AUSTRALIAN BANKERS' ASSOCIATION INC.

Brendon Harper
Associate Director, Industry Policy & Strategy

AUSTRALIAN BANKERS' ASSOCIATION INC.
Level 3, 56 Pitt Street, Sydney NSW 2000
p. +61 (0)2 8298 0409 **f.** +61 (0)2 8298 0402

www.bankers.asn.au

28 March 2014

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

Dear Neil,

Harmonising cross-industry risk management requirements

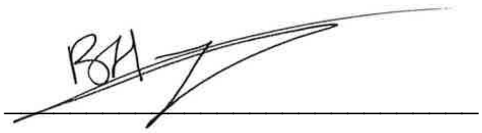
The Australian Bankers' Association (ABA) welcomes the opportunity to provide feedback on APRA's:

- Response to Submissions, Harmonising cross-industry risk management requirements; and
- Draft Prudential Practice Guide, CPG 220 – Risk Management.

The ABA and its members are supportive of APRA's ongoing commitment to improve risk management capabilities and the harmonisation of risk management practices across industries.

The attached submission is provided for APRA's consideration.

Yours sincerely,



Brendon Harper

AUSTRALIAN BANKERS' ASSOCIATION INC.

Submission

Harmonising cross-industry risk management requirements

28 March 2014

Australian Bankers' Association Inc. ARBN 117 262 978
(Incorporated in New South Wales). Liability of members is limited.

Contents

The Australian Bankers' Association (**ABA**) welcomes the opportunity to provide feedback on APRA's:

- Response to Submissions, *Harmonising cross-industry risk management requirements*; and
- Draft Prudential Practice Guide, *CPG 220 – Risk Management*.

The ABA and its members are supportive of APRA's ongoing commitment to improve risk management capabilities and the harmonisation of risk management practices across industries.

The following comments are provided for APRA's consideration.

1. Introduction

Sound risk management is essential for the safety, stability and ultimately the profitability of organisations; this is especially true for financial institutions. Australian banks have well established and well tested risk management processes and procedures. Conservative risk settings and robust risk management were key factors contributing to how well Australian banks withstood the Global Financial Crisis.

While the ABA supports moves to improve the quality and consistency of risk management (requirements) across the sector, it does have a number of concerns with APRA's recent response to submissions and draft CPG 220. The ABA's major concerns are:

- APRA's apparent view that certain Board Committees form part of the three Lines of Defence (**3LOD**); and
- the proposed substantial increase in requirements for Boards.

With regard to the first matter, the industry fundamentally disagrees with APRA's view that the Board Risk Committee (**BRC**) and Board Audit Committee (**BAC**) form part of Lines two and three, respectively, of the 3LOD. Industry considers these Committees as overseeing the 3LOD, on behalf of the Board.

With regard to the second matter, the ABA supports the view that Boards should be highly capable and qualified, and properly engaged. However, many of the proposed Board requirements (refer to Appendix A for details) are unnecessarily burdensome and, as previously highlighted by the ABA, may put at risk the capacity of banks to attract high quality board members. This is further exacerbated by some responsibilities being moved to the Board which the ABA believe should be the task of management.

Additionally, the ABA has a number of points on which it is seeking clarification in regards to the CPG 220.

2. Board requirements

Banking is a complex industry and a vital enabler of the Australian economy. As such, the community is right to hold high expectations of banks' Boards. Arguably, some of the bank failures experienced in other jurisdictions may have been avoided or minimised if Board members were more engaged and better understood the risks faced by their institutions. While being supportive of moves to improve risk management capabilities, the ABA would like to re-iterate its concerns that some elements of the proposals in CPS 220 and CPG 220 place a number of additional requirements on Boards.

2.1. Expanded role of the Board

In Australia, banks' Boards have proven to be conservative, engaged and subject to stringent requirements. Given this, the justification for the proposed substantial expansion of Board requirements is unclear.

Boards are already subject to strict requirements. Adding substantially more requirements may reduce the pool of potential board members that have all the required skills to be eligible to sit on banks' Boards. Furthermore, the proposed additional requirements may reduce the willingness of some potential board members to take on such a role. The (additional) personal liability implications stemming from the proposed requirements may also provide a disincentive.[1] Were ASIC to bring proceedings against directors for breach of their duty of care and diligence, a critically important question for the court would be to identify the 'responsibilities' of the directors. APRA's Prudential Standards and Practice Guides would provide evidence for the court concerning the details of those responsibilities.

On the basis of CPS 220 and draft CPG 220, directors would be exposed to an unacceptably high and unattainable level of responsibilities. This is further compounded by the requirements under CPS 520 for fitness and propriety, including requirements for independence and no conflict with other directorships. As such, these additional requirements may well further narrow the field of experienced and qualified candidates of potential board members that have all the required skills to be eligible to sit on banks' Boards.

The impact of a reduced pool of qualified potential board members and, of those, a reduced pool of willing board members is of real concern. Requirements that reduce the size and diversity of that pool may lead to increasingly homogenous Boards; this would be a perverse outcome and may reduce Boards' ability to anticipate and respond to new risks.

A further concern associated with the expanded responsibilities of the Board is that this may detract from the Board's focus on strategic, 'big picture' oversight and scanning of over the horizon risks. In particular, the requirements may limit capacity of Boards to effectively challenge and question management decisions and actions.

[1] This is an issue the ABA is still exploring.

2.2. Role of Board vs. role of management

The ABA is concerned with how APRA appears to be viewing the role of the Board and its Committees compared to the role of management. Management is responsible for the day-to-day operation of the business; while the function of the Board is to set the high-level direction for the institution and oversight implementation of this by management.

In its submission on the draft CPS, industry expressed its concerns with the use and intent of the word "ensure" in paragraph 13 - inferring a level of managerial ownership by the Board of the issues set out in that paragraph that is beyond being "reasonably satisfied" over these items. Unfortunately, neither the response nor the guidance from APRA have provided any further clarity or comfort to industry that expectations of Boards are not being significantly increased beyond today's levels. In the ABA's opinion, the guidance should make it clear that the Board can rely on management to implement the risk management framework provided there is appropriate inquiry and challenge by the Board and evidence demonstrating that this has been effectively completed.

In the ABA's view, the description articulated in the current APG 510 reflects a more appropriate and clearer distinction between Board and management responsibilities:

- The Board has ultimate responsibility for the sound and prudent management of a regulated institution. A well-functioning Board will review and approve business strategies and significant policies of the regulated institution. It will also satisfy itself that an effective system of risk management and internal control is established and maintained, and that senior management monitors the effectiveness of the risk management framework.
- Senior management has responsibility for day-to-day management of the regulated institution. This includes the implementation and monitoring of structures, processes, information and oversight arrangements used in managing the regulated institution.

2.3. The Board's role in the 3 Lines of Defence structure

The ABA disagrees with the way that APRA appears to view the role of the Board Committees in the 3LOD structure. The ABA considers that the Board and its Board Committees are served by, and oversee, the 3LOD structure in its entirety rather than being a part of it (as shown in the illustration in CPG 220 Appendix A Paragraph 10). In particular, the Board Risk Committee (BRC) is responsible for oversight of management's risk management practices across all 3LOD. It would not seem appropriate, therefore, to make them part of the second line of defence; similarly it would not seem appropriate to introduce a hierarchy within the Board whereby the BRC (as part of the second line of defence) is overseen by the BAC (in its third line of defence capacity).

In addition, mirroring management's risk management lines at Board level would not add the 'across all lines' view and would perpetuate the 'silo' approach between each line of defence, increasing the likelihood of issues 'falling between the silos' and being missed.

Furthermore, it is unclear how the BRC and BAC could have the same membership (as allowed under CPS 510) but provide different levels of assurance under 3LOD. This would appear to

represent a conflict of interest, which was defined in APRA's response to consultation as being where somebody would be "challenging their own decisions".

To illustrate the breadth of CPG 220, Appendix A of this submission summarises the potential additional requirements to Boards.

3. Points for clarification in CPG 220

3.1. Paragraph 6

The wording in Paragraph 6 suggests that the BRC is part of the second line of defence and somehow plays a role in developing risk management policies, systems, processes etc., providing specialist advice and training to the Board. The BRC is not a part of the second line of defence, and it does not develop risk management policies, systems, processes etc., nor provide specialist advice and training to the Board. Rather it provides oversight on behalf of the Board of the establishment, implementation and ongoing effectiveness of the risk management framework within the context of the risk appetite determined by the Board.

3.2. Paragraph 6(d)

Paragraph 6(d) refers to the second line of defence as having "oversight of the risk profile". The ABA notes that 'risk profile' is not defined by APRA in the Prudential Standard CPS 220 or CPG 220. However, it is defined by the Financial Stability Board (**FSB**) in its publication 'Principles for an effective risk appetite framework' released on 18 November 2013. Is APRA's interpretation of the definition of 'risk profile' consistent with the definition of the FSB?

3.3. Paragraphs 19-23 – Section 22

It is not clear what "corporate group" means - is APRA referring to an offshore entity of an Australian group and an onshore entity of an international group?

It is also not clear why APRA have just referred to group in paragraph 19-21 and changed the reference in section 22 to "corporate group".

In respect to paragraph 22, can APRA clarify what it means by saying it "expects the institution to assess the appropriateness of links with the group's risk management framework and be able to provide a summary of this assessment"? It is unclear what is meant by this; could APRA provide some examples of where Level 1 entities might have links to the Group's risk management frameworks?

As most Level 3 candidates have developed their frameworks from the outset and/or in parallel to fit all of their "cross-industry" APRA–authorised entities, it seems unnecessary duplication and counterintuitive to have these requirements. Is APRA able to offer a simpler solution for compliance? For example, where APRA is sufficiently comfortable, based on its (frontline supervisory) knowledge of the Level 3 candidate and its history, it could exempt an entity from needing to produce the summary assessments under paragraph 22.

3.4. Paragraph 26

To align paragraph 26 with the wording of paragraph 38, the ABA suggests the following change:

> *"APRA expects that … would be the management of risks in a way that is consistent with ~~both~~ the best interests of … policyholders, with the maintenance of the sound financial position of the institution and with the institution's strategic objectives and business plan."*

3.5. Paragraph 50

In relation to paragraph 50, the ABA acknowledges the guidance, but makes the observation that there may be circumstances where a risk exposure is outside risk tolerance, but after consideration and evaluation of the situation by an institution, a decision may be made to increase the risk tolerance.

3.6. Paragraph 53

This paragraph states that "the role of the APRA-regulated institution's risk management function is to assist the Board and senior management to develop, implement and maintain the risk management framework…." It is the belief of industry that it is not the Board's role to develop, implement and maintain the risk management framework – this is part of the day-to-day management responsibilities of management, and in turn management's performance is then subject to oversight, review and challenge by the Board/BRC.

3.7. Paragraph 54

Paragraph 54 discusses risk management assisting "the Board in building risk management capabilities throughout the APRA-regulated institution...." Again, it is the view of industry that it is not the Board's responsibility to be involved in the day-to-day activity of building risk management capabilities. This is a management function, and in turn the risk management capabilities throughout the institution should be reviewed as part of the Board/BRC's ongoing oversight, review and challenge of the effectiveness of the Risk Management Framework.

3.8. Paragraph 62 (last sentence)

It is unclear what is meant by this statement and it appears to go beyond any requirements stated in the Standard. Where the CRO of a Level 1 entity has direct access to the CEO and Board of that entity (even though that CRO's management reporting line is through to the Group CRO) industry's view is that the Level 1 entity Board is reliant on the Level 1 entity CRO and is not, therefore, dependent on the Group CRO "fulfilling his or her responsibilities to that institution on a Level 1 basis". Can APRA provide guidance on this point?

3.9. Paragraph 75

Paragraph 75 allows annual reviews of elements of the risk management framework to be performed on a rotational basis. However, the ABA notes that this paragraph requires "the annual review signoff would include those reviews conducted during the previous year." The ABA seeks clarification on the interpretation of this statement. For example, does previous year mean previous calendar year?

3.10. Paragraph 77

Paragraph 77 requires "the comprehensive review to be conducted by operationally independent, appropriately trained and competent persons at least every three years".

Can the third line of defence or external auditors perform this role? From a practical perspective internal/external auditors would likely be involved in the annual review. Would APRA be comfortable if the same people performed the more comprehensive review every three years, given its different remit (appropriateness and adequacy vs. compliance and effectiveness)?

3.11. Paragraphs 84-86

Can APRA provide clarity on the Risk Declaration requirements? In particular, can APRA confirm that it will be streamlining the requirements in APS 310 with regards to "risk management systems" now that they are covered in CPS 220 for ADIs and will the incoming 3PS 310 replace APS 310 for Level 3 groups headed by an ADI?

Paragraph 85 allows an "APRA-regulated institution's risk management declaration to be encompassed in the risk management declaration documentation of a Level 2 and/or Level 3 group" and that "where a Level 1 institution's declaration is encompassed within the group declaration, the Level 1 institution's Board remains responsible for any qualifications in the declaration that relate to that institution". Given the above statements, the ABA understands this to mean that a Level 1 institution within a Level 3 group is not required to provide a separate declaration to APRA where its declaration is encompassed in the Level 3 group declaration. However, does APRA expect Level 3 groups to develop an internal declaration process for Level 1 institutions in order to support a Level 3 risk management declaration?

Additionally, it is unclear to industry if there are different dates for when regulated institutions need to report to APRA. APRA's clarity on this point would be appreciated. If regulated institutions do need to report at different dates, the ABA has the following enquiry:

- Paragraph 86 provides guidance on when the risk management declaration is required to be submitted to APRA. In the event a Level 3 group comprises more than one regulated institution (for example, includes both an ADI and life insurance entity) and there is a conflict on the date which the accounts are to be submitted to APRA, which date will prevail?

3.12. Paragraph 5 of Appendix A

Paragraph 5 of Appendix A discusses the Board being responsible to ensure that risk management functions have adequately experienced staff with relevant technical knowledge and experience etc. It is the ABA's view that this is a day-to-day responsibility of management (not the Board). Additionally, this requirement appears to contradict obligations under CPS 520.

3.13. Paragraph 9 of Appendix A

This paragraph discusses the need to separate the BRC and Audit Committee, recognising "the distinct responsibilities for audit's role in the third line of defence and risk management's role in the second line of defence for independent assurance and risk management, respectively". The wording here is not clear, taking into account the wording in Paragraph 6 (referred to above). It again gives rise to a concern in relation to APRA's position on the role of the Board and its Committees. It appears, the second line of defence includes the risk management function and the third line of defence includes internal and external audit functions. The Board and its Committees are not part of the second and third lines of defence. Instead the Board and the Risk Committee receive reports from representatives within each of the 3LOD to assist the Board (and the Risk Committee) in carrying out its oversight function.

Appendix A – Extracts highlighting board responsibilities

Draft prudential practice guide – CPG 220 – Risk Management

(Excluding requirements that already form part of the prudential standard or provide clarification on the standard; emphasis added)

Section	Heading	Extract
6	Risk governance	The second line-of-defence comprises the specialist risk management function(s) and responsible Board Risk Committee(s) that are functionally independent from the first line-of-defence. The second line-of-defence **supports the Board of directors** (the Board)[2] in three key areas, by: (a) developing risk management policies, systems and processes to facilitate a consistent approach to the identification, assessment and management of risks; (b) providing specialist advice and **training to the Board** and first line-of-defence on risk related matters; (c) objective review and challenge of: (i) the consistent and effective implementation of the risk management framework throughout the APRA-regulated institution; and (ii) the data and information captured as part of the risk management framework which are used in the decision-making processes within the business, in particular the completeness and appropriateness of the risk identification and analysis, ongoing effectiveness of risk controls, and prioritisation and management of action plans; and (d) oversight of the risk profile and its reporting and **escalation to the Board.**

[2] For the purposes of this PPG, a reference to the Board, in the case of a foreign ADI, Category C insurer or an Eligible Foreign Life Insurance Company, is a reference to the Senior Officer Outside of Australia or Compliance Committee (as applicable) as referred to in Prudential Standard CPS 510 Governance (CPS 510).

Section	Heading	Extract
7	Risk Governance	The third line-of-defence comprises the independent assurance function and Board Audit Committee, each of whom provides independent assurance to the Board that: (a) the risk management framework is appropriate for the APRA-regulated institution, consistently implemented and operating effectively. This includes an assessment of the overall framework and the effectiveness of risk management practices, including its influence on decision-making; and (b) the policies, procedures and systems are appropriately designed and consistently implemented to operate effectively.
9	Role of the Board	**The Board may delegate responsibilities to its committees and senior management** but this **will not absolve the Board from ensuring its responsibilities are fulfilled**. APRA expects that any delegation of responsibilities will be accompanied by clearly documented roles and reporting structures to **ensure Board oversight is maintained**.
12	Role of the Board	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. For example, **APRA expects a Board would determine when risk issues should be escalated to it**. Where risk issues have failed to be appropriately escalated, **APRA expects the Board to remedy the failure**. APRA takes a pragmatic approach to assessing whether a Board is fulfilling its responsibilities in practice, and will assess steps taken by the Board to support an appropriate risk management framework.
27	Risk Management Framework	**APRA expects the Board** and senior management to **know and understand** the APRA-regulated institution's **operational structure and associated risks**. Risk can arise from structures that impede transparency, such as special-purpose or related structures. APRA **expects the Board** and senior management to **consider the implications of the institution's structure in facilitating effective risk management**.
28	Risk Management Framework	Stress testing, including both scenario analysis and sensitivity analysis, is used to assess a range of potential impacts on different material risks. Stress testing is important in considering potential changes that could occur in the external operating environment,

Section	Heading	Extract
		and provides a more forward-looking view of an APRA-regulated institution's risk profile. APRA expects that **stress testing** would be based on a combination of robust modelling and informed expert judgement, with effective senior management engagement and **Board oversight**.
40	Risk Appetite Statement	APRA expects that the **Board would be actively engaged in developing and reviewing the risk appetite statement**, and would be able to **demonstrate ownership of the statement**. APRA considers that this might be achieved, in part, through reporting and communication processes and structures that enable the Board and Board Risk Committee to: (a) identify the APRA-regulated institution's overall current risk profile and how this compares to its risk appetite and capital strength; (b) understand how senior management interprets and applies risk tolerances; (c) be satisfied that senior management's interpretation and application of the risk appetite is appropriate; (d) appropriately align risk appetite to the approach adopted in the risk management framework for assessing, monitoring and managing the different material risks; and (e) take factors (a), (b), (c) and (d) into account when reviewing the risk appetite statement.
43	Risk Appetite Statement	An APRA-regulated institution would generally use a variety of approaches and processes to assess different material risks. An institution with the capability to use risk quantification techniques would generally use them in the setting and monitoring of its risk appetite statement. Risk quantification techniques may provide an institution with assurance that the risk does not exceed the institution's risk tolerance and/or risk capacity. These techniques may not be appropriate for all types of risk. APRA expects that the **results of such analysis and testing would be reported to the Board** and/or Board Risk Committee and be taken into account when establishing or reviewing the risk appetite statement. APRA expects the **Board to understand the limitations and assumptions relating to any models used to measure components of risk that could materially affect its decision-making**.

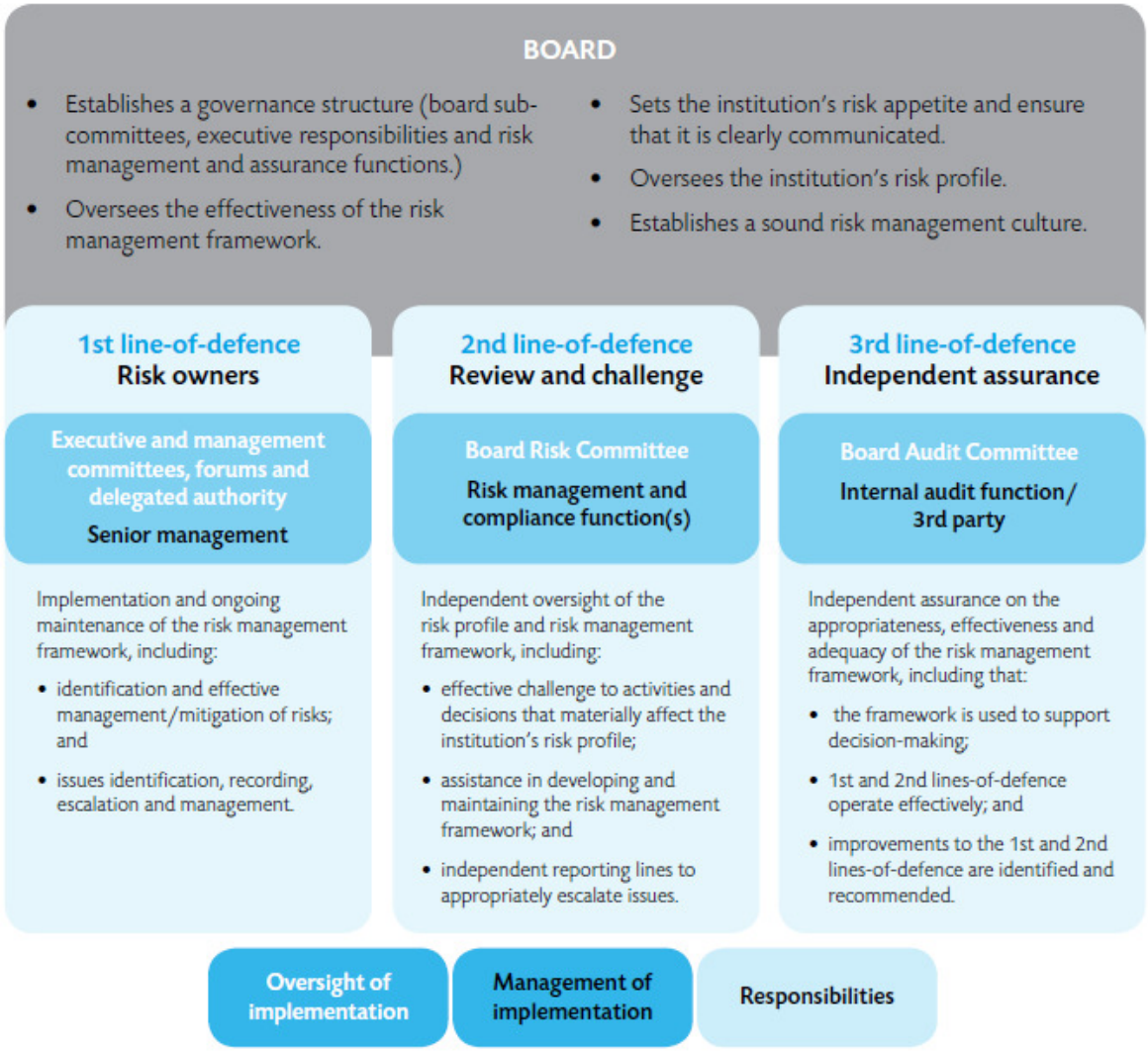
Section	Heading	Extract
61	Chief Risk Officer	CPS 220 sets out requirements for the independence of the CRO and specifies roles that cannot also be performed by the CRO. CPS 220 recognises that an APRA-regulated institution may seek approval for alternative arrangements to those required. This may be 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 to 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 the risk management framework will ensure these mitigants are adhered to**. APRA will assess the appropriateness of alternative arrangements on a case-by-case basis. APRA expects that the Board would take into account the following controls and other mitigating factors that manage conflicts of interests including, but not limited to: (a) alternative sources of risk-based challenge to business lines; (b) the resources allocated to risk management; (c) executive level engagement in risk issues; (d) the strength of compliance and audit mechanisms; (e) oversight from the Board and its committees; (f) the experience and capabilities of the other risk management function personnel; and (g) the robustness of the regulated institution's and, where appropriate, the group's risk management framework.
62	Chief Risk Officer	Further, the **Board of the Level 1 institution is expected to demonstrate that the group CRO is fulfilling his or her responsibilities to that institution on a Level 1 basis**.

Section	Heading	Extract
68	Monitoring and Reporting	**Oversight and escalation process** APRA expects an APRA-regulated institution's risk management framework to **ensure that the Board and senior management receive regular, concise and meaningful assessment of actual risks relative to the institution's risk appetite, and the operation and effectiveness of controls**.
85	Risk Management Declaration	CPS 220 allows an APRA-regulated institution's risk management declaration to be encompassed in the risk management declaration documentation of a Level 2 and/or Level 3 group, where applicable. Where a Level 1 institution's declaration is encompassed within the group declaration, the **Level 1 institution's Board remains responsible for any qualifications in the declaration that relate to that institution**. Where a risk management declaration is made on a Level 2 and/or Level 3 group basis, CPS 220 requires any qualification to identify whether it related to the Level 1 institution or the group's risk management framework. A qualification for the institution may not mean that a group-wide qualification needs to be made, and vice-versa. However, where a group's Board has taken the decision that a qualification at the institution level does not result in a group declaration qualification, the reason for this decision would be articulated.
Appendix A 5	Second Line-of-defence	In order to be effective, the Board would ensure that risk management functions have: (a) adequately experienced staff with relevant technical knowledge and experience to facilitate the development, ongoing review and validation of the risk management framework; and (b) appropriate seniority and authority, with independent reporting lines to the responsible board committees.

Paragraphs 8, 10, 11, 14, 15, 19, 34, 37, 52, 62, 84 and 89 of the guide also have references to Board responsibilities. However, these already form part of the standard or provide clarification.

Graphical Representation of a three-lines-of-defence risk governance model

(CPG 220 - Appendix paragraph 10)



Prudential Standard – CPS 220 – Risk Management

Section	Heading	Extract
Front Page	Objectives and key requirements	The Board of an APRA-regulated institution is ultimately responsible for having a risk management framework that is appropriate to the size, business mix and complexity of the institution or group it heads.
13	The Role of the Board	The **Board**[3] of an APRA-regulated institution is **ultimately responsible** for the institution's risk management framework. In particular, the Board **must ensure** that: (a) it defines the institution's risk appetite and establishes a risk management strategy; (b) a sound risk management culture is established and maintained throughout the institution; (c) **senior management** take the steps necessary to monitor and manage all material risks consistent with the strategic objectives, risk appetite statement and policies approved by the Board; (d) the operational structure of the institution facilitates effective risk management; (e) policies and processes are developed for risk-taking that are consistent with the risk management strategy and the established risk appetite; (f) sufficient resources are dedicated to risk management; (g) uncertainties attached to risk measurement are recognised, and the limitations and assumptions relating to any models used to measure components of risk are well understood; and (h) appropriate controls are established that are consistent with the institution's risk appetite, risk profile and capital strength, and are understood by, and regularly communicated to, relevant staff.

[3] A reference to the Board, in the case of a foreign ADI, Category C insurer or an Eligible Foreign Life Insurance Company, is a reference to the **senior officer outside of Australia** or **Compliance Committee** (as applicable) as referred to in *Prudential Standard CPS 510 Governance*

Section	Heading	Extract
14	Group Risk Management	An APRA-regulated institution that is part of a Level 2, Level 3 or other corporate group may meet requirements of this Prudential Standard on a group basis, provided that the **Board of the institution** is **satisfied** that the **requirements are met** in respect of that institution.
15	Group Risk Management	For the avoidance of doubt, compliance by a group with the requirements of this Prudential Standard **does not relieve the Board of an APRA-regulated institution within the group from the need to comply with any prudential requirements** of that institution**.**
18	Requirements of the Head of a Group	The Head of a group must develop and maintain processes to coordinate the identification, measurement, evaluation, monitoring, reporting, and controlling or mitigation of all material risks across the group, in normal times and periods of stress. The Head of a group must ensure its **Board has a comprehensive group-wide view of all material risks, including an understanding of the roles and relationships of subsidiaries to one another and to the Head.**
19	Requirements of the Head of a Group	The Head of a group must develop and maintain **a Board-approved liquidity management policy for the group** to adequately and consistently identify, measure, monitor, and manage its material liquidity risks. The policy must include a strategy that ensures the group has sufficient liquidity to meet its obligations as they fall due, including in stressed conditions, and outline processes to identify existing and potential constraints on the transfer of funds within the group.
27	Risk Management Framework	An APRA-regulated institution's MIS must **provide the Board, board committees and senior management with regular, accurate and timely information concerning the institution's risk profile**. The MIS must be supported by a robust data framework that enables the aggregation of exposures and risk measures across business lines, prompt reporting of limit breaches, and forward-looking scenario analysis and stress testing. The institution's data quality must be adequate for timely and accurate measurement, assessment and reporting on all material risks across the institution and must provide a sound basis for making decisions.

Section	Heading	Extract
29	Risk Appetite	**The Board must establish the risk appetite of the APRA-regulated institution**. The institution must maintain an appropriate, clear and concise risk appetite statement that addresses its material risks. **The Board must approve the risk appetite statement**.
31	Risk Management Strategy	An APRA-regulated institution must maintain a risk management strategy (RMS) that addresses each material risk listed under paragraph 28. **The RMS must be approved by the Board.**
33	Business Plan	An APRA-regulated institution must maintain a written plan that sets out its approach for the implementation of its strategic objectives (business plan). **The business plan** must be a **rolling plan of at least three years' duration** that is **reviewed at least annually**, with the **results of the review reported to the Board. The business plan must cover the entirety of the institution and be approved by the Board**.
38	Risk Management Function	An APRA-regulated institution must have a designated risk management function that, at a minimum: **(a) is responsible for assisting the Board, board committees and senior management to develop and maintain the risk management framework**; (b) is appropriate to the size, business mix and complexity of the institution; (c) is operationally independent; (d) has the necessary authority and reporting lines to the Board, board committees and senior management to conduct its risk management activities in an effective and independent manner; (e) is resourced with staff who have clearly defined roles and responsibilities and who possess appropriate experience and qualifications to exercise those responsibilities; (f) has access to all aspects of the institution that have the potential to generate material risk, including information technology systems and systems development resources; and

Section	Heading	Extract
		(g) is required to **notify the Board of any significant breach of, or material deviation from, the risk management framework**.
41	Risk Management Function	**The CRO must** have a direct reporting line to the CEO, and **have regular and unfettered access to the Board** and the Board Risk Committee.
49	Risk Management Declaration	**The Board must make an annual declaration to APRA on risk management** (risk management declaration) that must satisfy the requirements set out in Attachment A to this Prudential Standard. **The declaration must be signed by the chairperson of the Board** and the chairperson of the Board Risk Committee. In the case of a Category C insurer, foreign ADI, or EFLIC, the risk management declaration must be signed by the senior officer outside Australia or two members of the Compliance Committee, as relevant.
50	Risk Management Declaration	**The Board must qualify the risk management declaration if there has been any significant breach of, or material deviation from, the risk management framework or the requirements set out in Attachment A** to this Prudential Standard. Any qualification must include a description of the cause and circumstances of the qualification and steps taken, or proposed to be taken, to remedy the problem.[4]
52	Notification Requirements	An APRA-regulated institution must on adoption, and following any material revisions, **submit to APRA a copy** of its: (a) risk appetite statement; (b) business plan; (c) RMS; and (d) where applicable, group liquidity management policy as soon as practicable, and no more than 10 **business days**, after **Board approval.**

[4] Where relevant, any qualification of a risk management declaration must identify where the material deviation has occurred and whether it was on a **Level 1** and/or group basis.

Section	Heading	Extract
Attachment A	Risk Management Declaration	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**: (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).