Superannuation (prudential standard) determination No. 4 of 2012

Prudential Standard SPS 232 Business Continuity Management

Superannuation Industry (Supervision) Act 1993

I, Ross Jones, delegate of APRA, under subsection 34C(1) of the *Superannuation Industry (Supervision) Act 1993* (the Act), DETERMINE *Prudential Standard SPS 232 Business Continuity Management* in the form set out in the Schedule, which applies to all RSE licensees.

This instrument takes effect upon registration on the Federal Register of Legislative Instruments.

Dated: 15 November 2012

[signed]

Ross Jones
Deputy Chair

Interpretation

In this instrument:

APRA means the Australian Prudential Regulation Authority.

Federal Register of Legislative Instruments means the Register kept under the *Legislative Instruments Act 2003.*

RSE licensee has the meaning given in section 10(1) of the Act.

Note 1 It is a condition imposed on all RSE licences that the RSE licensee and, if the RSE licensee is a group of individuals, each of the members of the group, must comply with the RSE licensee law [section 29E(1)(a)]. RSE licensee law includes the prudential standards [section 10(1)]. APRA may direct an RSE licensee to comply with a specified condition of its RSE licence by a specified time if APRA has reasonable grounds to believe that the RSE licensee has breached the condition [section 29EB]. A failure to comply with a direction may lead to cancellation of the RSE licence [section 29G] and may be an offence attracting a penalty of 60 penalty units [section 29JB].

Schedule

Prudential Standard SPS 232 Business Continuity Management comprises the 7 pages commencing on the following page.

Prudential Standard SPS 232

Business Continuity Management

Objectives and key requirements of this Prudential Standard

This Prudential Standard requires each RSE licensee to implement a whole-of-business approach to business continuity management that is appropriate to the size, business mix and complexity of its business operations. Business continuity management increases resilience to business disruption arising from internal and external events and may reduce the impact on the RSE licensee's business operations.

The ultimate responsibility for the business continuity of an RSE licensee's business operations rests with its Board of directors.

The key requirements of this Prudential Standard are that:

- an RSE licensee must identify, assess and manage potential business continuity risks to ensure that it is able to meet its obligations to beneficiaries and protect the financial position of the RSE licensee, any of its RSEs or connected entities;
- the Board of the RSE licensee must consider business continuity risks and controls as part of its overall risk management framework and approve a Business Continuity Management Policy;
- an RSE licensee must develop and maintain a business continuity plan that documents procedures and information which enable the RSE licensee to manage business disruptions;
- an RSE licensee must review the business continuity plan annually and periodically arrange for its review by the internal audit function or an appropriate external expert; and
- an RSE licensee must notify APRA in the event of certain disruptions.

Federal Register of Legislative Instruments F2012L02224

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 applies whether or not activities are outsourced.[2] This Prudential Standard also applies to arrangements where the service provider is located outside of Australia or the functions are performed outside Australia.

5. Nothing in this Prudential Standard prevents an RSE licensee from adopting and applying a group policy used by a connected entity or a related body corporate within the group[3], provided that the policy has been approved by the Board of the RSE licensee (the Board) and meets the requirements of this Prudential Standard.[4]

6. Subject to paragraph 32, this Prudential Standard commences on 1 July 2013.

The role of the Board and senior management

7. An RSE licensee must identify, assess, manage, mitigate and report on potential business continuity risks to ensure that it is able to meet its obligations to beneficiaries and protect the financial position of the RSE licensee, any of its RSEs or connected entities.[5]

8. The Board is ultimately responsible for business continuity management (BCM) of the RSE licensee's business operations.

9. The Board must ensure that the RSE licensee's approach to BCM is appropriate to the size, business mix and complexity of its business operations.

---

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

2 Refer to *Prudential Standard SPS 231 Outsourcing* (SPS 231) for requirements relating to outsourcing.

3 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*.

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.

5 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' and 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.

10. The Board may delegate day-to-day operational responsibility for BCM to a responsible committee and/or senior management. The operational responsibility must be clearly expressed in the charter of the committee and/or in the performance objectives of the responsible senior management.

11. The Board must ensure that the RSE licensee's business continuity risks and controls for its business operations are taken into account as part of its overall risk management framework and when completing a risk management declaration required to be provided to APRA.[6]

Business continuity management

12. BCM is a whole-of-business approach that includes policies, standards and procedures for ensuring that critical business activities can be maintained or recovered in a timely fashion, in the event of a disruption. Its purpose is to minimise the financial, legal, regulatory, reputational and other material consequences arising from a disruption.

13. 'Critical business activities' are the business functions, resources and infrastructure that may, if disrupted, have a material impact on the interests, or reasonable expectations, of beneficiaries or the financial position of the RSE licensee, any of its RSEs or connected entities.

14. An RSE licensee's BCM must, at a minimum, include:

    (a) a BCM Policy in accordance with paragraphs 15 and 16;

    (b) a business impact analysis (BIA) including risk assessment in accordance with paragraphs 17 and 18;

    (c) recovery objectives and strategies in accordance with paragraphs 19 and 20;

    (d) a business continuity plan (BCP) including crisis management and recovery in accordance with paragraphs 21 to 24 inclusive; and

    (e) programs for:

        (i) review and testing of the BCP in accordance with paragraph 25; and

        (ii) training and ensuring awareness of staff in relation to BCM.

Business Continuity Management Policy

15. An RSE licensee must have an up-to-date and documented Business Continuity Management Policy (BCM Policy) that is approved by the Board.

16. An RSE licensee's BCM Policy must clearly state the roles, responsibilities and authorities to act in relation to the BCM Policy.

---

6 Refer to *Prudential Standard SPS 220 Risk Management* (SPS 220) for requirements relating to the risk management framework and declaration.

Business impact analysis

17. A BIA involves identifying all critical business activities of an RSE licensee and assessing the impact of a disruption on these.

18. When conducting the BIA, an RSE licensee must consider:

    (a) plausible disruption scenarios over varying periods of time;

    (b) the period of time for which the RSE licensee could not operate without each of its critical business activities;

    (c) the extent to which a disruption to the critical business activities might have a material impact on the interests, or reasonable expectations, of beneficiaries; and

    (d) the financial, legal, regulatory and reputational impact of a disruption to an RSE licensee's critical business activities over varying periods of time.

Recovery objectives and strategies

19. Recovery objectives are pre-defined goals for recovering critical business activities to a specified level of service (recovery level) within a defined period (recovery time), following a disruption.

20. An RSE licensee must identify and document appropriate recovery objectives and implementation strategies based on the results of the BIA and the size, business mix and complexity of the RSE licensee's business operations.

Business continuity planning

21. An RSE licensee must maintain at all times a documented BCP that meets the objectives of the BCM Policy.[7]

22. An RSE licensee's BCP must document procedures and information that enable the RSE licensee to:

    (a) manage an initial business disruption (crisis management); and

    (b) recover critical business activities.

23. An RSE licensee's BCP must reflect the specific requirements of the RSE licensee and must identify:

    (a) critical business activities;

    (b) recovery levels and recovery times for each critical business activity;

    (c) recovery strategies for each critical business activity;

[7] A reference to a 'BCP' includes reference to more than one BCP where appropriate. An RSE licensee may have a number of BCPs. A BCP may include a separate crisis management plan and disaster recovery plan.

(d) infrastructure and resources required to implement the BCP;

(e) roles, responsibilities and authorities to act in relation to the BCP; and

(f) communication plans with staff and external stakeholders.

24. Where material business activities are outsourced, an RSE licensee must satisfy itself as to the adequacy of the outsourced service provider's BCP and must consider any dependencies between the two BCPs.

Review and testing of the BCP

25. An RSE licensee must review and test its BCP at least annually, or more frequently if there are material changes to its business operations, to ensure that the BCP can meet the BCM objectives. The results of the testing must be formally reported to the Board or to delegated management.[8]

26. The BCP must be updated if shortcomings are identified as a result of the review and testing required under paragraph 25.

27. Where material business activities are outsourced, an RSE licensee must satisfy itself that the outsourced service provider adequately reviews and tests its BCP at least annually, or more frequently if there are material changes to business operations, to ensure that the BCP can meet the BCM objectives of the RSE licensee. The results of the testing, including any change to the service provider's BCP, must be formally reported to the RSE licensee by the outsourced service provider as soon as practicable.

Notification requirements

28. An RSE licensee must notify APRA as soon as possible, and no later than 24 hours, after experiencing a major disruption that has the potential to have a material impact on the interests, or reasonable expectations, of beneficiaries or the financial position of the RSE licensee, any of its RSEs or connected entities.[9] The RSE licensee must explain to APRA the nature of the disruption, the action being taken, the likely effect and the timeframe for returning to normal operations. The RSE licensee must notify APRA when normal operations resume.

29. The information or notifications required by this Prudential Standard must be given in such form, if any, and by such procedures, if any, as APRA determines and publishes on its website from time to time.[10]

---

8 A material change to business operations includes a change in a material outsourcing arrangement. Refer to SPS 231 for further information on outsourcing.

9 This applies whether the major disruption affects the business operations of the RSE licensee or an outsourced service provider of the RSE licensee.

10 Where this Prudential Standard provides for APRA to determine the form of information or notifications, or otherwise exercise a power or discretion, the power or discretion is to be exercised in writing.

Audit arrangements

30. An RSE licensee's internal audit function, or an appropriate external expert, must periodically review the BCP and provide an assurance to the Board or to delegated management that:

    (a) the BCP is in accordance with the RSE licensee's BCM Policy and addresses the risks it is designed to control; and

    (b) testing procedures are adequate and have been conducted satisfactorily.

31. APRA may request the external auditor of the RSE licensee, or another appropriate external expert, to provide an assessment of the RSE licensee's BCM arrangements. Any such report must be paid for by the RSE licensee and must be made available to APRA.[11]

Commencement and transitional arrangements

32. Paragraphs 33 and 34 of this Prudential Standard commence on the date of registration of this Prudential Standard on the Federal Register of Legislative Instruments (registration date).

33. An RSE licensee must ensure that, when entering into an arrangement covered by this Prudential Standard on and from the day after the registration date, it complies with paragraphs 24 and 27.

34. Where an RSE licensee has entered into an arrangement covered by this Prudential Standard prior to the registration date, the RSE licensee must, for each arrangement:

    (a) assess the provisions of the arrangement against paragraphs 24 and 27;

    (b) identify whether it is satisfied as to the matters in paragraphs 24 and 27;

    (c) where the RSE licensee is not satisfied as to the matters in paragraphs 24 and 27, identify the anticipated end date of the arrangement;

    (d) where the anticipated end date of the arrangement is on or after 1 January 2014, take all reasonable steps to adjust the terms of the arrangement in order to ensure that the RSE licensee complies with paragraphs 24 and 27;

    (e) where, as a result of the reasonable steps taken under paragraph 34(d), the RSE licensee determines that, if it were to renegotiate the terms of the arrangement, it would not be acting in the best interests of beneficiaries, demonstrate to APRA why it considers the arrangement should continue; and

    (f) report to APRA before 1 July 2013 the extent of any non-compliance with paragraphs 24 and 27 and the anticipated end date of the arrangement.

[11] Refer to *Prudential Standard SPS 310 Audit and Related Matters*.

Adjustments and exclusions

35. 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.[12]

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