Prudential Standard CPS 231

Outsourcing

Objective and key requirements of this Prudential Standard

This Prudential Standard requires that all outsourcing arrangements involving material business activities entered into by an APRA-regulated institution be subject to appropriate due diligence, approval and ongoing monitoring. All risks arising from outsourcing material business activities must be appropriately managed to ensure that the regulated institution is able to meet its financial and service obligations to its depositors and/or policyholders.

The ultimate responsibility for the outsourcing policy 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 a regulated institution must:

- have a policy, approved by the Board, relating to outsourcing of material business activities;
- have sufficient monitoring processes in place to manage the outsourcing of material business activities;
- for all outsourcing of material business activities with third parties, have a legally binding agreement in place, unless otherwise agreed by APRA;
- consult with APRA prior to entering into agreements to outsource material business activities to service providers that conduct their activities outside Australia; and
- notify APRA after entering into agreements to outsource material business activities.

Where a regulated institution is the Head of a Level 2 group, this Prudential Standard requires that any outsourcing arrangements involving material business activities entered into by members of the group must be subject to appropriate due diligence, approval and on-going monitoring, and the provisions of this Prudential Standard must be are 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:

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

   (b) all general insurers, including **Category C insurers**, 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.

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

3. A requirement imposed upon a regulated institution that is also the Head of a Level 2 group[1] is to be read as requiring that regulated institution to ensure that the requirement is applied appropriately throughout the Level 2 group.[2]

4. All 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.

5. Nothing in this Prudential Standard prevents a regulated institution from adopting and applying a group policy used by a **related body corporate**[3],

---

1 Paragraph 9 defines Head of a Level 2 group.
2 Paragraph 8 defines Level 2 group.
3 Related body corporate has the meaning given in section 50 of the *Corporations Act 2001*.

provided that the policy has been approved by the **Board**[4] and meets the requirements of this Prudential Standard.

6. This Prudential Standard commences on 1 January ~~2013~~2015.

Interpretation

7. Terms that are defined in *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.

8. A 'Level 2 group' is:

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

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

9. The 'Head of a Level 2 group' 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.

10. 'Outsourcing' involves a regulated institution entering into an arrangement with another party (including a related body corporate) to perform, on a continuing basis, a business activity that currently is, or could be, undertaken by the regulated institution itself.

11. For the purposes of this Prudential Standard, 'offshoring' means the outsourcing by a regulated institution of a material business activity associated with its Australian business to a service provider[5] (including a related body corporate) where the outsourced activity is to be conducted outside Australia. Offshoring includes arrangements where the service provider is incorporated in Australia, but the physical location of the outsourced activity is outside Australia. Offshoring does not include arrangements where the physical location of an outsourced activity is within Australia but the service provider is not incorporated in Australia.

12. The **international business** of a Level 2 group does not constitute offshoring as defined in paragraph 11; therefore, the requirements of this Prudential Standard relating to offshoring do not apply to the international business of a Level 2 group. However, the Board of the Head of a Level 2 group must comply with

---

[4] 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* (CPS 510).

[5] Service provider is a reference to the institution providing the outsourced services to the regulated institution.

any requirement relating to offshoring in respect of any other activity falling within the meaning of offshoring under this Prudential Standard.

Materiality

13. This Prudential Standard only applies to the outsourcing of a material business activity as defined in this Prudential Standard.

14. A 'material business activity' is one that has the potential, if disrupted, to have a significant impact on the regulated institution's business operations or its ability to manage risks effectively, having regard to such factors as:

    (a) the financial and operational impact and impact on reputation of a failure of the service provider to perform over a given period of time;

    (b) the cost of the outsourcing arrangement as a share of total costs;

    (c) the degree of difficulty, including the time taken, in finding an alternative service provider or bringing the business activity in-house;

    (d) the ability of the regulated institution to meet regulatory requirements if there are problems with the service provider;

    (e) potential losses to the regulated institution's customers and other affected parties in the event of a service provider failure; and

    (f) affiliation or other relationship between the regulated institution and the service provider.

15. For the purposes of this Prudential Standard, the internal audit function is a material business activity.

The role of the Board and senior management

16. A regulated institution must identify, assess, manage, mitigate and report on risks associated with outsourcing to ensure that it can meet its financial and service obligations to its depositors, policyholders and other stakeholders.

17. A regulated institution must have procedures to ensure that all its relevant business units are made aware of, and have processes and control for monitoring compliance with, the outsourcing policy.

18. The Board is ultimately responsible for any outsourcing of a material business activity undertaken by a regulated institution. Although outsourcing may result in the service provider having day-to-day managerial responsibility for a business activity, the regulated institution is responsible for complying with all **prudential requirements** that relate to the outsourced business activity.

Outsourcing policy

19. The Board must approve the regulated institution's outsourcing policy, which must set out its approach to outsourcing of material business activities,

including a detailed framework for managing all such outsourcing arrangements.

20. The Board of the Head of a Level 2 group must have an outsourcing policy that includes a strategy for the outsourcing of material business activities for both Australian and international businesses of the Level 2 group.

21. The Board must ensure that the regulated institution's outsourcing risks and controls are taken into account as part of its overall **risk management strategy** ~~systems~~ and when completing a **risk management declaration** required to be provided to APRA.[6]

22. A regulated institution's outsourcing policy must set out specific requirements in relation to outsourcing to related bodies corporate and outsourcing to service providers conducting the material business activity outside Australia.

Assessment of outsourcing options

23. A regulated institution must be able to demonstrate to APRA that, in assessing the options for outsourcing a material business activity to a 'third-party'[7], it has:

    (a) prepared a business case for outsourcing the material business activity;

    (b) undertaken a tender or other selection process for service providers;

    (c) undertaken a due diligence review of the chosen service provider;

    (d) involved the Board, Board committee, or **senior manager** with delegated authority from the Board, in approving the agreement;

    (e) considered all the matters outlined in paragraph 26, that must, at a minimum, be included in the outsourcing agreement itself;

    (f) established procedures for monitoring performance under the outsourcing agreement on a continuing basis;

    (g) addressed the renewal process for outsourcing agreements and how the renewal will be conducted; and

    (h) developed contingency plans that would enable the outsourced business activity to be provided by an alternative service provider or brought in-house if required.

---

6 For details of the **risk management framework** for regulated institutions refer to *Prudential Standard CPS 220 Risk Management*. ~~for general insurers, refer to *Prudential Standard GPS 220 Risk Management*. For details of the risk management framework for life companies, refer to *Prudential Standard LPS 220 Risk Management*. While ADIs are not, at present, subject to formal prudential requirements with regard to their risk management framework, APRA expects that an ADI's risk management framework will cover the risks associated with outsourcing a material business activity; refer to *Prudential Standard APS 310 Audit and Related Matters*.~~

7 Third party is a reference to an institution that is not the regulated institution or a related body corporate of the regulated institution.

24. A regulated institution must be able to demonstrate to APRA that, in assessing the options for outsourcing to related bodies corporate, it has taken into account:

    (a) the changes to the risk profile of the business activity that arise from outsourcing the activity to a related body corporate and how this changed risk profile is addressed within the regulated institution's **risk management framework**;

    (b) that the related body corporate has the ability to conduct the business activity on an ongoing basis;

    (c) the required monitoring procedures to ensure that the related body corporate is performing effectively and how potential inadequate performance would be addressed;

    (d) contingency issues in accordance with *Prudential Standard CPS 232 Business Continuity Management* (CPS 232) should the outsourced activity need to be brought in-house; and

    (e) the need to apply any of the requirements set out in paragraph 23 to the extent they are relevant to outsourcing agreements with related bodies corporate.

The outsourcing agreement

25. Except where otherwise provided in this Prudential Standard, all outsourcing arrangements must be contained in a documented legally binding agreement. The agreement must be signed by all parties to it before the outsourcing arrangement commences.

26. At a minimum, the agreement (including arrangements with related bodies corporate) must address the following matters:

    (a) the scope of the arrangement and services to be supplied;

    (b) commencement and end dates;

    (c) review provisions;

    (d) pricing and fee structure;

    (e) service levels and performance requirements;

    (f) audit and monitoring procedures;

    (g) business continuity management;

    (h) confidentiality, privacy and security of information;

    (i) default arrangements and termination provisions;

    (j) dispute resolution arrangements;

(k) liability and indemnity;

(l) sub-contracting;

(m) insurance; and

(n) to the extent applicable, offshoring arrangements (including through sub-contracting).

27. A regulated institution that outsources a material business activity must ensure that its outsourcing agreement includes an indemnity to the effect that any sub-contracting by a third-party service provider of the outsourced function will be the responsibility of the third-party service provider, including liability for any failure on the part of the sub-contractor.

28. The requirements in paragraph 25 do not apply to an outsourcing arrangement with a related body corporate unless:

(a) after having consulted with the regulated institution, APRA notifies the regulated institution, in writing, that the outsourcing arrangement must be evidenced by a documented legally binding agreement;

(b) another prudential standard requires the arrangement to be undertaken under a documented legally binding agreement; or

(c) in the case of a **general insurer**, the outsourcing arrangement is between a **Category D insurer**[8] and a related body corporate.

29. Where a foreign ADI, Category C insurer or EFLIC enters into an outsourcing arrangement with its head office, the requirements of subparagraph 24(d) and 25 do not apply.

30. Where a regulated institution enters into an outsourcing agreement as a result of an unexpected extreme event that results in:

(a) the regulated institution invoking its Business Continuity Plan[9]; or

(b) the sudden financial or operational failure of an existing service provider,

then paragraphs 23 to 28 inclusive, 34 and 35 need be complied with only to the extent that is reasonably possible having regard to the nature of the extreme event. The regulated institution must notify APRA as soon as practicable of any such outsourcing arrangement.

APRA access to service providers

31. An outsourcing agreement must include a clause that allows APRA access to documentation and information related to the outsourcing arrangement. In the normal course, APRA will seek to obtain whatever information it requires from

[8] Refer to GPS 001.
[9] Refer to CPS 232.

the regulated institution; however, the outsourcing agreement must include the right for APRA to conduct on-site visits to the service provider if APRA considers this necessary in its role as prudential supervisor. APRA expects service providers to cooperate with APRA's requests for information and assistance. If APRA intends to undertake an on-site visit to a service provider, it will normally inform the regulated institution of its intention to do so.

32. Where a regulated institution enters into an outsourcing arrangement with a related body corporate, the Board of the regulated institution must ensure that access by APRA to the related body corporate is not impeded.

33. The regulated institution must take all reasonable steps to ensure that a service provider will not disclose or advertise that APRA has conducted an on-site visit, except as necessary to coordinate with other institutions regulated by APRA that are existing clients of the service provider.

Notification requirement

34. A regulated institution must notify APRA as soon as possible after entering into an outsourcing agreement, and in any event no later than 20 **business days** after execution of the outsourcing agreement. This notification requirement applies to all outsourcing of material business activities.

35. When a regulated institution notifies APRA of a new outsourcing agreement, it must also provide a summary to APRA of the key risks involved in the outsourcing arrangement and the risk mitigation strategies put in place to address these risks. APRA may request additional material where it considers it necessary in order to assess the impact of the outsourcing arrangement on the regulated institution's risk profile.

Offshoring arrangements – requirement for consultation

36. A regulated institution must consult with APRA prior to entering into any offshoring agreement involving a material business activity so that APRA may satisfy itself that the impact of the offshoring arrangement has been adequately addressed as part of the regulated institution's risk management framework.

37. If, in APRA's view, the offshoring agreement involves risks that the regulated institution is not managing appropriately, APRA may require the regulated institution to make other arrangements for the outsourced activity as soon as practicable.

Monitoring the relationship

38. A regulated institution must ensure it has sufficient and appropriate resources to manage and monitor the outsourcing relationship at all times. The type and extent of resources required will depend on the materiality of the outsourced business activity. At a minimum, monitoring must include:

    (a) maintaining appropriate levels of regular contact with the service provider. This will range from daily operational contact to senior management involvement; and

(b) a process for regular monitoring of performance under the agreement, including meeting criteria concerning service levels.

39. A regulated institution must advise APRA of any significant problems that have the potential materially to affect the outsourcing arrangement and, as a consequence, materially affect the business operations, profitability or reputation of the regulated institution.

40. Where an outsourcing agreement is terminated, a regulated institution must notify APRA as soon as practicable and provide a statement about the transition arrangements and future strategies for carrying out the outsourced material business activity.

Audit arrangements

41. A regulated institution's internal audit function must review any proposed outsourcing of a material business activity and regularly review and report to the Board or Board Audit Committee on compliance with the regulated institution's outsourcing policy. Where APRA has exempted a regulated institution from having a dedicated internal audit function, or approved alternative arrangements under CPS 510, APRA may also vary the requirements of this paragraph.

42. APRA may request the external auditor of a regulated institution, or an appropriate external expert, to provide an assessment of the risk management processes in place with respect to an arrangement to outsource a material business activity. This could cover areas such as information technology systems, data security, internal control frameworks and business continuity plans. Such reports will be paid for by the regulated institution and must be made available to APRA.

Adjustments and exclusions

43. 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 regulated institution.[10]

Determinations made under previous prudential standards

44. 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 231 Outsourcing* made on 29 September 2006, as amended;

[10] 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 231 Outsourcing* made on 23 June 2008;

(c) *Prudential Standard LPS 231 Outsourcing* made on 29 September 2006, as amended;

(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 outsourcing; and

(e) *Prudential Standard CPS 231 Outsourcing* made on 9 September 2011.