



Prudential Standard CPS 231

Outsourcing

Objective and key requirements of this Prudential Standard

The ultimate responsibility for the outsourcing policy 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 all outsourcing arrangements involving material business activities entered into by an APRA-regulated entity are 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 entity is able to meet both its financial and service obligations to its depositors and/or policyholders.

The key requirements of this Prudential Standard include that an APRA-regulated entity 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 who conduct their activities outside Australia; and
- notify APRA after entering into agreements to outsource material business activities.

Where an APRA-regulated entity is the Head of a Level 2 group, it must also ensure that any outsourcing arrangements involving material business activities entered into by members of the Level 2 group are subject to appropriate due diligence, approval

and on-going monitoring 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 46 and 47, 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 the **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 business carried on in Australia by that foreign ADI, Category C insurer or EFLIC.
6. This Prudential Standard only applies only to the **outsourcing** of a **material business activity** as defined in this Prudential Standard.

¹ Paragraph 10 defines Head of a Level 2 group.

² Paragraph 9 defines Level 2 group.

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

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

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 which has a Board of directors;
 - (d) **related body corporate** has the meaning given in section 50 of the *Corporations Act 2001*;
 - (e) **service provider** is a reference to the person providing the outsourced services to the APRA-regulated entity; and
 - (f) **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.
13. Outsourcing involves an APRA-regulated entity entering into an arrangement with another party (including a related body corporate) to perform, on a continuing basis, a business activity which currently is, or could be, undertaken by the APRA-regulated entity itself.
14. For the purposes of this Prudential Standard, **offshoring** means the outsourcing by an APRA-regulated entity of a material business activity associated with its Australian business to a service provider (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.
15. The international business of a Level 2 group does not constitute offshoring as defined in paragraph 14; 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 any requirement relating to offshoring in respect of any other activity falling within the meaning of offshoring under this Prudential Standard.

Materiality

16. A material business activity is one that has the potential, if disrupted, to have a material impact on the APRA-regulated entity'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 entity to meet regulatory requirements if there are problems with the service provider;
 - (e) potential losses to the APRA-regulated entity's customers and other affected parties in the event of a service provider failure; and
 - (f) affiliation or other relationship between the APRA-regulated entity and the service provider.
17. For the purposes of this Prudential Standard, the internal audit function is a material business activity.

The role of the Board and senior management

18. An APRA-regulated entity 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, policy-holders and other creditors.
19. An APRA-regulated entity must have procedures to ensure that all its relevant business units are fully aware of, and comply with, the outsourcing policy.
20. The Board is ultimately responsible for any outsourcing of a material business activity and for any other activity undertaken by an APRA-regulated entity. Although outsourcing may result in the service provider having day-to-day managerial responsibility for a business activity, the APRA-regulated entity and the Board are responsible for complying with all **prudential requirements**⁴ that relate to the outsourced business activity.
21. The Board must approve the APRA-regulated entity's outsourcing policy, which must set out its approach to outsourcing of material business activities, including a detailed framework for managing all outsourcing arrangements.
22. 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.
23. The Board must take into account the APRA-regulated entity's outsourcing risks and controls as part of its overall risk management systems and when completing a risk management declaration required to be provided to APRA.⁵

⁴ 'Prudential requirements' include requirements under the applicable Prudential Act, including any regulations made under that Prudential Act, any applicable Prudential Standards, the *Financial Sector (Collection of Data) Act 2001* and any Reporting Standards made under that Act, conditions on an authority to carry on banking business, a general insurer's authorisation and a life company's registration, and any other requirements imposed by APRA in writing.

⁵ For details of the risk management framework for general insurers, refer to *Prudential Standard GPS 220 Risk Management* and *Prudential Standard GPS 221 Risk Management Level 2*

24. An APRA-regulated entity'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

25. An APRA-regulated entity must be able to demonstrate to APRA that, in assessing the options for outsourcing a material business activity to a third party, 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 or Board committee, in approving the agreement;
 - (e) considered all the matters outlined in paragraph 28, 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.
26. An APRA-regulated entity 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 APRA-regulated entity'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;

Insurance Groups. 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*.

- (d) contingency issues in accordance with *Prudential Standard CPS 232 Business Continuity Management* should the outsourced activity need to be brought in-house; and
- (e) the need to apply any of the requirements set out in paragraph 25 to the extent they are relevant to outsourcing agreements with related bodies corporate.

The outsourcing agreement

- 27. 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.
- 28. 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).
- 29. An APRA-regulated entity 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.

30. The requirements in paragraph 27 do not apply to an outsourcing arrangement with a related body corporate unless:
- (a) after having consulted with the APRA-regulated entity, APRA notifies the APRA-regulated entity, 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 insurer⁶ and a related body corporate.
31. Where an APRA-regulated entity enters into an outsourcing agreement as a result of an unexpected extreme event which results in:
- (a) the APRA-regulated entity invoking its Business Continuity Plan⁷; or
 - (b) the sudden financial or operational failure of an existing service provider,
- then paragraphs 25 to 29 inclusive, 35 and 36 need be complied with only to the extent that is reasonably possible having regard to the nature of the extreme event. The APRA-regulated entity must notify APRA as soon as practicable of any such outsourcing arrangement.

APRA access to service providers

32. 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 entity; 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 entity of its intention to do so.
33. Where an APRA-regulated entity enters into an outsourcing arrangement with a related body corporate, the Board of the APRA-regulated entity must ensure that access by APRA to the related body corporate is not impeded.
34. The APRA-regulated entity 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 which are existing clients of the service provider.

⁶ Refer to GPS 001.

⁷ Refer to CPS 232.

Notification requirement

35. An APRA-regulated entity 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.
36. When an APRA-regulated entity 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 APRA-regulated entity's risk profile.

Offshoring arrangements – requirement for consultation

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

Monitoring the relationship

39. An APRA-regulated entity 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.
40. An APRA-regulated entity 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 APRA-regulated entity.
41. Where an outsourcing agreement is terminated, an APRA-regulated entity 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

42. An APRA-regulated entity'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 APRA-regulated entity's outsourcing policy. Where APRA has exempted an APRA-regulated entity from having a dedicated internal audit function, or approved alternative arrangements under CPS 510, APRA may also vary the requirements of this paragraph.
43. APRA may request the external auditor of an APRA-regulated entity, 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 APRA-regulated entity and must be made available to APRA.

Commencement and transitional arrangements

44. This Prudential Standard commences on [date] (**effective date**).
45. Upon commencement of this Prudential Standard, the existing requirements contained in *Prudential Standard APS 231 Outsourcing (APS 231)*, *Prudential Standard GPS 231 Outsourcing (GPS 231)* and *Prudential Standard LPS 231 Outsourcing (LPS 231)* will cease to have effect.

Adjustments and exclusions

46. 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.⁸

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:

- (a) APS 231 made on 29 September 2006, as amended;
- (b) GPS 231 made on 23 June 2008; and
- (c) LPS 231 made on 29 September 2006, as amended.

⁸ 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.