



15th November 2010

To: All Trustees
APRA regulated superannuation funds

OUTSOURCING AND OFFSHORING

Specific considerations when using cloud computing services

Although the use of cloud computing¹ is not yet widespread in the financial services industry, several trustees and superannuation fund administrators 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 core business processes, including both approval and decision-making, and can be material and critical to ongoing operations of the trustee and the superannuation fund.

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:

- the ability to continue operations and meet core obligations, following a loss of cloud computing services;
- confidentiality and integrity of sensitive (e.g. member) 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: Superannuation Industry (Supervision) Act 1993 Reg 4.16, Superannuation Guidance Note SGN 130.1 and Prudential Practice Guide PPG231;
- Business Continuity: 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

Trustees are requested to consult with APRA prior to entering into any offshoring agreement, either directly or via a service provider, involving a *material* business activity (as per the prudential requirements applicable to other regulated industries). For the purposes of this letter, the definition of '*material*' includes circumstances where arrangements have the potential, if disrupted, to have a significant impact on the trustee and superannuation fund's operations or its ability to manage risks effectively (refer to the guidance note on outsourcing for further details).

As part of their consultations with APRA, trustees 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 trustee'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 (member 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 trustees and superannuation funds, 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