



Information Paper

OUTSOURCING INVOLVING SHARED COMPUTING SERVICES (INCLUDING CLOUD)

6 July 2015

Disclaimer and Copyright

While APRA endeavours to ensure the quality of this publication, it does not accept any responsibility for the accuracy, completeness or currency of the material included in this publication and will not be liable for any loss or damage arising out of any use of, or reliance on, this publication.

© Australian Prudential Regulation Authority (APRA)

This work is licensed under the Creative Commons Attribution 3.0 Australia Licence (CCBY 3.0). This licence allows you to copy, distribute and adapt this work, provided you attribute the work and do not suggest that APRA endorses you or your work. To view a full copy of the terms of this licence, visit www.creativecommons.org/licenses/by/3.0/au/.

Table of contents

Table of contents	3
Introduction	4
Chapter 1 – The changing landscape	5
Increased usage of shared computing services	5
Chapter 2 – APRA notification & consultation	7
Risks must be adequately understood and managed	7
Materiality & notification	7
Consultation	7
Chapter 3 – Risk management considerations	9
Introduction	9
Strategy	9
Governance	9
Selection process	10
Transition approach	11
Risk assessments & security	11
Ongoing management of material service providers	13
Business disruption	13
Assurance	14
Conclusion	16

Introduction

Prudential Standard CPS 231 Outsourcing (CPS 231) and *Prudential Standard SPS 231 Outsourcing* (SPS 231) include requirements relating to the risk management of outsourcing arrangements. In November 2010, APRA wrote to all regulated entities highlighting key prudential concerns that should be addressed when outsourcing includes the use of cloud computing services.

More recently, APRA has observed an increase in the volume, materiality and complexity of outsourcing arrangements involving shared computing services (including cloud) submitted to APRA under the consultation and notification requirements of CPS 231 and SPS 231.

APRA's review of these arrangements has identified some areas of weakness, reflecting risk management and mitigation techniques that are yet to fully mature in this area. Further guidance may therefore be beneficial. This Information Paper outlines prudential considerations and key principles that could be considered when contemplating the use of shared computing services.

This Information Paper is relevant for a broad audience including senior management, risk management, technical specialists and Internal Audit.

Finally, APRA has a number of existing prudential standards and practice guides¹ that are pertinent to shared computing services. This Information Paper applies the concepts included in those standards and guides.

¹ Prudential Standards and Prudential Practice Guides: *CPS 231 Outsourcing*; *SPS 231 Outsourcing*; *CPG 231 Outsourcing*; *SPG 231 Outsourcing*; *CPS 232 Business Continuity Management*; *SPS 232 Business Continuity Management*; *CPG 233 Pandemic Planning*; *CPG 234 Management of Security Risk in Information and Information Technology*; *CPG 235 Managing Data Risk*.

In this Information Paper, the following definitions are used:

Cloud computing

A delivery model which leverages technologies (e.g. virtualisation and networking) to enable *sharing* of IT assets (hardware, software and/or data storage).

Shared computing services

The term 'cloud computing' is used to describe a broad variety of arrangements.

This information paper focuses on 'shared computing services' which refers to arrangements involving the sharing of IT assets with other parties (whether labelled cloud or otherwise). This excludes those arrangements where IT assets are dedicated to a single APRA-regulated entity (including 'private cloud' arrangements²).

² As distinct from 'virtual private cloud' arrangements which share IT assets with other parties.

Chapter 1 – The changing landscape

Increased usage of shared computing services

The use of shared computing services, such as data centre facilities and, in some instances, server and storage environments³, has occurred for many years. A generally agreed set of industry-accepted risk management practices has been established for these types of arrangements.

More recently, there has been a trend for sharing across a larger cross-section of entities (including non-financial industry entities) and the introduction of higher-order shared computing services (e.g. software). Risk management practices, including risk identification and mitigation techniques, are still maturing for these types of arrangements, elevating the level of risk to APRA-regulated entities.

Examples of shared computing services

Infrastructure	Data centre facilities
	Server environments
	Data storage
Software	Productivity software (e.g. word processing, spreadsheets, email)
	Content and document management
	HR & Payroll
	General ledger
	Customer relationship management

While shared 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. For instance, many shared computing service usages have low risk. Other usages, however, have heightened inherent risk, including increased security risk. This necessitates a greater degree of

³ A number of ADI's use this approach as part of a closed community of financial industry entities.

caution and supervisory interest (refer to Chapter 2).

Use of shared computing services with low risk

Examples of shared computing usage with low risk include:

- shared facilities, with each entity's IT assets located on separate hardware; and
- shared infrastructure hosting the following:
 - applications and data stores with low criticality⁴ and sensitivity⁵ (as classified by the APRA-regulated entity);
 - non-production environments (e.g. test and development) populated with desensitised⁶ data; and
 - websites that deliver publicly available information.

Use of shared computing services with heightened inherent risk

Arrangements involving highly critical and/or sensitive IT assets that result in either an increased likelihood of a disruption⁷ or where a disruption would result in a significant impact. Typically heightened inherent risk would be present where one or more of the following apply:

- exposure to un-trusted⁸ environments;
- exposure to environments where tenancy is

⁴ A measure of the impact of a loss of availability.

⁵ A measure of the impact of a loss of either confidentiality or integrity.

⁶ Desensitisation techniques include data transposition, data anonymisation, data randomisation, and data encryption. The strength of the desensitisation techniques used would be commensurate with the sensitivity of the data.

⁷ Including a compromise of confidentiality, integrity or availability.

⁸ Un-trusted refers to environments where an APRA-regulated institution is unable to enforce its IT security policy. Refer to *Prudential Practice Guide CPG 234 - Management of Security Risk in Information and Information Technology for additional guidance*.

available to non-financial industry entities (i.e. 'public cloud'⁹);

- unproven track record of: the provider, the shared 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;
- high degree of difficulty in transitioning to alternate arrangements;
- provider has a high degree of freedom to alter the underlying service and control environment;
- 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.

APRA's stance aligns with the position of other international financial regulators who also question the appropriateness of transitioning systems of record to a public cloud environment.

Use of shared computing services that, if disrupted, can have an extreme impact

Hosting systems of record holding information essential to determining obligations to customers (such as customer identity, current balance/benefits and transaction history).

In light of weaknesses in arrangements observed by APRA, it is not readily evident that risk management and mitigation techniques for public cloud arrangements have reached a level of maturity commensurate with usages having an extreme impact if disrupted¹⁰. Extreme impacts can be financial and/or reputational, potentially threatening the ongoing ability of the APRA-regulated entity to meet its obligations.

⁹ As distinct from a financial sector 'community cloud' where tenants have comparable security requirements, risk profiles and risk appetites.

¹⁰ Including a compromise of confidentiality, integrity or availability

Chapter 2 – APRA notification & consultation

Risks must be adequately understood and managed

CPS 231 requires an APRA-regulated entity to ‘identify, assess, manage, mitigate and report on risks associated with outsourcing to ensure that it can meet its financial and service obligations to its depositors, policyholders and other stakeholders.’ SPS 231 has an equivalent requirement for RSE licensees.

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

- ability to continue operations and meet obligations following a loss of service;
- preservation of the quality (including security) of critical and/or sensitive data/information;
- 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).

The above is relevant whether the shared computing service is provided directly or through sub-contracting / on-sourcing¹¹ arrangements entered into by the provider, initially or subsequently. This necessitates careful consideration of what is permissible within the agreement and awareness of changes to the way services are provided.

¹¹ On-sourcing refers to an outsourcing provider entering into arrangements with other parties to support the provision of the outsourced services.

Materiality & notification

Under CPS 231 and SPS 231, 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 standard defines a material business activity as one which ‘has the potential, if disrupted, to have a significant impact on the regulated institution’s/RSE licensee’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.

It would be prudent for an assessment of materiality to consider both criticality and sensitivity, taking into account the IT assets involved and the associated business processes impacted. This would include consideration of critical and/or sensitive IT assets which are accessible from the shared computing service and the projected and/or aggregated materiality of the arrangement.

Additionally, the use of scenario analysis to consider plausible security events (including a compromise of confidentiality, integrity and availability) is a useful technique to fully understand the materiality of the arrangement.

Consultation

Under CPS 231 and SPS 231, regulated entities are required to consult with APRA prior to entering into an outsourcing arrangement involving a material business activity where offshoring is involved.

Similarly, when the use of shared computing services involves heightened inherent risks, APRA encourages prior consultation, regardless of

whether offshoring is involved. The intent is to ensure that the APRA-regulated entity has adequate capability to understand and manage the heightened risks.

Heightened inherent risk derives from either an increased likelihood of a disruption or where a disruption would result in a significant impact. Examples of arrangements which exhibit these characteristics are listed in Chapter 1.

To facilitate the consultation process, regulated entities could provide documentation used to inform the internal governance mechanisms discussed further in Chapter 3.

Chapter 3 – Risk management considerations

Introduction

This chapter outlines other areas for consideration by APRA-regulated entities when utilising shared computing services, including areas where APRA has identified weaknesses as part of its ongoing supervisory activities. It is important to note, however, it does not address all aspects of the management of shared computing services. In addition, the relevance and importance of the following considerations will vary in line with the nature, usage and risk profile of the shared computing services involved.

Strategy

When considering the use of shared computing services an appropriate amount of rigour would typically be applied to the planning of the 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.

Observed weaknesses

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

Governance

The governance framework, as established by the APRA-regulated entity, would normally outline the decision making and oversight responsibilities with respect to outsourcing (including the use of shared computing services). Areas addressed typically include the role of 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 would typically 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 the mitigants in place.

It is important that the appropriate governance authority is informed of all *material* initiatives involving shared computing arrangements. This includes the receipt of appropriately detailed information at significant stages; for example:

Once a firm proposal has been identified:

- alignment to 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;
- 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 (including assurance obtained).

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

- governance, project, risk management and assurance frameworks (initial and ongoing);
- operating model¹² and security model¹³ to be applied, and associated

¹² Comprises processes for managing and monitoring the IT environment (both shared and dedicated components)

roles/responsibilities of all parties (including handover and escalation points);

- 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 resilience, recovery and provider failure considerations;
- organisational change management and transition plan; and
- project structure and schedule (including key stages, milestones and timeframes).

During the execution phase, the appropriate governance authority would normally be kept informed, as appropriate, regarding the current status and emerging risks and issues.

Selection process

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

Observed weaknesses

- solutions not aligned to the desired enterprise architecture;
- bypassing established risk management and outsourcing frameworks; and

including asset lifecycle, change, process scheduling, capacity, performance, incidents, security, access, backups and logging.

13 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.

- failure to engage with the risk, security, outsourcing and assurance functions at the initiation stage.

A comprehensive due diligence process (including independent assessments¹⁴ and customer references) would normally be conducted 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 shared 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 trust¹⁵ placed in the shared computing services control environment.

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

- Australian¹⁶ hosted options, if available, in the absence of any compelling business rationale to do otherwise; and
- shared computing services only used by parties that have comparable security requirements, risk profiles and risk appetites (such as other financial sector entities).

Some shared 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.

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

14 Rather than sole reliance placed on attestations by the provider.

15 Trust in this context refers to reliance on the provider to maintain effective security controls for ensuring confidentiality, integrity and availability.

16 Australian hosting eliminates a number of additional risks which can impede a regulated entity's ability to meet its obligations.

- ability to meet performance, capacity, security, resilience, recoverability and other business requirements;
- adequacy of secure design principles and development practices utilised;
- adequacy of processes to verify that software operates as intended within the shared computing service; and
- critical and/or sensitive IT assets which are accessible from the shared computing service.

Additionally, under CPS 231 and SPS 231, APRA-regulated entities must develop contingency plans that allow for the shared computing service to be transitioned to an alternative service provider (or brought in-house), if required. This would typically be achieved through:

- the development 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
- removal of sensitive IT assets from the incumbent 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.

Transition approach

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

- piloting on low risk initiatives;
- assessment of the appropriateness of the service and provider for future stages;
- organisational change management including assessment of the capability to oversee and manage the arrangement;
- 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 for each stage.

Observed weaknesses

- a 'fast track' transition rather than a cautious and measured approach; and
- impediments placed on APRA access rights to the service provider (refer CPS 231 and SPS 231).

Regulated entities using shared computing services would typically ensure clarity as to the operating model and security model to be applied and associated roles/responsibilities of all parties (including handover and escalation points).

Risk assessments & security

An APRA-regulated entity would normally conduct security and risk assessments, initially, periodically and on material change. The level of thoroughness would typically be commensurate with the usage and nature of the shared computing service.

This allows for consideration of the broader risk and security landscape, including plausible worst case scenarios. This provides greater clarity regarding alignment to an APRA-regulated entity's risk appetite, including identification of any areas outside of risk appetite and timely enactment of remediation actions, if required.

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), criticality and sensitivity of the IT assets involved, the transition process (delivery risk), and the target operating model (delivered risk).

Additionally, risk assessments are generally more effective when the risks are clearly described and at a level of granularity which allows for a meaningful understanding of the actual risk and identification of specific mitigating controls (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 shared computing service.

Observed weaknesses

- high-level risk descriptions that lack clarity or are documented as statements of control weaknesses;
- lack of consideration of critical and/or sensitive IT assets which are accessible from the shared computing service;
- inadequate consideration of the sensitivity of data (collectively and at the individual field level) when considering implementation solution options for shared computing services;
- cursory risk assessments which fail to consider specific risks and any changes to the risk profile; 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; and the level of trust that will be placed on the shared computing service environment. 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 protect critical and/or sensitive IT assets from unauthorised activity by provider staff with highly privileged access (e.g. system administrators);
- controls relating to console system administration (either internally or externally hosted) 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 at rest, through cryptographic

techniques;

- controls to protect critical and/or sensitive IT assets that are accessible from the shared 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:

- 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;
- two-person rule applied to high impact activities (e.g. deletion of an entire environment);
- administration tools, systems, consoles and other related software restricted to only those authorised;
- restrictions on the location and number of authorised¹⁷ system administrators;
- multi-factor authentication for system administrator access and activities;
- logging and other detective controls for monitoring system administrator activities;
- backup and log data protected through segregation of administrator duties and environments.

¹⁷ It is appropriate for a regulated entity to have visibility of system administrators which could impact the entity's environment.

Ongoing management of material service providers

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 which facilitate: assessment of performance against agreed service levels, assessment of the ongoing viability of the provider and the service, notification of change¹⁸, 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 to those provided by the shared computing service. This includes performance, capacity, security, resilience and recoverability requirements.

Additionally, the contract for the shared 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 CPS 231 and SPS 231.

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

¹⁸ This includes 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.

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

The ability to recover from a business disruption event is an important consideration when using shared computing services. Recovery capability ensures that the IT environment can meet business recovery objectives in the event that IT assets become unavailable, and reduces the impact of an incident.

It is important to distinguish recovery from resilience when considering the use of shared computing services. Resilience refers to techniques that ensure IT assets remain available in the event of the failure of individual components. Recovery refers to the capability to ensure that the IT environment can meet business recovery objectives in the event that IT assets have become unavailable. In general, resilience reduces the likelihood of IT assets becoming unavailable, whereas recovery reduces the impact of an incident that has compromised availability. APRA-regulated entities need to maintain recovery capability regardless of the level of resilience in place.

Observed weaknesses

- inadequate consideration of point-in-time recovery capability with reliance placed upon resilience; 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 shared computing services, can be informed by a set of plausible disruption scenarios. This would generally include consideration of: the failure of resilience mechanisms (both hardware and software), a 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 effective recovery capability when using shared computing services:

- clarity regarding roles and responsibilities of the shared 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 shared computing service will be recovered and the impact this has on recovery and backup activities of the APRA-regulated entity and other parties. This includes consideration of data, software and software configuration;
- ensuring that the security control environment of the alternate site meets production requirements;
- ensuring that recovery strategies, when using shared computing services, are not exposed to the risk of the same event impacting production and recovery environments (e.g. use of out-of-band¹⁹ data backups, platform and physical segregation); and
- a testing regime that verifies that recovery plans and strategies, when using shared computing services, are effective, and ensure business requirements (including recovery objectives relating to time, point, capacity and performance) are met in the event of a loss of availability.

Assurance

An APRA-regulated entity would 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. As a general principle, the assurance model would achieve the same level of

¹⁹ The term refers to the creation of backup copies via a different mechanism to that used for real time replication (as typically used for high-availability/resilient 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.

assurance as that provided by an Internal Audit function.

One of the challenges for obtaining an adequate level of assurance over shared 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.

Better practice is for the design of an assurance model to take into account: the auditable universe, 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 shared 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.

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

Observed weaknesses

- Reliance on key control testing alone for services that involve heightened inherent risk.

The use of shared computing services may expose critical and/or sensitive IT assets to environments where an APRA-regulated entity is unable to enforce its IT security policy, such as public networks and shared infrastructure (i.e. 'un-trusted'). To mitigate this, an APRA-regulated entity could develop a schedule of assurance testing²⁰ that ensures that all aspects of the IT security control environment, both of the APRA-regulated entity and the service provider, are assessed over time. The auditable universe

²⁰ Including penetration, vulnerability and IT general controls testing.

comprises a number of dimensions²¹. 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.

²¹ Industry agreed control libraries such as Control Objectives for Information and Related Technology (COBIT) can provide a more comprehensive view of the auditable universe.

Conclusion

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

Use of shared computing services by APRA-regulated entities is expected to continually evolve, along with the maturity of the risk management and mitigation techniques applied. Hence, APRA encourages ongoing dialogue to ensure prudent practices are in place and risks are adequately mitigated when regulated entities seek the advantages that shared computing services can realise. Prudent practices would normally include a well-considered strategy, effective governance arrangements, appropriate consideration of IT risk (including security and recovery) and sufficient assurance mechanisms.



Telephone
1300 55 88 49

Email
info@apra.gov.au

Website
www.apra.gov.au

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