Prudential Standard CPS 231

Outsourcing

Objectives 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 and a Head of a group 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 APRA-regulated institution, or the group it heads, is able to meet its financial and service obligations to its depositors and/or policyholders.

The Board of an APRA-regulated institution and the Board of a Head of a group, respectively, have ultimate responsibility for the outsourcing policy 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 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 an APRA-regulated institution is the Head of a 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 ongoing monitoring, 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 20 to 46 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 231 Outsourcing* (SPS 231) for requirements relating to the outsourcing arrangements of 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. Nothing in this Prudential Standard prevents an APRA-regulated institution from adopting and applying a group policy used by a **related body corporate**,[3] 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 July 2017.

Interpretation

7. 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.

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

9. 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.

10. 'Outsourcing' involves an APRA-regulated institution, or an institution within a group that is not an APRA-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 institution itself.

11. For the purposes of this Prudential Standard, 'offshoring' means the outsourcing by an APRA-regulated institution of a material business activity associated with

---

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

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

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. Where the **international business** of a group outsources activities to a service provider in its local jurisdiction, this does not constitute offshoring as defined in paragraph 11.

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 APRA-regulated institution's or group'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 APRA-regulated institution or member of the group to meet regulatory requirements if there are problems with the service provider;

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

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

15. For the purposes of this Prudential Standard, the internal audit function and the risk management function are material business activities.

Additional requirements of the Head of a group

16. The Head of a group must maintain a group outsourcing policy that meets the requirements of paragraphs 23 to 25 on a group basis. The group outsourcing

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

policy must include a strategy for the outsourcing of material business activities that applies to all members of the group.

17. The Head of a group must, except where an APRA-regulated institution within the group has otherwise notified APRA of that information:

    (a) notify APRA in accordance with paragraphs 37 to 38 in respect of each outsourcing agreement for a material business activity across the group;

    (b) consult with APRA in accordance with paragraphs 39 to 40 in respect of each offshoring agreement for a material business activity across the group;

    (c) advise APRA of any significant problems that have the potential to materially affect the outsourcing arrangement and, as a consequence, materially affect the business operations, profitability or reputation of the group; and

    (d) notify APRA in accordance with paragraph 43 where an outsourcing agreement for a material business activity across the group is terminated.

18. The group internal audit function must review any proposed outsourcing of a material business activity of the group, except where the internal audit function of an APRA-regulated institution within the group has reviewed the proposed outsourcing. The group internal audit function must regularly review and report to the Board of the Head of the group or group Board Audit Committee on compliance with the group outsourcing policy.

19. Where an institution within the group that is not an APRA-regulated institution outsources business activities that are material to the group, the Head of the group must ensure that the outsourcing of those business activities is undertaken in a way that complies with the group outsourcing policy.[6]

The role of the Board and senior management

20. An APRA-regulated institution must identify, assess, manage, mitigate and report on risks associated with outsourcing to meet the institution's financial and service obligations to its depositors, **policyholders** and other stakeholders.

21. An APRA-regulated institution must have procedures to ensure that all the institution's relevant business units are made aware of, and have processes and controls for monitoring compliance with, the outsourcing policy.

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

---

6 This paragraph does not override any requirements applying to an RSE licensee in SPS 231.

Outsourcing policy

23. The Board of an APRA-regulated institution must approve the institution's outsourcing policy, which must set out the approach to outsourcing of material business activities, including a detailed framework for managing all such outsourcing arrangements.

24. The Board of an APRA-regulated institution must **ensure** that outsourcing 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.[7]

25. The 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

26. An APRA-regulated institution must be able to demonstrate to APRA that, in assessing the options for outsourcing a material business activity to a 'third party',[8] it has:

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

    (b) undertaken a tender or other selection process for selecting the service provider;

    (c) undertaken a due diligence review of the chosen service provider, including the ability of the service provider to conduct the business activity on an ongoing basis;

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

    (e) considered all the matters outlined in paragraph 29, 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.

---

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

8 For the purposes of this Prudential Standard, 'third party' is a reference to an institution that is not the APRA-regulated institution or a related body corporate of the APRA-regulated institution.

27. An APRA-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 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 26 to the extent they are relevant to outsourcing agreements with related bodies corporate.

The outsourcing agreement

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

29. 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) the form in which data is to be kept and clear provisions identifying ownership and control of data;

    (g) reporting requirements, including content and frequency of reporting;

    (h) audit and monitoring procedures;

    (i) business continuity management;

(j) confidentiality, privacy and security of information;

(k) default arrangements and termination provisions;

(l) dispute resolution arrangements;

(m) liability and indemnity;

(n) sub-contracting;

(o) insurance; and

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

30. An APRA-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.

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

(a) after having consulted with the APRA-regulated institution, APRA notifies the APRA-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**[9] and a related body corporate.

32. Where a foreign ADI, Category C insurer or EFLIC enters into an outsourcing arrangement with its head office, the requirements of subparagraph 27(d) and paragraph 28 do not apply.

[9] Refer to GPS 001.

33. Where:

    (a) an APRA-regulated institution invokes the institution's Business Continuity Plan[10] as a result of an unexpected event; or

    (b) there is a sudden financial or operational failure of an existing service provider,

    and, as a result, enters into a new outsourcing agreement, the APRA-regulated institution must comply with paragraphs 26 to 31 inclusive, 37, 38, and 39 only to the extent that is reasonably possible having regard to the nature of the extreme event or sudden failure. The APRA-regulated institution must notify APRA as soon as practicable of any such outsourcing arrangement.

APRA access to service providers

34. 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 the APRA-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 APRA-regulated institution of its intention to do so.

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

36. An APRA-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

37. An APRA-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.

38. When an APRA-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 institution's risk profile.

---

[10] Refer to CPS 232.

Offshoring arrangements – requirement for consultation

39. An APRA-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 institution's risk management framework.

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

Monitoring the relationship

41. An APRA-regulated institution must ensure the institution has sufficient and appropriate resources to manage and monitor each 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.

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

43. Where an outsourcing agreement is terminated, an APRA-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

44. An 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 institution's outsourcing policy. Where APRA has exempted an institution from having a dedicated internal audit function, or approved alternative arrangements under *Prudential Standard CPS 510 Governance,* APRA may also vary the requirements of this paragraph.

45. APRA may request the external auditor of an 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 institution and must be made available to APRA.

Adjustments and exclusions

46. APRA may adjust or exclude a specific prudential requirement in this Prudential Standard in relation to an APRA-regulated institution.[11]

Determinations made under previous prudential standards

47. 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 231 Outsourcing*;

    (b) *Prudential Standard GPS 231 Outsourcing*;

    (c) *Prudential Standard LPS 231 Outsourcing*; and

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

[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.