Prudential Standard CPS 232

Business Continuity Management

Objective and key requirements of this Prudential Standard

This Prudential Standard requires each APRA-regulated institution ~~and Level 2 group~~ to implement a whole-of-business approach to business continuity management that is appropriate to the nature and scale of its and the group's operations. Business continuity management increases resilience to business disruption arising from internal and external events and may reduce the impact on the regulated institution's or group's business operations, reputation, profitability, depositors, policyholders and other stakeholders.

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

The key requirements of this Prudential Standard are that:

- an APRA-regulated institution 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, policyholders and other ~~creditors~~stakeholders;
- the Board of the regulated institution must consider business continuity risks and controls as part of its overall risk management systems and approve a Business Continuity Management Policy;
- a regulated institution must develop and maintain a ~~B~~business ~~C~~continuity ~~P~~plan that documents procedures and information which enable the regulated institution to manage business disruptions;
- a regulated institution must review the ~~B~~business ~~C~~continuity ~~P~~plan annually and periodically arrange for its review by the internal audit function or an appropriate external expert; and
- a regulated institution must notify APRA in the event of certain disruptions.

Where a regulated institution is the Head of a ~~Level 2~~ group, the group must have in place business continuity management appropriate to the nature and scale of its

operations, and the provisions of this Prudential Standard must be applied appropriately throughout the group.

Authority

1. This Prudential Standard is made under:

   (a) section 11AF of the *Banking Act 1959* (Banking Act) in relation to **authorised deposit-taking institutions** (**ADIs**) and **non-operating holding companies** authorised under the Banking Act (authorised banking NOHCs);

   (b) section 32 of the *Insurance Act 1973* (Insurance Act) in relation to **general insurers** and **non-operating holding companies** authorised under the Insurance Act (authorised insurance NOHCs) and **parent entities** of **Level 2 insurance groups**; and

   (c) section 230A of the *Life Insurance Act 1995* (Life Insurance Act) in relation to **life companies**, including **friendly societies**, and **non-operating holding companies** registered under the Life Insurance Act (registered life NOHCs).

Application

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

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

   (b) ~~all~~ general insurers, including **Category C insurers**, and 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 registered life NOHCs~~.~~; and

   (d) Heads of groups.[1]

   ~~These institutions are collectively referred to as 'regulated institutions' in this Prudential Standard.~~

~~3. A requirement imposed upon a regulated institution that is also Head of a Level 2 group[2] is to be read as requiring that regulated institution to ensure that the applicable provision is applied appropriately throughout the Level 2 group.[3]~~

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 business** of that institution.

---

[1] For the purposes of this Prudential Standard, a reference to a 'Head of a group' is a reference to a Level 2 Head and a Level 3 Head.

~~[2] Paragraph 10 defines Head of a Level 2 group.~~

~~[3] Paragraph 9 defines Level 2 group.~~

4. A requirement that is expressed as applying to a Head of a group is to be read as requiring the Head of a group to ensure that the requirement is applied appropriately throughout the group.[4]

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**[5], provided that the policy has been approved by the **Board**[6] of the regulated institution and meets the requirements of this Prudential Standard.

7. This Prudential Standard commences on 1 January ~~2013~~2014.

Interpretation

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

9. For the purposes of this Prudential Standard, a reference to a 'group' is a reference to a Level 2 group and a Level 3 group.

~~9.~~10. A 'Level 2 group' is:

(a) the consolidation of entities defined as **Level 2** in APS 001; or

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

11. A 'Level 3 group' comprises all institutions that are part of a consolidated entity, adjusted to include or exclude institutions as determined by APRA by notice in writing to the Level 3 Head, of which the Level 3 Head is:

(a) the **ultimate holding company**;

(b) the **ultimate Australian parent**; or

(c) a reporting entity as defined in *Statement of Accounting Concepts SAC1 Definition of the Reporting Entity* that is required to prepare consolidated financial reports in accordance with Part 2M.3 of the Corporations Act 2001 (Corporations Act) and the relevant Australian Accounting Standards.

---

[4] 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 Head of the Level 3 group.

[5] Related body corporate has the meaning given in section 50 of the Corporations Act ~~*2001*~~.

[6] A reference to the Board, in the case of a foreign ADI, Category C insurer or an EFLIC, is a reference to the **senior officer outside Australia** or Compliance Committee (as applicable) as referred to in *Prudential Standard CPS 510 Governance*.

~~10.~~12. A '~~Head of a~~ Level 2 ~~group~~'Head' is:

(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.

13. A 'Level 3 Head' is:

(a) an ADI or authorised NOHC under the Banking Act;

(b) a general insurer or authorised NOHC under the Insurance Act; or

(c) a life company or registered NOHC under the Life Insurance Act,

in respect of which APRA has made a determination under paragraph 3 of 3PS 001.

Requirements of the Head of a group

14. The Head of a group must develop and maintain a business continuity management policy for the group.

15. Where a member of a 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 requirements of this Prudential Standard.

The role of the Board and senior management

~~11.~~16. An APRA-regulated institution 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, policyholders and other ~~creditors~~stakeholders.

~~12.~~17. The Board is ultimately responsible for the business continuity of the APRA-regulated institution. The Board remains responsible for business continuity management (BCM) whether or not business operations are outsourced or are part of a **corporate group**.[7]

~~13.~~18. The Board may delegate day-to-day operational responsibility for BCM to a responsible committee, including 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 objectives of the responsible senior management.

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

~~14. The Board must approve the regulated institution's Business Continuity Management Policy (BCM Policy) (refer to paragraphs 25 and 26).~~

~~15.~~19. The Board must ensure that the APRA-regulated institution's business continuity risks and controls are taken into account as part of its overall risk management systems and when completing a **risk management declaration** required to be provided to APRA.[8]

Business continuity management

~~16.~~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.

~~17.~~21. Critical business operations are the business functions, resources and infrastructure that may, if disrupted, have a material impact on the APRA-regulated institution's or group's business functions, reputation, profitability, depositors and/or policyholders.

~~18.~~22. An APRA-regulated institution's BCM must, at a minimum, include:

(a) a BCM Policy in accordance with paragraphs 24 and 26;

(b) a business impact analysis (BIA) including risk assessment in accordance with paragraphs 27 and 28;

(c) recovery objectives and strategies~~;~~ in accordance with paragraphs 29 and 30;

(d) a business continuity plan (BCP) including crisis management and recovery in accordance with paragraphs 31 to 34~~ 33~~; and

(e) programs for:

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

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

~~19.~~23. 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;

---

[8] Refer to *Prudential Standard CPS 220 Risk Management*. ~~*Prudential Standard APS 310 Audit and Related Matters* (APS 310), *Prudential Standard GPS 220 Risk Management* and *Prudential Standard LPS 220 Risk Management*~~.

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

(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.

~~BCM~~ Business Continuity Management Policy

24. The Board must approve the APRA-regulated institution's Business Continuity Management Policy (BCM Policy).

~~20.~~25. An APRA-regulated institution must have an up-to-date and documented BCM Policy that sets out its objectives and approach in relation to BCM.

~~21.~~26. The BCM Policy must clearly state the roles, responsibilities and authorities to act in relation to the BCM Policy.

Business impact analysis

~~22.~~27. A BIA involves identifying all critical business functions, resources and infrastructure of the APRA-regulated institution or group and assessing the impact of a disruption on these.

~~23.~~28. 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 regulated institution or group 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 regulated institution or group; and

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

Recovery objectives and strategies

~~24.~~29. 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.

~~25.~~30. 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 regulated institution or group.

Business continuity planning

~~26.~~31. An APRA-regulated institution must maintain at all times a documented BCP that meets the objectives of the BCM Policy.[9]

~~27.~~32. The BCP must document procedures and information that enable the APRA-regulated institution to:

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

(b) recover critical business operations.

~~28.~~33. The BCP must reflect the specific requirements of the APRA-regulated institution or group 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.

~~29.~~34. 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.

Review and testing of the BCP

~~30.~~35. An APRA-regulated institution 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.[10]

~~31.~~36. The BCP must be updated if shortcomings are identified as a result of the review and testing required under paragraph 35.

Notification requirements

~~32.~~37. An APRA-regulated institution 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 regulated institution's risk profile, or affect its financial soundness. The regulated institution must explain to APRA the nature

---

[9] A reference to a 'BCP' ~~may be~~ includes a reference to ~~an individual BCP or to a collection of them~~ more than one BCP where appropriate. An APRA-regulated entity may have a number of BCPs. A BCP may include a separate crisis management plan and disaster recovery plan.

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

of the disruption, the action being taken, the likely effect and the timeframe for returning to normal operations. The regulated institution must notify APRA when normal operations resume.

~~33.~~38. 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 in writing and publishes on its website from time to time.[11]

Audit arrangements

~~34.~~39. An APRA-regulated institution's internal audit function, or an appropriate external expert, must periodically review the BCP and provide an assurance to the regulated institution's Board or to delegated management that:

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

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

~~35.~~40. APRA may, in writing, request the external auditor of the APRA-regulated institution, or another appropriate external expert, to provide an assessment of the regulated institution's BCM arrangements. Any such report must be paid for by the regulated institution and must be made available to APRA.[12]

Adjustments and exclusions

~~36.~~41. APRA may, by notice in writing to an APRA-regulated institution, adjust or exclude a specific prudential requirement in this Prudential Standard in relation to that regulated institution.[13]

Determinations made under previous prudential standards

~~37.~~42. 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) *Prudential Standard APS 232 Business Continuity Management* (including *Guidance Note* AGN 232.1 *Risk Assessment and Business Continuity Management*) made on 18 April 2005;

---

11 Where this Prudential Standard provides for APRA to require an APRA-regulated institution to make other arrangements, or otherwise exercise a power or discretion, the power or discretion is to be exercised in writing.

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

13 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.

(b) *Prudential Standard GPS 222 Business Continuity Management* (including *Guidance Note* GGN 222.1 *Risk Assessment and Business Continuity Management*) made on 18 April 2005;

(c) *Prudential Standard LPS 232 Business Continuity Management* made on 23 March 2007;

(d) *Prudential Standard GPS 221 Risk Management: Level 2 Insurance Groups* (GPS 221) made on 17 December 2008, to the extent that GPS 221 related to business continuity management; ~~and~~

(e) *Prudential Standard CPS 232 Business Continuity Management* made on 9 September 2011~~.~~; and

(f) *Prudential Standard CPS 231 Business Continuity Management* made on 30 November 2012.