Australian Prudential Regulation Authority

400 George Street (Level 26)
Sydney NSW 2000

GPO Box 9836
Sydney NSW 2001

T 02 9210 3000
F 02 9210 3411
W www.apra.gov.au

15th November 2010

To: ADIs, GIs, LIs (including Friendly Societies)

OUTSOURCING AND OFFSHORING
Specific considerations when using cloud computing services

Although the use of cloud computing[1] is not yet widespread in the financial services industry, several APRA-regulated institutions are considering, or already utilising, selected cloud computing based services. Examples of such services include mail (and instant messaging), scheduling (calendar), collaboration (including workflow) applications and CRM solutions. While these applications may seem innocuous, the reality is that they may form an integral part of an institution's core business processes, including both approval and decision-making, and can be material and critical to the ongoing operations of the institution.

APRA has noted that its regulated institutions do not always recognise the significance of cloud computing initiatives and fail to acknowledge the outsourcing and/or offshoring elements in them. As a consequence, the initiatives are not being subjected to the usual rigour of existing outsourcing and risk management frameworks, and the board and senior management are not fully informed and engaged.

Prudential concerns

Accordingly, APRA wishes to emphasise the need for proper risk and governance processes for all outsourcing and offshoring arrangements, including cloud computing. Key prudential concerns that should be addressed relate to the potential compromise of:

- a financial institution's ability to continue operations and meet core obligations, following a loss of cloud computing services;
- confidentiality and integrity of sensitive (e.g. customer) data/information; and
- compliance with legislative and prudential requirements.

Additionally, APRA's ability to fulfil its duties as prudential regulator should not be compromised.

[1] The term generally describes a delivery model where dedicated or shared IT assets (software, hardware and data/information) are consumed as a service. This can involve the provision of IT assets by a third party located offshore.

APRA's prudential regulation

While APRA has no specific prudential requirements in this area, the principles in the following materials are pertinent to cloud computing:

- Outsourcing: Prudential Standards APS231, GPS231 and LPS231 and Prudential Practice Guide PPG231;
- Business Continuity: Prudential Standards APS232, GPS222 and LPS 232, Guidance Notes AGN232 and GGN222 and Prudential Practice Guide PPG233; and
- Management of security risk in information and information technology: Prudential Practice Guide PPG234. Pertinent areas include risk management, resilience and recovery (including offshore IT assets) and service provider management.

Materiality and risk assessments

Regulated institutions are reminded that, under the prudential standards on outsourcing, they are required to consult with APRA prior to entering into any offshoring agreement involving a *material* business activity. The definition of '*material*' refers to circumstances where arrangements have the potential, if disrupted, to have a significant impact on the institution's business operations or its ability to manage risks effectively (refer to the prudential standards on outsourcing for further details).

As part of their consultations with APRA, regulated institutions are expected to provide a comprehensive risk assessment. This would typically include an assessment of the specific arrangements underlying the services offered, the service provider, the location from which the services are to be provided and the criticality and sensitivity of the IT assets involved. APRA would expect the risks to be periodically reassessed in line with the institution's risk management framework.

In APRA's view, both materiality and risk assessments necessitate a detailed understanding of the extent and nature of the business processes (including those pertaining to decision-making and support), the technology architecture and the sensitive information (customer or other) impacted by the outsourcing arrangement. APRA has observed that, to date, assessments of cloud computing proposals typically lack sufficient consideration of these factors.

As part of its regular onsite review processes, APRA will continue to examine outsourcing/offshoring arrangements of regulated institutions, including those involving cloud computing, to ensure prudential concerns are adequately addressed.

Should you have any questions or comments, please contact Mr David Pegrem, Head of IT Risk, on (02) 9210 3324 or email david.pegrem@apra.gov.au.

Yours sincerely

Puay Sim
General Manager
Supervisory Support Division