PRUDENTIAL PRACTICE GUIDE

CPG 220 Risk Management

April 2018

Disclaimer and Copyright

This prudential practice guide is not legal advice and users are encouraged to obtain professional advice about the application of any legislation or prudential standard relevant to their particular circumstances and to exercise their own skill and care in relation to any material contained in this guide.

APRA disclaims any liability for any loss or damage arising out of any use of this prudential practice guide.

Contents

About this guide

Prudential practice guides (PPGs) provide guidance on APRA's view of sound practice in particular areas. PPGs frequently discuss legal requirements from legislation, regulations or APRA's prudential standards, but do not themselves create enforceable requirements.

This PPG aims to assist APRA-regulated institutions in complying with *Prudential Standard CPS 220 Risk Management* (CPS 220) and, more generally, to outline prudent practices in relation to risk management.

CPS 220 sets out requirements in relation to the risk management framework of an APRA-regulated institution, and Level 2 and Level 3 groups. These requirements include the need for an institution and group to have a risk management framework that is consistent and integrated with the risk profile and capital strength of the organisation, supported by a risk management function and subject to comprehensive review.

In this PPG, the term 'APRA-regulated institution' refers to an authorised deposit-taking institution (ADI), a general insurer, a life company, a private health insurer, an authorised non-operating holding company (NOHC) and, where applicable, Level 2 and Level 3 groups.

This PPG is designed to be read together with CPS 220 and does not address all prudential requirements in relation to risk management.

Subject to meeting CPS 220, an APRA-regulated institution has the flexibility to configure its approach to risk management in a manner best suited to achieving its business objectives. Not all of the practices outlined in this PPG will be relevant for every institution and some aspects may vary depending upon the size, business mix and complexity of the institution.

Introduction

1. The information in this guide supports compliance with *Prudential Standard CPS 220 Risk Management* (CPS 220).

Risk Governance

2. Risk governance refers to the formal structure used to support risk-based decision-making and oversight across all operations of an APRA-regulated institution. This typically consists of board committees and management committees, delegations, management structures and related reporting. The risk governance of an institution forms an integral part of its risk management framework.

3. The risk governance structure will be dependent on the size, business mix and complexity of the APRA-regulated institution. The concepts of risk ownership, functionally independent review and challenge, and independent assurance provide a sound basis for ensuring risks are appropriately identified, assessed and managed.

4. The objective of this PPG is to encourage an effective risk governance model that contains checks and balances to support appropriate consideration of risk management throughout an APRA-regulated institution. One such model that is widely used and provides an effective framework for risk governance is the three lines of defence risk management and assurance model. This model provides defined risk ownership responsibilities with functionally independent oversight and assurance. Institutions may choose to use alternatives to the three lines of defence model if similar outcomes can be achieved. The detail of the implementation of the model will often vary in different institutions. The following paragraphs are based on the three lines of defence model.

The first line of defence

5. The first line of defence comprises the business management[1] who have ownership of risks. Accordingly, business management is responsible for day-to-day risk management decision-making involving risk identification, assessment, mitigation, monitoring and management. APRA expects the roles and responsibilities of risk owners to be clearly defined and, where appropriate, incorporated into performance reviews.

6. A key tenet of the three lines of defence model is that business management cannot abrogate its responsibility for risk management. The first line of defence is responsible for:

    a) effective implementation of the risk management framework, including reporting and escalation of relevant information to responsible senior management, the second line

[1] Business management typically includes all levels of management responsible for business decision-making. The first line of defence also includes relevant management committees.

of defence or as far as the board committees or the Board of directors (the Board)[2], as necessary; and

b) managing risk in a way that is consistent and integrated with the risk management framework.

7. Executive and senior business management would ensure risk ownership is clearly defined and that the risk management framework is effectively implemented and supports decision-making. This would usually include reporting, escalation and monitoring procedures that are appropriate for the management of different risk categories.

The second line of defence

8. The second line of defence comprises the specialist risk management function(s) that are functionally independent of the first line of defence. The second line of defence supports the Board and its committees 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, board committees 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 level of risk in the institution and its relationship to the risk appetite, and any necessary reporting and escalation to the Board or its committees.

9. In order to be effective, risk management functions would have:

   a) adequately experienced staff with relevant technical knowledge who facilitate the development, ongoing review and validation of the risk management framework; and
   b) appropriate seniority and authority, with access to the responsible board committees.

10. Smaller and less complex APRA-regulated institutions often combine risk management roles with other roles or functions. Where such dual roles exist, APRA expects that appropriate care would be taken to ensure that the objectiveness of the risk management function is maintained and that any conflicts of interest are identified and appropriately managed.

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

The third line of defence

11. The third line of defence comprises the function(s) that, in accordance with CPS 220, provide to the Board and its committees:

    a) at least annually, independent assurance that the risk management framework has been complied with and is operating effectively; and
    b) at least every three years, a comprehensive review of the appropriateness, effectiveness and adequacy of the risk management framework.

12. The application of the third line of defence would vary depending on the size, business mix and complexity of an APRA-regulated institution. The independent assurance function could, for example, include internal audit, a third-party assurance provider or a combination of the two. A key consideration would be appropriate independence, technical knowledge and experience.

13. While findings raised by the third line of defence would typically be utilised by management to increase business efficiency and inform decision-making, these benefits are secondary to the primary assurance objective.

14. A graphical representation of a sample implementation of the three lines of defence model is provided at Appendix A.

Role of the Board

15. Under CPS 220, the Board is ultimately responsible for the risk management framework of the APRA-regulated institution and is responsible for the oversight of its operation by management. An institution must have, at all times, a risk management framework that governs the way the institution manages risks arising in the institution. Together, the Board Risk Committee and Board Audit Committee assist the Board in its oversight of the operation by management of the overall risk management framework.

16. The Board Audit Committee assists the Board to fulfil its corporate governance and oversight responsibilities in relation to an entity's financial reporting, internal control system, risk management framework and internal and external audit functions (i.e. independent assurance).

17. Consistent with normal practice, for the purpose of discharging its responsibilities, the Board is able to obtain such recommendations and advice from board committees, external advisers and management as it considers prudent. The Board is entitled to place reasonable reliance on those inputs, provided directors approach their tasks with an enquiring mind and make an independent assessment of the matters for decision.

18. The Board is directly responsible for the broader strategy of the APRA-regulated institution and is required to approve the risk appetite statement, business plan and risk management strategy. Effective design of these documents and related processes by the institution will facilitate their integration, with each process appropriately supporting the others.

19. The Board approval and oversight responsibilities for the risk management framework are unaffected if risk management and business operations are outsourced to a third party or are performed by another part of a group.

20. In determining whether the Board has met its responsibilities under CPS 220, APRA will assess the steps taken by the Board to ensure it meets those responsibilities. For example, APRA expects senior management to report on the material risks and escalate material risk issues to the Board or the Board Risk Committee level. The Board and/or Board Risk Committee could also obtain independent views and reports as they deem appropriate, as well as consider risk issues escalated from the risk management function. APRA expects that the Board would clearly communicate its expectations in respect of the reporting and escalation to be provided by management, the risk management function(s) and internal audit. Where the Board considers that the risk reporting is ineffective or that material risk issues have failed to be escalated, APRA expects the Board to adopt all appropriate measures (including directions for management remedial actions and reports) to identify and address the reasons for the failure.

Risk management culture

21. CPS 220 requires a Board to ensure that they form a view of the risk culture in the institution and the extent to which that culture supports the ability of the institution to operate consistently within its risk appetite, identify any desirable changes to the risk culture and ensure the institution takes steps to address those changes. APRA's view is that a sound risk culture is a core element of an effective risk management framework. Risk culture refers to 'the norms of behaviour for individuals and groups within an organisation that determine the collective ability to identify, understand, openly discuss and act on the organisation's current and future risk'[3]. APRA expects that the Board would have a view of the risk culture that is appropriate for ensuring that the institution operates within the risk appetite.

22. An institution's risk culture is strongly influenced by the 'tone at the top'. APRA expects the Board and senior management to demonstrate their commitment to risk management and foster a sound risk management environment in which staff will be actively engaged with risk management processes and outcomes, and a risk management function that is influential and respected. The development of the risk culture is likely to occur through an iterative process involving both the Board and senior management.

23. An APRA-regulated institution influences and communicates its desired risk culture through its business strategy, risk appetite, and understanding of key risks and capabilities, as well as how risk management behaviours are encouraged and rewarded.

[3] Refer to the Institute of International Finance (2009) *"Reform in the financial services industry: Strengthening Practices for a More Stable System"*.

In fostering an effective risk culture it is important that there is consideration of the culture across the whole organisation.

24. A sound risk culture:

    a) supports transparency and openness of risks, events and issues, and facilitates effective internal controls and risk reporting;
    b) encourages awareness of risks and responsibility for managing those risks;
    c) ensures that appropriate actions are taken in a timely manner for issues and risks identified that are outside of set thresholds and tolerances/limits. For example, risk indicators that remain 'red' for extended periods of time could indicate complacency or a lack of funding in the overall management of risk; and
    d) rewards staff for appropriate risk management behaviours. Typically, this would be achieved through incorporating risk management as a core responsibility within individual roles and responsibilities.

25. APRA considers that the development of the desired risk culture would be assisted by a Code of Conduct, ongoing risk education and awareness training programs, processes to ensure behaviour is monitored and managed within the risk appetite, and robust and prudent risk management policies.

26. Remuneration policies will positively influence the desired risk culture if they are designed to encourage and provide incentives for employees to act responsibly and with integrity, in a manner consistent and integrated with the APRA-regulated institution's risk management framework[4].

Group risk management

27. CPS 220 allows an APRA-regulated institution that is part of a group to meet the requirements of the standard on a group basis provided that the Board of the institution is satisfied that the requirements are met in respect to that institution.

28. APRA expects that the appropriateness of using a group risk management framework would be assessed by that APRA-regulated institution according to the size, business mix and complexity of that institution's operations. The purpose of this assessment is to ensure that the group's framework is 'fit for purpose' for the institution. APRA expects that the assessment would be appropriately documented.

29. APRA expects this assessment by the APRA-regulated institution to be conducted prior to using the group's framework and after any changes to the group or the institution that may materially impact on the risk management framework. The institution needs to have a clear understanding of the reliance on, and interaction with the group's risk management framework, and understand the consequences of these arrangements for the risk profile of the institution.

[4] Authorised deposit taking institutions, general insurers and life insurers should refer to *Prudential Standard CPS 510 Governance* and *Prudential Practice Guide PPG 511 Remuneration* on the design of remuneration policies.

Risk management framework

30. A risk management framework enables an APRA-regulated institution to identify, analyse and manage the current and emerging material risks within its business. Effective approaches to risk management provide meaningful information that appropriately supports decision-making and oversight at each level within the institution. The risk management framework will ideally support an institution in:

    a) identifying, analysing and understanding each of the material risks at all levels of the institution;
    b) ensuring that appropriate strategies and policies, and effective operating controls and other mitigants, are in place and operating effectively;
    c) providing reliable and meaningful risk information (reporting) to decision makers;
    d) ensuring that there is adequate oversight of the risk profile and management framework; and
    e) facilitating a sound risk culture.

31. This is achieved, in part, through a clearly articulated risk appetite statement that outlines the APRA-regulated institution's risk appetite and risk tolerances within its risk capacity[5].

32. APRA expects that the primary focus of an APRA-regulated institution's risk management framework would be the management of risks in a way that is consistent with the best interests of depositors and/or policyholders, the maintenance of the sound financial position of the institution and the institution's strategic objectives and business plan.

33. A regulated institution would ordinarily ensure that appropriate controls are established that are consistent with the risk appetite, risk profile and capital strength, and steps are taken to ensure they are appropriately communicated within the institution. In order to assess whether the communication of controls has been appropriate, an institution would ordinarily take steps to assess whether the information has been received and understood.

34. CPS 220 requires the Board to ensure that it recognises uncertainties, limitations and assumptions attached to the measurement of each material risk. In addition to recognition of these matters by the Board, APRA expects that they would be well understood within the institution.

35. Risk can arise from structures that impede transparency, such as special-purpose or related structures. APRA expects that the APRA-regulated institution's operational structure and associated risks would be well understood in the institution, recognised by the Board, taken into account in the risk management framework and reported, as appropriate (including to the Board or its committees where necessary).

[5] Refer to *Prudential Standard CPS 220 Risk Management* for the definitions of risk appetite and risk tolerance. Risk capacity is the maximum risk an institution can bear.

36. Stress testing, including both scenario analysis and sensitivity analysis is used to assess a range of potential impacts as a result of different material risks. Stress testing is important in considering potential changes that could occur in the external operating environment, 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 appropriate Board oversight.

37. As good practice, an APRA-regulated institution would publicly disclose in an appropriate way (such as its published annual report where applicable) an outline of its risk management policies, including where relevant the policies governing dealings between the institution and other group members.

Integration of the risk management framework and Internal Capital Adequacy Assessment Process

38. The risk management framework supports the Board and senior management in obtaining an appropriate view of the APRA-regulated institution's overall risk profile. Reporting facilitates decision-making and oversight, taking into consideration the overall structure and nature of the institution's business and different approaches to managing different material risks. In understanding the overall risk profile of the institution, specific consideration would be given to:

    a) identifying risks throughout the institution that, in combination, may have a material impact on the institution;
    b) understanding the interaction of material risks throughout the institution. For example, a failure in processes or systems (operational risk) may result in excess claims being paid (underwriting risk); and
    c) risks of contagion arising from issues identified with related parties (including any non-APRA-regulated activities).

39. APRA requires an APRA-regulated institution, excluding foreign ADIs, to have an Internal Capital Adequacy Assessment Process (ICAAP), or, in the case of private health insurers a Capital Management Policy (CMP)[6]. These documents involve an integrated approach to capital adequacy and risk management aimed at ensuring that the capital held is adequate in the context of the risk profile and risk appetite of that institution. An institution's risk management framework and ICAAP/CMP are required to be integrated and consistent.

40. An APRA-regulated institution is not required to duplicate content between its ICAAP summary statement or ICAAP report and its risk management strategy, or in the case of a private health insurer between its CMP and its risk management strategy. However, APRA expects that the risk management strategy would contain sufficient detail to provide a holistic view of the institution's strategy for managing risk without having to

[6] Refer to *Prudential Standard APS 110 Capital Adequacy*, *Prudential Standard GPS 110 Capital Adequacy*, *Prudential Standard LPS 110 Capital Adequacy*, *Prudential Standard 3PS 110 Capital Adequacy*, *Prudential Standard HPS 110 Capital Adequacy*, and *Prudential Practice Guide CPG 110 Internal Capital Adequacy Assessment Process and Supervisory Review*.

source other documents. Where other documentation contains additional detail, APRA expects that cross-references will be clear and up-to-date to facilitate consistency and integration between the documents.

Material risks

41. CPS 220 identifies categories of risk that the risk management framework must, at a minimum, cover. APRA's view is that the emphasis on each risk category is likely to differ according to the size, business mix and complexity of the APRA-regulated institution. APRA expects that an institution would be able to demonstrate how it determines the 'materiality' of risk categories and to identify the key risk drivers within each category. Communicating what the institution views as material is important to ensure that its approach is understood by its staff and is consistently applied across its operations.

Strategic and business planning

42. CPS 220 requires an APRA-regulated institution maintain a business plan that sets out its approach for the implementation of its strategic objectives. The business plan is an important management and control tool that enables an institution to identify how it will achieve its strategic objectives.

43. Fundamental to an effective risk management framework is a sound business plan that is consistent and integrated with the risk management strategy and risk appetite statement. APRA expects that the APRA-regulated institution's risk management framework will provide relevant information to senior management and the Board to facilitate their respective roles in the strategy and business planning process (e.g. areas of increased risk, changes in the environment, prioritisation and allocation of resources). APRA also expects that the relevant components of the risk management framework would be reviewed in the context of the institution's strategic and business planning processes.

44. CPS 220 requires a rolling business plan of at least three years' duration that is reviewed at least annually. A rolling plan supports a medium to long-term view of business objectives, while the annual review ensures it is dynamic and updated to reflect current goals.

45. APRA expects the APRA-regulated institution's business plan review process would consider the impact on the risk profile of the institution's operations and identify the potential changes to the material risks. This would ordinarily include formal consideration of issues arising from planned material changes to the institution's operations and risks.

Risk appetite statement

46. The risk appetite statement is used to communicate the Board's expectations of how much risk the APRA-regulated institution is willing to accept. APRA notes that, in practice it is likely that the risk appetite and risk appetite statement will be developed through an iterative process involving the Board and management. APRA's view is that a reasonable and easily understood risk appetite statement that aligns to the approaches used to identify, assess and manage material risk is fundamental to risk management.

47. The articulation of risk appetite and risk tolerances is central to a risk appetite statement. Risk appetite is the degree of risk an APRA-regulated institution is prepared to accept in the pursuit of its strategic objectives and business plan. Risk tolerances support the translation of the risk appetite by management into operational limits for the day-to-day management of material risks. It may not be possible to set quantitative tolerances or limits for all risks.

48. The development and review of an APRA-regulated institution's risk appetite statement will generally be performed as part of the strategic and business planning process. The risk appetite statement would provide relevant information on the Board's expectations regarding the risk appetite, and would in turn be updated to reflect any changes as a result of the strategic and business planning process.

49. APRA expects that the Board would be actively engaged with management 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/or 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) be satisfied that senior management's interpretation and application of the risk appetite and tolerances is appropriate; and
    c) appropriately align risk appetite to the approach adopted in the risk management framework for assessing, monitoring and managing the different material risks.

50. APRA expects an APRA-regulated institution to communicate appropriate aspects of its risk appetite statement throughout its operations to ensure that the risk appetite statement is understood and consistently implemented. An appropriate summary of the risk appetite statement would include relevant information for the intended audience.

51. Risk appetite is a key consideration in developing policies in relation to key decision-making processes. For example, when an APRA-regulated institution develops a business case or agrees to contractual and service level agreements for a material outsourced arrangement, APRA expects that the risk management framework would be used to identify and assess risks, and that the risk appetite is considered in the decision making and implementation process.

52. 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 senior management to assess the appropriateness of such techniques before they are adopted and on an ongoing basis. 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 and/or Board Risk Committee to recognise the limitations and assumptions relating to any models used to measure components of risk that could materially affect its decision-making.

53. Where an international insurance or banking group operates both a subsidiary and a branch in Australia, APRA requires each APRA-regulated institution to have a risk appetite statement that is tailored to its risk profile. Although risk appetite may be set by the overseas group on a divisional basis, APRA nevertheless expects the branch risk appetite statement to appropriately address the risk profile of the Australian branch operation.

Risk appetite

54. Risk appetite expresses the aggregate level and types of risk that an APRA-regulated institution is willing to assume to achieve its strategic objectives and business plan before breaching its obligations or constraints determined by regulatory capital, liquidity or other needs.

55. In APRA's experience, the risk appetite can be expressed in a number of ways to ensure that it is commonly understood and consistently applied across an APRA-regulated institution. Generally, the risk appetite is expressed in the form of high level qualitative statements that clearly capture the institution's attitude to and level of acceptance of different risks. Where appropriate, the risk appetite statement would include quantitative measures.

Risk tolerance

56. Risk tolerances are established for each material risk, taking into consideration the risk appetite. Risk tolerances are based on the maximum level of acceptable risk. To facilitate implementation and monitoring of the risk appetite in day-to-day business activities, an APRA-regulated institution may also decide to set risk limits for more granular risks within each material risk.

57. Risk tolerances can be expressed in a number of different forms depending on the nature of the risk being managed. They can act as triggers for considering whether action is necessary in relation to the risk. Where possible, risk tolerance would be expressed as a measurable limit to enable a clear and transparent monitoring process that ensures the

APRA-regulated institution remains within the determined risk tolerance. An institution may also define key indicators with thresholds around the risk tolerance.

58. APRA recognises that, for some risks, a qualitative risk tolerance may be appropriate. In these circumstances, the APRA-regulated institution would be expected to ensure the tolerance is well articulated to enable consistent implementation across the institution's operations and to determine when the risk tolerance has been exceeded.

59. Where a risk exposure falls outside the APRA-regulated institution's risk tolerance, APRA expects the institution would promptly develop and implement a plan of action to review the risk and ensure that it is brought within an acceptable tolerance.

Risk management strategy

60. CPS 220 requires an APRA-regulated institution to formulate, maintain and give effect to a risk management strategy that provides an overview of how the risk management framework addresses each material risk for the institution, with reference to the relevant policies, standards and procedures.

61. APRA expects that a risk management strategy would contain sufficient information to communicate, in general terms the APRA-regulated institution's approach to risk management. This includes how it identifies, measures, evaluates, monitors, reports and controls or mitigates the material risks of its operations. CPS 220 requires that the risk management strategy list the policies and procedures dealing with risk management matters. Where these policies and procedures require Board approval under other prudential standards, approval of the strategy does not negate the Board's responsibility to approve those individual documents.

Risk management function

62. A key role of an APRA-regulated institution's risk management function is to provide independent and objective review and challenge, oversight, monitoring and reporting in relation to material risks arising from the institution's operations. An additional responsibility is to provide technical support and assist the Board, relevant committees and senior management to fulfil their respective roles in relation to the risk management framework.

63. APRA expects the risk management function would also facilitate the building of risk management capabilities throughout the APRA-regulated institution by providing specialist education, training and advice to directors, senior management and staff of the institution. It would also typically facilitate the development of the Board's view of risk culture.

64. APRA expects the roles and responsibilities of the risk management function to be clearly defined and documented as part of the risk management framework. These responsibilities include assisting with the development and maintenance of the risk management framework.

65. APRA expects a risk management function to be appropriately structured to fulfil its roles and responsibilities. This may include co-locating risk management personnel with the business line divisions or functions that they are responsible for monitoring. For example, risk managers who focus on market risk may be assigned to a specialist market risk team that is physically located with the relevant trading/investment functions. Where risk management personnel are co-located in this way with different businesses across the APRA-regulated institution, these personnel would be organisationally independent of the business reporting lines and remain part of the overall risk management function's reporting structure. It is important that the roles and responsibilities are clearly understood with clear reporting and escalation lines to the designated head of the risk management function, referred to as the Chief Risk Officer (CRO) and responsible committees.

Chief risk officer

66. APRA expects the risk management function to have sufficient stature, authority and resourcing to support sound risk-based decision-making. This is reflected in the requirement in CPS 220 that the CRO must have authority to provide effective challenge to activities and decisions that may materially affect the institution's risk profile.

67. This can be further evidenced by a CRO who is appropriately skilled, unencumbered by conflicts of interest with their risk management role and can speak with candour to the Chief Executive Officer (CEO), the Board and relevant committees. Under a three lines of defence model, the role and responsibilities of the CRO are clearly within the second line.

68. The stature and authority of the CRO would be supported by their being a senior executive, having an ability to influence material decisions and remuneration appropriate to their responsibilities. APRA expects that the CRO's authority and participation in decision-making would support risk-based considerations that are consistent with the institution's risk appetite statement, risk management strategy and business plan. It is important that the CRO provides effective challenge as part of their participation in the decision-making process, ensuring that material decisions are risk based.

69. CPS 220 requires an APRA-regulated institution to have a process for identifying, monitoring and managing perceived, potential and actual conflicts of interest. APRA's requirement for a 'designated' rather than 'dedicated' CRO provides scope for the person to have other roles and responsibilities, so long as there is no conflict of interest.

70. 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 other reasons particular to that institution. APRA expects these instances normally to be limited to smaller and less complex institutions, but will consider applications from all APRA-regulated institutions, provided the applicant clearly sets out the exceptional circumstances that might warrant APRA considering the alternative proposal. 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.

71. CPS 220 requires that the risk management function, via a CRO, has direct and unfettered access to the CEO, Board, Board Risk Committee and senior management. CPS 220 also requires the reporting line for the risk management function to be independent from business lines and to directly report to the CEO. Where an APRA-regulated institution is part of a group, including a Level 2 and/or Level 3 group, the CRO of that institution may report to the group CRO as long as the group CRO reports directly to the group CEO.

72. CPS 220 recognises that an Australian branch operation may seek an alternative arrangement for the requirement that the CRO report to the CEO. A number of Australian branch operations use a regional or global CRO who assumes the risk responsibilities for the branch. Due to their regional or global reporting lines, it may be impractical to require the CRO to report to the Australian branch's CEO. Where this is the case, APRA expects that the designated CRO has sufficient oversight of, and involvement with, the management of risk in the branch. APRA expects the branch would be able to demonstrate that the CRO can fulfil his or her roles and responsibilities to the Australian institution, evidenced by regular and unfettered access to the Australian branch Senior Officer Outside of Australia or Compliance Committee.

73. For the avoidance of doubt, CPS 220 does not require the designated head of the risk management function to be called a CRO.

Compliance function

74. CPS 220 requires a designated compliance function to have a reporting line independent from business lines to support clear and timely reporting of compliance risks. APRA envisages that the CRO would be able to provide this independent reporting line and that they may have responsibility for the compliance function. Where a CRO is also the head of the compliance function, he or she is expected to effectively fulfil the responsibilities for each function.

75. The structure of the compliance function is a matter for the regulated institution. Where an APRA-regulated institution combines its risk and compliance functions, APRA expects

that the institution would allocate sufficient resourcing to fulfil the roles and responsibilities of each function.

Outsourcing

76. APRA does not expect that outsourcing the risk management and/or compliance functions would be a common practice. Where an APRA-regulated institution considers there is adequate justification, this is considered to be a material business activity for the purposes of *Prudential Standard CPS 231 Outsourcing* (CPS 231) and *Prudential Standard HPS 231 Outsourcing*.

Monitoring and reporting

Oversight and escalation processes

77. 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.

78. An APRA-regulated institution's formal escalation procedures would ordinarily cover reporting of exceptions to risk appetite, risk tolerances and more granular risk limits. This reporting would include sufficient commentary to facilitate management review and understanding of the report content, where necessary.

Information systems for business reporting

79. APRA expects that an APRA-regulated institution would, as part of its risk management framework, establish, maintain and document effective Management Information Systems (MIS) commensurate with the size, business mix and complexity of its operations.

80. Effective MIS provide appropriate information at each level of management and decision-making within the APRA-regulated institution. Such information systems assists in the management, communication and reporting of risk issues and outcomes and assist the management of the institution to appropriately monitor and manage different material risks. The MIS would be sufficiently flexible to support decision-making during periods of stress, when the institution's risk profile may significantly change.

81. APRA envisages that an APRA-regulated institution would implement controls for ensuring data in information and reporting systems is sufficiently current, accurate and complete such that data quality is adequate for timely and accurate analysis and

reporting of risk. Internal information and reporting systems would be secure and supported by adequate business continuity and disaster recovery arrangements[7].

82. A well-functioning information and reporting system would typically:

a) produce appropriate risk and compliance data and reports;
b) incorporate information that is relevant to decision-making;
c) report accurate, reliable and timely information;
d) allow the institution to identify, assess and monitor business activities, existing and emerging risks, financial position and performance;
e) allow the institution to monitor the effectiveness of, and compliance with, its internal control systems and report any exceptions that arise; and
f) be reviewed regularly to assess the timeliness and relevance of information generated and the adequacy, quality and accuracy of the system's performance over time.

Review of the risk management framework

83. CPS 220 requires an APRA-regulated institution to have two types of reviews of its risk management framework:

a) an annual review that covers compliance with, and effectiveness of, the risk management framework by internal and/or external audit; and
b) a three-yearly comprehensive review of the appropriateness, effectiveness and adequacy of the framework by operationally independent persons.

Annual review

84. APRA will accept annual reviews that explore particular elements of the risk management framework in depth and on a rotational basis. For example, if an institution's risk management framework has six material elements, it may choose to review two of these every year. The structure of such a program of review is at the discretion of the regulated institution. The annual review sign-off would include those reviews conducted during the year since the previous such sign-off. APRA expects that all elements of the risk management framework would be subject to review at least every three years. For general and life insurers, the annual review required by CPS 220 is separate from the assessment of the suitability and adequacy of the risk management framework conducted by the Appointed Actuary[8]. This review must be reported to the Board Audit Committee or, in the case of a Category C insurer, foreign ADI, or eligible foreign life insurance company (EFLIC) to the Senior Officer Outside of Australia or the Compliance Committee.

[7] Refer to *Prudential Practice Guide CPG 235 Managing Data Risk* for further guidance.

[8] Refer to *Prudential Standard GPS 320 Actuarial and Related Matters*, *Prudential Standard LPS 320 Actuarial and Related Matters*.

85. APRA envisages that some branch operations would be subject to group internal audits of compliance with, and effectiveness of, its risk management framework. APRA may approve alternative timing to this annual review, such as on a biennial basis if satisfied that those arrangements will, in APRA's view, achieve the objectives of this requirement. APRA will assess the appropriateness of alternative arrangements on a case-by-case basis with considerations including, but not limited to, the:

    a) size, business mix and complexity of the branch operations;
    b) process the Senior Officer Outside of Australia or Compliance Committee has undertaken to satisfy themselves that an alternate timing of review is appropriate;
    c) additional controls in place to mitigate the risk of non-compliance in interim years; and
    d) robustness of the branch operations and, where appropriate, the robustness of the group's risk management framework.

Comprehensive review

86. CPS 220 requires the comprehensive review to be conducted by operationally independent, appropriately trained and competent persons at least every three years. There is no requirement that the comprehensive review must be undertaken by a party external to the institution. This review must be reported to the Board Risk Committee or, in the case of some private health insurers, the Board Audit Committee, and for Category C insurers, foreign ADIs, or EFLICs, to the Senior Officer Outside of Australia or the Compliance Committee.

87. APRA expects the comprehensive review to include a comparison of the institution's current practice against any identified better practice. Where any gaps are identified, APRA expects the review to outline steps to address these differences or identify why changing current practice is not considered appropriate. The review may draw upon the APRA-regulated institution's internal resources, such as internal audit reports, to the extent that the independence of the review is not undermined. For insurers, the Financial Condition Report assessment of the risk management framework[9] would be taken into account, but not solely relied upon, for the purposes of the comprehensive review. This forward-looking review is intended to assist the Board Risk Committee, or, in the case of some private health insurers, the Board Audit Committee, to oversee the implementation and appropriateness of the institution's risk management framework, while any compliance issues identified would be reported to the Board Audit Committee.

88. APRA expects these reviews would include an assessment as to whether the framework remains appropriate for the institution and the risks it faces, whether the framework has been consistently implemented, whether there are appropriate procedures in place to ensure that the framework addresses any new risks or changes to existing risks, including lessons learnt from risk incidents and near misses, and consideration as to

[9] Refer to *Prudential Standard GPS 320 Actuarial and Related Matters*, *Prudential Standard LPS 320 Actuarial and Related Matters* and *Prudential Standard HPS 320 Actuarial and Related Matters*.

whether the framework is effective in providing appropriate, effective and timely information to inform decision-makers.

89. An APRA-regulated institution may coordinate the comprehensive review with the review of its ICAAP, or, in the case of private health insurers, the CMP. Capital management is an essential part of the institution's risk management framework. APRA expects the comprehensive review would not simply be a review of the ICAAP/CMP, but would assess how the ICAAP/CMP is integrated with other elements of the risk management framework that are beyond capital management.

90. In considering whether a person is operationally independent, an APRA-regulated institution would take into account any role that the person may have in connection with the development or implementation of the framework, or the activities under review, that may impact on their ability to perform an objective review. Where an institution is using the group risk management framework, APRA expects that a person would not be operationally independent if they have been involved in the development or implementation of that framework.

Difference between the annual and comprehensive review

91. The difference between the annual and comprehensive review is the depth and scope of the assessment. The annual review is focused on particular elements of the risk management framework. Given the depth of the review, APRA expects internal and/or external audit would cover all aspects of the risk management framework according to a rolling audit plan.

92. In contrast, the three-year review provides holistic, institution-wide view of the risk management framework, including the interaction between its constituent elements. While the annual review is focused on the current state of the risk management framework, the comprehensive review is to provide an assessment and recommendations on the ongoing appropriateness of the framework. APRA expects that the comprehensive review would draw upon the annual review reports when assessing how the particular elements of the risk management framework interact.

Risk management declaration

93. CPS 220 requires the Board to provide APRA with a risk management declaration on an annual basis. While this declaration does not have to be audited, APRA expects that the Board would have obtained reasonable assurance and, if necessary, considered independent advice on the matters covered by the declaration, prior to the signing of the declaration by the required signatories. The extent of enquiry required prior to making the declaration is a matter for the judgment of each Board of an APRA-regulated institution. The wording of the declaration allows materiality to be taken into account when making the declaration.

94. 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.

95. CPS 220 requires the risk management declaration to be submitted to APRA in accordance with reporting standards made under the *Financial Sector (Collection of Data) Act 2001*, which include:

    a) within four months of its annual balance date if it is an ADI or authorised banking NOHC that is not a disclosing entity within the meaning of the *Corporations Act 2001*;
    b) within four months of its annual balance date if it is a Level 3 Head; or
    c) for all other APRA-regulated institutions, within three months of its annual balance date[10].

96. Where a Level 1 institution's declaration is encompassed within the group declaration, the combined declaration can be submitted to APRA at the time the risk management declaration of the Head of the Group is required to be submitted.

97. Subparagraph 1(f) of the risk management declaration in Attachment A to CPS 220 includes the statement that '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)'. APRA's expectation is that the term 'financial information' in this part of the declaration would be read broadly and capture more than information related to the financial statements. For example, prudential returns, disclosures made under *Prudential Standard APS 330 Public Disclosure* and other similar documents/information would ordinarily also be considered for the purposes of the declaration.

APRA notification requirements

98. CPS 220 requires an APRA-regulated institution to notify APRA of material changes to the size, business mix and complexity of the institution's business operations. APRA expects that this would include, but not be limited to, the following changes where material:

    a) events such as proposals relating to major modifications to, or the re-organisation of, the functions of the institution;
    b) proposed acquisitions;
    c) changes to business lines and products;
    d) changes in organisational structure; and

[10] For private health insurers, the annual balance date is 30 June each year.

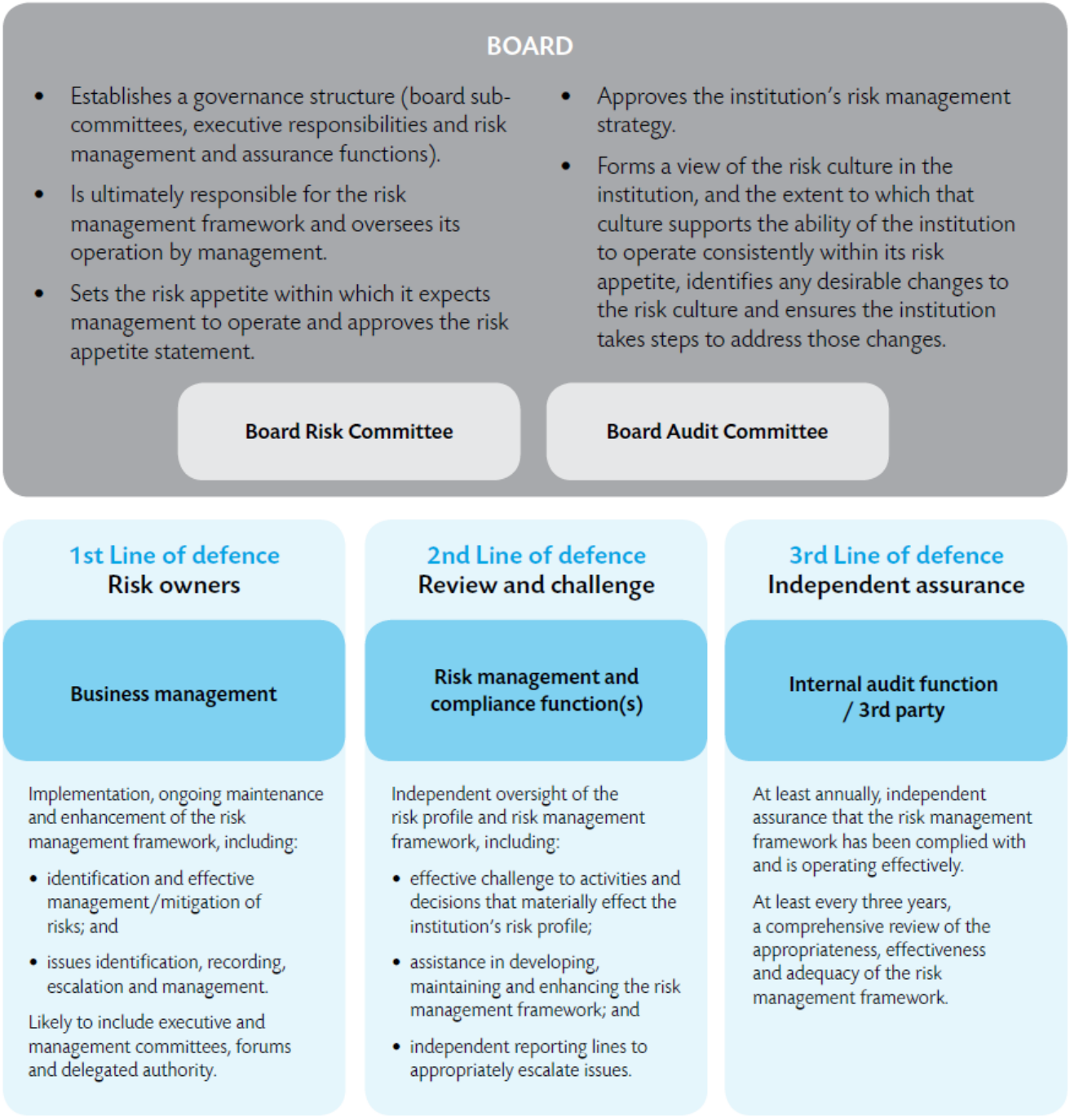
e) deviations from the risk management strategy.

99. CPS 220 requires an APRA-regulated institution that conducts business outside of Australia to notify APRA when it becomes aware that its right to conduct business in any other jurisdiction has been materially affected. A restriction on the ability of an institution to conduct business overseas could impact on its Australian operations, and may have resulted from weaknesses in risk management. APRA expects to be informed, at a minimum, when the institution's right to conduct business has:

    a) ceased in a jurisdiction;
    b) been limited by a law of any jurisdiction in which business is being conducted;
    c) been otherwise materially affected under a law of any jurisdiction in which business is being conducted; or
    d) otherwise been withdrawn; and where applicable, changes to the ability of a group member to conduct business that materially impacts on the Australian operation's risk profile.

100. APRA expects that an APRA-regulated institution would be in regular dialogue with its supervisors about potential material changes to the institution. APRA expects that, at the latest, notification in accordance with the requirements in CPS 220 would be made within 10 business days of the Board becoming aware of a current or proposed material change to the institution's risk profile or business operations.

Appendix A – Three lines of defence risk governance model



APRA