

DRAFT



APRA

Prudential Practice Guide

PPG 231 – Outsourcing

March 2006

Disclaimer and copyright

This prudential practice guide is not legal advice and users are encouraged to obtain professional advice about the application of any legislation or prudential standard relevant to their particular circumstances and to exercise their own skill and care in relation to any material contained in this guide.

APRA disclaims any liability for any loss or damage arising out of any use of this prudential practice guide.

This prudential practice guide is copyright. You may use and reproduce this material in an unaltered form only for your personal, non-commercial use or non-commercial use within your organisation. Apart from any use permitted under the *Copyright Act 1968*, all other rights are reserved. Requests for other types of use should be directed to APRA.

About this guide

Prudential Standard APS 231 Outsourcing, Prudential Standard GPS 231 Outsourcing and Prudential Standard LPS 231 Outsourcing (Prudential Standards) set out APRA's requirements in relation to outsourcing.

This prudential practice guide aims to assist regulated institutions in complying with those requirements and, more generally, to outline prudent practices in relation to managing outsourcing arrangements. For the purposes of this guide, 'regulated institution' refers to an authorised deposit-taking institution (ADI) or a general insurer or life company regulated by APRA.

Subject to the requirements of the Prudential Standards, regulated institutions have the flexibility to manage their outsourcing arrangements in the way most suited to achieving their business objectives.

Not all the practices outlined in this prudential practice guide will be relevant for every regulated institution and some aspects may vary depending upon the size, complexity and risk profile of the institution.

Materiality

1. The Prudential Standards apply to arrangements to outsource material business activities.
2. Outsourcing involves a regulated institution entering into an agreement¹ 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 regulated institution.
3. APRA is not opposed to regulated institutions outsourcing material business activities² to service providers. The requirements in the Prudential Standards are imposed to ensure regulated institutions are aware of and adequately address the risks which arise from outsourcing material business activities.
4. As a guide, a material business activity may include a significant part of a regulated institution's information technology functions supporting its core businesses, investment management functions, professional services (such as accounting, internal audit and actuarial), loan or claim processing (as the case may be), marketing and research, personnel function, custodial or administration arrangements, treasury or dealing operations (for ADIs) and payment processing (for ADIs).
5. It is not envisaged that a material business activity would ordinarily include contractor relationships – that is, relationships where there are numerous service providers in the marketplace, the agreement is relatively short-term and the cost and inconvenience of switching between providers is low. Examples of contractor relationships include utility services (such as mail and telephone services), legal services, advertising, employee recruiting and other personnel functions, printing services, travel

agency and transportation services, repair and maintenance of fixed assets, purchase of goods, specialised training, background investigation and/or information services and software licensing arrangements.

Resources for managing outsourcing arrangements

6. The Prudential Standards require a regulated institution to demonstrate that it has done certain things when assessing options for outsourcing.
7. When assessing options for outsourcing material business activities, a regulated institution could consider establishing an outsourcing team consisting of individuals from the relevant business area and others with the necessary skills to assess the risks involved in outsourcing. They may include specialists in the relevant risk areas and external experts. This team would ensure that the outsourcing policy is followed at all times, including the tender and due diligence processes, evaluation of the outsourcing options and the making of recommendations to senior management and the Board.

Business continuity management (BCM)

8. *Prudential Standard GPS 222 Business Continuity Management* and *Prudential Standard APS 232 Business Continuity Management* set out business continuity management (BCM) requirements.
9. Where a regulated institution outsources a material business activity APRA envisages that its BCM documentation would outline the procedures to be followed in the event that the service provider is unable to fulfil its obligations under the outsourcing agreement.³

¹ Outsourcing includes any subsequent subcontracting arrangements being the transfer of an activity (or a part thereof) from the service provider to a third party.

² As defined in the Prudential Standards.

³ While there is no prudential standard relating to BCM for life companies, APRA envisages that a life company would outline, in any documentation relating to BCM, the procedures to be followed in the event that the service provider is unable to fulfil its obligations under the outsourcing agreement.

Outsourcing policy

10. The Prudential Standards require the risk management framework of a regulated institution to deal with the risks associated with the outsourcing of a material business activity.
11. The risks associated with the outsourcing of a material business activity would typically be managed and addressed in a manner similar to that if the activity were performed 'in-house'.
12. When managing an outsourced activity, the regulated institution could consider:
 - (a) having policies and procedures in place to address the additional risks arising from the outsourcing of the activity; and
 - (b) incorporating such policies and procedures into its existing risk management framework.

Contractual agreements

13. Under APRA's Prudential Standards, all outsourcing arrangements must be undertaken using a written, legally binding agreement except in certain cases. This agreement must address certain issues at a minimum.
14. Typically, an outsourcing agreement covers a specified period and contains both start and finish dates and includes a clause allowing for periodic review of the agreement and renegotiation if appropriate.
15. Ideally, the agreement specifies the content, frequency and format of the service being provided. The agreement typically also states time lines for receipt and delivery of work and specifies priorities. In addition, the agreement normally contains performance benchmarks, including default benchmarks which, if not met, would result in penalties being applied or, in the extreme, termination of the agreement. Further, the agreed service levels would be specified in service level agreements.
16. The agreement typically addresses any subcontracting or outsourcing by the service provider and includes specific rules or limitations to such arrangements (for example, notification to the regulated institution prior to entering into a subcontracting arrangement). In particular, APRA envisages that the same standards which apply to the service provider in respect of security and confidentiality of information, offshoring,⁴ compliance with relevant legislation and regulations, and APRA's access to information, would apply to subcontractors or outsourcing arrangements by the primary service provider. Also, consideration would usually be given to the extent of liability to both the regulated institution and service provider in relation to subcontracting arrangements, as outlined in paragraph 24 of this guide.
17. The agreement would typically be sufficiently flexible to accommodate changes to existing processes and to envisage new processes in the future.
18. APRA envisages that the agreement would clearly set out the procedures in place to allow the regulated institution to effectively monitor the performance of the service provider. This would typically include the extent to which the regulated institution's internal or external auditors can obtain sufficient information (including through on-site inspections or the appointment of an external party) to satisfy themselves as to the adequacy of risk management systems. Also, consideration would usually be given to including provisions requiring an annual review of the service provider's internal control systems by an independent expert.
19. In addition, APRA envisages that the agreement would include details covering BCM to ensure that acceptable service levels are maintained in the event of problems occurring with the service provider. This requirement would, under the agreement, apply to any subcontracting or outsourcing by the service provider.

⁴ As defined in the Prudential Standards.

20. With respect to default arrangements, the agreement would typically clearly specify what constitutes a default event, identify how it is to be rectified and specify any indemnity provisions.
21. The circumstances that lead to a termination of the outsourcing arrangement would typically be clearly specified in the agreement. As a guide, an agreement would set out possible reasons for termination and procedures to be followed in the event of termination, including notice periods, the rights and responsibilities of the respective parties and transition arrangements. The latter would address access to, and ownership of, documents, records, software and hardware. Termination clauses would typically also specify the time period over which the business activity continues to be undertaken by the service provider and its role in transitional arrangements if the activity is brought back in-house within the regulated institution or outsourced to another service provider.
22. APRA envisages that the agreement would set out explicit pricing arrangements, covering issues such as frequency of payment, invoicing and payment procedures.
23. Formal dispute resolution mechanisms may be incorporated into the agreement. These mechanisms would enable the continued operation of the outsourced activity while specific issues are being dealt with, including conciliation and arbitration arrangements.
24. The agreement would typically specify the extent of liability for each party and, in particular, whether liability for negligence is limited. It would also specify any indemnities and provide details of any insurance arrangements.
25. APRA envisages that the agreement would include specific provisions for outsourcing to service providers conducting the outsourced activity from outside Australia. As a guide, a regulated institution could consider the provisions contained in paragraph 33 of this guide.
26. The regulated institution could consider obtaining legal advice in assessing the agreement.

Management and control of the outsourcing relationship

27. The Prudential Standards require a regulated institution to devote sufficient resources to managing and monitoring the outsourcing relationship.
28. APRA envisages that the monitoring framework of a regulated institution would reflect the size and nature of the arrangements. Importantly, the regulated institution could consider specifically assigning accountability for managing the outsourcing arrangement to an individual or team/committee. This would ensure a continued focus on the outsourcing arrangement.
29. The monitoring process could involve the use of internal (or, where considered relevant or more appropriate, external) audit to ensure compliance with outsourcing policies and procedures. The audit function can be used to:
 - (a) ensure compliance with the regulated institution's risk management policies and procedures;
 - (b) ensure appropriate internal controls are in place; and
 - (c) ensure that reporting is adequate, accurate and timely.
30. To support the audit function, the regulated institution would typically arrange for access to records held by the service provider which are adequate for audit trail purposes.

Offshoring

31. An 'offshoring' arrangement gives rise to a number of particular risks, including:
- (a) country risk – the risk that overseas economic, political and/or social events will have an impact upon the ability of the overseas service provider to continue to provide an outsourced service to the regulated institution;
 - (b) compliance (legal) risk – the risk that offshoring arrangements will have an impact upon the regulated institution's ability to comply with relevant Australian and overseas laws and regulations (including accounting practices);
 - (c) contractual risk – the risk that the regulated institution's ability to enforce the offshoring agreement may be limited or completely hindered;
 - (d) access risk – the risk that the ability of the regulated institution to obtain information and to retain records is partly or completely hindered. This risk also refers to the potential difficulties or inability of APRA to gain access to the service provider and the material business activity being conducted for prudential review purposes; and
 - (e) counterparty risk – the risk arising from the obligor's failure to meet the terms of any agreement with the regulated institution or to otherwise perform as agreed.
32. Typically, these and other risks would be specifically addressed during the preparation of a business case, when conducting the due diligence and during contract negotiations. These risks would also be considered when conducting the ongoing monitoring and control of that material business activity. Specific risk management expertise may be required when assessing, monitoring and controlling material business activities outsourced to service providers conducting the activities outside Australia.
33. An offshoring agreement would typically include the following additional provisions:
- (a) choice of law – typically, the agreement would specify under which particular jurisdiction contractual disputes will be resolved. The due diligence process may include an examination of the relevant overseas legislation and regulations by a suitably qualified expert to ensure that contractual provisions are recognised by the overseas jurisdiction and are able to be enforced in the chosen jurisdiction;
 - (b) security and confidentiality of information – as a guide, contractual provisions in relation to data would be of the same standard as those required of a domestic service provider and in accordance with requirements under Australian legislation and regulations. The agreement would also ensure that all information forwarded to the service provider by the regulated institution (as well as any information forwarded by the service provider to third parties in the course of providing that service, such as to a back-up disaster recovery provider) remains the property of the regulated institution; and
 - (c) access to information/persons – typically, any agreement with a service provider would not restrict access to information by APRA or external auditors, independent third parties or representatives of the regulated institution for the purposes of confirming the performance of the risk management systems. Also, the regulated institution could consider undertaking legal due diligence prior to the execution of the agreement to ensure that there are no legal impediments to APRA's access to information and/or relevant persons employed by the regulated institution or service provider for the purposes of prudential supervision of the regulated institution's activities.

34. To address the risks associated with offshoring arrangements, APRA suggests that a regulated institution maintain copies of important documents related to the arrangement at the regulated institution's Australian office and preferably in English. Such documents would typically include:
- (a) a copy of the contractual agreement;
 - (b) a copy of the due diligence assessment;
 - (c) a copy of the service provider's BCM documentation and details of the latest testing of BCM processes undertaken; and
 - (d) copies of financial statements, reports and any other information the regulated institution considers critical to the ongoing monitoring and control of the outsourcing arrangement with the service provider.
35. In addition, the regulated institution could consider on-going monitoring of, the economic, social and political conditions within the host country to assess the ability of the service provider to continue to adequately perform the contracted service.

Related body corporate arrangements

36. Subject to any contrary APRA requirement, the Prudential Standards exempt outsourcing arrangements between a regulated institution and its related body corporate⁵ from the requirement for written legally binding arrangements.
37. Unless APRA has required a written legally binding arrangement, an outsourcing arrangement between a regulated institution and its related body corporate may be in the form of a service level agreement to demonstrate compliance with the minimum requirements for related body corporate arrangements.

⁵ As defined in the Prudential Standards.



Telephone
1300 13 10 60

Email
contactapra@apra.gov.au

Web site
www.apra.gov.au

Mail
GPO Box 9836
in all capital cities
(except Hobart and Darwin)