



Response to Submissions

Harmonising cross-industry risk management requirements


January 2014

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/.

Preamble

In May 2013, APRA proposed 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). This standard would apply to authorised deposit-taking institutions, general insurers and life insurers, authorised non-operating holding companies, and Level 2 and Level 3 groups. CPS 220 does not apply to the superannuation industry. APRA also proposed enhancements to *Prudential Standard CPS 510 Governance* (CPS 510) to ensure risk management governance principles were aligned with draft CPS 220.

APRA is now releasing the final CPS 220 and CPS 510, accompanied by this response to submissions. APRA is also releasing for consultation a draft prudential practice guide that provides guidance on the application of CPS 220.

Written submissions on the draft guidance should be sent to riskmanagement@apra.gov.au by 28 March 2014 and addressed to:

Neil Grummitt
General Manager, Policy Development
Policy, Research and International
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

Glossary	5
Executive summary	6
Chapter 1 – Introduction	7
1.1 Background	7
1.2 Feedback from consultation	8
1.3 Draft guidance	8
1.4 Timetable	8
1.5 Structure of this paper	8
Chapter 2 – Risk management (CPS 220)	9
2.1 Independence of the CRO	9
2.2 Reporting line of a CRO	10
2.3 Management Information Systems	10
2.4 Role of the Board	10
2.5 General insurance requirements	11
Chapter 3 – Governance (CPS 510)	12
3.1 Separating the BRC and BAC	12
Chapter 4 – Australian branch operations	13
4.1 Application to Australian branch operations	13

Glossary

ADI	An authorised deposit-taking institution under the <i>Banking Act 1959</i> (Banking Act)
Appointed Actuary	An actuary appointed by the insurer under the <i>Insurance Act 1973</i> (Insurance Act) or the <i>Life Insurance Act 1995</i> (Life Insurance Act)
APRA	Australian Prudential Regulation Authority
APRA-regulated institution	An ADI, Extended Licensed Entity, insurer, Level 2 Head or Level 3 Head
Authorised NOHC	A non-operating holding company authorised under the Banking Act or Insurance Act or registered under the Life Insurance Act
BAC	Board Audit Committee
BRC	Board Risk Committee
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CPG 220	<i>Prudential Practice Guide CPG 220 Risk Management</i>
CPS 220	<i>Prudential Standard CPS 220 Risk Management</i>
CPS 510	<i>Prudential Standard CPS 510 Governance</i>
CRO	Chief Risk Officer or equivalent head of the risk management function
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 life insurer
Level 2 Head	An APRA-regulated institution heading a Level 2 group
Level 3 Head	An APRA-regulated institution heading a Level 3 group
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
May 2013 discussion paper	Discussion Paper, <i>Harmonising cross-industry risk management requirements</i> , May 2013
MIS	Management information systems. IT systems that can measure, assess and report on all material risks across an institution
Non-APRA-regulated institution	An institution other than an APRA-regulated institution or an RSE licensee
RSE licensee	A registrable superannuation entity licensee as defined in the <i>Superannuation Industry (Supervision) Act 1993</i>

Executive summary

This response paper sets out APRA's responses to submissions received during consultation on draft *Prudential Standard CPS 220 Risk Management* (CPS 220) and *Prudential Standard CPS 510 Governance* (CPS 510). APRA has now released CPS 220 and CPS 510 in final form. CPS 220 harmonises and consolidates the current risk management requirements that apply to ADIs, general insurers and life insurers (insurers), and authorised non-operating holding companies (NOHCs). CPS 220 also incorporates a number of enhancements to APRA's existing prudential requirements to reflect and make more explicit APRA's heightened expectations in this area. CPS 510 was also amended to ensure that governance requirements related to risk management are aligned with those in CPS 220.

The consolidated CPS 220 will ensure that consistent prudential requirements apply across the ADI and insurance industries, except where there are particular reasons for maintaining an industry-specific approach. Since its establishment, APRA has sought to take a consistent, harmonised approach to the setting of prudential requirements for APRA-regulated institutions, where appropriate, irrespective of the industry in which the institutions operate. In this way, similar risks are treated in a similar manner. Harmonisation also creates a common language and simplifies compliance, particularly for groups that operate across more than one regulated industry. APRA has already introduced cross-industry prudential standards addressing governance, fitness and propriety, outsourcing, and business continuity management. Further, for Level 2 and Level 3 groups, the harmonisation of prudential requirements will support the oversight and management of risks across the group, including material risks from non-APRA-regulated institutions within the group.

The enhancements to APRA's risk management requirements will underpin the improvements that have been made in risk management practices in response to lessons learned from 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 globally.

The most important of APRA's proposed risk management enhancements, which also attracted the largest number of submissions, were:

- the requirement that APRA-regulated 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; and
- the requirement that institutions have a Board Risk Committee (BRC) that provides the Board with objective non-executive oversight of the implementation and on-going operation of the institution's risk management framework.

Submissions raised concerns about potential resourcing constraints in having a CRO that does not have dual-hatting responsibilities. Submissions also sought clarification on why the BRC needs to be separate from the Board Audit Committee (BAC).

APRA has retained requirements to have a designated person, referred to in CPS 220 as the CRO, responsible for the risk management function. APRA has, however, revised CPS 220 to clarify that the CRO can fulfil other roles and responsibilities. Further, CPS 220 has been revised to allow APRA, where appropriate, to consider alternative arrangements for institutions that can demonstrate they meet, in substance, the principles underlying the CRO requirements; such arrangements would be expected to apply to smaller and less complex institutions. APRA has not changed its proposal to require a separate BRC and BAC but has provided additional rationale in this response paper.

This response paper is accompanied by CPS 220 and CPS 510 in final form as well as a draft prudential practice guide for risk management. The draft guidance is open for consultation until 28 March 2014, while CPS 220 and the revised CPS 510 will become effective from 1 January 2015.

Registrable superannuation entity (RSE) licensees will not be subject to CPS 220 but will be required to comply with the superannuation-specific *Prudential Standard SPS 220 Risk Management* (SPS 220), which commenced on 1 July 2013. SPS 220 is substantially consistent with CPS 220 although it reflects aspects of risk management that are specific to the superannuation industry.

Chapter 1 – Introduction

1.1 Background

In its May 2013 discussion paper, APRA outlined its proposed approach to harmonising, consolidating and enhancing a number of risk management requirements, which are set out in existing prudential standards that apply to ADIs, 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 governance, fitness and propriety, outsourcing and business continuity management. These prudential standards apply equally to ADIs, insurers and authorised NOHCs. APRA proposed to continue this process of harmonisation with CPS 220, a consolidated risk management standard that would also apply to Level 2 and Level 3 groups. APRA did not propose to apply CPS 220 to the APRA-regulated superannuation industry.

Draft CPS 220 intended to consolidate APRA's existing risk management requirements for insurers and replace some ADI risk management requirements that are currently included in a number of ADI prudential standards. APRA will revoke *Prudential Standard GPS 220 Risk Management (GPS 220)* and *Prudential Standard LPS 220 Risk Management (LPS 220)* by 1 January 2015.

In addition, draft CPS 220 proposed a number of enhancements to APRA's existing prudential requirements to reflect and make more explicit heightened expectations in this area. In some respects, the enhancements will underpin the improvements that have been made in risk management practices in response to lessons learned from the global financial crisis.

APRA also proposed to update CPS 510 to ensure that governance requirements related to risk management were aligned with those in CPS 220.

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

- the requirement that APRA-regulated institutions designate a 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. In particular, APRA proposed that the CRO cannot be the Chief Executive Officer (CEO), Chief Financial Officer (CFO), the Appointed Actuary or the Head of Internal Audit; and
- the requirement that institutions have a BRC that provides the Board with objective non-executive oversight of the implementation and operation of the institution's risk management framework. APRA proposed that this committee must operate under a different charter than the BAC, although APRA's composition requirements would not prohibit the same people sitting on both committees.

APRA proposed to maintain its principles-based approach to the application of its risk management requirements and indicated that it would, where appropriate, consider alternative arrangements for institutions that can demonstrate they meet, in substance, the principles underlying the requirements. APRA expects that alternative arrangements would be limited to smaller and less complex institutions, as outlined in draft *Prudential Practice Guide CPG 220 Risk Management (CPG 220)*.

APRA has considered issues raised in submissions and made amendments to the draft prudential standards, where appropriate. This response paper summarises the main issues raised in submissions, along with APRA's response. APRA is now releasing CPS 220 and CPS 510 in final form. The new risk management requirements will become effective from 1 January 2015.

1.2 Feedback from consultation

APRA received 44 submissions from a wide range of stakeholders, including ADIs, insurers and industry and professional bodies, on the proposals contained in the May 2013 discussion paper, released with draft CPS 220 and CPS 510. In addition to these submissions, APRA has received feedback via industry workshops and meetings with institutions and other stakeholders.

Most feedback was supportive of APRA's objectives and the broad direction of the proposed CPS 220 and CPS 510. However, some concerns were raised about specific aspects of the proposals, which APRA has addressed in this paper.

1.3 Draft guidance

Submissions sought additional guidance on APRA's expectations for risk management in a number of areas. APRA has addressed these areas in draft CPG 220, which accompanies the release of this response paper. Consultation on draft CPG 220 closes on 28 March 2014 and APRA expects to release the final CPG 220 in the first half of 2014.

1.4 Timetable

A number of submissions were concerned with the proposed implementation date of 1 January 2014 for CPS 220 and CPS 510. In response, APRA indicated in its letter of 14 August 2013¹ to ADIs, insurers and Level 2 Heads that it was delaying the implementation date of the finalised CPS 220 and CPS 510 to 1 January 2015. APRA considers this will provide industry with sufficient time to comply fully with the new requirements.

As indicated in the May 2013 discussion paper, CPS 220 will replace a number of requirements for ADIs, insurers and Level 2 Heads. APRA will assess what consequential changes need to be made to other prudential standards and will remove any duplication over 2014. The existing industry-specific risk management requirements and the existing version of CPS 510 will continue to apply to ADIs, insurers and Level 2 Heads until 1 January 2015.

¹ <http://www.apra.gov.au/CrossIndustry/Consultations/Pages/May-2013-Consultation-Risk-Management.aspx>

1.5 Structure of this paper

Chapters 2 and 3 discuss submissions on the CPS 220 proposals and CPS 510 proposals, respectively. Chapter 4 clarifies APRA's expectations on the application of the risk management requirements to Australian branch operations.

Chapter 2 – Risk management (CPS 220)

APRA proposed that each APRA-regulated institution establish and maintain a risk management function headed by a designated CRO to support sound, risk-based decision-making in the institution. To heighten the importance and stature of a CRO within an institution, draft CPS 220 proposed that the CRO must:

- be independent from business lines, other revenue-generating responsibilities and the finance function;
- be explicitly excluded from also being the CEO, CFO, Appointed Actuary or the Head of Internal Audit; and
- have a direct reporting line to the CEO, and regular and unfettered access to the Board and BRC.

2.1 Independence of the CRO

Comments received

Submissions suggested that it was more important to have an objective rather than an operationally independent CRO, given that integration with business operations facilitates an understanding of the risks to the business. Further, a number of submissions argued that the CRO should not be prohibited from dual-hatting with the roles identified in CPS 220, particularly the Appointed Actuary.

APRA's response

APRA expects that, consistent with the three lines-of-defence model², a risk management function's responsibility is to establish systems and controls to support risks being managed by the first line-of-defence i.e. business operations. An effective risk management function would interact and engage with personnel across an APRA-regulated institution to understand the risks to that institution. APRA expects the risk management function to have influence on and provide appropriate challenge to the first line-of-defence, but does not expect the function to be undertaking the roles and responsibilities or owning the risks undertaken by the first line-of-defence.

Draft CPS 220 reflected the importance of having a person with clear responsibility for the risk management function and who can objectively challenge activities and decisions that may materially affect the institution's risk profile. APRA has revised the wording in the standard to clarify its intent that institutions must 'designate' (rather than 'dedicate') a person responsible for the risk management function. This means that, firstly, institutions are not required to classify such a person as a 'CRO'. APRA has referred to such a role as a CRO for ease of reference.

Secondly, institutions may allocate roles and responsibilities to the CRO, other than those explicitly excluded, so long as any actual or potential conflict of interest is appropriately managed or mitigated. A CRO that engages in dual-hatting would be subject to a conflict of interest where he or she is effectively challenging their own decisions. However, an institution may deem it appropriate to have a CRO who, for example, is also the head of the compliance function.

CPS 220 recognises that an institution may seek approval for alternative arrangements where the institution is materially constrained in appointing a CRO who is free from conflicts of interest, or for reasons particular to that institution. APRA expects these instances would be limited to smaller and less complex institutions. Where an institution seeks an alternative arrangement 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 the additional risk, and is satisfied that these mitigants are adhered to. APRA will assess the appropriateness of alternative arrangements on a case-by-case basis. Draft CPG 220 provides a set of factors that APRA expects a Board to consider when applying for alternative arrangements. APRA expects that institutions will already have persons responsible for risk management or who, with the appropriate training, could undertake such a role. An Appointed Actuary has to provide an opinion on the financial position and value of liabilities of the institution and

² For additional guidance see draft CPG 220, which has been released with this response paper.

has other responsibilities that are considered part of the first line-of-defence. These responsibilities include an assessment of the suitability and adequacy of the risk management framework.³ These roles and responsibilities of the Appointed Actuary mean that, if he or she were also the CRO, the objectiveness of the assessment of the risk management framework may be compromised. For the above reasons, the final CPS 220 continues to preclude the Appointed Actuary from being the CRO.

2.2 Reporting line of a CRO

Comments received

Submissions acknowledged the importance of the CRO having unfettered access to the Board, the BRC and the CEO. However, submissions suggested that the CRO should not be required to report directly to the CEO, as the Board of an APRA-regulated institution should decide what reporting structure is appropriate to its operations.

APRA's response

It is important that the CRO has the stature and authority to influence actions and decisions that may materially impact on an APRA-regulated institution's risk profile. To reflect this importance, the CRO needs to have a seat at the executive management table, members of which report directly to the CEO. Accordingly, APRA has not changed its position on the CRO reporting to the CEO and has maintained this requirement in the final CPS 220.

2.3 Management Information Systems

The May 2013 discussion paper proposed that APRA-regulated institutions must have adequate management information systems (MIS) for the purpose of measuring, assessing and reporting on all material risks. Draft CPS 220 proposed that MIS must be able to produce regular, accurate and timely information on the institution's risk profile to support risk-based decision-making.

Comments received

Submissions noted that comprehensive MIS can be an expensive, complicated and time-consuming process. Submissions suggested that the requirements regarding MIS in CPS 220 should have regard to the relative size, business mix and complexity of the APRA-regulated institution.

APRA's response

MIS are key elements of the risk management framework of APRA-regulated institutions. MIS should be 'fit for purpose' and support the identification of exposures and risk measures across business lines, prompt reporting of limit breaches, and forward-looking scenario analysis and stress testing.

Accordingly, APRA has not amended draft CPS 220 as it already acknowledges that MIS would reflect the size, business mix and complexity of the institution.

2.4 Role of the Board

Draft CPS 220 identified key Board responsibilities to establish and maintain a sound risk management framework.

Comments received

Submissions sought to clarify APRA's intent for the requirement on the Board to 'ensure' it fulfils its responsibilities, given there are limitations on what a Board can ensure. Submissions suggested changing the requirement to the Board taking 'reasonable steps to ensure' its responsibilities are fulfilled. Submissions interpreted the word 'ensure' as also potentially blurring the roles and responsibilities of the Board and senior management.

³ Refer to *Prudential Standard GPS 320 Actuarial and Related Matters* and *Prudential Standard LPS 320 Actuarial and Related Matters*.

APRA's response

These comments appear to reflect a lack of understanding about what APRA means by the word 'ensure'. The Board is ultimately responsible for the APRA-regulated institution and APRA expects that Board members would meet their particular responsibilities for risk governance, including via the establishment of an appropriate governance structure, setting the institution's risk appetite, oversight of the effectiveness of the risk management framework, and setting the 'tone at the top' for a sound risk culture. The Board would take both active and reactive steps so that, to the best of its knowledge and having made appropriate enquiries, it meets its responsibilities. For example, when the Board approves the risk management strategy, it would consider what risk issues should be escalated to the Board. Where the Board becomes aware of any material issues with the risk management framework, APRA expects the Board to remedy those issues.

A Board can delegate to its committees and senior management the implementation of elements of the risk management framework. However, delegation of authority will not absolve the Board of accountability for overseeing the adequacy and appropriateness of the risk management framework and its implementation. APRA expects that any delegation of responsibilities will be accompanied by clearly documented roles and reporting structures to allow Board oversight to be maintained. APRA also expects that the Board's governance structure would clearly state the Board's responsibilities and explain how those responsibilities differ from, and relate to, the responsibilities of senior management. Accordingly, APRA has not changed the draft CPS 220.

2.5 General insurance requirements

In the May 2013 discussion paper, APRA indicated its intention to move the run-off plan requirements for run-off insurers, currently set out in paragraphs 22 to 28 of GPS 220, to another general insurance prudential standard. APRA will place the unchanged requirements in an attachment to *Prudential Standard GPS 110 Capital Adequacy* (GPS 110) that will be released to the general insurance industry in the second half of 2014.

In the discussion paper, APRA also indicated its intention to move the financial information declaration requirements to *Prudential Standard GPS 310 Audit and Related Matters* (GPS 310). APRA will release an updated version of GPS 310, with no changes to the requirements for the financial information declaration, to the general insurance industry in the second half of 2014.

Chapter 3 – Governance (CPS 510)

In the May 2013 discussion paper, APRA expressed its view that an independent BRC is essential to provide the Board with greater oversight of, and advice on, the risk management framework. Accordingly, APRA proposed new requirements in CPS 510 for the establishment of a BRC to strengthen its requirements in this area. The BRC would be responsible for advising the Board on the risk management framework, providing the Board with objective non-executive oversight of implementation of the framework, and ensuring that senior management are appropriately implementing the Board's strategy for managing risk.

APRA proposed that the BRC be composed of non-executive directors, chaired by an independent director who is not the chair of the Board, and provide its endorsement prior to the appointment and removal of the CRO. The proposed composition requirements in CPS 510 did not preclude the BRC having the same composition as the BAC. APRA noted that many APRA-regulated institutions already have a BRC in place.

3.1 Separating the BRC and BAC

Comments received

Submissions sought clarity on APRA's rationale for a BRC to be separate from the BAC, as some viewed this separation to be form over substance. Submissions identified that some APRA-regulated institutions currently have a combined committee overseeing both risk management and audit matters. Some submissions also noted that the Board is already overseeing both risk management and audit matters.

APRA's response

In APRA's view, it is important to separate the BRC and BAC to ensure a clear and distinct focus on the oversight of risk management and audit issues. From the perspective of the three lines-of-defence model, the BAC oversees independent assurance of the first and second lines-of-defence provided by auditors in the third line-of-defence. In contrast, the focus of the BRC is on oversight of implementation of the risk management framework, as provided by the risk management function in the second line-of-defence.

Clear delineation of oversight responsibilities supports the appropriate allocation of resources on both audit and risk management issues. Therefore, APRA has not changed the proposed requirements in CPS 510 for a separate BRC and BAC. To accommodate Boards of smaller and less complex institutions that, accordingly, may oversee fewer and less complex issues, the composition requirements in CPS 510 do not preclude the BRC having the same membership as the BAC. Nevertheless, APRA sees merit in appropriate diversity of membership to assist in the clear delineation of responsibilities and ensure that members can allocate sufficient resources to meet their responsibilities to the respective committees. For example, a Board may decide to have the same membership of both committees, but have different chairpersons. In APRA's view, the benefit of separating board committees outweighs the minor costs in making the adjustments to processes needed and has therefore maintained the requirement for separation in CPS 510.

Finally, the establishment of a separate BRC is also consistent with the elevated stature and authority of the designated risk management function, as outlined in Chapter 2.

Chapter 4 – Australian branch operations

The May 2013 discussion paper proposed that CPS 220 and CPS 510 apply to APRA-regulated institutions. In response to submissions, APRA has provided guidance to clarify its expectations on the application to Australian branch operations in draft CPG 220.

4.1 Application to Australian branch operations

Comments received

Submissions from Australian branch operations queried whether a group risk management framework can be used to meet the requirements in CPS 220.

APRA's response

CPS 220 requires Australian branch operations to have a designated CRO who is involved in, and provides effective challenge to, activities and decisions that may materially affect the institution's risk profile. In addition, the CRO is to be free from conflicts of interest and report to the CEO.

Australian branches may use an overseas group risk management function and/or audit function, including a regional or group CRO and/or auditors. APRA recognises that there may be practical impediments for an overseas CRO to report to the domestic CEO and that the practice of using overseas group auditors on a biennial basis may not comply with requirements to review the risk management framework annually.

Considering these practical impediments, Australian branches may seek APRA's approval for alternative arrangements where a Senior Officer Outside of Australia or Compliance Committee (as applicable) can demonstrate that the branch operations meet, in substance, the principles underlying the requirements.

As noted above, when considering alternative arrangements, APRA will take into account the size, business mix and complexity of the APRA-regulated institution. Draft CPG 220 provides additional guidance on APRA's expectations for branch operations seeking approval of alternative arrangements.



Telephone
1300 55 88 49

Email
info@apra.gov.au

Website
www.apra.gov.au

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