CLIFFORD
CHANCE

Briefing note July 2015

Managing the regulatory storm for cloud services – APRA's Information Paper

The Australian Prudential Regulation Authority (**APRA**) has released an information paper (**Information Paper**) on prudential considerations and key principles in relation to outsourcing involving shared computing services[1] (whether it be hardware infrastructure or software), including cloud services. The Information Paper follows APRA's observations of an increase in the volume, complexity and materiality of outsourcing arrangements involving shared computing services and an expectation that this will continue to evolve.

APRA acknowledges that while shared computing services may bring benefits, such as increased economies of scale, it will also bring its associated risks. The Information Paper identifies several risks associated with shared computing services and outlines various prudential considerations and the key risk management and mitigation principles that APRA-regulated entities (**Entity**) need to consider when contemplating the use of shared computing services.

The Information Paper reaffirms the need for an Entity to implement proper risk management practices when considering the use of shared computing services, and to ensure they meet their prudential obligations.

Risk Management Considerations

In APRA's view, public cloud[2] arrangements have not reached a level of maturity commensurate with usages, which would have an extreme impact if a disruption occurs. Accordingly, APRA has outlined the following areas for consideration by Entities when utilising shared computing services.

Strategy/Planning

Rigour must be exercised when planning a transition from the current state to the desired IT architecture and proposals should not be driven solely by cost considerations.

Governance

An Entity's board of directors, senior management and relevant internal governance body should form a view as to the adequacy of the risk and control frameworks to ensure that any shared computing services arrangement remains within the Entity's risk appetite.

The Board of directors, senior management and relevant internal governance body will need to understand the consequences if risks are realised and the adequacy of risk mitigation procedures in place, including any material changes to the shared computing arrangements.

Selection process

A comprehensive due diligence process (including independent risk assessments) would normally be conducted to verify the maturity, adequacy and appropriateness of the provider of shared computing services and the services selected.

Entity's governance authority should be informed of matters such as:

- both initial and ongoing risk management, assessments and assurance frameworks;
- results of any due diligence reports and any assurances;
- the relevant business case and any alternatives to shared computing platforms;
- operating and security models;
- relevant regulatory standards and guidance; and
- continuity of service strategy if an outage occurs.

APRA suggests that Entities should consider the use of Australian hosted solutions, and solutions that are used by other parties with comparable security requirements and risk profiles, as a means of reducing inherent risk of losing confidentiality and the integrity of shared computing systems.

Selection of providers should consider:

- ability to meet performance, security, resilience, recoverability and any other business requirements;
- adequacy of the external service provider's security systems and practices;
- adequacy of ongoing monitoring to ensure software operates as intended; and
- the ability to transition to an alternative service provider (including the ability remove sensitive it assets from the incumbent provider's environment).

Transition approach

When transitioning to shared computing services, Entities should take a cautious and measured approach, particularly if there are heightened risks[3]. Furthermore, transitions should take a staged approach.

Entities should:

- pilot transition with low risk initiatives and assess suitability before moving to more sensitive data;
- continually assess changes to risk profile during transition; and
- establish separate clearance procedures for each stage of the transition. environment).

Risk assessments & security

Entities are expected to conduct comprehensive security and risk assessments periodically and on material changes to circumstances.

A comprehensive risk assessment includes consideration of factors such as the nature of the service (including specific underlying arrangements, the provider and the location of the service), criticality[4] and sensitivity[5] of the IT assets and data involved, the transition process, and the operating model.

Reports on risks should be clearly described so that management and internal governance authorities have a comprehensive understanding of the actual risks, including through the use of a scenario analysis of possible security events.

Security considerations:

- appropriate isolation from third parties' information;
- restricting access based on time and capability to perform an authorised activity, as well as restricting the number of people who are able to access certain information;
- multi-factor authentication;
- protecting sensitive data, both in transit and at rest, through cryptographic techniques; and
- introduce logging and other control mechanisms for administrator functions.

Management of service providers

Entities benefit from proactive management of shared computing service providers and receiving information on a regular basis to enable effective oversight. This would typically include ongoing notification arrangements being put in place between the Entity and the service provider. Further, an Entity should have access to the service provider's information and personnel under various scenarios, including in the event of a security incident. APRA believes that ongoing management would generally include aligning and monitoring alignment of the Entity's IT environmental requirements to those provided by the shared computing service.

Business disruption

Recovery capability ensures that the IT environment can meet business recovery objectives in the event that IT assets become unavailable, whether in the event of a security incident or otherwise.

APRA has set out the following considerations as part of effective recovery capability.

Disruption considerations:

- clarify roles and responsibilities between the entity and service provider in the event of a disruption;
- clarify the state to which the shared computing service will be recovered and the effect this level would have on the entity's operations (including data, software and software configuration);
- ensure the recovery systems are not exposed to the risk of the same event impacting the primary systems; and
- test recovery platforms and plans to ensure readiness in the event of a disruption.

Assurance

An Entity should normally seek regular assurance that risk and control frameworks, and their application, are designed and operating effectively in order to manage the risks associated with the use of a shared computing service. This assurance should provide the Entity with the same level of assurance as an internal audit.

APRA acknowledges that providing this level of assurance may be a burden to the service provider. Therefore, the Entity is encouraged to undertake a collaborative assurance model where available sources of

assurance, such as certifications or internal audits from the service provider, are taken into account.

Additional assurance work may be necessary when there are material changes to the shared computing service.

Consultation with APRA

Entities are required to consult with APRA prior to them entering into an outsourcing agreement involving a material business activity where offshoring is involved.

However even where offshoring is not involved, APRA has encouraged Entities to engage with them in consultations where there is a proposed use of shared computing services involving heightened inherent risks. This is regardless of whether the heightened inherent risks come from an increased likelihood of disruption or where a disruption would result in a significant impact on the Entity's operations.

Conclusion

The Information Paper provides useful practical steps that can be taken to manage risks when transitioning to shared computing services. APRA has encouraged Entities to engage in ongoing dialogue with APRA to ensure that prudent practices are in place to mitigate any risks associated with the use of shared computing services. Given that the use of shared computing services is expected to continue to grow, evolve and become more complex in the future, this will continue to be a growing area of interest for APRA.

[1] "shared computing services" refers to arrangements involving the sharing of IT assets with other parties (whether labelled cloud or otherwise)
[2] as opposed arrangements where IT assets are dedicated to a single entity (including "private cloud" arrangements)
[3] Heightened risks occur when shared computing services involve highly critical or sensitive IT assets which can cause a significant impact on the Entity's operations if a disruption event, such as breach of confidentiality or system integrity, occurs.
[4] A measure of the impact of a loss of service availability.
[5] A measure of the impact of a loss of either confidentiality or integrity.

Contacts

Sydney

Diana Chang
Partner
T: +61 2 8922 8003
E: diana.chang@cliffordchance.com

Jerrem Ng
Senior Associate
T: +61 2 8922 8069
E: jerrem.ng@cliffordchance.com

Hong-Viet Nguyen
Senior Associate
T: +61 2 8922 8045
E: hong-viet.nguyen@cliffordchance.com

Nelda Turnbull
Counsel
T: +61 2 8922 8031
E: nelda.turnbull@cliffordchance.com

This publication does not necessarily deal with every important topic or cover every aspect of the topics with which it deals. It is not designed to provide legal or other advice.

SYD#7387477

Clifford Chance, Level 16, No. 1 O'Connell Street, Sydney, NSW 2000, Australia

© Clifford Chance 2015

Clifford Chance is a law firm with liability limited by a scheme approved under Professional Standards legislation

We use the word 'partner' to refer to a member of Clifford Chance LLP, or an employee or consultant with equivalent standing and qualifications

www.cliffordchance.com

Abu Dhabi ■ Amsterdam ■ Bangkok ■ Barcelona ■ Beijing ■ Brussels ■ Bucharest ■ Casablanca ■ Doha ■ Dubai ■ Düsseldorf ■ Frankfurt ■ Hong Kong ■ Istanbul ■ Jakarta* ■ Kyiv ■ London ■ Luxembourg ■ Madrid ■ Milan ■ Moscow ■ Munich ■ New York ■ Paris ■ Perth ■ Prague ■ Riyadh ■ Rome ■ São Paulo ■ Seoul ■ Shanghai ■ Singapore ■ Sydney ■ Tokyo ■ Warsaw ■ Washington, D.C.

*Linda Widyati & Partners in association with Clifford Chance.