Prudential Standard GPS 220

Risk Management

Objective and key requirements of this Prudential Standard

This Prudential Standard aims to ensure that a general insurer has systems for identifying, assessing, mitigating and monitoring the risks that may affect its ability to meet its obligations to policyholders. These systems, together with the structures, processes, policies and roles supporting them, are referred to in this Prudential Standard as a general insurer's **risk management framework**.

To meet the key requirements of this Prudential Standard a general insurer must:

- have in its risk management framework a documented Risk Management Strategy and also include sound risk management policies and procedures and clearly defined managerial responsibilities and controls;
- submit its Risk Management Strategy to APRA when any 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 all **insurers** authorised under the Act.[1]

3. Subject to any specific transition rules, an insurer must comply with this Prudential Standard from 1 July 2008 (**effective date**).

4. Where specifically indicated in this Prudential Standard, certain requirements may be complied with on an **insurance group** basis.

Interpretation

5. Unless otherwise defined in this Prudential Standard, expressions in bold are defined in *Prudential Standard GPS 001 Definitions*.

Risk management framework

6. An insurer must at all times have a risk management framework to manage the risks arising from its business.

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

8. For the purposes of this Prudential Standard:

   (a) the risk management framework is the totality of systems, structures, processes and people within the insurer that identify, assess, mitigate and monitor all internal and external sources of risk that could have a material impact on an insurer's operations; and

   (b) a reference to the insurer's operations is a reference to its operations in Australia and overseas through a branch.

9. An insurer'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[2] and in regard to which the Board is satisfied that:

[1] Refer sections 32 and 35 of the Act.

(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 9(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 insurer's risks are being prudently and soundly managed having regard to such factors as the size, business mix and complexity of the insurer's operations; and

(iii) it describes the review referred to in paragraph 11;

(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 insurer having regard to such factors as the size, business mix and complexity of the insurer's operations, and a review process to ensure that the risk management framework remains effective; and

(c) clearly defined managerial responsibilities and controls.

10. The material risks referred to in paragraph 9(b) above must, at a minimum, include:

(a) balance sheet and market risk;

(b) credit risk;

(c) operational risk (requirements for outsourcing and business continuity management are contained in *Prudential Standard GPS 231 Outsourcing* and *Prudential Standard GPS 222 Business Continuity Management)*;

(d) insurance risk;

(e) risks arising out of reinsurance arrangements – there must be a clear link between the insurer's risk management framework and the insurer's Reinsurance Management Strategy;

(f) concentration risk – including risk type, counterparty, geographical, and industry concentration risks which may arise as a result of any of the above-listed risk categories; and

(g) strategic and tactical risks that arise out of the insurer's Business Plan.

---

[2] In the case of a **Category C insurer**, a reference to the 'Board' in this Prudential Standard shall be taken to include a reference to the senior officer outside Australia to whom authority has been delegated in accordance with *Prudential Standard GPS 510 Governance* (**GPS 510**).

11. The insurer 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 insurer'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.[3]

12. For the purposes of paragraph 11, 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

13. An insurer must have a risk management function (or role) within the insurer 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.

    An insurer that is part of an insurance group may rely on the risk management function (or role) of the insurance group instead of having its own risk management function (or role) provided that the risk management function (or role) satisfies the criteria in paragraphs 13(a) to (c) in respect of the insurer.

14. 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

15. An insurer must at all times maintain a Business Plan (including a description of the insurer's approach to capital management) approved by the Board:

    a) prior to its adoption; and

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

---

[3] Also refer to GPS 510 for the internal audit function of an insurer to have among its objectives a review of the risk management framework.

16. Paragraph 15 does not apply to a run-off insurer provided that the run-off insurer maintains at all times a run-off plan[4] (including a description of the run-off insurer's approach to capital management) according to this Prudential Standard.

17. The insurer's Business Plan must be a three-year rolling plan and be reviewed at least annually (or as close to annually as is practicable).

18. An insurer 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.

19. Where the risk management framework covers an insurer's insurance group as a whole and APRA has not made a determination under paragraph 32, the insurer may submit to APRA a Business Plan in respect of the insurance group where:

    (a) the Business Plan covers that insurance group; and

    (b) it is practical to produce a single over-arching Business Plan covering that insurance group.

    An insurance group Business Plan must consider and deal with the matters typically covered by a Business Plan in respect of each insurer within the insurance group.

20. Where APRA has made a determination under paragraph 32 or where APRA is of the view that the insurance group Business Plan does not adequately address the risk management framework of each insurer, or is of the view that a different form of Business Plan is desirable to ensure that the requirements of this Prudential Standard are met, APRA may, in writing, do either or both of the following:

    (a) require one or more insurers within the insurance group to prepare and submit to APRA a separate Business Plan;

    (b) require the preparation and submission to APRA of a Business Plan for a different insurance group within the corporate group,

    within a reasonable time specified by APRA.

Run-off plan

21. Subject to paragraphs 59 and 60 of *Prudential Standard GPS 310 Audit and Actuarial Reporting and Valuation* (**GPS 310**), a **run-off insurer** must at all times maintain a run-off plan (including a description of the insurer's approach to capital management) unless otherwise agreed to by APRA.

[4] Referred to in paragraphs 21 to 27.

22. 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.

23. The insurer's run-off plan must be a three-year rolling plan and the insurer must review it at least annually (or as close to annually as is practicable). Under GPS 310, the **Appointed Actuary** of the insurer must also review the run-off plan according to the requirements of GPS 310.

24. The 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.

25. 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 23

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

26. An 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* are met.

27. A run-off plan must include the matters listed at Attachment A.

Risk Management Strategy

28. The RMS is a high level, strategic document intended to describe the key elements of an insurer's risk management framework set out in paragraph 9(a)(i).

29. The insurer must review its RMS at least annually (or as close to annually as is practicable) to ensure that it accurately documents the insurer's risk management framework.

30. Where there are material changes to the operations of an insurer, it must review and amend its risk management framework and, if appropriate, its 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.

31. An insurer may submit to APRA an RMS in respect of its insurance group where the risk management framework covers that insurance group and it is practical to produce a single over-arching RMS covering that insurance group.

An insurance group RMS must consider and deal with the risk management framework of each insurer within the insurance group as required by this Prudential Standard.

32. Where APRA is of the view that the insurance group RMS does not adequately address the risk management framework of each insurer, or is of the view that a different form of RMS is desirable to ensure that the requirements of this Prudential Standard are met, APRA may, in writing, do either or both of the following:

    (a) require one or more insurers within the insurance group to prepare and submit to APRA a separate RMS;

    (b) require the preparation and submission to APRA of an RMS for a different insurance group within the corporate group;

    within a reasonable time specified by APRA.

33. An insurer 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.

34. Where there are institutional, operational or other developments relating to the insurer's operations that materially affect the risk profile of the insurer, the insurer 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.

35. An insurer'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 insurer (or insurance group) 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 Minimum Capital Requirement (**MCR**);

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

(j) if the insurer 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 an insurer's risk management framework is controlled by another entity in the group, or by head office, describe how this arrangement works; and

(vi) where an insurer:

(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 insurer that could impact on the Australian operations of the insurer.

Risk Management Declaration

36. The Board must provide APRA with a declaration on risk management (**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. This declaration is set out at Attachment B.

37. The Risk Management Declaration must be submitted to APRA on, or before, the day that the insurer's **yearly statutory accounts** 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**).

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

39. Where the risk management framework covers an insurer's insurance group as a whole and APRA has not made a determination under paragraph 32, the insurer may submit to APRA:

    (a) a Risk Management Declaration in respect of the insurance group, where it is practical to provide a single over-arching Risk Management Declaration for that insurance group; or

    (b) a Risk Management Declaration for each insurer in the insurance group.

40. A single Risk Management Declaration for the insurance group, as referred to in paragraph 39(a), must adequately consider and deal with the risk management framework applicable to each insurer in the insurance group as required by this Prudential Standard.

41. Where APRA has made a determination under paragraph 32 or where APRA is of the view that the insurance group Risk Management Declaration does not adequately address the risk management framework applicable to each insurer in the group, or that a separate Risk Management Declaration is desirable to ensure that the requirements of this Prudential Standard are met, APRA may, in writing, do either or both of the following:

    (a) require one or more insurers within the insurance group to prepare and submit to APRA a separate Risk Management Declaration;

    (b) require the preparation and submission to APRA of a Risk Management Declaration for a different insurance group within the corporate group,

    within a reasonable time specified by APRA.

Financial Information Declaration

42. An insurer 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.

43. The Financial Information Declaration must be submitted to APRA on, or before, the day that the insurer's yearly statutory accounts are required to be submitted to APRA according to reporting standards made under the Collection of Data Act.

44. 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

45. Where an insurer 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; or

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

(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.

Written notification must be provided to APRA within 10 business days of the event occurring.

Determinations made under previous GPS 220

46. An approval, determination, direction or requirement made by APRA under a provision specified in Column 1 of the following table that is in operation immediately prior to the commencement of this Prudential Standard is taken, on and from the effective date, to have been made under the provision of this Prudential Standard specified in the same row of Column 2 of the table.

Column 1: Provision of *Prudential Standard GPS 220 Risk Management* made on 9 February 2006	**Column 2: Provision of this Prudential Standard**
Paragraph 21(a): require one or more insurers within an insurance group to prepare and submit a separate RMS.	Paragraph 32(a)
Paragraph 21(b): require the preparation and submission of an RMS	Paragraph 32(b)

Column 1: Provision of *Prudential Standard GPS 220 Risk Management* made on 9 February 2006	**Column 2: Provision of this Prudential Standard**
for a different insurance group within a corporate group.	
Paragraph 30(a): require one or more insurers within an insurance group to prepare and submit a separate Risk Management Declaration.	Paragraph 41(a)
Paragraph 30(b): require the preparation and submission of a Risk Management Declaration for a different insurance group within a corporate group.	Paragraph 41(b)

Attachment A

Matters to be included in a run-off plan

For the purposes of paragraph 27 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[5]
(a) Business overview, including details of significant changes to the insurer's liability portfolio, assets, capital position or operating environment	Significant issues or material anomalies
(b) Details of the 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 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 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 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 insurer's risk management framework	Suitability and adequacy of the risk management framework

[5] A review of the run-off plan by the Appointed Actuary is required under GPS 310.

Attachment B

Risk Management Declaration

The Board must (by the time provided for in paragraph 37 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 insurer has systems in place for the purpose of ensuring compliance with the Act, the Regulations, prudential standards, the Collection of Data Act, reporting standards, authorisation conditions, directions 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 insurer;

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

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

(e) the insurer 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 insurer'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 43 of this Prudential Standard) provide APRA with a Financial Information Declaration, signed by both of them, 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 insurer 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 **Appointed Auditor** and Appointed Actuary for the purpose of enabling them to undertake their roles and responsibilities is accurate and complete, consistent with the accounting records of the insurer, and a true representation of the transactions for the year and the financial position of the insurer;[6] and

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

[6] Refer to the Act and *Prudential Standard GPS 310 Audit and Actuarial Reporting and Valuation* for the roles and responsibilities of **Appointed Auditors** and **Appointed Actuaries**.