequent responses have been discussed by the APRA Chairman in a recent speech. See J. F. Laker, 'The Importance of Good Governance', Speech to the Australian British Chamber of Commerce, 27 February 2013.

taken in the existing risk management prudential standards for insurers. For example, draft CPS 220 does not prescribe the requirements for managing the operational risks associated with outsourcing and business continuity management, as they are addressed in the relevant prudential standards.

## 1.4 Timetable

APRA's intention is that the new CPS 220 and the revised CPS 510 will become effective on 1 January 2014. During the remainder of 2013, APRA will consult on a *Prudential Practice Guide CPG 220 Risk Management* that provides further guidance on good risk management practices.

## 1.5 Structure of this paper

This discussion paper outlines APRA's approach to harmonising its existing risk management prudential requirements (Chapter 2) and its proposed enhancements to these requirements to align with and underpin emerging good practice (Chapter 3). It also invites comments on the costs and benefits of APRA's proposals (Chapter 4).



## Chapter 2 – Harmonising existing risk management requirements

This chapter discusses APRA's approach to a new, consolidated prudential standard that harmonises the requirements of existing prudential standards GPS 220 and LPS 220 and incorporates risk management requirements for ADIs that are currently included in a number of ADI prudential standards. This new prudential standard is intended to apply to ADIs and insurers as well as Level 2 and Level 3 groups.

### 2.1 Harmonisation

Where there are differences in the current industry-specific prudential standards, APRA has retained the requirement that best reflects its current views. For example, where there is an inconsistency in the wording of current requirements that are similar in substance, APRA has chosen wording in draft CPS 220 that best reflects the substance of those requirements.

The main proposed changes to harmonise APRA's various risk management requirements are:

- the extension of the general insurance and life insurance minimum risk management framework requirements to ADIs. These minimum requirements include that an APRA-regulated institution must create and maintain:
  - a risk appetite statement;
  - a risk management strategy;
  - a business plan;
  - a designated risk management function; and
  - processes for reviewing the appropriateness, effectiveness and adequacy of the risk management framework;
- refining the definition of material risks to ensure applicability and consistency for ADIs and insurers;
- the extension of current insurer requirements for an annual and a three-year comprehensive risk management framework review to ADIs; and
- the alignment of annual risk management declaration requirements, which currently differ between industries.

APRA understands that ADIs largely meet these requirements in substance as part of their existing risk management practices. For example, the new

requirement for ADIs to have a risk management strategy is substantively aligned with the detailed descriptions of risk management systems required under *Prudential Standard APS 310 Audit and Related Matters* (APS 310). APRA therefore anticipates that these new requirements will not be onerous but will simply confirm accepted industry good practice.

### 2.2 General insurer requirements

APRA intends to move the general insurer run-off plan requirements, currently set out in paragraphs 22 to 28 of GPS 220, to either another existing prudential standard or a new stand-alone prudential standard applicable to run-off insurers. Further, APRA intends to move the general insurer financial information declaration requirements to *Prudential Standard GPS 310 Audit and Related Matters* (GPS 310). APRA is considering extending the financial information declaration requirements to ADIs, life insurers, Level 2 ADI groups and Level 3 groups, in the relevant industry-specific audit prudential standards. APRA intends to consult separately on these matters in the second half of 2013.

### 2.3 APRA-regulated institutions that are part of a group

APRA requires each APRA-regulated institution to meet its prudential requirements on an individual basis. Draft CPS 220 proposes that an institution that is part of a group can meet its risk management requirements on a group basis, provided that the Board of each regulated institution within the group is satisfied that it continues to meet its individual risk management obligations. APRA will retain its ability to require Level 1 institutions that APRA determines are not managing their risks appropriately to meet their risk management requirements on a separate basis from the group<sup>4</sup>.

Currently, there are different requirements between industries in relation to attestations regarding the adequacy of the risk management framework of an institution. In aligning its requirements in this area,

<sup>4</sup> APRA already has this ability in the case of Level 2 insurance groups.

APRA proposes that the chair of the Board and the chair of the Board Risk Committee (see Chapter 3) make an annual attestation as to the adequacy and effectiveness of its risk management framework. APRA will allow the Board of the Head of a Level 2 or Level 3 group to make a risk management attestation on behalf of the group and the Level 1 institutions within it.

## **2.4 APRA-regulated institutions that are the Head of a Level 2 group**

Under existing prudential requirements, APRA-regulated institutions that are the Head of a Level 2 group must establish a group-wide risk management framework to ensure that its Board oversees the risks of the group<sup>5</sup>. APRA proposes to clarify this requirement in draft CPS 220. It is proposing that a group-wide risk management framework must co-ordinate, identify, measure, evaluate, report and control or mitigate all material risks across the group. Further, this framework must capture material risks from the non-APRA-regulated institutions within the group. The purpose of the framework is to ensure that the Boards of the Heads of such APRA-regulated groups have oversight of the material risks across the group, including the material risks from non-APRA-regulated members. This requirement broadly reflects current industry practice. APRA observes that Boards of groups typically oversee all material risks to the group, whether these risks arise from APRA-regulated or non-APRA-regulated institutions in the group.

<sup>5</sup> These requirements are set out in *Prudential Standard APS 222 Associations with Related Entities* and GPS 220.

## Chapter 3 – Enhancing risk management requirements

Draft CPS 220 also incorporates a number of enhancements that reflect and make more explicit APRA's heightened expectations of risk management. These enhancements will underpin improvements in good practice in risk management, locally and globally, in response to the lessons learned in the global financial crisis. APRA also proposes to amend CPS 510 to ensure that it aligns with CPS 220 in relation to risk management governance requirements. This chapter discusses the key enhancements APRA proposes to make in draft CPS 220 and revised CPS 510.

APRA's proposed risk management governance amendments, which are highlighted in the draft CPS 510, apply as well to Level 3 groups and are in addition to the proposed Level 3-specific enhancements published by APRA in December 2012. APRA is currently reviewing submissions on the Level 3 draft CPS 510.

### Risk Management (CPS 220)

#### 3.1 Board oversight of risk management

Boards of APRA-regulated institutions have ultimate responsibility for their institution's risk management framework. APRA proposes to reinforce this principle by articulating specific requirements for Boards related to that ultimate responsibility.

#### 3.2 Risk management culture

The establishment and maintenance of a strong risk management culture is essential to the continued effectiveness of the risk management framework. Recent global experience has highlighted the importance of a strong risk management culture to effective risk management, in good times and bad. It is important that Boards set the 'tone at the top' to ensure that risk management is embedded in the daily operations and decision-making of their institutions. Draft CPS 220 makes explicit the responsibility of the Board for establishing and maintaining a strong risk management culture.

#### 3.3 Management information systems

Draft CPS 220 proposes that APRA-regulated institutions must have adequate management

information systems for the purpose of measuring, assessing and reporting on all material risks. Such systems are vital in providing clear oversight of risk throughout an organisation. APRA proposes that institutions must ensure their management information systems are able to produce regular, accurate and timely information on their risk profile to support risk-based decision-making.

#### 3.4 Risk management function and the Chief Risk Officer

Draft CPS 220 proposes that APRA-regulated institutions must establish and maintain designated risk management functions that have sufficient stature, authority and resourcing to support sound, risk-based decision-making. The risk management function is fundamental to an effective risk management framework. APRA also proposes to require institutions to designate a Chief Risk Officer (CRO) who is involved in, and provides effective challenge to, activities and decisions that may materially affect the risk profile of the institution. To reflect the importance of the role, draft CPS 220 proposes that the CRO be independent from business lines and the finance function. This requirement is intended to ensure that the CRO does not have other responsibilities that may conflict with his or her risk management role (i.e. no 'dual-hatting'). Draft CPS 220 proposes to explicitly exclude the CRO from also being the Chief Executive Officer (CEO), Chief Financial Officer, Appointed or Group Actuary (if applicable) or the Head of Internal Audit. Further, draft CPS 220 is intended to support the stature of the CRO role by proposing that it have a direct reporting line to the CEO and unfettered access to the Board.

#### 3.5 Consistency between business objectives and risk management framework

Draft CPS 220 proposes that there must be consistency between the business objectives of APRA-regulated institutions and their risk management framework to support sound, risk-based decision-making throughout the organisation. The risk appetite and business objectives should be commensurate with the risk profile and capital strength of the institution.

## Governance (CPS 510)

### 3.6 Board Risk Committee

In APRA's view, an independent Board Risk Committee is essential in providing the Board with greater oversight of and advice on the risk management framework. APRA proposes to include new requirements in CPS 510 for the establishment of a Board Risk Committee. Such a Committee would explicitly strengthen the governance, effectiveness and resourcing of the risk management framework. The Committee would be responsible for advising the Board on the appropriateness of the risk management framework, for providing the Board with objective non-executive oversight of the implementation of the framework, and for ensuring that senior management are appropriately implementing the Board's strategy for managing risk.

The proposals require the Committee to be composed of non-executive directors, be chaired by an independent director who is not the chair of the Board, and to provide endorsement prior to the appointment and removal of the CRO. This latter responsibility is consistent with the elevated stature and authority of the risk management function. The requirement for independent chairs of the Board Risk Committee and Board Audit Committee ensures that the Board maintains objective non-executive oversight of the risk management framework and financial reporting, respectively. The proposed composition requirements in CPS 510 for the Board Risk Committee do not preclude this Committee having the same composition as the Board Audit Committee. Nevertheless, APRA sees merit in appropriate diversity of membership of Board committees to assist in the clear delineation of oversight responsibilities. APRA notes that many APRA-regulated institutions already have a Board Risk Committee in place.

### 3.7 Board Audit Committee

The Board Audit Committee will continue to have responsibility for providing the Board, *inter alia*, with an objective review of the effectiveness of the institution's risk management framework.

CPS 510 also proposes to require the Board Audit Committee's prior endorsement of the appointment and removal of the external auditor and Head of Internal Audit. This extends the Committee's current responsibility for oversight of the appointment of the external auditor and APRA believes that this requirement is also appropriate for the Head of Internal Audit, who has a similarly important role in APRA-regulated institutions.

### APRA-regulated institutions that are the Head of a group

As noted earlier, APRA-regulated institutions that are the Head of a Level 2 group must establish a group-wide risk management framework to ensure that its Board oversees and manages the risks of the group under the existing prudential requirements. APRA proposes to extend these group requirements in draft CPS 220 to the Heads of Level 3 groups.

APRA also proposes to require that the Head of a Level 2 and/or Level 3 group develop and maintain a Board-approved liquidity management policy. APRA views liquidity management across a group as a fundamental component of the prudent operation of a group. Recent international experience has highlighted the detrimental financial impact on groups that have encountered material liquidity risks arising from business activities of the group that are not prudentially regulated.

## Chapter 4 – Cost-benefit analysis information

To improve the quality of regulation, the Australian Government requires all proposals to undergo a preliminary assessment to establish whether it is likely that there will be business compliance costs. In order to perform a comprehensive cost-benefit analysis, APRA welcomes information from interested parties on the financial impact of the changes proposed in this discussion paper and any other substantive costs associated with the proposed changes. These costs could include the impact on balance sheets, profit and loss, and capital.

As part of the consultation process, APRA also requests respondents to provide an assessment of the compliance impact of the proposed changes. Given that APRA's proposed requirements may impose some compliance and implementation costs, respondents may also indicate whether there are any other requirements that should be improved or removed to reduce compliance costs. In doing so, please explain what they are and why they need to be improved or removed.

Respondents are requested to use the Business Cost Calculator (BCC) to estimate costs to ensure that the data supplied to APRA can be aggregated and used in an industry-wide assessment. APRA would appreciate being provided with the input to the BCC as well as the final result. The BCC can be accessed at [www.finance.gov.au/obpr/bcc/index.html](http://www.finance.gov.au/obpr/bcc/index.html)



Telephone  
1300 55 88 49

Email  
[info@apra.gov.au](mailto:info@apra.gov.au)

Website  
[www.apra.gov.au](http://www.apra.gov.au)

Mail  
GPO Box 9836  
in all capital cities  
(except Hobart and Darwin)