Prudential Standard CPS 232

Business Continuity Management

Objective and key requirements of this Prudential Standard

The ultimate responsibility for the business continuity of an APRA-regulated entity (or of the members of a Level 2 group) rests with the Board of directors or equivalent.

This Prudential Standard aims to ensure that each APRA-regulated entity and Level 2 group implements a whole-of-business approach to business continuity management, appropriate to the nature and scale of its operations and to that of the group (where applicable). Business continuity management increases resilience to business disruption arising from internal and external events and may reduce the impact on the APRA-regulated entity's or group's business operations, reputation, profitability, depositors, policyholders and other stakeholders.

The key requirements of this Prudential Standard include that:

- an APRA-regulated entity must identify, assess and manage potential business continuity risks to ensure that it is able to meet its financial and service obligations to its depositors, policy-holders and other creditors;

- the Board of the APRA-regulated entity must consider business continuity risks and controls as part of its overall risk management systems and approve a Business Continuity Management Policy;

- an APRA-regulated entity must:

(a) develop and maintain a Business Continuity Plan that documents procedures and information which enable the APRA-regulated entity to manage business disruptions;

(b) allocate and maintain sufficient infrastructure, budgetary and other resources to implement the Business Continuity Plan;

(c) review the Business Continuity Plan annually and periodically arrange for its review by the internal audit function or an external expert; and

(d) notify APRA in the event of certain disruptions.

Where an APRA-regulated entity is the Head of a Level 2 group, it must also ensure that the Level 2 group has in place Business Continuity Management appropriate to the nature and scale of its operations and that the provisions of this Prudential Standard are applied appropriately throughout the Level 2 group.

Authority

1. Authority for the making of this Prudential Standard is as follows:

   (a) to the extent that this Prudential Standard operates in relation to authorised deposit-taking institutions (**ADIs**) and non-operating holding companies authorised under the *Banking Act 1959* (**Banking Act**) (**authorised banking NOHCs**), it is made under section 11AF of the Banking Act;

   (b) to the extent that this Prudential Standard operates in relation to general insurers and non-operating holding companies authorised under the *Insurance Act 1973* (**Insurance Act**) (**authorised insurance NOHCs**), it is made under section 32 of the Insurance Act; and

   (c) to the extent that this Prudential Standard operates in relation to life companies, including friendly societies, and non-operating holding companies registered under the *Life Insurance Act 1995* (**Life Insurance Act**) (**registered life NOHCs**), it is made under section 230A of the Life Insurance Act.

Application

2. This Prudential Standard applies to all **APRA-regulated entities** which, for the purposes of this Prudential Standard, means:

   (a) all ADIs, including foreign ADIs, and authorised banking NOHCs;

   (b) all general insurers, including Category C insurers, and authorised insurance NOHCs; and

   (c) all life companies, including friendly societies and eligible foreign life insurance companies (**EFLICs**), and registered life NOHCs.

3. Subject to paragraphs 40 and 41, APRA-regulated entities must comply with this Prudential Standard according to its terms.

4. For the purposes of this Prudential Standard, a requirement which is imposed upon an APRA regulated-entity which is also **Head of a Level 2 group**[1] is to be read as requiring that APRA regulated-entity to ensure that the applicable provision is applied appropriately throughout the **Level 2 group**.[2]

5. 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 business carried on in Australia by that foreign ADI, Category C insurer or EFLIC.

6. This Prudential Standard applies whether or not activities are outsourced to related bodies corporate or third-party service providers. This Prudential

---

1 Paragraph 10 defines Head of a Level 2 group.

2 Paragraph 9 defines Level 2 group.

Standard also applies to arrangements where the service provider is located outside Australia or the functions are performed outside Australia.

7. Nothing in this Prudential Standard prevents an APRA-regulated entity from adopting and applying a group policy that is also used by a related company, provided that the policy has been approved by the Board and meets the requirements of this Prudential Standard.

Interpretation

8. By operation of subsection 13(1) of the *Legislative Instruments Act 2003*, a term which is not defined in this Prudential Standard or, for general insurers and authorised insurance NOHCs, in *Prudential Standard GPS 001 Definitions* (**GPS 001**), but which is defined in one of the **Prudential Acts**[3] has the same meaning in this Prudential Standard as in the applicable Prudential Act when applied to an APRA-regulated entity authorised under that Act.

9. For the purposes of this Prudential Standard, a Level 2 group means:

   (a) in the case of the application of this Prudential Standard to ADIs and authorised banking NOHCs, a Level 2 group as referred to in *Prudential Standard APS 110 Capital Adequacy*; and

   (b) in the case of the application of this Prudential Standard to general insurers and authorised insurance NOHCs, a Level 2 insurance group as defined in GPS 001.

10. For the purposes of this Prudential Standard, Head of a Level 2 group means:

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

   (b) where an ADI that is a member of a Level 2 group is an immediate 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.

11. For the purposes of this Prudential Standard, a reference to the **Board** is to be read as**:**

   (a) in the case of a foreign ADI or a Category C insurer, a reference to the senior officer outside Australia with delegated authority from the Board (**senior officer outside Australia**) as referred to in *Prudential Standard CPS 510 Governance* (**CPS 510**); and

   (b) in the case of an EFLIC, a reference to the **Compliance Committee** with delegated authority from the Board as referred to in CPS 510; and

[3] Paragraph 12(a) defines Prudential Acts which is used in this Prudential Standard for ease of reference.

(c) in all other cases, a reference to the Board of directors.

12. For the purposes of this Prudential Standard:

(a) a reference to Prudential Acts is a reference to the Banking Act, the Insurance Act and the Life Insurance Act;

(b) a reference to a **Board member** or **member of a Board** is a reference to a director, the senior officer outside Australia or a member of the Compliance Committee, as the context requires;

(c) a reference to a **director** is a reference to a director of an APRA-regulated entity or of a related body corporate of the APRA-regulated entity;

(d) **related body corporate** has the meaning given in section 50 of the *Corporations Act 2001*;

(e) a reference to a **corporate group** is a reference to group comprising more than one company, where the companies are related bodies corporate;

(f) a reference to a **service provider** is a reference to the person providing the services to the APRA-regulated entity; and

(g) a reference to a **third party** is a reference to an entity that is not an APRA-regulated entity or a related body corporate of the APRA-regulated entity.

The role of the Board and senior management

13. An APRA-regulated entity must identify, assess, manage, mitigate and report on potential business continuity risks to ensure that it is able to meet its financial and service obligations to its depositors, policy-holders and other creditors.

14. The Board is ultimately responsible for the business continuity of the APRA-regulated entity. The Board remains responsible for Business Continuity Management (**BCM**) whether or not business operations are outsourced or are part of a corporate group.[4]

15. The Board may delegate day to day operational responsibility for the BCM to a responsible committee of the Head of the Level 2 group and/or senior management. The operational responsibility must be clearly expressed in the charter of the committee and/or in the performance objective of the responsible senior management.

16. The Board must approve the APRA-regulated entity's Business Continuity Management Policy (**BCM Policy**).

17. The Board must take into account the APRA-regulated entity's business continuity risks and controls as part of its overall risk management systems and

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

when completing a risk management declaration required to be provided to APRA.[5]

18. The Board must ensure that sufficient infrastructure, budgetary and other resources are allocated and maintained to enable the APRA-regulated entity to fulfil the objectives of the BCM Policy and to implement the Business Continuity Plan (**BCP**).

Business Continuity Management

19. 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.

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

21. An APRA-regulated entity's BCM must, at a minimum, include:

    (a) a BCM Policy;

    (b) a Business Impact Analysis (**BIA**) including risk assessment;

    (c) recovery objectives and strategies;

    (d) a BCP including crisis management and recovery; and

    (e) programs for:

        (i) review and testing of the BCP; and

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

22. In addition to the requirements stated elsewhere in this Prudential Standard, the Board of the Head of a Level 2 group must:

    (a) ensure that the Level 2 group's BCM is appropriate to the nature and scale of its operations and is consistent with the Level 2 group's risk management strategy or framework;

    (b) consistently apply BCM for each part of the Level 2 group;

    (c) apply BCM to risk assessments and risk processes at a functional level in the Level 2 group, where appropriate; and

---

[5] Refer to *Prudential Standard APS 310 Audit and Related Matters* (**APS 310**), *Prudential Standard GPS 220 Risk Management*, *Prudential Standard GPS 221 Risk Management: Level 2 Insurance Group* and *Prudential Standard LPS 220 Risk Management.*

(d) ensure that the Level 2 group's BCP is reviewed at least annually by responsible senior management of the Head of the Level 2 group.

Business Continuity Management Policy

23. An APRA-regulated entity must have an up-to-date documented BCM Policy that sets out its objectives and approach in relation to BCM.

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

Business Impact Analysis

25. BIA is the process of identifying and measuring (quantitatively and qualitatively) the business impact of the loss or disruption of critical business operations.

26. When conducting the BIA, the APRA-regulated entity must consider:

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

(b) the period of time for which the APRA-regulated entity 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 APRA-regulated entity; and

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

Recovery objectives and strategies

27. 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.

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

Business Continuity Plan

29. An APRA-regulated entity must maintain at all times a documented BCP which meets the objectives of the BCM Policy.[6]

[6] A reference to a BCP may be a reference to an individual BCP or to a collection of them. An APRA-regulated entity may have a number of BCPs. A BCP may include a separate crisis management plan and disaster recovery plan.

30. The BCP must document procedures and information which enable the APRA-regulated entity to:

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

    (b) recover critical business operations.

31. The BCP must reflect the specific requirements of the APRA-regulated entity 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 plan;

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

    (f) communication plans with staff and external stakeholders.

Review and testing of the BCP

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

33. The BCP must be updated if shortcomings are identified as a result of the review and testing required under paragraph 32.

Notification requirements

34. An APRA-regulated entity 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 its risk profile, or to affect the APRA-regulated entity's financial soundness. The APRA-regulated entity must explain to APRA the nature of the disruption, the action being taken, the likely effect and the timeframe for return to normal operations. The APRA-regulated entity must notify APRA when normal operations resume.

35. 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.

---

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

Audit arrangements

36. An APRA-regulated entity's internal audit function, or an 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 APRA-regulated entity's BCM Policy and addresses the risks it is designed to control; and

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

37. APRA may request the external auditor of the APRA-regulated entity, or an appropriate external expert, to provide an assessment of the APRA-regulated entity's BCM arrangements. Such reports must be paid for by the APRA-regulated entity and must be made available to APRA.[8]

Commencement and transitional arrangements

38. This Prudential Standard commences on [date] (**effective date**).

39. Upon commencement of this Prudential Standard, the existing requirements contained in *Prudential Standard APS 232 Business Continuity Management* (**APS 232**) (including *Guidance Note AGN 232.1 Risk Assessment and Business Continuity Management* (**AGN 232.1**)), *Prudential Standard GPS 222 Business Continuity Management* (**GPS 222**) (including *Guidance Note GGN 222.1 Risk Assessment and Business Continuity Management* (**GGN 222.1**)) and *Prudential Standard LPS 232 Business Continuity Management* (**LPS 232**) will cease to have effect.

Adjustments and exclusions

40. APRA may, by notice in writing to an APRA-regulated entity, adjust or exclude a specific prudential requirement in this Prudential Standard in relation to that regulated entity.[9]

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:

    (a) APS 232 (including AGN 232.1) made on 18 April 2005;

    (b) GPS 222 (including GGN 222.1) made on 18 April 2005;

---

8 Refer to APS 310, *Prudential Standard GPS 310 Audit and Actuarial Reporting and Valuation* 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.

(c) LPS 232 made on 23 March 2007.