Prudential Standard CPS 220 Risk Management

Objectives and key requirements of this Prudential Standard

This Prudential Standard requires an APRA-regulated institution and a Head of a group 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 or group's risk management framework.

The Board of an APRA-regulated institution and the Board of a Head of a group, respectively, are 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. The risk management framework must also be consistent with the institution's or group's strategic objectives and business plan.

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

- maintain a risk management framework that is appropriate to the size, business mix and complexity of the institution or group, as relevant;
- maintain a Board-approved risk appetite statement;
- maintain a Board-approved risk management strategy that describes the key elements of the risk management framework that give effect to the approach to managing risk;
- maintain a Board-approved business plan that sets out the approach for the implementation of the strategic objectives of the institution or group;
- maintain adequate resources to 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);

   (b) section 32 of the *Insurance Act 1973* (Insurance Act);

   (c) section 230A of the *Life Insurance Act 1995* (Life Insurance Act); and

   (d) section 92 of the *Private Health Insurance (Prudential Supervision) Act 2015* (PHIPS Act).

Application

2. This Prudential Standard applies to all 'APRA-regulated institutions'[1] defined as:

   (a) **authorised deposit-taking institutions** (**ADIs**), including **foreign ADIs**, and **non-operating holding companies** authorised under the Banking Act (authorised banking NOHCs);

   (b) **general insurers**, including **Category C insurers**, non-operating holding companies authorised under the Insurance Act (authorised insurance NOHCs) and **parent entities** of **Level 2 insurance groups**;

   (c) **life companies**, including **friendly societies** and **eligible foreign life insurance companies** (EFLICs), and non-operating holding companies registered under the Life Insurance Act (registered life NOHCs); and

   (d) **private health insurers** registered under the PHIPS Act.

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',[2] it must comply with a requirement of this Prudential Standard:

   (a) in its capacity as an APRA-regulated institution;

   (b) by ensuring that the requirement is applied appropriately throughout the group, including in relation to institutions that are not APRA-regulated; and

   (c) on a group basis.

---

1 Note, for the purposes of this Prudential Standard, an **RSE licensee** is not treated as an 'APRA-regulated institution'. Refer to *Prudential Standard SPS 220 Risk Management* (SPS 220) for requirements relating to the risk management of an RSE licensee.

2 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.

In applying the requirements of this Prudential Standard on a group basis, references in paragraphs 9, 19 to 56, and Attachment A to an 'APRA-regulated institution' should be read as 'Head of a group' and references to 'institution' should be read as 'group'.

5. This Prudential Standard commences on 1 April 2018.

Interpretation

6. In this Prudential Standard:

   (a) terms that are defined in *Prudential Standard 3PS 001 Definitions*, *Prudential Standard APS 001 Definitions* (APS 001), *Prudential Standard GPS 001 Definitions* (GPS 001), *Prudential Standard LPS 001 Definitions* or *Prudential Standard HPS 001 Definitions* appear in bold the first time they are used; and

   (b) unless the contrary intention appears, a reference to an Act, Regulations or Prudential Standard is a reference to the Act, Regulations or Prudential Standard as in force from time to time.

7. Where this Prudential Standard provides for APRA to exercise a power or discretion, this power or discretion is to be exercised in writing.

8. For the purposes of this Prudential Standard:

   'group' means a Level 2 group or a **Level 3 group**, as relevant;

   'Head of a group' means a Level 2 Head or **Level 3 Head**, as relevant;

   'Level 2 group' means the entities that comprise:

   (a) **Level 2** as defined in APS 001; or

   (b) a Level 2 insurance group as defined in GPS 001;

   'Level 2 Head' means:

   (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.

The role of the Board

9. The **Board**[3] of an APRA-regulated institution is ultimately responsible for the institution's **risk management framework** and is responsible for the oversight of its operation by management. In particular, the Board must **ensure** that:

   (a) it sets the risk appetite within which it expects management to operate and approves the institution's risk appetite statement and **risk management strategy** (RMS);

   (b) it forms 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 ensures the institution takes steps to address those changes;

   (c) **senior management** of the institution 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 RMS and the established risk appetite;

   (f) sufficient resources are dedicated to risk management; and

   (g) it recognises uncertainties, limitations and assumptions attached to the measurement of each material risk.

Use of group risk management by an APRA-regulated institution

10. An APRA-regulated institution that is part of a group or other **corporate group** may meet requirements of this Prudential Standard using group risk management frameworks, policies, procedures or functions, provided that the Board of the institution is satisfied that the requirements are met in respect of that institution.

11. For the avoidance of doubt, compliance by a group with the requirements of this Prudential Standard does not relieve an APRA-regulated institution within the group from the need to comply with any prudential requirements of that institution.

12. 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:

[3] A reference to the Board in the case of a foreign ADI, is a reference to the **senior officer outside Australia.**

(a) whether the APRA-regulated institution's risk management framework is derived wholly or partially from group risk management frameworks, policies, procedures 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.

13. 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.

Additional requirements of the Head of a group

14. As part of the group risk management framework (see paragraphs 19 to 25), the Head of a group must 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 of a group.

15. The group risk management function (see paragraphs 37 to 42) does not need to be a function of the Head of a group, but may be a function located elsewhere in the group. The group chief risk officer (CRO) cannot be the roles specified in paragraph 39 for any institution within the group.

16. The Head of a group must notify APRA in accordance with paragraphs 52 to 55 in respect of the group risk management framework, except where an APRA-regulated institution within the group has otherwise notified APRA of that information.

17. The Head of a group must 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. The Head of a group must submit to APRA a copy of its group liquidity management policy as soon as practicable, and no more than 10 **business days**, after Board approval.

18. Where an institution within the group that is not an APRA-regulated institution engages in business activities that may pose a material risk to the group, the Head

of the group must ensure that the risk management framework addresses the risks posed by that institution to the group and depositors, **policyholders** or **RSE** beneficiaries.[4]

Risk management framework

19. An APRA-regulated institution must maintain a risk management framework for the institution that enables it to appropriately develop and implement strategies, policies, procedures and controls to manage different types of material risks, and provides the Board with a comprehensive institution-wide view of material risks.[5]

20. The risk management framework is the totality of systems, structures, policies, processes and people within an institution that identify, measure, evaluate, 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.

21. The risk management framework must be consistent with the **business plan** required under paragraph 31.

22. The risk management framework must provide a structure for identifying and managing each material risk to ensure the institution is being prudently and soundly managed, having regard to the size, business mix and complexity of its operations.

23. The risk management framework must, at a minimum, include:

    (a) a risk appetite statement;

    (b) an RMS;

    (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)[6];

---

4 This paragraph does not override any requirements applying to an RSE licensee in SPS 220.

5 For life companies and private health insurers, this includes a view of the material risks at the level of individual statutory or health benefit funds respectively.

6 Refer to *Prudential Standard APS 110 Capital Adequacy*, *Prudential Standard GPS 110 Capital Adequacy* and *Prudential Standard LPS 110 Capital Adequacy*. A Level 3 Head is not required to have a group ICAAP. For private health insurers, ICAAP refers to the Capital Management Policy requirements contained in *Prudential Standard HPS 110 Capital Adequacy*.

(g) a management information system(s) (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.

24. The risk management framework must include forward-looking scenario analysis and stress testing programs, commensurate with the institution's size, business mix and complexity, and which are based on severe but plausible assumptions.

25. The MIS must provide the Board of the APRA-regulated institution, board committees of the APRA-regulated institution and senior management of the institution 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. 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.

Material risks

26. The risk management framework must, at a minimum, address:

(a) credit risk;

(b) market and investment risk;

(c) liquidity risk;

(d) insurance risk;

(e) operational risk;

(f) risks arising from the 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

27. An APRA-regulated institution must maintain an appropriate, clear and concise risk appetite statement for the institution that addresses the institution's material risks. The Board is responsible for setting the risk appetite of the institution and must approve the institution's risk appetite statement.

28. The 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

29. An APRA-regulated institution must maintain an RMS for the institution that addresses each material risk listed under paragraph 26. The RMS must be approved by the Board.

30. The RMS is a document that describes the 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 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 of the APRA-regulated institution, board committees of the APRA-regulated institution and senior management of the institution 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 as it relates to their role and for instilling an appropriate risk culture across the institution.

Business plan

31. An APRA-regulated institution must maintain a written plan for the institution that sets out its approach for the implementation of its strategic objectives (business plan).

32. 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 the institution's strategic objectives and business plan, and must explicitly manage these risks through the risk management framework, including how changing these plans affects the institution's 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 GPS 110 Capital Adequacy*.

Policies and procedures

35. The policies and procedures required under subparagraph 30(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[7];

(g) the process for ensuring consistency across the risk management framework, including the components identified under paragraph 23;

(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.

---

7 'Prudential requirements' include requirements under the respective Banking Act, the Insurance Act, the Life Insurance Act, the PHIPS Act, the *Banking Regulations 1966*, the *Life Insurance Regulations 1995*, the *Insurance Regulations 2002*, *APRA Private Health Insurance Rules*, prudential standards, reporting standards, the *Financial Sector (Collection of Data) Act 2001*, licence conditions, authorisations, directions and any other requirements imposed by APRA under legislation.

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 for the institution that, at a minimum:

    (a) is responsible for assisting the Board of the APRA-regulated institution, board committees of the APRA-regulated institution and senior management of the institution to 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 of the APRA-regulated institution, board committees of the APRA-regulated institution and senior management of the institution 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 must designate a person to be responsible for that function, referred to in this standard as a CRO. The CRO must be involved in, and have 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, other revenue-generating responsibilities and the finance function. 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. Where an APRA-regulated institution believes that the requirements in paragraphs 39 and 400 are inappropriate for its particular circumstances, it may propose alternative arrangements to APRA. Proposals for alternative arrangements must outline the circumstances that are particular to that institution and include details of, and supporting reasons for, these arrangements. APRA may approve alternative arrangements for the institution if satisfied that those

arrangements, in APRA's view, achieve the objectives of this Prudential Standard.

42. An APRA-regulated institution may engage the services of an external service provider to perform part of the risk management function where the APRA-regulated institution can demonstrate to APRA that the risk management function meets the requirements in paragraph 37.[8]

Compliance function

43. An APRA-regulated institution must have a designated compliance function that assists senior management of the institution 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

44. An APRA-regulated institution must ensure that compliance with, and the effectiveness of, the risk management framework of the institution is subject to review by internal and/or external audit at least annually. The results of this review must be reported to the institution's Board Audit Committee, the senior officer outside of Australia or Compliance Committee, as relevant.

45. An APRA-regulated institution must, in addition to paragraph 44, ensure that the appropriateness, effectiveness and adequacy of the institution's 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.[9] The results of this review must be reported to the institution's Board Risk Committee, the senior officer outside Australia or Compliance Committee, as relevant.

46. The scope of the comprehensive review must have regard to the size, business mix and complexity of the institution, the extent of any change to its operations or risk appetite, and any changes to the external environment in which the institution operates.

47. The comprehensive review of the risk management framework must, at a minimum, assess whether:

    (a) the framework is implemented and effective;

    (b) it remains appropriate, taking into account the current business plan;

---

8 Outsourcing any part of the risk management function by an APRA-regulated institution must also meet the requirements in *Prudential Standard CPS 231 Outsourcing* or *Prudential Standard HPS 231 Outsourcing*.

9 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*, *Prudential Standard LPS 320 Actuarial and Related Matters* and *Prudential Standard HPS 320 Actuarial and Related Matters*.

(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 the risk management framework that give effect to the strategy for managing risk.

48. Where a material change to the size, business mix and complexity of the operations is identified outside the review required in paragraph 45, the APRA-regulated 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

49. The Board of an APRA-regulated institution must make an annual declaration to APRA on risk management of the institution (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. The Board of an APRA-regulated institution must qualify the risk management declaration of the institution 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.[10]

51. Unless otherwise approved by APRA, an APRA-regulated institution must submit the risk management declaration of the institution to APRA:

(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] 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**/individual APRA-regulated institution basis and/or group basis.

Notification requirements

52. An APRA-regulated institution must on adoption, and following any material revisions, submit to APRA a copy of the institution's:

    (a) risk appetite statement;

    (b) business plan; and

    (c) RMS

    as soon as practicable, and no more than 10 business days, after Board approval.

53. An APRA-regulated institution must notify APRA as soon as practicable, and no more than 10 business days, after it becomes aware:

    (a) of a significant breach of, or material deviation from, the risk management framework of the institution; or

    (b) that the risk management framework of the institution did not adequately address a material risk.

54. 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.

55. 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, after it becomes 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

56. APRA may adjust or exclude a specific requirement in this Prudential Standard in relation to an APRA-regulated institution.[11]

Determinations made under previous prudential standards

57. 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 any versions of:

    (a) *Prudential Standard GPS 220 Risk Management*;

[11] Refer to subsection 11AF(2) of the Banking Act, subsection 32(3D) of the Insurance Act, subsection 230A(4) of the Life Insurance Act and subsection 92(4) of the PHIPS Act.

(b) *Prudential Standard GPS 221 Risk Management: Level 2 Insurance Groups*; and

(c) *Prudential Standard LPS 220 Risk Management.*

Attachment A – Risk Management Declaration

1. For the purposes of paragraph 49 of this Prudential Standard, the Board of an APRA-regulated institution must provide APRA with a risk management declaration of the institution stating that, to the best of its knowledge and having made appropriate enquiries, in all material respects:

   (a) the 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;

   (c) the risk management and internal control systems in place are operating effectively and are adequate having regard to the risks of the institution 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 APRA-regulated institution is satisfied with the efficacy of the processes and systems surrounding the production of financial information at the institution.