



## Prudential Standard CPS 220

### Risk Management

#### Objectives and key requirements of this Prudential Standard

This Prudential Standard requires an APRA-regulated institution to have systems for identifying, measuring, evaluating, monitoring, reporting, and controlling or mitigating material risks that may affect its ability, or the ability of the group it heads, to meet its obligations to depositors and/or policyholders. These systems, together with the structures, policies, processes and people supporting them, comprise an institution's risk management framework.

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. The risk management framework must also be consistent with the institution's strategic objectives and business plan.

The key requirements of this Prudential Standard are that an APRA-regulated institution must:

- have a risk management framework that is appropriate to its size, business mix and complexity;
- maintain a Board-approved risk appetite;
- maintain a Board-approved risk management strategy that describes the key elements of the risk management framework to give effect to its approach to managing risk;
- have a Board-approved business plan that sets out its approach for the operational implementation of its strategic objectives;
- maintain adequate resources to manage, mitigate and monitor material risks, and ensure compliance with this Prudential Standard; and
- notify APRA when it becomes aware of a significant breach of, or material deviation from, the risk management framework, or that the risk management framework does not adequately address a material risk.

## Authority

1. This Prudential Standard is made under:
  - (a) section 11AF of the *Banking Act 1959* (Banking Act) in relation to authorised deposit-taking institutions (**ADIs**) and **Non-Operating Holding Companies** authorised under the Banking Act (authorised banking NOHCs);
  - (b) section 32 of the *Insurance Act 1973* (Insurance Act) in relation to **general insurers** and **non-operating holding companies** authorised under the Insurance Act (authorised insurance NOHCs) and **parent entities of Level 2 insurance groups**; and
  - (c) section 230A of the *Life Insurance Act 1995* (Life Insurance Act) in relation to **life companies**, including **friendly societies**, and **non-operating holding companies** registered under the Life Insurance Act (registered life NOHCs).

## Application

2. This Prudential Standard applies to ‘APRA-regulated institutions’, defined as:
  - (a) ADIs, including **foreign ADIs**, and authorised banking NOHCs;
  - (b) general insurers, including **Category C insurers**, and authorised insurance NOHCs;
  - (c) life companies, including friendly societies and **eligible foreign life insurance companies** (EFLICs), and registered life NOHCs; and
  - (d) Heads of groups.<sup>1</sup>
3. APRA-regulated institutions must comply with this Prudential Standard in its entirety, unless otherwise expressly indicated. The obligations imposed by this Prudential Standard on, or in relation to, a foreign ADI, a Category C insurer or an EFLIC apply only in relation to the Australian branch operations of that institution.
4. Where an APRA-regulated institution is the Head of a group, a requirement that is expressed as applying to a Head of a group is to be read as requiring that institution to ensure that the requirement is applied appropriately throughout the group.<sup>2</sup>
5. This Prudential Standard commences on 1 January 2014.

---

<sup>1</sup> For the purposes of this Prudential Standard, a reference to a ‘Head of a group’ is a reference to a Level 2 Head or **Level 3 Head**, as relevant.

<sup>2</sup> Where a Level 2 group operates within a Level 3 group, a requirement expressed as applying to a Head of a group is to be read as applying to the Level 3 Head.

## Interpretation

6. Terms that are defined in *Prudential Standard 3PS 001 Definitions* (3PS 001), *Prudential Standard APS 001 Definitions* (APS 001), *Prudential Standard GPS 001 Definitions* (GPS 001) or *Prudential Standard LPS 001 Definitions* (LPS 001) appear in bold the first time they are used in this Prudential Standard.
7. For the purposes of this Prudential Standard, a reference to a 'group' is a reference to a Level 2 group and/or a Level 3 group.
8. A 'Level 2 group' is:
  - (a) the consolidation of institutions defined as **Level 2** in APS 001; or
  - (b) a Level 2 insurance group as defined in GPS 001.
9. A 'Level 3 group' means a group of entities of which a Level 3 Head is the parent entity. APRA may, by notice in writing, adjust the group to include or exclude entities.
10. A 'Level 2 Head' is:
  - (a) where an ADI that is a member of a Level 2 group is not a **subsidiary** of an authorised banking NOHC or another ADI, that ADI;
  - (b) where an ADI that is a member of a Level 2 group is a subsidiary of an authorised banking NOHC, that authorised banking NOHC; or
  - (c) the parent entity of a Level 2 insurance group as defined in GPS 001.
11. A 'Level 3 Head' is:
  - (a) an ADI or authorised banking NOHC under the Banking Act;
  - (b) a general insurer or authorised insurance NOHC under the Insurance Act;  
or
  - (c) a life company or registered life NOHC under the Life Insurance Act

in respect of which APRA has made a determination under paragraph 2 of *Prudential Standard 3PS 110 Capital Adequacy* (3PS 110).

## The role of the Board

12. The **Board** 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 uncertainties relating to the output of 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.

### **Group risk management**

13. An APRA-regulated institution that is part of a 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.
14. 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, unless specifically excluded by a paragraph in this Prudential Standard.
15. Where an APRA-regulated institution is part of a group and any element of the risk management framework is controlled or influenced by another entity in the group, the institution's risk management framework must specifically take into account risks arising from the group framework, and clearly identify:
  - (a) whether the institution's risk management framework is derived wholly or partially from group risk management policies or functions;
  - (b) the linkages and significant differences between the institution's and the group's risk management framework;
  - (c) how these linkages and significant differences change the risk profile of the institution; and
  - (d) the process for monitoring by, or reporting to, the group on risk management including the key procedures, the frequency of reporting and the approach to reviews of the risk management framework.
16. Where APRA is of the view that the fulfilment of a requirement of this Prudential Standard by a group does not adequately address the requirement for

an APRA-regulated institution within that group, APRA may require that institution to meet the requirement on a separate basis within a reasonable timeframe specified by APRA.<sup>3</sup>

### Requirements of the Head of a group

17. The Head of a group must develop and maintain processes to coordinate the identification, measurement, evaluation, reporting, and control 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.
18. 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.
19. Where a **non-APRA-regulated institution** of a group engages in business activities that may pose a material risk to the group, the Head of a group must ensure that the risk management framework addresses the risks posed by that institution to the group and **APRA beneficiaries**.

### Risk management framework

20. An APRA-regulated institution must maintain a risk management framework that enables it to appropriately develop and implement strategies, policies, procedures and controls to manage different types of material risks. The institution must have policies and procedures that provide the Board with a comprehensive institution-wide view of its material risks.<sup>4</sup>
21. For the purposes of this Prudential Standard, the risk management framework is the totality of systems, structures, policies, processes and people within an APRA-regulated institution that identify, measure, monitor, report and control or mitigate all internal and external sources of material risk. Material risks are those that could have a material impact, both financial and non-financial, on the institution or on the interests of depositors and/or **policyholders**.
22. An APRA-regulated institution's risk management framework must be consistent with its business plan identified under paragraph 32.
23. An APRA-regulated institution's risk management framework must provide reasonable assurance that each material risk to the institution is being prudently

---

<sup>3</sup> Where this Prudential Standard provides for APRA to require an APRA-regulated institution to make other arrangements, or otherwise exercise a power or discretion, the power or discretion is to be exercised in writing.

<sup>4</sup> For life insurers, this includes a view of the material risks at the level of individual statutory funds.

and soundly managed, having regard to the size, business mix and complexity of its operations.

24. An APRA-regulated institution's risk management framework must, at a minimum, include:
- (a) a risk appetite;
  - (b) a risk management strategy;
  - (c) a business plan;
  - (d) policies and procedures supporting clearly defined and documented roles, responsibilities and formal reporting structures for the management of material risks throughout the institution;
  - (e) a designated risk management function that meets the requirements of paragraph 37;
  - (f) an Internal Capital Adequacy Assessment Process (ICAAP)<sup>5</sup>;
  - (g) a management information system (MIS) that is adequate, both under normal circumstances and in periods of stress, for measuring, assessing and reporting on all material risks across the institution; and
  - (h) a review process to ensure that the risk management framework is effective in identifying, measuring, evaluating, monitoring, reporting, and controlling or mitigating material risks.
25. An APRA-regulated institution's risk management framework must include forward-looking scenario analysis and stress testing programmes, commensurate with its size, nature and complexity, and which are based on severe but plausible assumptions.
26. 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 provides a sound basis for making decisions.

### Material risks

27. An APRA-regulated institution's risk management framework must, at a minimum, address:

---

<sup>5</sup> Refer to 3PS 110, *Prudential Standard APS 110 Capital Adequacy*, *Prudential Standard GPS 110 Capital Adequacy* and *Prudential Standard LPS 110 Capital Adequacy*.

- (a) credit risk;
- (b) market and investment risk;
- (c) liquidity risk;
- (d) insurance risk;
- (e) operational risk;
- (f) risks arising from its strategic objectives and business plans; and
- (g) other risks that, singly or in combination with different risks, may have a material impact on the institution.

### **Risk appetite**

- 28. 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.
- 29. An APRA-regulated institution's risk appetite statement must, at a minimum, convey:
  - (a) the degree of risk that the institution is prepared to accept in pursuit of its strategic objectives and business plan, giving consideration to the interests of depositors and/or policyholders (risk appetite);
  - (b) for each material risk, the maximum level of risk that the institution is willing to operate within, expressed as a risk limit and based on its risk appetite, risk profile and capital strength (risk tolerance);
  - (c) the process for ensuring that risk tolerances are set at an appropriate level, based on an estimate of the impact in the event that a risk tolerance is breached, and the likelihood that each material risk is realised;
  - (d) the process for monitoring compliance with each risk tolerance and for taking appropriate action in the event that it is breached; and
  - (e) the timing and process for review of the risk appetite and risk tolerances.

### **Risk management strategy**

- 30. An APRA-regulated institution must maintain a risk management strategy (RMS) that addresses each material risk listed under paragraph 27. The RMS must be approved by the Board.
- 31. An RMS is a document that describes the APRA-regulated institution's strategy for managing risk and the key elements of the risk management framework that give effect to this strategy. At a minimum, an RMS must:

- (a) describe each material risk identified, and the institution's approach to managing these risks;
- (b) list the policies and procedures dealing with risk management matters;
- (c) summarise the role and responsibilities of the risk management function;
- (d) describe the risk governance relationship between the Board, board committees and senior management with respect to the risk management framework; and
- (e) outline the approach to ensuring all persons within the institution have awareness of the risk management framework and for instilling an appropriate risk culture across the institution.

### **Business plan**

- 32. An APRA-regulated institution must maintain a written plan that sets out its approach for the operational 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.
- 33. An APRA-regulated institution must identify and consider the material risks associated with its strategic objectives and business plan, and must explicitly manage these risks through the risk management framework, including how changing these plans affects its risk profile.
- 34. The requirement for a business plan does not apply to a **run-off insurer** provided that the run-off insurer complies with Prudential Standard (TBD).

### **Policies and procedures**

- 35. The policies and procedures identified under paragraph 31(b) must include:
  - (a) the process for identifying and assessing material risks and controls;
  - (b) the process for the validation, approval and use of any models to measure components of risk;
  - (c) the process for establishing, implementing and testing mitigation strategies and control mechanisms for material risks;
  - (d) the process for monitoring, communicating and reporting risk issues, including escalation procedures for the reporting of material events and incidents;
  - (e) the process for identifying, monitoring and managing potential and actual conflicts of interest;



- (f) the mechanisms in place for monitoring and ensuring ongoing compliance with all prudential requirements<sup>6</sup>;
  - (g) the process for ensuring consistency across the risk management framework, including the components identified under paragraph 24;
  - (h) the process for establishing and maintaining appropriate contingency arrangements (including robust and credible recovery plans where warranted) for the operation of the risk management framework in stressed conditions; and
  - (i) the process for review of the risk management framework.
36. An APRA-regulated institution must monitor the date when each policy or procedure was last revised, the date that it is next due for review, and who is responsible for the review.

### **Risk management function**

37. 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
  - (g) is required to notify the Board of any significant breach of, or material deviation from, the risk management framework.
38. An APRA-regulated institution's risk management function must be headed by a designated Chief Risk Officer (CRO). The CRO must be involved in, and have

---

<sup>6</sup> 'Prudential requirements' include requirements under the respective Banking Act, the Insurance Act, the Life Insurance Act (collectively, the 'Prudential Acts'), the *Life Insurance Regulations 1995*, the *Insurance Regulations 2002* (collectively, the 'Regulations'), prudential standards, reporting standards, the *Financial Sector (Collection of Data) Act 2001* (FSCODA), licence conditions, authorisations, directions and any other requirements imposed by APRA under legislation.

the authority to provide effective challenge to, activities and decisions that may materially affect the institution's risk profile.

39. The CRO must be independent from business lines, the finance function and other revenue-generating responsibilities. The CRO must not be the Chief Executive Officer (CEO), Chief Financial Officer, Appointed Actuary or Head of Internal Audit.
40. 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.
41. An APRA-regulated institution may engage the services of an external service provider to perform part of the risk management function where the institution can demonstrate to APRA that the risk management function meets the requirements in paragraph 37.<sup>7</sup>

### Compliance function

42. An APRA-regulated institution must have a designated compliance function that assists senior management in effectively managing compliance risks. The compliance function must be adequately staffed by appropriately trained and competent persons who have sufficient authority to perform their role effectively, and have a reporting line independent from business lines.

### Review of the risk management framework

43. An APRA-regulated institution must ensure the compliance with, and the effectiveness of, the risk management framework is subject to review by internal and/or external audit at least annually. The results of this review must be reported to the Board Audit Committee.
44. An APRA-regulated institution must, in addition to paragraph 43, ensure that the appropriateness, effectiveness and adequacy of its risk management framework are subject to a comprehensive review by operationally independent, appropriately trained and competent persons (this may include external consultants) at least every three years<sup>8</sup>. The results of this review must be reported to the Board Risk Committee.
45. The scope of the comprehensive review must have regard to the size, business mix and complexity of the APRA-regulated institution, the extent of any change to its operations or risk appetite, and any changes to the external environment in which the institution operates. The review of the risk management framework must, at a minimum, assess whether:
  - (a) the framework is implemented and effective;

---

<sup>7</sup> Outsourcing any part of the risk management function by an APRA-regulated institution must also meet the requirements in *Prudential Standard CPS 231 Outsourcing*.

<sup>8</sup> For insurers, the review must take into account the Appointed Actuary's annual **Financial Condition Report** assessments required under *Prudential Standard GPS 320 Actuarial and Related Matters* and *Prudential Standard LPS 320 Actuarial and Related Matters*.

- (b) it remains appropriate for the institution, taking into account its current business plan;
  - (c) it remains consistent with the Board's risk appetite;
  - (d) it is supported by adequate resources; and
  - (e) the RMS accurately documents the key elements of risk management framework that give effect to its strategy for managing risk.
46. Where a material change to the size, business mix and complexity of an APRA-regulated institution is identified outside the review required in paragraph 44, the institution must assess whether any amendment to, or a review of, the risk management framework is necessary to take account of these developments at that time.

### Risk management declaration

47. 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.
48. 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.<sup>9</sup>
49. An APRA-regulated institution must submit the risk management declaration to APRA on, or before, the day that the institution's annual information is required to be submitted to APRA in accordance with reporting standards made under FSCODA.<sup>10</sup>

### Notification requirements

50. 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

---

<sup>9</sup> 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.

<sup>10</sup> For insurers when the **yearly statutory accounts** are submitted, and for ADIs as at the end of financial year.

- (d) where applicable, group liquidity management policy
- as soon as practicable, and no more than 10 **business days**, after Board approval.
51. An APRA-regulated institution must notify APRA as soon as practicable, and no more than 10 business days, of becoming aware:
- (a) of a significant breach of, or material deviation from, the risk management framework; or
  - (b) that the risk management framework did not adequately address a material risk.
52. An APRA-regulated institution must notify APRA as soon as practicable, and no more than 10 business days, after it becomes aware of any material or prospective material changes to the size, business mix and complexity of the institution.
53. Where an APRA-regulated institution conducts business in a jurisdiction outside Australia, it must notify APRA as soon as practicable, and no more than 10 business days, of becoming aware that its right to conduct business in that jurisdiction has been materially affected by the law of that jurisdiction or its right to conduct business has ceased.

### **Adjustments and exclusions**

54. APRA may adjust or exclude a specific requirement in this Prudential Standard in relation to that APRA-regulated institution.<sup>11</sup>

### **Determinations made under previous prudential standards**

55. An exercise of APRA's discretion (such as an approval, waiver or direction) under a previous version of a risk management prudential standard continues to have effect as though exercised pursuant to a corresponding power (if any) exercisable by APRA under this Prudential Standard. For the purposes of this paragraph, 'a previous version of a risk management prudential standard' includes:
- (a) *Prudential Standard GPS 220 Risk Management* (GPS 220) made on 30 November 2012;
  - (b) GPS 220 made on 23 June 2008;
  - (c) GPS 220 made on 9 February 2006;
  - (d) *Prudential Standard GPS 221 Risk Management: Level 2 Insurance Groups* (GPS 221) made on 9 September 2011;

---

<sup>11</sup> Refer to subsection 11AF(2) of the Banking Act, subsection 32(3D) of the Insurance Act and subsection 230A(4) of the Life Insurance Act.

- (e) GPS 221 made on 17 December 2008;
- (f) *Prudential Standard LPS 220 Risk Management* (LPS 220) made on 30 November 2012; and
- (g) LPS 220 made on 27 March 2007.

**Attachment A****Risk management declaration**

1. For the purposes of paragraph 47 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 an 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 (ReMS)** 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).