Note for consultation:
Yellow highlights changes made in the August 2014 version which have been through public consultation.
Blue highlights clarifications with respect to Board requirements.

Prudential Standard CPS 232

Business Continuity Management

Objective and key requirements of this Prudential Standard

This Prudential Standard requires each APRA-regulated institution and Head of a group ~~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~~the 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 Board of an APRA regulated institution and the Board of a Head of a group, respectively, have~~The~~ ultimate responsibility for the business continuity of the institution or group. ~~an APRA-regulated institution (or of the members of a Level 2 group) rests with its the Board of the APRA-regulated institution or Board of the Head of the group, as relevant of directors (or equivalent).~~

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;
- ~~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~~ framework~~and approve a Business Continuity Management Policy~~;
- ~~a regulated institution must~~ maintain a b~~B~~usiness c~~C~~ontinuity p~~P~~lan that documents procedures and information which enable the ~~regulated~~ institution to manage business disruptions;
- ~~a regulated institution must~~ review the b~~B~~usiness c~~C~~ontinuity p~~P~~lan 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 an APRA-regulated institution is the Head of a ~~Level 2~~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 ~~must be~~ 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**) ~~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'[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**, ~~and~~ 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). ~~Heads of groups.~~[2]

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

   ~~(e)~~(c) ~~A requirement imposed upon a regulated institution that is also Head of a Level 2 group[3] is to be read as requiring that regulated institution to ensure that applicable provision is applied appropriately throughout the Level 2 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 For the purposes of this Prudential Standard, a reference to a 'Head of a group' is a reference to a Level 2 Head or a **Level 3 Head**, as relevant.~~

~~3 Paragraph 10 defines Head of a Level 2 group.~~

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**~~ Australian branch operations of that institution.

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.~~Where an APRA-regulated institution is the 'Head of a group'[4], 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'.

~~3.~~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.

~~4.~~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**[5] of the regulated institution and meets the requirements of this Prudential Standard.

~~5.~~7. This Prudential Standard commences on ~~1 January 2015~~1 July 2017.

Interpretation

~~6.~~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.

---

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 Level 3 Head.

5 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*~~.

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

~~For the purposes of this Prudential Standard:, a reference to a~~

10.

'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;

~~A~~ 'Level 2 group' ~~is~~means the entities that comprise:

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

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

~~(c)~~(b)

~~The 'Head of a Level 2 group'~~ 'Level 2 Head' ~~is~~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 r~~R~~equirements of the Head of a group

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

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 ~~business continuity management (~~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**;

~~oversee the appropriateness of BCM across the group;~~

(b) ~~apply BCM to risk assessments and risk processes at a functional level in the group, where appropriate~~; 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 ~~**non-APRA-regulated institution** within the group~~ 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 ~~business continuity management~~ BCM policy.

The role of the Board and senior management

~~7.~~17. An APRA-regulated institution must identify, assess, manage, mitigate and report on potential business continuity risks to ensure that ~~it~~ the institution is able to meet its financial and service obligations to its depositors, **policyholders** and other ~~creditors~~stakeholders.

~~8.~~18. The Board is ultimately responsible for the business continuity of the ~~APRA-regulated~~ institution. The Board remains ultimately responsible for ~~business continuity management (~~BCM~~)~~ of the institution whether or not business operations are outsourced or are part of a **corporate group**.[6]

~~9. The Board may delegate day-to-day operational responsibility for BCM of the institution 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 objective of the responsible senior management.~~

~~10.~~

~~11. The Board must approve the regulated institution's Business Continuity Management Policy (BCM Policy).~~

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

~~12.~~19. The Board must ensure that the ~~APRA-regulated institution's~~ business continuity risks and controls are taken into account as part of ~~its~~ the institution's ~~overall~~ **risk management strategy** and when completing a **risk management declaration** required to be provided to APRA.[7]

Business continuity management

~~13.~~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.

~~14.~~21. Critical business operations are the business functions, resources and infrastructure that may, if disrupted, have a material impact on the ~~regulated~~ institution's business functions, reputation, profitability, depositors and/or policyholders.

~~15.~~22. ~~A regulated institution's~~ BCM must, at a minimum, include:

(a) a BCM policy in accordance with paragraphs 23 ~~and~~ 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 ~~business continuity plan (~~BCP~~)~~ ~~including crisis management and recovery~~ in accordance with paragraphs 30 to 33; and

(e) programs for:

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

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

~~(iii) In addition to the requirements stated elsewhere in this Prudential Standard, the Board of the Head of a Level 2 group must:~~

~~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;~~

~~consistently apply BCM for each part of the Level 2 group;~~

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

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

~~(iv)~~(ii) ~~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 ~~C~~continuity ~~M~~management ~~Policy~~policy

23. The Board must approve the institution's ~~Business Continuity Management Policy (~~BCM ~~P~~policy~~).~~

~~16.~~24. ~~A regulated institution~~The BCM policy must ~~have an~~be up-to-date, documented ~~BCM Policy that~~and must set~~s~~ out the~~its~~ objectives and approach in relation to BCM.

~~17.~~25. The BCM ~~Policy~~ policy must clearly state the roles, responsibilities and authorities to act in relation to the BCM ~~Policy~~policy.

Business impact analysis

~~18.~~26. A BIA involves identifying all critical business functions, resources and infrastructure of the ~~regulated~~ institution and assessing the impact of a disruption on these.

~~19.~~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 ~~regulated~~ 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 ~~regulated~~ institution; and

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

Recovery objectives and strategies

~~20.~~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.

~~21.~~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 ~~regulated~~ institution.

Business continuity planning

~~22.~~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 p~~P~~olicy.[8]

~~23.~~31. The BCP must document procedures and information that enable the ~~regulated~~ institution to:

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

(b) recover critical business operations.

~~24.~~32. The BCP must reflect the specific requirements of the ~~regulated~~ 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.

Review and testing of the BCP

~~25.~~34. An ~~APRA-~~regulated institution must review and test ~~its~~ 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.[9]

~~26.~~35. The BCP must be updated if shortcomings are identified as a result of the review and testing required under paragraph 34.

Notification requirements

~~27.~~36. An ~~APRA-~~regulated institution must notify APRA as soon as possible and no later than 24 hours after the institution ~~experiencing~~ experiences a major disruption that has the potential to have a material impact on the ~~regulated~~

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

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

institution's risk profile, or affect its financial soundness. The APRA-regulated ~~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 ~~regulated~~ institution must notify APRA when normal operations resume.

~~28.~~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

~~29.~~38. An ~~regulated~~ institution's internal audit function, or an appropriate external expert, must periodically review the BCP and provide an assurance to the ~~institution's~~ Board or to delegated management that:

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

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

~~30.~~39. APRA may request the external auditor of the ~~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.[10]

Adjustments and exclusions

~~31.~~40. APRA may ~~, by notice in writing to a regulated institution,~~ adjust or exclude a specific ~~prudential~~ requirement in this Prudential Standard in relation to ~~that~~ an APRA-regulated institution.[11]

Determinations made under previous prudential standards

~~32.~~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*) ~~made on 18 April 2005~~;

10 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*.

11 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~~; and

(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.~~;~~

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

~~*Prudential Standard CPS 232 Business Continuity Management* made on 30 November 2012.~~