Prudential Standard GPS 220

Risk Management

Objective and key requirements of this Prudential Standard

This Prudential Standard sets out the requirements for a general insurer and a Level 2 insurance group to maintain a risk management framework and strategy that is appropriate to the nature and scale of its operations.

The ultimate responsibility for the general insurer's and Level 2 insurance group's risk management framework and strategy rests with its Board of directors or, in the case of a Category C insurer, the senior officer outside Australia with delegated authority from the Board.

A general insurer's and Level 2 insurance group's systems, processes, structures, policies and people for identifying, assessing, mitigating and monitoring risks are referred to in this Prudential Standard as the risk management framework.

The key requirements of this Prudential Standard are that a general insurer and a Level 2 insurance group must:

- have in its risk management framework a documented Risk Management Strategy and include sound risk management policies and procedures, and clearly defined managerial responsibilities and controls;
- submit its Risk Management Strategy to APRA when material changes are made;
- have a dedicated risk management function (or role) responsible for assisting in the development and maintenance of the risk management framework;
- submit a three-year Business Plan to APRA and re-submit after each annual review and when any material changes are made;
- submit a Risk Management Declaration to APRA on an annual basis; and
- submit a Financial Information Declaration to APRA on an annual basis.

Authority

1. This Prudential Standard is made under section 32 of the *Insurance Act 1973* (the Act).

Application

2. This Prudential Standard applies to each:

   (a) **general insurer** authorised under the Act (**insurer**); and

   (b) **Level 2 insurance group** as defined in *Prudential Standard GPS 001 Definitions* (GPS 001).

   Where a requirement applies to a Level 2 insurance group, the requirement is imposed on the **parent entity** of the Level 2 insurance group.

3. This Prudential Standard applies to insurers and Level 2 insurance groups (**regulated institutions**) from 1 January 2013.

4. For the avoidance of doubt, compliance by a Level 2 insurance group with the requirements of this Prudential Standard does not relieve the **Board** of an insurer within the group from the need to comply with any **prudential requirements** that are specific to the insurer, unless specifically excluded by a paragraph in this Prudential Standard.

Level 2 insurance groups

5. Certain adjustments to the risk management requirements outlined in this Prudential Standard apply to Level 2 insurance groups. These adjustments are set out in Attachment D.

Interpretation

6. Terms that are defined in GPS 001 appear in bold the first time they are used in this Prudential Standard.

7. For the purposes of this Prudential Standard:

   (a) 'risk management framework' includes systems (including the structures, processes, policies and roles supporting them) for identifying, assessing, mitigating and monitoring the risks that may affect a regulated institution's ability to meets its obligations to policyholders;

   (b) a reference to the regulated institution's 'operations' is a reference to:

      (i) its operations in Australia and overseas through a branch for an insurer; or

(ii) its operations in Australia and overseas for a Level 2 insurance group;

(c) the term 'auditor' is used to refer to the **Appointed Auditor**, **Group Auditor** and **responsible auditor** except where otherwise specified; and

(d) the term 'actuary' is used to refer to the **Appointed Actuary** and **Group Actuary** except where otherwise specified.

Compliance on an insurance group basis

8. Subject to paragraph 9, an insurer that is part of an **insurance group** may meet certain requirements on a group basis, provided that the Board of the insurer is satisfied that the requirements of this Prudential Standard are met in respect of the insurer. These requirements are:

(a) a risk management framework in accordance with paragraph 10;

(b) a Risk Management Strategy in accordance with paragraph 12(a);

(c) a risk management function in accordance with paragraph 16;

(d) a Business Plan in accordance with paragraph 18; and

(e) a declaration on risk management (Risk Management Declaration) in accordance with paragraph 37.

9. Where APRA is of the view that the fulfilment of a requirement referred to in paragraph 8 by an insurance group does not adequately address the requirement for an insurer within that insurance group, APRA may, in writing, require that insurer to meet the requirement on a separate basis within a reasonable time specified by APRA.

Risk management framework

10. A regulated institution must at all times have a risk management framework to manage the risks arising from its business.

11. The regulated institution's risk management framework must provide a reasonable assurance that the regulated institution's risks are being prudently and soundly managed, having regard to such factors as the size, business mix and complexity of the regulated institution's operations.

12. A regulated institution's 'risk management framework' must, at a minimum, include:

    (a) a written 'Risk Management Strategy' (RMS) that complies with this Prudential Standard, is approved by the Board and in regard to which the Board is satisfied that:

        (i) it describes the key elements of the risk management framework (including the risk appetite, policies, procedures, management responsibilities and controls referred to in paragraphs 12(b) and (c), and the other matters that this Prudential Standard requires to be included in an RMS);

        (ii) the risk management framework described in the RMS is appropriate and provides reasonable assurance that the regulated institution's risks are being prudently and soundly managed having regard to such factors as the size, business mix and complexity of the regulated institution's operations; and

        (iii) it describes the review referred to in paragraph 14;

    (b) risk management policies and procedures to identify, assess, monitor, report on and mitigate all material risks, financial and non-financial, likely to be faced by the regulated institution having regard to such factors as the size, business mix and complexity of the regulated institution's operations, and a review process to ensure that the risk management framework remains effective; and

    (c) clearly defined managerial responsibilities and controls.

13. The material risks referred to in paragraph 12(b) above must, at a minimum, include:

    (a) asset risk, including asset and liability mismatch and credit risk;

    (b) asset concentration risk;

    (c) operational risk (requirements for outsourcing and business continuity management are contained in *Prudential Standard CPS 231 Outsourcing* and *Prudential Standard CPS 232 Business Continuity Management*);

    (d) insurance risk;

    (e) insurance concentration risk, including concentrations due to portfolio composition, geographical exposures and reinsurance arrangements; and

    (f) strategic and tactical risks that arise out of the regulated institution's Business Plan.

14. The regulated institution must ensure that its risk management framework is subject to effective and comprehensive review by operationally independent, appropriately trained and competent staff (including external consultants), and

that the frequency and scope of this review is appropriate having regard to such factors as the size, business mix, complexity of the regulated institution's operations and the extent of any change to its business profile or its risk appetite. The review must include:

(a) a review of the risk management function (or role);

(b) a review of the RMS; and

(c) a review of the internal control system.[1]

15. For the purposes of paragraph 14, a person is deemed not to be operationally independent if the person has played, or is playing, a significant role in the development or implementation of the risk management framework.

Risk management function

16. A regulated institution must have a 'risk management function' (or role) within the regulated institution that:

(a) is appropriate to the nature, scale and diversity of its operations;

(b) is sufficiently resourced; and

(c) has the necessary authority to conduct its activities in an effective and independent manner.

17. The risk management function (or role) is responsible for assisting the Board, any Board committee and senior management in developing and maintaining the risk management framework.

Business Plan

18. A regulated institution must at all times maintain a 'Business Plan' approved by the Board:

a) prior to its adoption; and

b) at any time it is revised during its operational cycle.

19. Paragraph 18 does not apply to a **run-off insurer** provided that the run-off insurer maintains at all times a 'run-off plan'[2] (including a description of the run-off insurer's approach to capital management) according to this Prudential Standard.

---

1 Also refer to *Prudential Standard CPS 510 Governance*, which requires that a regulated institution's internal audit function must have among its objectives a review of the risk management framework.

2 Referred to in paragraphs 22 to 28.

20. The regulated institution's Business Plan must be a three-year rolling plan and be reviewed at least annually.

21. A regulated institution must submit to APRA:

    (a) a Business Plan after each annual review; and

    (b) any revised Business Plan within 10 **business days** of Board approval.

Run-off plan

22. Subject to paragraphs 52 and 53 of *Prudential Standard GPS 320 Actuarial and Related Matters* (GPS 320), a run-off insurer must at all times maintain a 'run-off plan' (including a description of the run-off insurer's approach to capital management), unless otherwise agreed to by APRA.

23. The run-off plan must be approved by the Board:

    (a) prior to its adoption; and

    (b) at any time it is amended during its operational cycle.

24. The run-off insurer's run-off plan must be a three-year rolling plan and the run-off insurer must review it at least annually (or as close to annually as is practicable). Under GPS 320, the Appointed Actuary of the run-off insurer must also review the run-off plan according to the requirements of GPS 320.

25. The run-off insurer must submit to APRA:

    (a) a run-off plan after each annual review; and

    (b) any amended run-off plan within 10 business days of Board approval.

26. APRA may, in writing, specify that a run-off plan be:

    (a) a rolling plan of more or less than three years; and

    (b) reviewed less frequently than as required in paragraph 24

    if, having regard to the particular circumstances of the run-off insurer, APRA considers it unnecessary for the purposes of the prudential supervision of the run-off insurer.

27. A run-off insurer that is both a **Category C insurer** and a run-off insurer must prepare a run-off plan in respect of the Australian branch operation but with consideration given to the ability of the insurer to transfer assets into Australia in order to ensure that the requirements in *Prudential Standard GPS 110 Capital Adequacy* (GPS 110) are met.

28. A run-off plan must include the matters listed in Attachment A.

Risk Management Strategy

29. The RMS is a high level, strategic document intended to describe the key elements of a regulated institution's risk management framework set out in paragraph 12(a)(i).

30. The regulated institution must review its RMS at least annually to ensure that it accurately documents the regulated institution's risk management framework.

31. Where there are material changes to the operations of a regulated institution, it must review and amend its risk management framework and, if appropriate, it's RMS to take account of the changes. Such RMS must be approved by the Board and submitted to APRA within 10 business days of Board approval.

32. A regulated institution must not intentionally deviate in a material way from its RMS except where this deviation has been approved by the Board and notified to APRA prior to the deviation occurring.

33. Where there are institutional, operational or other developments relating to the regulated institution's operations that materially affect the risk profile of the regulated institution, the regulated institution must notify APRA as soon as practicable after the event has happened and amend its risk management framework and, if appropriate, the RMS to take account of the change.

34. A regulated institution's RMS must, at a minimum:

    (a) outline the risk governance relationship between the Board, Board committees and senior management;

    (b) describe the processes for identifying and assessing risks;

    (c) describe the process for establishing mitigation and control mechanisms for individual risks;

    (d) describe the process for monitoring and reporting risk issues (including communication and escalation mechanisms);

    (e) describe the approach to ensuring relevant staff have an awareness of risk issues and instilling an appropriate risk culture, including the level of accessibility of the RMS;

    (f) identify those persons and their positions in the regulated institution, or groups of persons with managerial responsibility for the risk management framework, and set out their roles and responsibilities;

    (g) describe the process by which the risk management framework (including the RMS) is reviewed, and outline the broad coverage for these reviews;

    (h) provide an overview of the mechanisms in place for monitoring and ensuring continual compliance with the **Prudential Capital Requirement** (PCR);

(i) provide an overview of the processes and controls in place for ensuring compliance with all **prudential requirements**;

(j) if the regulated institution is part of an Australian or global **corporate group**, or is a Category C insurer:

(i) include a summary of the group policy objectives and strategies;

(ii) state whether the local RMS is derived wholly or partially from the group risk management arrangements;

(iii) summarise the linkages and significant differences between the local RMS and group risk management arrangements, including relevant local business and other conditions;

(iv) outline the process for monitoring by, or reporting to, the parent entity or head office. A summary of the key procedures, the frequency of reporting and the approach to reviews must be provided;

(v) where any element of a regulated institution's risk management framework is controlled by another entity in the group, or by head office, describe how this arrangement works; and

(vi) where a regulated institution:

(A) is part of a global insurance group where the head office or ultimate holding company is outside of Australia; or

(B) is a Category C insurer,

include a summary of the home regulator's supervisory arrangements regarding risk management; and

(k) cover both the Australian operations and the risks arising from the overseas operations of the regulated institution that could impact on the Australian operations of the regulated institution.

Integration of risk management framework and Internal Capital Adequacy Assessment Process

35. Under GPS 110, a regulated institution is required to have an **Internal Capital Adequacy Assessment Process** (ICAAP). An ICAAP involves an integrated approach to capital and risk management for a regulated institution, aimed at ensuring that the capital held is adequate in the context of the risk profile and risk appetite of that regulated institution. A regulated institution's risk management framework and ICAAP must be consistent with one another.

36. A regulated institution is not required to duplicate content between its ICAAP summary statement or ICAAP report required under GPS 110 and its RMS.

Cross-references are appropriate to facilitate integration between the two documents.

Risk Management Declaration

37. The Board must provide APRA with a Risk Management Declaration signed by two **directors** or, in the case of a Category C insurer, the **senior officer outside Australia** with delegated authority from the Board.

38. The requirements for the Risk Management Declaration are set out in Attachment B.

39. The Risk Management Declaration must be submitted to APRA on, or before, the day that the insurer's **yearly statutory accounts** or Level 2 insurance group's annual accounts (as appropriate) are required to be submitted to APRA in accordance with reporting standards made under the *Financial Sector (Collection of Data) Act 2001* (Collection of Data Act).

40. If the Board qualifies the Risk Management Declaration, the qualified Risk Management Declaration must include a description of any material deviation from the regulated institution's obligations, and the steps taken, or proposed to be taken, to remedy those breaches.

Financial Information Declaration

41. A regulated institution must provide to APRA a declaration on financial information (Financial Information Declaration) signed by:

    (a) the chief executive officer (CEO) (by whatever name called, or for a Category C insurer, the local equivalent); and

    (b) the chief financial officer (CFO) (by whatever name called, or for a Category C insurer, the local equivalent).

    This declaration is set out in Attachment C. Where the CEO and the CFO are the same person, the Financial Information Declaration must be signed by that person and another person to be agreed upon with APRA.

42. The Financial Information Declaration must be submitted to APRA on, or before, the day that the insurer's yearly statutory accounts or Level 2 insurance group's annual accounts (as appropriate) are required to be submitted to APRA in accordance with reporting standards made under the Collection of Data Act.

43. If the CEO or CFO qualifies the Financial Information Declaration, the qualified Declaration must include a description of the cause and circumstances of the qualification, and steps taken, or proposed to be taken, to remedy the problem.

Other notification requirements

44. Where a regulated institution conducts **insurance business** outside Australia, it must notify APRA, in writing, if it becomes aware that:

    (a) its right to conduct business in that jurisdiction has ceased;

    (b) its right to conduct insurance business has been limited by a law of the jurisdiction in which the business is being conducted;

    (c) its right to conduct insurance business has been otherwise materially affected under a law of the jurisdiction in which the business is being conducted; or

    (d) its right to conduct insurance business has otherwise been withdrawn.

    This notification must be provided within 10 business days of the event occurring for an insurer, or within one month of the event occurring for a Level 2 insurance group.

Adjustments and exclusions

45. APRA may, by notice in writing to a regulated institution, adjust or exclude a specific requirement of this Prudential Standard in relation to that regulated institution.

Determinations made under previous prudential standards

46. 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 23 June 2008;

    (b) GPS 220 made on 9 February 2006;

    (c) *Prudential Standard GPS 221 Risk Management: Level 2 Insurance Groups* (GPS 221) made on 9 September 2011; and

    (d) GPS 221 made on 17 December 2008.

Attachment A

Matters to be included in a run-off plan

For the purposes of paragraph 28 of this Prudential Standard, the following matters must be included in a run-off plan, where relevant:

Matters to be addressed in a run-off plan (to be prepared by run-off insurer)	Areas to be reviewed and assessed by Appointed Actuary[3]
(a) Business overview, including details of significant changes to the run-off insurer's liability portfolio, assets, capital position or operating environment	Significant issues or material anomalies
(b) Details of the run-off insurer's recent experience, including the profitability for the most recent year	Significant variations between actual and expected experience, and the adequacy of past estimates
(c) Assessment of the run-off insurer's expected future claims run-off experience on a rolling three-year basis	Appropriateness of the insurer's expected future claims run-off assessment
(d) Details of the run-off insurer's asset and liability management processes, including the insurer's investment and liquidity strategies	Appropriateness of the insurer's asset and liability management processes, and investment and liquidity strategies, in light of the expected future claims run-off
(e) Details of the run-off insurer's current and projected future capital adequacy and a discussion of the insurer's approach to capital management	Appropriateness and reasonableness of the assumptions used for the capital projections and for scenario/stress-testing
(f) Assessment of the suitability and adequacy of reinsurance arrangements, including recoverability of reinsurance, documentation of reinsurance arrangements and the existence and impact of any limited risk transfer arrangements	Appropriateness of the insurer's reinsurance arrangements in light of the expected future claims run-off
(g) Details of the run-off insurer's risk management framework	Suitability and adequacy of the risk management framework

[3] A review of the run-off plan by the Appointed Actuary is required under GPS 320.

Attachment B

Risk Management Declaration

The Board must (by the time provided for in paragraph 39 of this Prudential Standard) provide APRA with a Risk Management Declaration stating that, to the best of their knowledge and belief having made appropriate enquiries:

(a) the regulated institution has systems in place for the purpose of ensuring compliance with the Act, the *Insurance Regulations 2002* (the Regulations), prudential standards, the Collection of Data Act, reporting standards, conditions imposed under the Act on the insurer's authorisation, directions issued by APRA pursuant to the Act and any other requirements imposed by APRA, in writing;

(b) the Board and senior management are satisfied with the efficacy of the processes and systems surrounding the production of financial information at the regulated institution;

(c) the regulated institution has in place an RMS, developed in accordance with the requirements of this Prudential Standard, setting out its approach to risk management;

(d) the regulated institution has in place a **Reinsurance Management Strategy** (ReMS), developed in accordance with *Prudential Standard GPS 230 Reinsurance Management*, for selecting and monitoring reinsurance programs;

(e) the regulated institution has, over the last **financial year**, substantially complied with its RMS and ReMS, and that these strategies are operating effectively in practice, having regard to the risks they are designed to control; and

(f) copies of the regulated institution's current RMS and ReMS have been lodged with APRA.

Attachment C

Financial Information Declaration

The CEO and the CFO must (by the time provided for in paragraph 42 of this Prudential Standard) provide APRA with a Financial Information Declaration, signed by both of them,[4] stating that for the last financial year, to the best of their knowledge and belief having made appropriate enquiries:

(a) the financial information that the regulated institution has lodged with APRA has been prepared in accordance with the Act, Regulations, prudential standards, the Collection of Data Act, accounting standards and other mandatory professional reporting requirements in Australia, to the extent that the accounting standards and professional reporting requirements do not contain any requirements contrary to the aforementioned legislative and prudential requirements;

(b) the information provided to the auditor for the purpose of enabling them to undertake their roles and responsibilities is accurate and complete, consistent with the accounting records of the regulated institution, and a true representation of the transactions for the year and the financial position of the regulated institution;[5] and

(c) the financial information lodged with APRA is accurate and complete, consistent with the accounting records of the regulated institution, and represents a true and fair view of the transactions for the year and the financial position of the regulated institution.

[4] As per paragraph 41 of this Prudential Standard, where the CEO and the CFO are the same person, the Financial Information Declaration must be signed by that person and another person to be agreed upon with APRA.

[5] Refer to the Act and GPS 310 for the roles and responsibilities of auditors.

Attachment D

Level 2 insurance groups

1. This Attachment applies adjustments to the requirements outlined in this Prudential Standard and Attachments A to C for Level 2 insurance groups.

2. The Board of the parent entity of a Level 2 insurance group must take a whole-of-business[6] approach in ensuring compliance with this Prudential Standard, including taking into account the **Australian business** and **international business** of the Level 2 insurance group. Therefore, the risk management framework, RMS, Risk Management Declaration and Financial Information Declaration must cover the Level 2 insurance group's international business.

3. In addition to the requirements in this Prudential Standard, the Risk Management Declaration of a Level 2 insurance group must make an attestation as to the compliance of any entity in the group carrying on insurance business in a foreign jurisdiction with the applicable minimum capital requirements, if any, in that jurisdiction. Any instances where an entity of the group does not satisfy the local minimum capital requirements in a foreign jurisdiction must be noted in the attestation. Reasons for not complying with any relevant capital requirements must also be provided.

4. Where a Level 2 insurance group contains an entity that meets the **controlled entity** definition over which the parent entity cannot exercise operational or financial control, APRA may adjust or exclude a specific requirement in this Prudential Standard that would otherwise apply in relation to that specific entity within the Level 2 insurance group. The parent entity must apply for such a determination. The application must demonstrate that the parent entity of the Level 2 insurance group does not control the internal operations of an entity and also indicate how it has addressed this situation in its risk management framework.

[6] Whole-of-business must incorporate, but is not limited to, any entity that forms part of the Level 2 insurance group that conducts insurance business or business related to insurance business.