# Prudential Standard SPS 220

# Risk Management

## Objectives and key requirements of this Prudential Standard

This Prudential Standard establishes requirements for an RSE licensee to have systems for identifying, assessing, managing, mitigating and monitoring material risks that may affect its ability to meet its obligations to beneficiaries. These systems, together with the structures, policies, processes and people supporting them, comprise an RSE licensee's risk management framework.

The Board of an RSE licensee is ultimately responsible for having a risk management framework that is appropriate to the size, business mix and complexity of the RSE licensee's business operations and that enables the RSE licensee to implement risk management approaches that appropriately manage different types of risk. The risk management framework must also be aligned with the RSE licensee's business plan.

The key requirements of this Prudential Standard are that an RSE licensee must also:

- have a written business plan that sets out the high-level strategic direction on the RSE licensee's approach to managing its business operations;
- 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 RSE licensee's strategy for managing risk;
- notify APRA when the RSE licensee becomes aware of a significant breach of, or material deviation from, the risk management framework, or discovers that the risk management framework does not adequately address a material risk; and
- maintain adequate technical, human and financial resources at a level that is adequate for the RSE licensee's business operations.

## Authority

1. This Prudential Standard is made under section 34C of the *Superannuation Industry (Supervision) Act 1993* (SIS Act).

## Application

2. This Prudential Standard applies to all registrable superannuation entity (RSE) licensees (RSE licensees) under the SIS Act.[1]

3. All RSE licensees must comply with this Prudential Standard in its entirety, unless otherwise expressly indicated.

4. This Prudential Standard commences on 1 July 2013.

## The role of the Board and senior management

5. An RSE licensee must at all times have a risk management framework to appropriately manage the risks to its business operations.[2]

6. For the purposes of this Prudential Standard, the risk management framework is the totality of systems, structures, policies, processes and people within an RSE licensee's business operations that identify, assess, manage, mitigate and monitor all internal and external sources of inherent risk that could have a material impact on the RSE licensee's business operations or the interests of beneficiaries (material risks).[3]

7. The Board of the RSE licensee (the Board) is ultimately responsible for the risk management framework.[4]

8. The Board is ultimately responsible for maintaining the solvency of the RSE licensee and ensuring that the RSE licensee's business operations have adequate resources to undertake the activities for which it holds an RSE licence.

---

1 For the purposes of this Prudential Standard, 'RSE licensee' has the meaning given in section 10(1) of the SIS Act.

2 For the purposes of this Prudential Standard, an 'RSE licensee's business operations' includes all activities as an RSE licensee (including the activities of each RSE of which it is the licensee), and all other activities of the RSE licensee to the extent that they are relevant to, or may impact on, its activities as an RSE licensee. The risk management framework must also cover risks that arise from functions that are outsourced; refer to *Prudential Standard SPS 231 Outsourcing* (SPS 231).

3 For the purposes of this Prudential Standard, a reference to 'beneficiaries' is a reference to 'beneficiaries of an RSE within the RSE licensee's business operations'.

4 For the purposes of this Prudential Standard, a reference to 'the Board' is a reference to the Board of directors or group of individual trustees of an RSE licensee and 'group of individual trustees' has the meaning given in section 10(1) of the SIS Act.

## RSE licensees that are part of a group[5]

9. Where an RSE licensee is part of a corporate group, and the RSE licensee utilises group policies or functions, the Board must approve the use of group policies and functions and must ensure that these policies and functions give appropriate regard to the RSE licensee's business operations and its specific requirements.

## Material risks

10. An RSE licensee must, at a minimum, ensure that its risk management framework covers all material risks, both financial and non-financial, to the RSE licensee's business operations, having regard to the size, business mix and complexity of those operations.

11. An RSE licensee must assess the materiality of each risk with reference to its business operations as a whole, each RSE within those operations and the impact of the risk on the obligations of the RSE licensee to its beneficiaries.

12. An RSE licensee's risk management framework must, at a minimum, cover:

    (a) governance risk[6];

    (b) investment governance risk[7];

    (c) liquidity risk, including the liquidity characteristics of investment options offered or proposed to be offered[8];

    (d) operational risk[9];

    (e) insurance risk[10];

    (f) strategic and tactical risks that arise out of the RSE licensee's strategic and business plans; and

    (g) other risks that may have a material impact on the RSE licensee's business operations.

13. Where an RSE licensee conducts business that has a purpose other than superannuation[11], its risk management framework must cover all material

---

5 For the purposes of this Prudential Standard, a reference to 'a group' is a reference to a group comprising the RSE licensee and all connected entities and all related bodies corporate of the RSE licensee, 'connected entity' has the meaning given in section 10(1) of the SIS Act and 'related body corporate' has the meaning given in section 50 of the *Corporations Act 2001*.

6 Refer to *Prudential Standard SPS 510 Governance*, *Prudential Standard SPS 520 Fit and Proper* and *Prudential Standard SPS 521 Conflicts of Interest*.

7 Refer to *Prudential Standard SPS 530 Investment Governance* (SPS 530).

8 Refer to SPS 530.

9 Refer to *Prudential Standard SPS 114 Operational Risk Financial Requirement* (SPS 114), SPS 231 and *Prudential Standard SPS 232 Business Continuity Management* (SPS 232).

10 Refer to *Prudential Standard SPS 250 Insurance in Superannuation*.

11 Refer to section 62 of the SIS Act for details of the sole purpose test to identify business that has a purpose other than superannuation.

contagion risks that any non-superannuation business conducted by the RSE licensee might have on the superannuation business.

### Risk management framework

14. An RSE licensee's risk management framework must enable the RSE licensee to develop and implement strategies, policies, procedures and controls to appropriately manage different types of material risk.

15. An RSE licensee's risk management framework must provide reasonable assurance that each material risk to the RSE licensee's business operations is being prudently and soundly managed, having regard to the size, business mix and complexity of those operations.

16. An RSE licensee's risk management framework must, at a minimum, include:

    (a) the risk appetite statement;

    (b) the risk management strategy (RMS);

    (c) a designated risk management function that meets the requirements of paragraph 25;

    (d) all risk management policies, procedures and controls to identify, assess, monitor, report on, mitigate and manage each material risk;

    (e) clearly defined and documented roles, responsibilities and formal reporting structures for the management of material risks throughout the RSE licensee's business operations; and

    (f) a review process to ensure that the risk management framework remains effective.

17. Where an RSE licensee is part of a corporate group and any element of the RSE licensee's risk management framework is controlled or influenced by, or is subject to approval by another entity in the group, the RSE licensee's risk management framework must specifically take into account risks arising from group policy objectives and strategies, and clearly identify:

    (a) whether the RSE licensee's risk management framework is derived wholly or partially from group risk management policies or functions;

    (b) the linkages and significant differences between the RSE licensee's risk management framework and group risk management policies or functions; and

    (c) 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.

## Strategic and business planning

18. An RSE licensee must have a written plan that sets out the strategic direction of the RSE licensee's approach to managing its business operations (business plan). The business plan must cover the entirety of the RSE licensee's business operations, be aligned with the risk management framework and be approved by the Board prior to its adoption and at any time that it is materially revised. The business plan must be a rolling plan of at least three, but no more than five, years' duration that is reviewed at least annually (or as close to annually as is practical), with the results of the review reported to the Board.

19. An RSE licensee's strategic and business planning process must:

    (a) identify and consider those material risks associated with the RSE licensee's strategic objectives and business plan that are required to be explicitly addressed and managed through the risk management framework; and

    (b) consider the material risks that have been identified by the risk management framework.

## Risk appetite statement

20. An RSE licensee must maintain an up-to-date risk appetite statement that covers the RSE licensee's business operations and each category of material risk. The risk appetite statement must be approved by the Board.

21. An RSE licensee's risk appetite statement must, at a minimum, articulate:

    (a) the degree of risk that the RSE licensee is prepared to accept in pursuit of its strategic objectives, giving consideration to the interests of beneficiaries (risk appetite);

    (b) for each material risk, the maximum level of risk that the RSE licensee is willing to operate within expressed as a risk limit that, where possible, is based on a measurable limit of the risk remaining, after taking into account the mitigants for the risk where appropriate (risk tolerance);

    (c) the process for ensuring that risk tolerances are set at an appropriate level, based on an estimation of the impact on the interests of beneficiaries 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 taking appropriate action in the event of a breach of the RSE licensee's risk tolerance; and

    (e) the timing and process for review of the risk appetite and risk tolerances.

## Risk management strategy

22. An RSE licensee must maintain an up–to-date RMS for its business operations that covers each material risk identified under paragraphs 10 to 13 inclusive. The RMS must be approved by the Board.

23. An RMS is a strategic document that describes the RSE licensee's strategy for managing risk and the key elements of the risk management framework that give effect to this strategy. At a minimum, an RSE licensee's RMS must describe:

    (a) each material risk identified under paragraphs 10 to 13 inclusive and the RSE licensee's approach to managing these risks;

    (b) the policies and procedures dealing with the following risk management matters, including 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:

        (i) the processes for identifying and assessing material risks and controls;

        (ii) the process for establishing, implementing and testing mitigation strategies and control mechanisms for material risks;

        (iii) the process for monitoring, communicating and reporting risk issues, including escalation procedures for the reporting of material events and incidents;

        (iv) the mechanisms in place for monitoring and ensuring ongoing compliance with all prudential requirements[12]; and

        (v) the process for ensuring continued alignment between the risk management framework and the business plan;

    (c) the role and responsibilities of the risk management function;

    (d) the relationships between the Board, board committees and senior management with respect to the risk management framework;

    (e) those with managerial responsibility for the risk management framework, and their roles and responsibilities;

    (f) the approach to ensuring all persons within the RSE licensee's business operations have awareness of the risk management framework and for instilling an appropriate risk culture across the RSE licensee's business operations; and

[12] 'Prudential requirements' include requirements under the SIS Act, the *Superannuation Industry (Supervision) Regulations 1994*, the prudential standards, reporting standards, the *Financial Sector (Collection of Data) Act 2001* (FSCOD Act), licence conditions, authorisations, superannuation data and payment standards, directions and any other requirements imposed by APRA under legislation.

(g) the process by which the risk management framework is reviewed and the intended coverage and timing for these reviews.

24. APRA may require an RSE licensee to amend its RMS or develop and maintain a separate RMS with respect to one or more RSEs within its business operations where APRA considers that the RSE licensee's RMS does not adequately cover the risks to that RSE.[13]

## Risk management function

25. An RSE licensee must have a designated risk management function that, at a minimum:

(a) is responsible for assisting the Board, board committees and senior management to develop and maintain the risk management framework;

(b) is appropriate to the size, business mix and complexity of the RSE licensee's business operations and is operationally independent from the business units of the RSE licensee;

(c) is resourced with staff who have clearly defined roles and responsibilities and who possess appropriate experience and qualifications to exercise those responsibilities;

(d) has access to all aspects of the RSE licensee's business operations that have the potential to generate material risk, including information technology systems and systems development resources;

(e) has the necessary authority and reporting structure to the Board, board committees and senior management to conduct its risk management activities in an effective and independent manner; and

(f) is required to notify the Board of any material deviation from, or material breach of, the risk management framework.

26. An RSE licensee that is part of a corporate group may rely on a risk management function located in another entity in the group where the risk management function satisfies the criteria set out in paragraph 25 in respect of the RSE licensee's business operations.

27. An RSE licensee may engage the services of an external service provider to perform all or part of the risk management function where the RSE licensee can demonstrate to APRA that the external risk management function meets the requirements in paragraph 25.[14]

---

13 Where this Prudential Standard provides for APRA to require an RSE licensee to amend its RMS, or otherwise exercise a power or discretion, the power or discretion is to be exercised in writing.

14 Outsourcing of the risk management function by an RSE licensee must also meet the requirements in SPS 231.

## Review of the risk management framework

28. An RSE licensee must ensure that the appropriateness, effectiveness and adequacy of its risk management framework are subject to a comprehensive review by operationally independent, appropriately trained and competent persons at least every three years.

29. An RSE licensee must also undertake, for each year during which a comprehensive review does not take place, a review of the appropriateness, effectiveness and adequacy of the risk management framework.

30. The scope of the comprehensive review of an RSE licensee's risk management framework must have regard to the size, business mix and complexity of the RSE licensee's business operations, the extent of any change to those operations or its risk appetite and any changes to the external environment in which the RSE licensee operates. The review of the risk management framework must, at a minimum, include a review of:

    (a) whether the risk management framework remains appropriate for the RSE licensee's business operations;

    (b) the specific resources utilised, at a minimum, to undertake the risk management activities required by this Prudential Standard;

    (c) the risk appetite statement;

    (d) the RMS, to ensure that it accurately documents the RSE licensee's risk management framework and the RSE licensee's strategy for managing risk;

    (e) all risk management policies and procedures; and

    (f) all risk management and internal control systems.

31. An RSE licensee must implement satisfactory internal audit procedures and external audit arrangements to ensure compliance with the risk management framework and enable the RSE licensee to attest that the risk management and internal control systems in place are operating effectively and are adequate.[15]

32. Where institutional, operational or other developments that materially affect the size, business mix and complexity of an RSE licensee's business operations are identified outside the comprehensive review required in paragraph 28, the RSE licensee must assess whether any amendment to, or a review of, the risk management framework is necessary to take account of these developments.

[15] Refer to *Prudential Standard SPS 310 Audit and Related Matters* and SPS 510 for requirements relating to external audits and internal audits respectively.

## Risk management declaration

33. The Board must, on an annual basis, provide APRA with a declaration on risk management (risk management declaration) signed by two directors that satisfies the requirements set out in Attachment A to this Prudential Standard.

34. An RSE licensee must submit the risk management declaration to APRA on, or before, the day that the RSE licensee is required to submit annual information under reporting standards made by APRA under the *Financial Sector (Collection of Data) Act 2001*.

35. If the Board qualifies the risk management declaration, the qualified declaration must include a description of any material deviation from the RSE licensee's risk management framework and the steps taken, or proposed to be taken, to remedy those deviations.

## Adequacy of resources

36. An RSE licensee must maintain financial resources at a level adequate to ensure its ongoing solvency and adequate liquidity to support its business operations. This requirement is in addition to the operational risk financial requirement required in SPS 114.

37. An RSE licensee must maintain human resources at a level adequate for its business operations, where 'human resources' includes, but is not limited to, adequate levels of personnel with the necessary knowledge, skills and expertise to enable the RSE licensee to effectively carry out its operations and support its risk management framework, including its business continuity and disaster recovery plans.[16]

38. An RSE licensee must maintain technical resources at a level adequate for its business operations, where 'technical resources' includes, but is not limited to:

    (a) technical systems, including adequate hardware, data quality and software;

    (b) systems and resources to ensure protection, security and privacy of confidential, personal and sensitive material;

    (c) resources to handle transaction processing and other operations;

    (d) technical resources to handle any significant changes or increases in size, business size or complexity that are planned, forecast or likely to occur;

    (e) a business continuity plan; and

    (f) records maintenance systems.

39. An RSE licensee must be able to demonstrate to APRA that it has a process to determine the levels of resources that are adequate based on an assessment of

[16] Refer to SPS 232.

the business plan, risk management framework and the size, business mix and complexity of the RSE licensee's business operations.

40. An RSE licensee may hold the resources required in paragraphs 36 to 38 inclusive itself or have the resources available under an enforceable agreement.

## Notification requirements

41. An RSE licensee must notify APRA within 10 business days when it:

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

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

42. An RSE licensee must notify APRA, as soon as practicable, when it becomes aware of any material changes to the size, business mix and complexity of the RSE licensee's business operations.

## Adjustments and exclusions

43. APRA may, by notice in writing to an RSE licensee, adjust or exclude a specific prudential requirement in this Prudential Standard in relation to that RSE licensee.[17]

[17] Refer to section 34C(5) of the SIS Act.

## Attachment A

## Risk management declaration

For the purposes of paragraph 33 of this Prudential Standard, an RSE licensee's risk management declaration must cover the following matters:

(a) the RSE licensee has in place systems for ensuring compliance with all prudential requirements;

(b) the systems and resources that are in place for managing and monitoring risks, and the risk management framework, are appropriate to the RSE licensee, having regard to the size, business mix and complexity of the RSE licensee's business operations;

(c) the RSE licensee has assessed the risks of outsourcing any business activity, and is satisfied that the risks and relevant controls relating to these risks are appropriate to the RSE licensee, having regard to the size, business mix and complexity of the RSE's licensee's business operations and the operational capabilities of the RSE licensee itself;

(d) the risk management and internal control systems in place are operating effectively and are adequate having regard to the risks they are designed to control;

(e) the RSE licensee has an RMS that complies with this Prudential Standard, and that the RSE licensee has complied with each measure and control described in the RMS;

(f) the RSE licensee is satisfied with the efficacy of the processes and systems surrounding the production of financial information for each RSE within its business operations;

(g) the RSE licensee has adequate reporting systems and internal controls supporting the preparation and reporting of accurate financial and statistical information to APRA; and

(h) information provided to APRA accurately represents the transactions for the year and financial position at year end in accordance with the provisions of the SIS Act and FSCOD Act.