Prudential Standard CPS 232

Business Continuity Management

Objectives and key requirements of this Prudential Standard

This Prudential Standard requires each APRA-regulated institution and Head of a group to implement a whole-of-business approach to business continuity management that is appropriate to the nature and scale of the operations. Business continuity management increases resilience to business disruption arising from internal and external events and may reduce the impact on the institution's or group's business operations, reputation, profitability, depositors, policyholders and other stakeholders.

The Board of an APRA regulated institution and the Board of a Head of a group, respectively, have ultimate responsibility for the business continuity of the institution or group.

The key requirements of this Prudential Standard are that an APRA-regulated institution and a Head of a group must:

- maintain a business continuity management policy for the institution or group, approved by the Board;
- identify, assess and manage potential business continuity risks to ensure that it is able to meet its financial and service obligations to its depositors, policyholders and other stakeholders;
- consider business continuity risks and controls as part of its risk management framework;
- maintain a business continuity plan that documents procedures and information which enable the institution to manage business disruptions;
- review the business continuity plan annually and periodically arrange for its review by the internal audit function or an appropriate external expert; and
- notify APRA in the event of certain disruptions.

Where an APRA-regulated institution is the Head of a group, this Prudential Standard requires that the group has in place business continuity management appropriate to the nature and scale of the group's operations, and the provisions of this Prudential Standard are applied appropriately throughout the group, including in relation to institutions that are not APRA-regulated. In addition, where specified, the Head of a group must comply with the requirements on a group basis.

Authority

1. This Prudential Standard is made under:

   (a) section 11AF of the *Banking Act 1959* (**Banking Act**);

   (b) section 32 of the *Insurance Act 1973* (Insurance Act); and

   (c) section 230A of the *Life Insurance Act 1995* (Life Insurance Act).

Application

2. This Prudential Standard applies to all 'APRA-regulated institutions',[1] defined as:

   (a) all **authorised deposit-taking institutions** (**ADIs**), including **foreign ADIs**, and **non-operating holding companies** authorised under the Banking Act (authorised banking NOHCs);

   (b) all **general insurers**, including **Category C insurers**, non-operating holding companies authorised under the Insurance Act (authorised insurance NOHCs) and **parent entities** of **Level 2 insurance groups**; and

   (c) all **life companies**, including **friendly societies** and **eligible foreign life insurance companies** (EFLICs), and non-operating holding companies registered under the Life Insurance Act (registered life NOHCs).

3. All APRA-regulated institutions have to comply with this Prudential Standard in its entirety, unless otherwise expressly indicated. The obligations imposed by this Prudential Standard on, or in relation to, a foreign ADI, a Category C insurer or an EFLIC apply only in relation to the Australian branch operations of that institution.

4. Where an APRA-regulated institution is the 'Head of a group',[2] it must comply with a requirement of this Prudential Standard:

   (a) in its capacity as an APRA-regulated institution;

   (b) by ensuring that the requirement is applied appropriately throughout the group, including in relation to institutions that are not APRA-regulated; and

   (c) on a group basis.

   In applying the requirements of this Prudential Standard on a group basis, references in paragraphs 17 to 40 to an 'APRA-regulated institution' should be read as 'Head of a group' and references to 'institution' should be read as 'group'.

---

1 Note, for the purposes of this Prudential Standard, an **RSE licensee** is not treated as an 'APRA-regulated institution'. Refer to *Prudential Standard SPS 232 Business Continuity Management* (SPS 232) for requirements relating to business continuity management for an RSE licensee.

2 Where a Level 2 group operates within a Level 3 group, a requirement expressed as applying to a Head of a group is to be read as applying to the Level 3 Head.

5. This Prudential Standard applies whether or not activities are outsourced to **related bodies corporate** or third-party service providers. This Prudential Standard also applies to arrangements where the service provider is located outside Australia or the functions are performed outside Australia.

6. Nothing in this Prudential Standard prevents an APRA-regulated institution from adopting and applying a group policy used by a related body corporate, provided that the policy has been approved by the **Board**[3] of the regulated institution and meets the requirements of this Prudential Standard.

7. This Prudential Standard commences on 1 July 2017.

Interpretation

8. Terms that are defined in *Prudential Standard 3PS 001 Definitions*, *Prudential Standard APS 001 Definitions* (APS 001), *Prudential Standard GPS 001 Definitions* (GPS 001) or *Prudential Standard LPS 001 Definitions* appear in bold the first time they are used in this Prudential Standard.

9. Where this Prudential Standard provides for APRA to exercise a power or discretion, this power or discretion is to be exercised in writing.

10. For the purposes of this Prudential Standard:

    'group' means a Level 2 group or a **Level 3 group**, as relevant;

    'Head of a group' means a Level 2 Head or **Level 3 Head**, as relevant;

    'Level 2 group' means the entities that comprise:

    (a) **Level 2** as defined in APS 001; or

    (b) a Level 2 insurance group as defined in GPS 001;

    'Level 2 Head' means:

    (a) where an ADI that is a member of a Level 2 group is not a **subsidiary** of an authorised banking NOHC or another ADI, that ADI;

    (b) where an ADI that is a member of a Level 2 group is a subsidiary of an authorised banking NOHC, that authorised banking NOHC; or

    (c) the **parent entity** of a Level 2 insurance group as defined in GPS 001.

Additional requirements of the Head of a group

11. The Head of a group must maintain business continuity management (**BCM**) for the group (see paragraphs 20 to 22) including a BCM policy for the group (see paragraphs 23 to 25).

---

[3] A reference to the Board in the case of a foreign ADI is a reference to the **senior officer outside Australia**.

12. The Head of a group must apply BCM to risk assessments and risk processes at a functional level in the group, where appropriate.

13. The Board of the Head of a group must:

    (a) **ensure** that the group's BCM is appropriate to the nature and scale of its operations and is consistent with the group's **risk management strategy** and **risk management framework**;

    (b) oversee the appropriateness of BCM across the group; and

    (c) ensure that the group's business continuity plan (**BCP**) is reviewed at least annually by responsible senior management of the Head of the group.

14. The Head of a group must notify APRA in accordance with paragraph 36 if the institution experiences a major disruption that has the potential to have a material impact on the institution's risk profile, or affect its financial soundness, except where an APRA-regulated institution within the group has otherwise notified APRA of that information.

15. The group internal audit function, or an appropriate external expert, must periodically review the group BCP and provide an assurance to the Board of the Head of the group, or delegated management, on the matters in paragraph 38 on a group basis.

16. Where an institution within the group that is not an APRA-regulated institution undertakes business operations critical to the group, the Head of the group must ensure that those business operations are undertaken in a way that complies with the group BCM policy.

The role of the Board and senior management

17. An APRA-regulated institution must identify, assess, manage, mitigate and report on potential business continuity risks to ensure that the institution is able to meet its financial and service obligations to its depositors, **policyholders** and other stakeholders.

18. The Board is ultimately responsible for the business continuity of the institution. The Board remains ultimately responsible for BCM of the institution whether or not business operations are outsourced or are part of a **corporate group**.[4]

19. The Board must ensure that the business continuity risks and controls are taken into account as part of the institution's **risk management strategy** and when completing a **risk management declaration** required to be provided to APRA.[5]

---

4 Refer to *Prudential Standard CPS 231 Outsourcing* (CPS 231) for further information on requirements relating to outsourcing.

5 For details of the **risk management framework** for regulated institutions refer to *Prudential Standard CPS 220 Risk Management.*

Business continuity management

20. BCM is a whole-of-business approach that includes policies, standards and procedures for ensuring that critical business operations 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.

21. Critical business operations are the business functions, resources and infrastructure that may, if disrupted, have a material impact on the institution's business functions, reputation, profitability, depositors and/or policyholders.

22. BCM must, at a minimum, include:

    (a) a BCM policy in accordance with paragraphs 23 to 25;

    (b) a business impact analysis (BIA) including risk assessment in accordance with paragraphs 26 and 27;

    (c) recovery objectives and strategies; in accordance with paragraphs 28 and 29;

    (d) a BCP in accordance with paragraphs 30 to 33; and

    (e) programs for:

        (i) review and testing of the BCP in accordance with paragraphs 34 and 35; and

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

Business continuity management policy

23. The Board must approve the institution's BCM policy.

24. The BCM policy must be up-to-date, documented and must set out the objectives and approach in relation to BCM.

25. The BCM policy must clearly state the roles, responsibilities and authorities to act in relation to the BCM policy.

Business impact analysis

26. A BIA involves identifying all critical business functions, resources and infrastructure of the institution and assessing the impact of a disruption on these.

27. When conducting the BIA, the APRA-regulated institution must consider:

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

    (b) the period of time for which the institution could not operate without each of its critical business operations;

(c) the extent to which a disruption to the critical business operations might have a material impact on the interests of depositors and/or policyholders of the institution; and

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

Recovery objectives and strategies

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

29. An APRA-regulated institution must identify and document appropriate recovery objectives and implementation strategies based on the results of the BIA and the size and complexity of the institution.

Business continuity planning

30. An APRA-regulated institution must maintain at all times a documented BCP for the institution that meets the objectives of the institution's BCM policy.[6]

31. The BCP must document procedures and information that enable the institution to:

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

(b) recover critical business operations.

32. The BCP must reflect the specific requirements of the institution and must identify:

(a) critical business operations;

(b) recovery levels and time targets for each critical business operation;

(c) recovery strategies for each critical business operation;

(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.

33. Where material business activities are outsourced, an APRA-regulated institution must satisfy itself as to the adequacy of the outsourced service provider's BCP and must consider any dependencies between the two BCPs.

---

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

Review and testing of the Business Continuity Plan

34. An APRA-regulated institution must review and test the institution's 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. The results of the testing must be formally reported to the Board or to delegated management.[7]

35. The BCP must be updated if shortcomings are identified as a result of the review and testing required under paragraph 34.

Notification requirements

36. An APRA-regulated institution must notify APRA as soon as possible and no later than 24 hours after the institution experiences a major disruption that has the potential to have a material impact on the institution's risk profile, or affect its financial soundness. The APRA-regulated institution 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 APRA-regulated institution must notify APRA when normal operations resume.

37. 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.

Audit arrangements

38. An institution'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 institution's BCM policy and addresses the risks it is designed to control; and

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

39. APRA may request the external auditor of the institution, or another appropriate external expert, to provide an assessment of the institution's BCM arrangements. Any such report must be paid for by the institution and must be made available to APRA.[8]

Adjustments and exclusions

40. APRA may adjust or exclude a specific requirement in this Prudential Standard in relation to an APRA-regulated institution.[9]

---

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

8 Refer to *Prudential Standard 3PS 310 Audit and Related Matters*, *Prudential Standard APS 310 Audit and Related Matters*, *Prudential Standard GPS 310 Audit and Related Matters* and *Prudential Standard LPS 310 Audit and Related Matters*.

9 Refer to subsection 11AF(2) of the Banking Act, subsection 32(3D) of the Insurance Act and subsection 230A(4) of the Life Insurance Act.

Determinations made under previous prudential standards

41. An exercise of APRA's discretion (such as an approval, waiver or direction) under a previous version of this 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 this Prudential Standard' includes any versions of:

    (a) *Prudential Standard APS 232 Business Continuity Management* (including *Guidance Note AGN 232.1 Risk Assessment and Business Continuity Management*);

    (b) *Prudential Standard GPS 222 Business Continuity Management* (including *Guidance Note GGN 222.1 Risk Assessment and Business Continuity Management*);

    (c) *Prudential Standard LPS 232 Business Continuity Management*; and

    (d) *Prudential Standard GPS 221 Risk Management: Level 2 Insurance Groups* (GPS 221), to the extent that GPS 221 related to business continuity management.