



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 on an annual basis and re-submit the Risk Management Strategy 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 or 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 paragraph 32(1)(a) of the *Insurance Act 1973* (**the Act**).

Application

2. This Prudential Standard applies to all general insurers (**insurers**) authorised under the Act.¹
3. Subject to any specific transition rules set out in Attachment C, an insurer:
 - (a) must comply with this Prudential Standard from 1 October 2006 (**effective date**);
 - (b) must continue to comply with *Prudential Standard GPS 220 Risk Management for General Insurers* made on 7 February 2002 (**old Prudential Standard**) until the effective date.
4. Where specifically indicated in this Prudential Standard, certain requirements may be complied with on an insurance group basis provided APRA has agreed.
5. For the purposes of this Prudential Standard, an insurance group comprises:
 - (a) a company that is either:
 - (i) an insurer; or
 - (ii) an authorised non-operating holding company of an insurer; and
 - (b) one or more subsidiary companies of (a) that are insurers (but not any other subsidiary)

within a corporate group. A corporate group comprises two or more companies that are related bodies corporate within the meaning of section 50 of the *Corporations Act 2001*. There may be more than one insurance group within a corporate group.

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.

¹ Refer sections 32 and 35 of the Act.

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 Board² 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 subparagraphs (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 subparagraph 9(b) above must, at a minimum, include:
 - (a) balance sheet and market risk;
 - (b) credit risk;

2 In the case of a foreign general 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*.

- (c) operational risk (requirements for outsourcing and business continuity management are contained in *Prudential Standard GPS 221 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.
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 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.

Risk management function

12. 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.
13. 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

14. 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 prior to its adoption and at any time it is revised during its operational cycle.

15. 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).
16. Each Business Plan, and revised Business Plan, must be submitted to APRA within 10 business days of Board approval.

Risk Management Strategy

17. The RMS is a high level, strategic document intended to describe the key elements of an insurer's risk management framework set out in subparagraph 9(a)(i).
18. 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.
19. 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.
20. An insurance group may submit to APRA an RMS in respect of the 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.
21. 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.
22. 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.
23. 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.

24. 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;³
 - (j) if the insurer is part of an Australian or global corporate group, or is a foreign general insurer (**foreign 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;

3 Prudential requirements include all requirements under the Act, *Insurance Regulations 2002*, prudential standards, the *Financial Sector (Collection of Data) Act 2001*, reporting standards, conditions on a general insurance authority and any other requirements imposed by APRA in writing.

- (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 foreign 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

- 25. The Board must provide APRA with a declaration on risk management (**Risk Management Declaration**) signed by two directors or, in the case of a foreign insurer, the senior officer outside Australia with delegated authority from the Board. This declaration is set out in Attachment A to this Prudential Standard.
- 26. 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 under the *Financial Sector (Collection of Data) Act 2001* (**Collection of Data Act**).
- 27. 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.
- 28. Where the risk management framework covers the insurance group as a whole and APRA has not made a determination under paragraph 21, an insurance group 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.
- 29. A single Risk Management Declaration for the insurance group, as referred to in subparagraph 28(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.

30. Where APRA has made a determination under paragraph 21 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

31. An insurer must provide to APRA a declaration on financial information (**Financial Information Declaration**) signed by the chief executive officer (**CEO**) (by whatever name called, or for a foreign insurer, the local equivalent) and the chief financial officer (**CFO**) (by whatever name called, or for a foreign insurer, the local equivalent). This declaration is set out in Attachment B to this Prudential Standard.
32. 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 under the Collection of Data Act.
33. 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

34. 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.

Attachment A

Risk Management Declaration

The Board must (by the time provided for in paragraph 26 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 B

Financial Information Declaration

The CEO and the CFO must (by the time provided for in paragraph 32 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 Approved Auditor and Approved 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;⁴ 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.

⁴ Refer *Prudential Standard GPS 310 Audit and Actuarial Reporting and Valuation* for the meaning of and the roles and responsibilities of Approved Auditors and Approved Actuaries.

Attachment C

Transition Rules

Expiry date of this Attachment

This Attachment will no longer have effect after 31 December 2007.

Specific transition rules

The Risk Management Declaration required under paragraph 25 must be completed and submitted by the first required submission date after the effective date. However, the attestation provided in the Declaration may relate to requirements under the old Prudential Standard for the period covered by the Declaration before the effective date.

A Financial Information Declaration required under paragraph 31 must be completed and submitted by the first required submission date after the effective date. However, the attestation provided in the Declaration may relate to requirements under the old Prudential Standard for the period covered by the Declaration before the effective date.

Application for a later date to comply with particular requirements

APRA has the ability to determine a later date to comply with particular requirements of this Prudential Standard (**compliance date**), provided that APRA shall not determine a compliance date later than 31 December 2007. APRA cannot exercise this discretion where the failure of the insurer to be able to comply by the effective date is due to the inaction of the board and management in making adequate preparations to comply with this Prudential Standard.

In relation to an application for a compliance date later than the effective date, the criteria that APRA will consider in assessing the application are:

- (a) the insurer has submitted the application to APRA 20 business days before the effective date;
- (b) the insurer can demonstrate that since the determination date of this Prudential Standard, it has been taking reasonable actions to ensure that it will be in a position to comply with this Prudential Standard by the effective date; and
- (c) the insurer can demonstrate that since the determination date of this Prudential Standard, one of the following issues has given rise to the inability of the insurer to comply with this Prudential Standard by the effective date:
 - (i) an event has occurred, outside the insurer's control that has led to it being in a position where it cannot comply with this Prudential Standard (e.g. loss of a key person);

- (ii) the insurer has not been able to retain human resources of sufficient skill and experience after a genuine market search within a period that would enable the insurer to put in place the necessary policies, systems and procedures to ensure compliance with this Prudential Standard by the effective date; or
- (iii) for a foreign insurer, it cannot comply with this Prudential Standard by the effective date due to delays caused by home country regulatory issues relating to a significant demonstrable inconsistency between this Prudential Standard and legal requirements imposed by its home country regulator.