INFORMATION PAPER

OUTSOURCING INVOLVING CLOUD COMPUTING SERVICES

24 September 2018

Disclaimer and Copyright

Contents

Introduction

In July 2015, APRA published an information paper titled '*Outsourcing involving shared computing services (including cloud)*'[1] which outlined prudential considerations and key principles that should be considered when adopting use of cloud computing services. This paper updates the July 2015 paper.

The update is a response to APRA's observation of the growing usage of cloud computing services by APRA-regulated entities, an increasing appetite for higher inherent risk activities, as well as areas of weakness identified as part of supervisory activities.

Furthermore, since 2015, there has been continuous evolution of both cloud computing service offerings and APRA-regulated entities' risk management. Generally, service providers have strengthened their control environments, increased transparency regarding the nature of the controls in place, and improved their customers' ability to monitor their environments. APRA-regulated entities have also improved their management capability and processes for assessing and overseeing the services provided.

APRA recognises that the risks associated with the use of cloud computing services will depend on the nature of the usage, and for the purposes of this paper APRA has classified these risks into three broad categories: low, heightened and extreme.

- For arrangements with low inherent risk not involving off-shoring, APRA would not expect an APRA-regulated entity to consult with APRA prior to entering into the arrangement.
- For arrangements with heightened risk, APRA would expect to be consulted after the APRA-regulated entity's internal governance process is completed.
- For arrangements involving extreme inherent risk, APRA encourages earlier engagement as these arrangements will be subjected to a higher level of scrutiny.

APRA expects all risks to be managed appropriately commensurate with their inherent risk. However, for extreme inherent risk, APRA expects an entity will be able to demonstrate to APRA's satisfaction, prior to entering into the arrangement, that the entity understands the risks associated with the arrangement, and that its risk management and risk mitigation techniques are sufficiently strong.

This Information Paper is relevant for a broad audience including boards, senior management, risk management, technical specialists and internal audit.

Finally, APRA has a number of existing prudential standards and practice guides which are pertinent to cloud computing services.[2] This Information Paper applies the concepts

[1] Information paper: Outsourcing involving shared computing services (including cloud) July 2015

[2] Prudential Standards and Prudential Practice Guides: *CPS 231 Outsourcing*; *SPS 231 Outsourcing*; *HPS231 Outsourcing; PPG 231 Outsourcing*; *SPG 231 Outsourcing*; *CPS 232 Business Continuity Management*; *SPS 232 Business Continuity Management*; *CPG 233 Pandemic Planning*; (draft) CPS 234 Information Security, *CPG 234 Management of Security Risk in Information and Information Technology*; and *CPG 235 Managing Data Risk*.

included in those standards and guides and APRA intends to reflect the principles in this paper in future guidance updates. APRA-regulated entities are welcome to submit feedback, through their normal supervisory interaction with APRA, on aspects of this paper and any issues relevant to its use as prudential guidance.

Cloud computing services

Cloud computing provides scalable technology services through the sharing of IT assets (including computer processing, network, storage and software).

For the purposes of this Information Paper, 'cloud computing services' captures all arrangements involving the sharing of IT assets with other parties (whether labelled cloud or otherwise). This includes public cloud, virtual private cloud and community cloud arrangements, but excludes arrangements where IT assets are dedicated to a single APRA-regulated entity (i.e. private cloud).

Glossary

Desensitised data	Desensitised data is data for which the sensitive elements of the data (such as customer data) have been replaced with user-defined substitutes. Desensitisation techniques include data transposition, data anonymisation, data randomisation, and data encryption. The strength of the desensitisation techniques used would typically be commensurate with the sensitivity of the data.
IaaS	Infrastructure as a service. This service typically involves the sharing of physical hardware arrangements involving storage, servers, networking or virtualisation.
IT operating model	An IT operating model comprises processes for managing and monitoring the IT environment (both shared and dedicated components) including asset lifecycle, change, process scheduling, capacity, performance, incidents, security, access, backups and logging.
IT security model	An IT security model comprises the security management and control framework surrounding the arrangement including controls to isolate, delineate and protect the APRA-regulated entity's IT assets from other parties, operational security, identity management, administration rights and management of encryption keys.
Out-of-band data backups	The creation of backup copies via a different mechanism to that used for real time replication (as typically used for high-availability systems). The intent is to ensure that any fault or failure (either physical or logical) impacting the replication mechanisms does not impact on backup copies.
PaaS	Platform as a service. This service typically involves providing operating systems, middleware, database or runtime services.
SaaS	Software as a service. This refers to the provision of software for business users. Examples include customer relationship management, enterprise applications (e.g. payroll, human resource management, and general ledger) and productivity applications (e.g. word processing, spreadsheets, email).

Chapter 1 – Risks must be understood and managed

Risks are a function of usage

While cloud computing services may bring benefits, such as economies of scale, they also bring associated risks. These risks can vary considerably depending on the particular usage. *Prudential Standard CPS 231 Outsourcing (CPS 231), Prudential Standard SPS 231 Outsourcing (SPS 231)* and *Prudential Standard HPS 231 Outsourcing (HPS 231)* include requirements to ensure that risks associated with outsourcing arrangements are identified, assessed, managed and reported.

As with any outsourcing arrangement, it is prudent for an APRA-regulated entity to only enter into cloud computing arrangements where the risks are adequately understood and managed. This includes demonstration of:

- ability to continue operations and meet obligations following a loss of service and a range of other disruption scenarios;
- preservation of the quality (including security) of both critical and sensitive data;
- compliance with legislative and prudential requirements; and
- absence of jurisdictional, contractual or technical considerations which may inhibit APRA's ability to fulfil its duties as prudential regulator, including impediments to timely access to documentation and data/information.

These matters are relevant whether the cloud computing service is provided directly, or through sub-contracting/on-sourcing arrangements entered into by the provider, either initially or subsequently. This necessitates careful consideration of what is permissible within the outsourcing agreement, and ongoing awareness by the regulated entity of changes to the way services are provided.

The nature of the services consumed also presents different risk profiles. Offerings can be broadly classified into Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) arrangements. With the consumption of these services, APRA-regulated entities are placing reliance on the providers to manage an increasing aspect of the technology stack. Conceptually, this adds greater layers of abstraction and opaqueness, which can inhibit effective risk management.

Assessment of materiality

APRA recognises that the risks associated with the use of cloud computing services will depend on the nature of the usage. Therefore, for the purposes of this paper, risks are classified into three broad categories: low, heightened and extreme. APRA's expectations of APRA-regulated entities with respect to cloud computing services, and APRA's supervisory

approach, will depend on the scale of the associated risks. Refer to Chapter 3 for APRA's notification and consultation expectations in line with these categories.

Low inherent risk

Arrangements which could, if disrupted (where disruption includes a compromise of confidentiality, integrity or availability of systems and/or data) present a low or negligible impact to business operations and the ability of the regulated entity to meet its obligations.

Examples of cloud computing usage with low risk:

- applications and data stores with low criticality (a measure of the impact of a loss of availability) and sensitivity (a measure of the impact of a loss of either confidentiality or integrity) as classified by the APRA-regulated entity;
- non-production environments (e.g. test and development) populated with desensitised data; and
- websites that deliver publicly-available information.

Heightened inherent risk

Arrangements involving critical and/or sensitive IT assets that result in either an increased likelihood of a disruption or where a disruption would result in a significant impact to business operations and the ability of an APRA-regulated entity to meet its obligations.

Typically this would involve one or more of the following:

- exposure to environments which are available to non-financial industry entities (i.e. 'public cloud') – as distinct from financial sector 'community clouds' where tenants have comparable security requirements, risk profiles and risk appetites ;
- unproven track record of:
  - the provider;
  - the cloud computing service;
  - the specific usage;
  - the control environment; or
  - the APRA-regulated entity in managing an arrangement of comparable size, complexity and/or risk profile.
- a high degree of difficulty in transitioning to alternate arrangements;
- inability for an APRA-regulated entity to assess the design and ongoing operational effectiveness of the control environment;
- jurisdictional, contractual or technical considerations which may inhibit operational oversight or business continuity in the event of a disruption (including impediments to timely access to documentation and data/information); and/or
- transition to the arrangement involves a complex, resource intensive and/or time-constrained program of work.

Extreme inherent risk

Heightened inherent risk arrangements which could, if disrupted, result in an extreme impact. Extreme impacts can be financial and reputational, potentially threatening the ongoing ability of the APRA-regulated entity to meet its obligations.

Examples of extreme inherent risk include public cloud arrangements involving systems of record which maintain information essential to determining obligations to customers and counterparties, such as current balance, benefits and transaction history.

For usage of this nature, APRA would expect that entities can demonstrate that their risk management and mitigation techniques and capabilities are sufficiently strong.

Chapter 2 — Risk management considerations

Introduction

This chapter outlines issues for consideration by APRA-regulated entities when utilising cloud computing services, including where APRA has identified weaknesses as part of its ongoing supervisory activities.

This chapter does not address *all* aspects of the management of cloud computing services. In addition, the relevance and importance of the following considerations will vary in line with the nature, intended usage and risk profile of the cloud computing services involved.

Strategy

When an APRA-regulated entity is considering the use of cloud computing services, it would be expected to apply an appropriate amount of rigour to the planning of the target IT environment, and the transition from current state to the desired architecture and operating model. This would typically be informed by business and technology strategies, and consider integration with the broader IT environment and operating model.

Strategies would normally include consideration of organisational change and required capability to manage and operate such arrangements.

Observed weaknesses:

- proposals driven solely by cost considerations rather than a clearly defined strategy and architectural roadmap;
- business cases and reporting to the Board and/or senior management which only focuses on benefits and do not provide adequate visibility of associated risks; and
- changes in required organisational capability are not sufficiently understood or addressed.

Governance

An APRA-regulated entity's outsourcing governance framework should outline decision-making and oversight responsibilities with respect to outsourcing, including the use of cloud computing services. Areas addressed typically include the role of the board, senior management and any delegations resting with a specific governance body or individuals. For the purposes of this Information Paper, this is referred to as the 'appropriate governance authority'.

The appropriate governance authority should form a view as to the adequacy of the risk and control frameworks to manage the arrangement in line with the board risk appetite. This

would generally include undertaking sufficient due diligence and thorough analysis of the risks involved to understand the consequences if the risks are realised, and the adequacy of any mitigants in place.

It is important that the appropriate governance authority is informed of all material initiatives involving cloud computing arrangements. This includes the provision of appropriately detailed information at significant stages. Once a firm proposal has been identified this information would include:

- how the proposal aligns to the strategy, the business case, alternative options considered and rationale for the selected solution, including justification for additional risk exposures;
- IT assets in scope, categorised by sensitivity and criticality;
- materiality assessment, including impact on business processes, systems architecture, organisation and operating model;
- high-level risk and control assessments, risk profiles, plausible worst-case scenarios and alignment to risk appetite and tolerances;
- services selected, products and parties involved and delivery location(s); and
- due diligence undertaken and assurance obtained.

Once the detailed solution is designed and transition plans are in place:

- governance, project, risk management and assurance frameworks (initial and ongoing);
- IT operating model and IT security model to be applied, and associated roles/responsibilities of all parties;
- alignment to regulatory standards and guidance;
- architectural overview (including transitional states) for hardware, software and data stores;
- detailed risk and control assessments, risk profiles and alignment to risk appetite and tolerances;
- continuity of service strategy, including high-availability , recovery and provider failure considerations;
- organisational change management and transition plan; and
- project structure and schedule, including key stages, milestones and timeframes.

During project execution, the board, governance committee or other appropriate governance authority within the entity would normally be kept informed, as appropriate, regarding project status and emerging risks and issues.

For initiatives with heightened inherent risk, engagement with APRA would typically occur after the APRA-regulated entity has completed its internal governance processes, and the initiative has been fully risk-assessed and approved by the appropriate governance authority. For cloud initiatives with extreme inherent risk, it would be appropriate for regulated entities to engage with APRA once a firm proposal has been identified, and initial approval to proceed has been given by the appropriate governance authority.

For further information on APRA engagement refer to Chapter 3.

Solution selection process

The selection of the solution involving cloud computing would typically be conducted in a systematic and considered manner. This includes ensuring the selected solution minimises risk wherever possible, and complies with the processes established by the entity for changing the IT environment including security, risk management, IT architecture, procurement and supplier management.

Observed weaknesses:

- solutions not aligned to the desired enterprise architecture;
- bypassing established risk management and outsourcing frameworks; and
- failure to engage with the risk, security, outsourcing and assurance functions at the initiation stage.

A comprehensive due diligence process, including independent assessments, rather than placing sole reliance on attestations by the provider and customer references, would normally be conducted. The intent would typically be to verify the maturity, adequacy and appropriateness of the provider and services selected (including the associated control environment), taking into account the intended usage of the cloud computing service. The depth of due diligence undertaken would normally be commensurate with the criticality and/or sensitivity of the IT assets involved and the level of reliance the APRA-regulated entity places on the provider to maintain effective security controls.

An APRA-regulated entity should consider the benefits of the following factors as ways of reducing inherent risk as part of the solution selection process:

- Australian-hosted options, if available, in the absence of any compelling business rationale to do otherwise. Australian hosting eliminates a number of additional risks which can: impede a regulated entity's ability to meet its obligations; or impede APRA from fulfilling responsibilities considered necessary in its role as prudential regulator; and
- cloud computing services only used by parties which have comparable security requirements, risk profiles and risk appetites (such as other financial sector entities).

Some cloud computing services offer a high degree of flexibility in how the solution is implemented. In these circumstances, design and architectural considerations would include how to minimise the risk of a loss of confidentiality, integrity and availability. Better practice would be to design the solution and associated control on the assumption that the cloud environment is 'untrusted' and therefore could be compromised.

Once the solution design is completed, it would be appropriate to conduct a risk assessment considering the following:

- ability for the APRA-regulated entity to avoid a significant impact on business operations and meet obligations regardless of technology, people, process or service provider failure;
- ability to meet performance, capacity, security, high-availability , recoverability and other business requirements;
- adequacy of secure design principles and development practices;
- adequacy of processes to verify that software operates as intended within the cloud computing service;
- critical and/or sensitive IT assets which are accessible from the cloud computing service;
- ability to meet legislative and prudential requirements (including the outsourcing standards); and
- any impediments which could inhibit APRA's ability to fulfil its duties as a prudential regulator.

Additionally, under the outsourcing standards, APRA-regulated entities must develop contingency plans that allow for the cloud computing service to be provided through alternate means if required (e.g. transitioned to an alternative service provider or brought in-house), if required. This would typically be achieved through:

- the development and periodic validation of exit strategies to be enacted on contract expiry (or otherwise), including consideration of the contractual and technical ability to isolate and clearly identify IT assets for transition to another arrangement or in-house; and
- consideration of the removal of sensitive IT assets from the provider's environment (including from backups and other copies).

The intent of these contingency plans is to enable an orderly transition, if needed, while continuing to meet obligations.

APRA access and ability to act

The APRA outsourcing standards require APRA-regulated entities to include an APRA-access clause in the outsourcing agreement. This includes access to both documentation and information, and the right for APRA to conduct onsite visits of the service provider.

Observed weaknesses:

- impediments placed on APRA-access rights to the service provider (outsourcing standards). Examples include placing caveats on APRA's ability to access documents, information or the service provider.

The APRA access clause is an important prudential tool, as it aims to remove legal impediments which could inhibit APRA's ability to fulfil its duties as a prudential regulator (e.g. when resolving an APRA-regulated entity, including implementation of the Financial Claims Scheme (FCS) in accordance with *Prudential Standard APS 910 Financial Claims Scheme*).

Transition approach

It is important that a cautious and measured approach is adopted for transitioning to a cloud computing service, particularly where risks are heightened. This would typically involve defined stages of transition which allow for:

- piloting on lower-risk initiatives;
- assessment of the appropriateness of the service and provider for higher-risk future stages;
- organisational change management, including assessment of the capability to oversee and manage proposed arrangements;
- assessment of any changes to the risk profile and alignment to risk appetite;
- consolidation of lessons learned and completion of any remediation activities; and
- clear go/no-go criteria and approval processes for each stage.

Observed weaknesses:
• a 'fast track' transition to a cloud computing service rather than a cautious and measured approach.

Regulated entities using cloud computing services would typically ensure clarity as to the operating model and security model to be applied, and associated roles/responsibilities of all parties.

Risk assessments and security

An APRA-regulated entity would normally conduct initial and periodic security and risk assessments of all material service provision arrangements. Security and risk assessments would typically be conducted whenever a material change to existing arrangements occur. Comprehensive risk assessments typically include consideration of factors such as:

- the nature of the service (including specific underlying arrangements);
- the provider and the location of the service;
- the criticality and sensitivity of the IT assets involved;
- the transition process; and
- the target operating model.

Risk assessments are generally more effective when the risks are clearly described, and at a level of granularity that allows for a meaningful understanding of the actual risks and mitigating controls associated with each risk, including any required remediation actions.

Scenario analysis of plausible security events, including a loss of availability, is a useful technique to understand risks associated with the arrangement. This includes consideration of the risks to critical and/or sensitive IT assets which are accessible from the cloud computing service.

Observed weaknesses:

- high-level risk descriptions that lack clarity or describe control weaknesses rather than risks;
- lack of consideration of critical and/or sensitive IT assets which are accessible from the cloud computing service;
- inadequate consideration of the sensitivity of data (collectively and at the individual field level) when considering implementation solution options for cloud computing services;
- cursory risk assessments which fail to consider specific risks and changes to the risk profile;
- control design and operation, and assurance obtained, do not accurately reflect APRA-regulated entity responsibilities for operating and managing the arrangement; and
- limited due diligence and assurance activities undertaken, with heavy reliance placed on provider attestations and/or usage by other organisations.

It is important that the strength of the control environment is commensurate with:

- the risks involved;
- the sensitivity and criticality of the IT assets involved;
- the level of trust that will be placed on the cloud computing service environment; and
- the shared responsibilities between the service provider and entity.

The aspects of the control environment which would typically be managed by an APRA-regulated entity include: maintaining data quality, information security (such as identity and access management, incident detection and response management, data loss prevention, vulnerability management, configuration management, encryption and key management) and the ongoing monitoring of control effectiveness.

An understanding of the nature and strength of controls required is typically achieved through initial and periodic (or on material change) assessments of design and operating effectiveness, including alignment with industry-agreed practices.

Observed weaknesses

Inadequate consideration of the following:

- controls to prevent, detect and respond in a timely manner to unauthorised access and changes to the APRA-regulated entity's environment by internal staff and service provider staff, service accounts, other customers or third parties, including any changes to the environment which may weaken preventative controls (e.g. configuration changes to the entity's environment or platform);
- access rights, ensuring they are limited to those required for the assigned role – for example, a Platform as a Service (PaaS) provider requires access to maintain the platforms supporting the customer's environment but not the ability to access the virtual assets within that environment;
- controls relating to administration console system access and encryption key management;
- controls to ensure appropriate isolation from third parties to protect against intentional or inadvertent security incidents;

- protection of sensitive data, both in transit and storage, through cryptographic techniques;
- controls to protect critical and/or sensitive IT assets which are accessible from the cloud computing service;
- protection (e.g. using desensitisation) of sensitive data in non-production environments (e.g. development and test); and
- alignment of the disaster recovery environment with the security requirements of the production systems.

System administrator capabilities enable the execution of high impact activities and potentially provide unauthorised access to sensitive IT assets. Consequently, system administrator access entitlements would normally be subject to stronger controls, commensurate with the heightened risks involved. Additional controls relating to system administrator capabilities could include:

- administration tools, systems, consoles and other related software restricted to only those with authorisation;
- access restricted to the minimum time and capability required to perform an authorised activity;
- system administrators restricted from accessing sensitive IT assets through the use of cryptographic, authentication and other techniques;
- four-eyes principle (also known as two-person rule) applied to high impact activities (e.g. deletion of an entire environment);
- restrictions on the location and number of authorised system administrators (an APRA-regulated entity should have visibility of system administrators which could impact the entity's environment);
- multi-factor authentication for system administrator access and activities;
- logging and other detective controls for monitoring system administrator activities; and
- backup and log data protected through segregation of administrator duties and environments.

Implementation of controls

The nature of cloud computing services necessitates the allocation of responsibility for the implementation of controls between the provider and the client. This is commonly referred to as the shared responsibility model. Due to the myriad of cloud computing service offerings that can be consumed, it would be prudent for APRA-regulated entities to carefully consider the differing levels of responsibility for operating and managing these arrangements. Accordingly, an APRA-regulated entity's responsibilities would typically reflect both the combination of controls implemented and assurance obtained from the provider.

An APRA-regulated entity would normally have the capability to evaluate the design and operating effectiveness of controls within the shared responsibility model (both provider and APRA-regulated entity), with a level of assessment commensurate with the impact on the APRA-regulated entity if the service is compromised.

This normally involves evaluations initiated by the APRA-regulated entity (resourced internally and via independent expertise) as well as the leveraging of audit reports initiated by the service provider, conducted by an independent third party. Common examples include Service Organisation Control reports (SOC 1/2/3) and ISO27001/2, ISO 27017, CSA STAR, NIST Cyber Security Framework.[3] It is important, however, that the APRA-regulated entity considers the adequacy of audit reports initiated by the service provider for this purpose and supplement these where considered deficient.

[3] Service Organisation Control (SOC) reports are issued by the International Auditing and Assurance Standards Board (IAASB) and American Institute of Certified Public Accountants (AICPA). ISO standards are issued by the International Organization for Standardization. Security, Trust and Assurance Registry (STAR) is issued by the Cloud Security Alliance. The Cyber Security Framework is issued by the National Institute of Standards and Technology (NIST)

Common areas of responsibility for the different cloud computing models

Areas of responsibility	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)
Ongoing monitoring for control effectiveness	Customer	Customer	Customer
Customer side information security[4]	Customer	Customer	Customer
Data quality	Customer	Customer	Customer
Application management	Customer	Customer	Provider
Virtual machines and networks	Customer	Provider	Provider
Cloud infrastructure[5]	Provider	Provider	Provider

An important control objective is the timely detection of unauthorised access and usage of the APRA-regulated entity's environment by the service provider's staff, service accounts, other customers or third parties.[6] This includes any changes to the environment which may weaken preventative controls (e.g. configuration changes to the entity's environment or platform). An APRA-regulated entity would normally have controls for responding in a timely manner to these alerts.

Observed weaknesses

Inadequate consideration of the following:

- roles and accountabilities under the shared responsibility model;
- controls for which the APRA-regulated entity is responsible for under the shared responsibility model. Examples include identity and access management, incident detection and response management, data loss prevention, vulnerability management, configuration management, encryption and key management; and
- scope and coverage of audits initiated by the service provider for sufficiency.

[4] This includes customer side: user identity and access, interface control, vulnerability and threat management, maintenance of IT asset currency, incident detection and response, configuration management, encryption and key management.

[5] This includes: data centres, servers, networks, cloud fabric, customer access as well as information security controls such as vulnerability and threat management, incident detection, response and client notification.

[6] Cloud service providers provide access to information (such as activity and access logs) which can be leveraged for this purpose.

Ongoing oversight

Regulated entities benefit from managing material service providers pro-actively, and receiving sufficient information on a regular basis to enable effective oversight. This typically includes formal notification arrangements as part of change and incident management processes.

Effective management is typically achieved through the development and maintenance of ongoing operational and strategic oversight mechanisms. These facilitate assessment of performance against agreed service levels, assessment of the ongoing viability of the provider and the service, timely notification of change (including changes to service location, key personnel, sub-contracting arrangements, control environment, relevant policies/standard/procedures and IT assets, either by service provider or other customers, as relevant) and a timely response to issues and emerging risks.

Observed weaknesses:

- lack of consideration of the framework for ongoing management including operational oversight, risk management and assurance.

Ongoing management would generally include monitoring alignment of the APRA-regulated entity's IT environmental requirements with those provided by the cloud computing service. This includes performance, capacity, security, high-availability and recoverability requirements.

The contract for the cloud computing service arrangement would typically address the APRA-regulated entity's access to the service provider's information and personnel under various scenarios. This is both for oversight and assurance purposes as well as in the event of a security incident. The provisions would also allow access by APRA in accordance with the outsourcing standards.

An APRA-regulated entity would benefit from developing an engagement model between the internal risk function and that of the service provider to facilitate greater understanding and influence regarding the risk profile and associated control environment. This would typically be facilitated by joint forums and the sharing of risk and control assessments.

Business disruption

APRA expects that an APRA-regulated entity would continue to meet its obligations regardless of disruptions resulting from a failure of technology, people, process or service providers.

To this end, APRA-regulated entities have taken advantage of the high-availability solutions inherent in many of the cloud computing offerings. However, it is important to distinguish between high-availability and recovery capability when considering the use of cloud computing services. High-availability refers to techniques which reduce the likelihood of IT

assets becoming unavailable in the event of failure of individual components. Recovery refers to techniques to restore IT assets to a known state following a compromise of integrity or availability, thereby reducing the impact of a business disruption. Both high-availability and recovery capability aim to ensure that the business can continue to meet objectives in the event of disruption to IT assets.

APRA-regulated entities need to maintain recovery capability regardless of the level of high-availability in place. In addition, contingency plans are also relevant in the case of provider failure for material arrangements (refer to Solution Selection Section).

Observed weaknesses:

- inadequate consideration of how the regulated entity will continue to meet obligations for a variety of scenarios, including provider failure – either technological or financial;
- inadequate consideration of point-in-time recovery capability with reliance placed upon high-availability solutions;
- inadequate contingency plans which enable critical business activities to be delivered through alternate means, such as via an alternate provider or reverting to operating in-house; and
- inadequate segregation between production and the IT assets necessary to enact recovery, such that a single incident could compromise recovery capability.

Recovery planning, when using cloud computing services, can be informed by a set of plausible disruption scenarios. This would generally include consideration of the failure of high-availability mechanisms (both hardware and software), compromise of a management console(s) and logical failure(s) (e.g. software errors, replication malfunction or a failed change).

In addition, the following are important considerations as part of an effective recovery capability when using cloud computing services:

- clarity regarding roles and responsibilities of the cloud computing service provider, the APRA-regulated entity and other parties in the event of a disruption event (including crisis management, recovery initiation, co-ordination of recovery activities and communication);
- clarity regarding the state to which the cloud computing service will be recovered and the impact this has on recovery and backup activities of the APRA-regulated entity or other parties. This includes consideration of software and data hosted on the service and configuration settings;
- ensuring that the security control environment of the recovery solution meets production requirements;
- ensuring that recovery strategies are not exposed to the risk of the same event impacting production and recovery environments (e.g. use of out-of-band data backups, platform and physical segregation); and
- a testing regime which verifies that recovery plans and strategies are effective and ensures business requirements (including recovery objectives relating to time, point, capacity and performance) are met in the event of a loss of availability.

Audit and assurance

An APRA-regulated entity would normally provide assurance to the board that material service provision arrangements are appropriately managed, and that the service provision management framework is effective. This includes assurance over the design and operating effectiveness of controls in place.

The assurance model normally involves a combination of internal audits (resourced internally and via independent expertise) as well as the leveraging of audit reports initiated by the service provider, conducted by an independent third party (as outlined under the Implementation of Controls Section). It is important, however, that internal audit assess the audits initiated by the service provider for adequacy of assurance. As a general principle, the assurance model would achieve the same level of assurance as that provided by an internal audit function.

One of the challenges for obtaining an adequate level of assurance over cloud computing services is balancing the needs of multiple customers with the practicalities of not overburdening the service provider. This could be addressed through a collaborative assurance model where assurance work is designed to meet the needs of the various customers.

The assurance model would typically take into account the potential range of audit activities, the available sources of assurance (i.e. internal audit, external experts, provider attestations/certifications and the provider's internal audit function) and the level of assurance required in light of the risks associated with the cloud computing service. Assurance activity would normally be executed through a formal program of work that facilitates a systematic assessment of the risk and control environment over time.

The auditable universe comprises a number of dimensions[7]. It is important that all of the dimensions are assessed over time, commensurate with the risks involved, including (but not limited to) assessment of the following:

- legal, regulatory and contractual compliance;
- management and oversight of the arrangement, including reporting mechanisms;
- IT asset lifecycle management processes including: change, process scheduling, capacity, performance, incidents, access, software development and maintenance, backups, and logging;
- security management including roles/responsibilities, security solutions deployed, vulnerability and patch management, incident detection and response, encryption key management and the boundaries isolating the APRA-regulated entity from other parties; and
- business continuity and disaster recovery management, including backup and testing arrangements for data, software and software configuration.

[7] Industry agreed control libraries such as Control Objectives for Information and Related Technology (COBIT) can provide a more comprehensive view of the auditable universe.

Additional assurance work may be triggered by material changes to the cloud computing service, or associated vulnerabilities, threats or usage.

Observed weaknesses:

- reliance on key control testing alone for services that involve heightened inherent risk;
- internal audit not assessing the adequacy of provider-supplied assurance of information security and other controls it is responsible for under the shared responsibility model; and
- the regulated entity not systematically testing the sufficiency of the information security controls that it is responsible for under the shared responsibility model.

Chapter 3 – APRA notification and consultation

Materiality and notification

Under the outsourcing prudential standards, APRA-regulated entities are required to notify APRA after entering into a material outsourcing agreement. The intent is to ensure APRA remains apprised of changes to the regulated entity's risk profile through an understanding of the solution selected and the associated impact on the entity.

The outsourcing prudential standards define a material business activity as one which 'has the potential, if disrupted, to have a significant impact on the regulated institution's business operations or its ability to manage risks effectively'. In order to meet the objective of the prudential standard, it is important that the materiality of shared computing service arrangements is properly assessed.

Materiality assessments would normally consider both criticality and sensitivity of the IT assets involved and the associated business processes impacted, as well as the proposed usage of the service. This would include consideration of critical and/or sensitive IT assets which are accessible from the cloud computing service and the projected and/or aggregated materiality of the arrangement.

The use of scenario analysis to consider plausible security events, including a compromise of confidentiality, integrity and availability, is a useful technique to assess the materiality of proposed arrangements.

Consultation

Under the outsourcing standards, regulated entities are required to consult with APRA prior to entering into an outsourcing arrangement involving a material business activity where offshoring is involved.

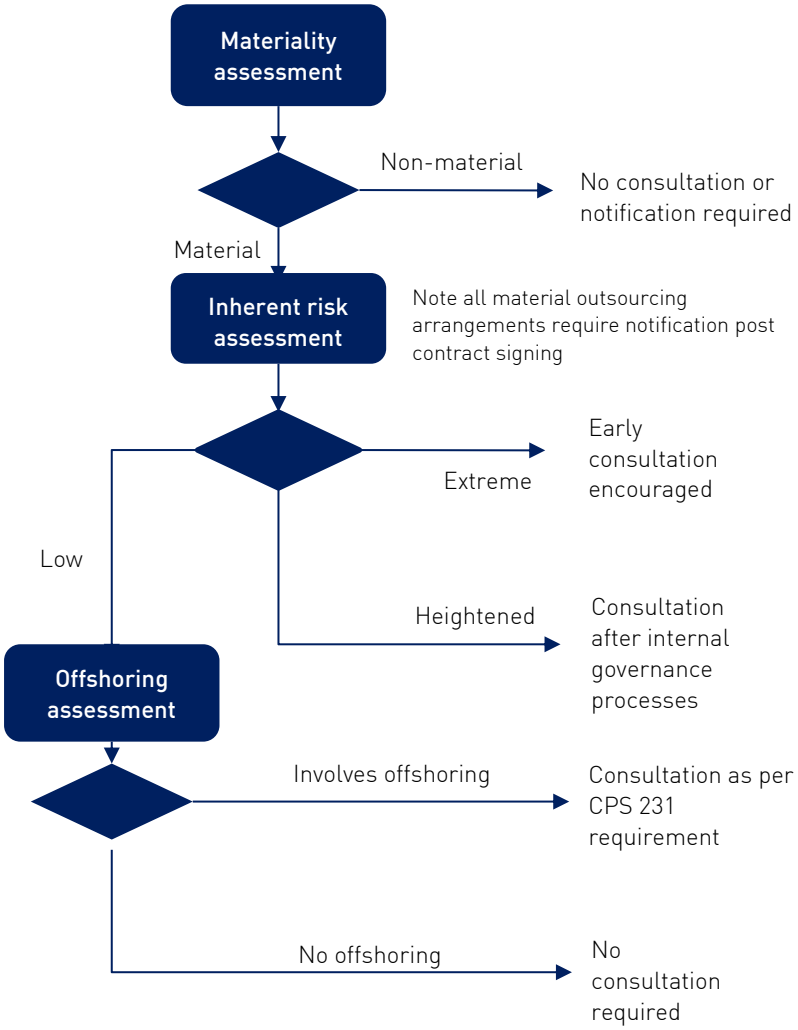
When the proposed use of cloud computing services involves heightened or extreme inherent risks, APRA encourages consultation prior to entering into any arrangement, regardless of whether offshoring is involved. This is to ensure that the APRA-regulated entity understands and has the capability to manage these risks. For clarity, there is no need for consultation with APRA prior to entering into low inherent risk arrangements.

Formal consultation for initiatives with heightened inherent risk would typically take place after the regulated entity has completed its internal governance processes, and the initiative has been fully risk-assessed and approved by the appropriate governance authority.

For uses involving extreme inherent risk, APRA encourages early engagement. This provides APRA with the ability to provide feedback on any areas of potential concern prior to the APRA-regulated entity committing large amounts of resources to the initiative. Proposals

with extreme inherent risk will be subject to a greater level of scrutiny by APRA, both initially and as the initiative progresses.

An overview of the consultation and notification process is provided below:



The types of documents APRA typically expects to receive as part of the consultation process include:

- overview of the solution selected, including rationale, due diligence, IT assets in scope, services/products selected, parties involved and delivery location(s);
- the entity's materiality assessment including impact on business processes, systems architecture, organisation and operating model;
- risk and control assessments;
- disaster recovery strategy;
- contingency plans for provider failure; and
- evidence of approval by the appropriate governance authority.

To facilitate the consultation process, APRA-regulated entities could provide documentation used to inform the internal governance mechanisms discussed in Chapter 2. Given the need for early consultation for extreme inherent risk usage, APRA recognises that not all documentation specified above will be available or completed at the start of this assessment.

Conclusion

The use of cloud computing services represents a significant change to the way technology is employed. While cloud computing services may bring benefits, such as economies of scale, they also bring associated risks.

The use of cloud computing services by APRA-regulated entities is expected to continue to evolve, along with the maturity of the risk management and mitigation techniques applied. APRA will seek to ensure that regulated entities' risk management and mitigation techniques are sufficiently strong when utilising cloud computing services that involve heightened inherent risk or an extreme impact if disrupted.

APRA