Queensland Government Enterprise Architecture

ICT-as-a-service risk assessment guideline annexe

Risks/considerations

Final

February 2014

V1.0.0

PUBLIC

Document details

Security classification	PUBLIC		
Date of review of security classification	February 2014		
Authority	Queensland Government Chief Information Officer		
Author	Queensland Government Chief Information Office		
Documentation status	Working draft	Consultation release	☑ Final version

Contact for enquiries and proposed changes

All enquiries regarding this document should be directed in the first instance to:

Queensland Government Chief Information Office
ggcio@ggcio.qld.gov.au

Acknowledgements

This version of the *ICT-as-a-service risk assessment guideline annexe – risk/considerations* was developed and updated by the Queensland Government Chief Information Office.

Feedback was also received from a number of agencies, which was greatly appreciated.

Copyright

Cloud computing guideline

Licence

Information security

This document has been security classified using the Queensland Government Information Security Classification Framework (QGISCF) as PUBLIC and will be managed according to the requirements of the QGISCF.

Contents

1 Introduction

1.1 Purpose

This document provides supporting detail for the *ICT-as-a-service risk assessment guideline.* It is not intended to be read as a 'stand-alone' document. It is intended as a companion to the guideline and is focussed on providing further details regarding key as-a-service risks that agencies should consider during their risk assessment of as-a-service options.

Given the 'cloud first' philosophy of government, this document has primarily been developed with *cloud sourcing* in mind. However it is also applicable (for the most part) to managed service arrangements.

1.2 Sources of content

There are many existing and emerging sources of publicly available information regarding cloud risks, and the questions organisations need to ask when considering cloud services. Sources include cloud customers, other governments, vendors, industry analysts and cloud industry bodies. Many of the organisations that have published information are subject-matter-experts/authorities in their respective fields. Others have published information based on their own practical experiences from the use of cloud services.

The Queensland Government is only at the start of its journey to an ICT-as-a-service delivery model and consequently we are relatively immature in our understanding of the risk/questions that need to be addressed. This being the case, it is prudent that we take advantage of the body of information that others (who have more experience) have produced in this area rather than attempting to 'reinvent the wheel' ourselves. The majority of the questions identified in this document are therefore derived from, or reference other industry and organisation sources.

A full list of sources/artefacts that have influenced the content in this document can be found in appendix A. However, the primary sources of content are acknowledged below:

- Australian Government – AGIMO, Attorney General's Department and Australian Department of Defence (Defence Signals Directorate)
- Office of the Information Commissioner Queensland
- Queensland State Archives
- CAARA – Council of Australasian Archives and Record Authorities
- Public record Office Victoria
- Cloud Security Alliance.

1.3 Document structure/approach

The *ICT-as-a-service risk assessment guideline* identifies the following list of risk areas for agencies to consider as part of a risk assessment of ICT-as-a-service candidates:

Risk domain	Risk control area
Business	Workforce capability and organisational change management
	Data classification maturity
	Business models and processes
	Procurement and contract management
Technical	Solution architecture
	Service management tools
	Service integration and Interfaces
Strategic	Industry/vendor maturity
	Reputation/political
	Portability
	Financial
Information, data and recordkeeping management	Privacy and confidentiality
	Data ownership
	Data integrity and authenticity
Operational	Business continuity and disaster recovery
	Service performance
	SLA/incident management
	Security

The remainder of this document is broken into sections that align with the risk domains and control areas outlined in the table above. The following information is provided for each risk control area:

- context
- risk/s
- questions for agency's to consider as part of their *risk analysis*
- potential risk mitigation considerations for *risk evaluation/treatment* stage.

2 Business

2.1 Workforce capability and organisational change management

The shift from running an 'enterprise IT department' to an ICT-as-a-service approach will involve significant business change to IT services and also impact agency business practice, business operations and processes. Additionally staff skill sets, roles and responsibilities, contractual and financial operating models will need to be considered.

For agencies to readily consume and exploit new cloud capabilities and value sources, their IT workforce must become 'as-a-service minded'. This transformation will also see reduced reliance on 'hard' technical skills and an increased important of 'softer' business-focused skills. Increased cloud adoption will see an increase in requirement for the following skills:

- business analysts, architects, portfolio and program and change managers
- cloud applications development, cloud service management, contract negotiation and management.

Agency organisational change management competencies including a supportive change management culture will be important for implementing and managing changes in a controlled and systematic manner.

Risk	The agency may not have the capacity and/or capability to support the ICT-as-a-service solutions in their target operating environment.
Questions for agency to address	Do we have appropriate processes, people and skill sets developed and in place to manage an ICT-as-a-service solution? Key areas to consider include: • security and usage of cloud services • as-a-service contract and service level agreement (SLA) management • operational support skills • incident management processes • selection skills for cloud services/cloud architecture • integration skills of multiple cloud suppliers/services.
Mitigation considerations	The government has committed to migrating to an ICT-as-a-service delivery model, and consequently workforce capability should only be a transitory challenge. The pace of change, impacts of changes and rewards and benefits of changes will need to be carefully managed through an effective governance structure. Agencies need to identify capability/maturity issues and address these as part of their workforce capability planning processes. Communication, stakeholder management and staff training will also be fundamental to ensuring a smooth transition to cloud platforms. Wherever possible, agencies should view the take-up of a cloud service as being an opportunity to drive the required organisational skills transformation. Agencies could potentially adopt a strategy of developing maturity via migration of lower-risk workloads in the first instance. The use of an external *cloud broker* could assist with initial provisioning, migration and transition activities including ongoing management and

	monitoring capabilities. Agencies may also wish to supplement their internal workforce with *trusted industry advisors* to provide assistance in certain areas while agencies develop their own maturity[1].

2.2 Data classification maturity

The Queensland Government information security classification framework (QGISCF) (updated July 2013) provides a framework for Queensland Government agencies to classify their information in order to manage risks associated with confidentiality, integrity and availability. This framework allows for Queensland Government information to be classified by information custodians as PUBLIC, UNCLASSIFIED, X-IN-CONFIDENCE, PROTECTED or HIGHLY PROTECTED.

Data security classification is a primary factor in determining the appropriate type of ICT-as-a-service deployment model that may be used by a Queensland Government agency.

Agencies are at varying levels of maturity in information asset identification and information security classification which can expose agencies to unidentified risks when using cloud services.

Risk	Incorrect classification could lead to incorrect controls. This raises several risk scenarios: 1. Classify too low – An agency may assess the information classification to be lower than it should be and may consequently source a solution which does not have controls that align with policy/regulatory requirements. 2. Classify too high - An agency may assess the information classification to be higher than it needs to be and may consequently source a solution which is more costly or complex then was otherwise required. 3. Treat for exception rather than norm - An agency may have the maturity to correctly classify data and determine the sourcing model based on the exception rather than the norm. For example, an application may have 99% X-IN-CONFIDENCE Information but 1% HIGHLY-PROTECTED information and the agency may determine that the overall system treatment must be HIGHLY PROTECTED.
Questions for agency to address	• Is there a high-degree of confidence that data classification has been classified properly in accordance with the QGISCF? • Does the proposed service/deployment model support the expected controls commensurate with the data classification level? Have you checked this against guidance provided in the *ICT-as-a-service Service model selection* and *ICT-as-a-service deployment model selection* artefacts? • Are there multiple classification levels that may warrant different treatment/cloud sourcing models?

[1] Refer to the *Queensland Government Cloud Computing Implementation Model* for further details about the scope and timing of the Cloud Broker and Trusted Adviser roles

Mitigation considerations	• Agency capability: Agencies need to identify capability/maturity issues and address these as part of their workforce capability planning processes. Agencies may also wish to supplement their internal workforce with *trusted industry advisors* to provide assistance in this area whilst they develop their own maturity[2]. • Multiple classifications: Agencies will need to deal with this scenario on a case by case basis but should be open to the possibility of servicing requirements via multiple systems where this proves to be cost-effective. For example, in the scenario cited above in (3), it may be cost-effective to service the X-In-Confidence requirements via a commodity SaaS solution and then have a separate managed service set up for the Highly Protected component. The agency would most likely need to look at modifying business processes to adapt to this two system approach, however it may still be more-cost effective to the alternative of establishing a single solution (engineered to satisfy highly-protected requirements).

2.3 Business models and processes

Moving to an ICT-as-a-service approach will require more emphasis on business design where cloud services, in particular, will interface/impact business systems.

The transitioning of ICT functions to ICT-as-a-service solutions may impact agency business process and practices. ICT systems are inherently linked to agency service delivery and support internal processes and practices. Changes to ICT systems may require follow-on changes to interrelated and interdependent business processes, policies and practices.

Cloud services are highly standardised and therefore cannot accommodate the same level of customisation and integration possible (subject to cost) within traditional software solutions.

Prior to making a decision to move to an ICT-as-a-service approach, agencies must address the impact on business models/processes and eliminate any potential barriers.

Risk	The ICT-as-a-service delivery model may impact interrelated and inter-dependent business processes, policies and practices
Questions for agency to address	• Have you adequately considered the impact on business models/processes and eliminated any potential barriers? • Are any legislative changes required to facilitate changing business processes to suit commercially supplied cloud software?
Mitigation considerations	• Some cloud SaaS services provide in built PaaS frameworks which provide higher levels of configurability than other SaaS services, so this may be an option worth considering in some cases • It is important that agencies do not examine sourcing options with a pre-conceived idea of an outcome that supports a potentially flawed/legacy business process. Agencies should be open to the possibility of challenging existing business processes in order to achieve optimal cloud

[2] Refer to the *Queensland Government Cloud Computing Strategy* for further details about the scope and timing of the Trusted Adviser roles

	outcome. Early engagement with the business is a key requirement in managing this risk. Agencies need to understand and document existing business processes and practices and perform impact analysis based on potential cloud delivery options.

2.4 Procurement and contractual management

A shift to the use of 'pay as you go' cloud services introduces new contractual challenges that will require agencies to revise ICT legal contracts to cater for cloud providers. Establishing successful cloud contracts will require a new way of thinking to reflect a service-based focus rather than asset-based focus.

Risk	The agency may not have suitable expertise/maturity to establish legal contracts for cloud services, and may consequently not have adequate protections built into contracts to protect against data loss, interruptions to service delivery and other issues.

Considerations for agency to address	Areas that need to be addressed include:
	• protection of data/information/records
	• liability and indemnity
	• performance management (including escalation/exit criteria for non-performance)
	• ending the arrangement by either the customer or by the provider (minimising vendor lock in-in by ensuring portability including timely access to data in appropriate formats)
	• ensure data deletion does not occur without customer approval
	• ensure data is disposed of when requested by the customer
	• ensure that no copy of the data is retained post-termination of the contract (or vendor business failure)
	• ensure records are retained by the customer post termination of the contract (or vendor business failure)
	• ensure data is returned in a timely manner and suitable format
	• early warning of bankruptcy (or similar)
	• introduction of harmful code
	• compensation for data loss/misuse
	• change of control
	• rights and obligation changes relating to assignment, novation, and subcontractors
	• different credit allowances and time to pay invoices – late payment may mean the service is terminated/suspended until payment is made
	• change of terms at the discretion of the provider
	• trans-border data transfer
	• explicit service levels for security and service reliability/quality
	• dispute resolution
	  ○ Australian or foreign law applicability
	  ○ alternate dispute resolution mechanisms
	  ○ foreign law remedies available and if so are remedies suitable
	• data portability
	• data ownership is retained
	• data and associated metadata is returned
	• when requested
	• management and monitoring processes.

Mitigation considerations	• Risk management of the issues highlighted above needs particular attention if any data or system is outside the legal jurisdiction of the Queensland and/or Australia. • Contracts and/or agreements are to cover the service provider and all subcontractors involved in providing the cloud computing service. • Agencies should seek legal advice when drafting cloud contracts and understand legal issues associated with offshoring should it be part of an option analysis. • Agencies may wish to consider contracting trusted third party expertise to assist in drafting appropriate contractual clauses to support agency outcomes; this may be particularly relevant in the near-term whilst the agency is developing its own maturity/expertise with regards to contract management of cloud services. The agency remains the subject matter expert in regards to the solution sought. • Whilst the current Government Information Technology Conditions (GITC) contract is not specifically designed for cloud services it can still be utilised in its current form. There is an intention to develop a GITC 5 Cloud Module which, once developed, will assist agencies further with regards to appropriate contractual controls for procurement of cloud services. Agencies should remain informed of developments in this area. • There is expected to be a range of learnings regarding contractual best practices that emerge as agencies increase their take-up of cloud services. The establishment of a cloud email panel is one such example. Agencies should share their learnings, and seek out the learnings of others; this approach will benefit all Queensland Government agencies. • Over time a range of cloud services will be integrated into the Queensland Government CloudStore. These services will have been risk-assessed and contract-assessed by one or more agencies as part of their 'on-boarding' to the CloudStore. This does not negate the need for other agencies to undertake their own assessment of the solutions. However the work done by other agencies with regards to risk/contract assessment may be of assistance to others who wish to take up the same services.

3 Technical

3.1 Solution/architecture

Agencies need to mindful of the fact that cloud services evolve at a faster rate of change than their traditional systems. Indeed this 'Evergreen' approach can be one of the key benefits from adopting cloud computing. This rate of change can cause problems in planning and maintaining of solutions architectures especially if no one party is in full control of the solution components. Different solutions will evolve at different rates and interdependent components may from time to time become incompatible. Agencies should assess their approach to maintaining compatibility across solution architectures.

Risk	The performance/operation of cloud solution may be adversely impacted when a hardware/software upgrade of one service component may be incompatible with another component.

Questions for agency to address	• Does your agency have an approach to maintaining compatibility across solution architectures? • Does your agency have suitable capability and/or processes to properly monitor and manage the change in the solution architecture? Or can these be put in place? • Is the agencies ready to adopt agile architecture practices (such as continuous integration approaches & automated change testing) • Will the cloud service provider (and associated sub-contractors) provide a minimum notice period with regards to significant hardware/software update? • Is there an ability to accept/reject new functionality and changes from the service provider on a case-by-case basis if required?
Mitigation considerations	• Agencies should maintain an awareness of upcoming changes and plan/test integration where possible in advance. • Where possible, contract clause/s should be developed to ensure the cloud provider provides suitable notification to the agency regarding upcoming service changes, and allows 'opt-out' options.

3.2 Service management tools

Agencies need to be able to properly manage and monitor the ICT systems that they have moved to 'the cloud'. The system/service management tools that they have historically used to manage and monitor ICT assets (on their internal networks) may be different to those that are required to manage ICT services in the cloud. Furthermore, service providers might also place restrictions on the level of access provided to customers to manage their individual services.

Risk	The agency may not have suitable tools and/or access to properly monitor and manage the service provider.

Questions for agency to address	• Is your agency prepared to mature its monitoring and management from the traditional component focus to a service focus?
	• Does your agency have the necessarily tools/systems to manage the ICT workload in the cloud? These could include:
	  ○ integrity checking
	  ○ compliance checking
	  ○ security monitoring
	  ○ data encryption
	  ○ network management
	  ○ application performance management (APM)
	  ○ service level management (SLM)
	  ○ automation tools.
	• Does the cloud provider permit access to the cloud solution for monitoring purposes and if so what interfaces are offered?

Mitigation considerations	• Due to the rate of change often seen in cloud services, best of breed management and monitoring tools may provide more value than the traditional management integrated suites. This may in turn drive a proliferation of management tools in the environment until the toolset market starts to consolidate over time. If additional tools/systems are required then this cost will need to be factored into the overall decision of

	whether it is cost-effective to proceed with this solution. • Binding contract clause/s should be developed to ensure the cloud provider meets their obligation and to ensure that they allows your agency to monitor/manage services.

3.3 Service integration/interfaces

Using services from the cloud presents challenges when those services need to integrate with agency systems that are not in the cloud, or alternatively when integration/migration is required between multiple services from different cloud providers. The potential exists for inadvertent use of cloud services creating 'islands' of cloud technologies that will reduce interoperability across cloud types and associated implementations (for example, splitting collaboration components into multiple separate sourced solutions may not provide as feature rich an experience as sourcing these as a bundle).

Risk	Unable to make business applications interoperate effectively between different cloud providers, or between cloud providers and Traditional IT systems hosted on agency networks.
Questions for agency to address	• Have you properly considered how best to split application/workload sourcing and are you confident that inter-organisation data exchanges (e.g. CSP1 to CSP2, CSP1 to Legacy Agency system) will work effectively? • Does the service provider support open standards and interfaces that will maximise likelihood of interoperability across providers? • Have you verified that you can migrate agency data (and associated metadata) easily into and out of the cloud environment? Do you have a data migration strategy? • Does the services out-of-the box data taxonomy and meta-model align to agency requirements? Does the service support a level of configuration or extensibility?
Mitigation considerations	• The success of being able to procure and integrate services from multiple suppliers will be influenced by adoption of a loosely coupled architecture for the components that comprise an ICT solution. • Potential usage of cloud integration brokers to facilitate.

Risk	There is potential for increased security risk and/or data leakage if interfaces and data exchanges are ill-defined.
Questions for Agency to address	• Have you properly considered how best to split workloads and are you confident that inter-organisation data exchanges are well defined and secure? • Does the service provider support open standards and interfaces that will minimise likelihood of data leakage/security risks?
Mitigation considerations	• Testing strategies to reduce risk profile. • Use of cloud integration brokers to facilitate.

4 Strategic

4.1 Industry/vendor maturity

Cloud Computing is a relatively new area and is evolving rapidly. More and more applications/infrastructure domains will become increasingly suited to cloud delivery but at any given point in time it may be the case that there is no suitable cost-effective market option for certain workloads. Agencies need to be comfortable that the market options are sufficiently mature (with proven track record) to meet their business requirements.

Risk	The service provider may not have the capacity and/or capability to support the cloud solution in line with business expectations.
Questions for agency to address	• Can the cloud service provider provide a solution that meets agency business requirements? Has a proper assessment of functional/business requirements been undertaken? • What is the track record of the service provider in providing the same solution to organisations of similar size and complexity? • Have you properly considered changing business processes to enable use of a commodity cloud service? (In those situations where the lack of suitable vendors options is related to the customised/bespoke nature of the application) • Is the cloud service provider in full production or are they still operating on angel or venture funding?

Mitigation considerations	• There may be a genuine gap in industry capability in certain areas of cloud computing (at least in the near-term). It does not necessarily follow that the agency would need to retain system in-house. There are other options which could be considered, for example:
	  ○ business processes may be able to modified to use commodity applications instead of customised/bespoke applications
	  ○ if a SaaS option does not exist then perhaps the agency could at least migrate the application to an IaaS solution in the meantime to begin the journey to the cloud, and then revisit SaaS options at a later stage.
	• Ensure a solid exit strategy if the company has not yet publicly listed.

4.2 Reputation/political

Agencies need to consider the potential for damage to their (or Queensland Government's) reputation and loss of public confidence, in the event of a privacy or security breach.

Typically the controls associated with protection of data are driven by the information classification and sensitivity of data. In an outsourced environment, these controls will be contracted into vendor arrangements. Nonetheless, the potential for breach is always a possibility, and contract/financial penalties after the fact will not offset reputation/political damage or loss of public confidence in event of personal data being compromised.

Risk	Damage to the Queensland Government's reputation resulting from a privacy or security breach.
Questions for agency to address	• Have you ensured that sourcing model and controls are appropriate (and in accordance with policy) for the information classification of the workload in question? • Do you need additional controls/contingencies to cover for the scenario where there is a privacy or security breach? • In the event of a privacy or security breach, do you believe that potential damage to the Queensland Government's reputation or public confidence would be minimal, manageable or severe? • Are the technical/contractual controls of the CSP/MSP equal to or better than that which agency would typically have in place? (This would demonstrate a level of due diligence by the agency to provide a security solution better than it can provide itself.)
Mitigation considerations	• The issue here is not whether technical and contractual controls have been established. The issue to consider is that if a breach occurs, despite these controls being in place, then is the reputation/political impact manageable or not. • Agencies will need to implement appropriate governance processes and ensure that decisions are made by appropriate accountable officers in line commensurate with the risk level.

4.3 Portability

Agencies need to be able to change service providers easily without lengthy procurement and implementation cycles. Agencies need to avoid 'lock-ins' to long contracts and have the freedom to quickly adopt better value and more up-to-date solutions. Agencies also need to be able to migrate quickly to an alternate provider in the event that there current CSP/MSP goes out of business.

Risk	Applications and information cannot be easily retrieved and moved to another provider in the event that the agency chooses to move provider, or is forced to do so if their current provider ceases business.
Questions for agency to address	• Have you vetted the financial strength and competitive sustainability of the vendor? • If I want to move my data to my agency or to a different vendor, or if the vendor suddenly becomes bankrupt or otherwise quits the cloud business,

	how do I get access to my data (and associated metadata) in a vendor-neutral format to avoid vendor lock-in? How cooperative will the vendor be? • How do I ensure that my data is permanently deleted from the vendor's storage media (including the lawful destruction of digital public records)? • Will there be any additional charges levied by the CSP in the event of the agency seeking to remove information from 'the cloud' • For Platform-as–a-Service, which standards does the vendor use that facilitate portability and interoperability to easily move my application to a different vendor or to my agency? • What processes are used to sanitise the storage media storing my data at its end of life, and are the processes deemed appropriate? How are these processes verified? • When the agreement terminates what timeframes and data formats are appropriate for data retrieval?
Mitigation considerations	• Agencies will need to ensure that they have a clearly-defined exit strategy up-front, and are fully aware of any transition costs, before entering into an arrangement with the service provider. • Strategies regarding open standards, interoperability and data portability are key to reducing the risk of vendor lock-in. The requirement for open standards generally avoids platforms or technologies that 'lock' customers into a particular product. Open standards also guard against the inadvertent creation of 'islands' of cloud technologies that will reduce interoperability with other services and across cloud types and deployment models. • Strategies for minimising the cost and business impact associated with exchanging one provider for another are equally important. Government supplier contracts should stipulate certain pre-conditions around data management as well as reserving certain rights to enable alternative sourcing (e.g. allowance for data migration upon contact exit). Agencies will need to ensure that service provider contracts address the portability of data, and satisfactorily address the questions highlighted above. • 'On-boarding' of the proposed solution to the Queensland Government CloudStore should be considered. The brokerage model of the CloudStore will assist in maintaining portability amongst providers and minimising lock-in by ensuring strategically important control points are retained – identity information, controlling end-user access through a centralised gateway and brokering any data interchange.

4.4 Financial

The dynamic 'pay as you go' charging model for cloud services will be cost-effective for commodity/common workloads in most cases. However, there will be certain instances where the usage profile and architecture of the workload can be supported more cost-effectively on a traditional IT model.

It will be important to understand which infrastructure/applications should be maintained and leveraged, but also any instances where the current contractual models may present a potential impediment to cloud that needs to be addressed.

As an example, there are a number of issues relating to software licensing that need to be considered when utilising cloud services. These include – existing software investments, cloud usage restrictions, financially punitive lock in or lock out practices, concurrent use of traditional and cloud software, and ownership of cloud application data. If these issues cannot be resolved for the workload in question then traditional IT sourcing may be required. Traditional IT can be provided as a managed service (preferred) or by an agency.

Agencies are expected to demonstrate value for money when using cloud computing services. This value for money proposition requires lower total cost of ownership, reduced capital investment and lower ongoing cost of providing computer services.

Risk	Cloud service for the workload may not represent value-for-money for the Queensland Government.
Considerations for agency to address	Some specific financial considerations for the risk assessment are: • commercial principles associated with cloud computing • consistency with the Government Information Technology Contracting (GITC) framework • transitioning from capital expenditure to operational expenditure • hidden costs including exit fees, multi-tenanted infrastructure services • intangible benefits including improved service quality, delivery performance and greater productivity • adequate network connection • service level agreement (SLA) compensation • software licensing issues.

Mitigation considerations	• In some cases it may be possible to address issues such as software licensing issues via cloud computing architectures, procurement processes and service provider contracts. Agencies should examine such options before making a determination as to the most cost-effective approach.
	• For each risk identified or requirement to be met there must be a binding contract clause/s to ensure the cloud provider meets their obligation.
	• Agencies need to ensure that their overall TCO/business cases analysis includes consideration of a range of factors beyond just the cost of the solution itself. This can include:
	  ○ staff training
	  ○ implementation
	  ○ integration with existing systems
	  ○ data migration (in and out)
	  ○ risk reduction
	  ○ cost of remediation
	  ○ etc.

Risk	Agencies may not be ready to handle variable budget implications
Considerations for agency to address	Some specific financial considerations for the risk assessment are: • financial implications of a denial of service attack on cloud solution • contingency set aside budget vs. actual variance.
Mitigation considerations	• Agencies should perform a business risk impact assessment to determine the financial and business implications of cloud solution unavailability.

5 Information, data and records management

ICT-as-a-service solutions are typically provisioned on high-availability and elastic infrastructure across multiple data centres, potentially spread throughout the world. For cloud services in particular, the dynamic nature of the cloud could potentially mean that information could reside, or transition through, multiple different locations, legal jurisdictions and could also be co-located on infrastructure with other cloud customers.

There are a number of issues relating to data governance that need to be considered when utilising cloud services:

- privacy and confidentiality
- data ownership and protection
- data integrity and authenticity.

The guidance in this section is derived from several sources. In particular, however agencies are encouraged to refer to the following:

- The Office of the Information Commissioner (OIC) – The OIC has published specific advice on 'ICT as-a-service' and privacy of data which is available on the Commission's website.
- Queensland State Archives (QSA) – QSA has published specific advice around custody and ownership of public records during outsourcing or privatisation and on managing record keeping risks with cloud computing.

5.1 Privacy and confidentiality

The issue of compliance with information privacy legislation is often seen as an impediment to migration of in-house applications and datasets to an external service provider, particularly where that provider is located off-shore or sub-contracts off-shore. The service provider's facilities may be located in a jurisdiction which does not have similar privacy legislation to that covering the management of personal information held by a local organisation. Even locally, the situation is made more complex by the differing instances and applicability of privacy legislation.

The privacy of any data from a Queensland Government department or agency stored on an ICT-as-a-service solution must be maintained in accordance with the Information Privacy Act 2009, and the Queensland Government Information access and use policy (IS33). Privacy considerations apply to the ICT-as-a-service provider and all subcontractors in the supply chain.

If an agency contracts an external provider to collect and/or process personal information, the agency must take all reasonable steps to ensure the service provider is contractually bound to the obligations that the agency has under the Acts. Provided this

is done, there is no prima facie impediment to Queensland Government agencies contracting an external service provider to provide services which involve the processing or storage of personal information.

Risk	Third Party Access: Risk of compromise to confidential information through third party access to sensitive information. This can pose a threat to ensuring the protection of commercially-sensitive information, intellectual property (IP), and personal information.
Questions for agency to address	• Can you maintain privacy of information in accordance with Information Privacy Principles (Refer *to* *Cloud Computing and the Privacy Principles* for guidance)? • Will you be consulted regarding any third party seeking to have access to your records? • Can you obtain assurance that your records cannot be used for applications not specified in the contract? (for example, to data match with databases owned by other clients of the contractor) • Does the service provider have adequate protections in place to ensure that agency data cannot be mined or scraped by third parties (whether human or automated)? • Will the service provider commit to protect data appropriately depending on level of sensitivity? • How will the service provider cater for more sensitive data, individual confidential deeds for provider personnel and potentially restricting access to a limited set of provider personnel?
Mitigation considerations	• Agencies will need to ensure that service provider practices and contract satisfactorily address the questions highlighted above. • For each risk identified or requirement to be met there should be a binding contract clause/s to ensure the cloud provider meets their obligation.

Risk	Regulatory/Legislative: • The act of sending or storing of information outside Queensland/ Australia might in certain circumstances be a breach of state/federal legislative and regulatory requirements; • The Service Provider might fail to comply with the legislation or standards expected by the Queensland Government; • Information/records may be subject to legislation and other requirements of the storage jurisdiction.
Questions for agency to address	• Does my proposed service model/deployment model align with the *ICT-as-a-service service model selection* and *ICT-as-a-service deployment model selection* artefacts? • Does my proposed on-shoring/off-shoring decision align with the ICT-as-a-service offshore data and processing policy? • In which countries is my data stored, backed up and processed? Which foreign countries does my data transit? In which countries is the failover or redundant data centres? Will the service provider notify me if the answers to these questions change?

	• Do you have sufficient awareness of legislation and regulatory requirements (e.g. US Government's Patriot Act) in the other geographic regions where your data will be housed / traverse? Compliance may be a challenge in certain locations. • Can I meet my obligations to protect and manage my data under the *Information Privacy Act*, the *Public Records Act 2002*, *Information Standards IS40* and *IS31*? including but not limited to; ○ personal information is protected against loss and against unauthorised access, use, modification or disclosure and against other misuse ○ personal information is not use other than for the purposes of this agreement and/or customer contract, unless required or authorised by law ○ personal information is not disclosed without the written agreement of the customer unless required or authorised by law ○ personal information is not transferred outside of Australia without the consent of the customer ○ personal information is only accessed by authorised personnel who require access in order to perform their duties ○ immediately notify the customer (mandatory reporting) if the provider becomes aware that a disclosure of personal information is, or may be, required or authorised by law For further advice the Office of the Privacy Commission (OIC) has published specific advice around cloud and privacy of data which available on the Commission's website. • Will the vendor contractually accept adhering to these obligations to help me ensure that the obligations are met to the satisfaction of the Queensland Government?
Mitigation considerations	• Agency legal/contract staff in particular need to develop an awareness of legislation and regulatory requirements in Queensland, Australia and internationally. Key points to address if off-shoring include[3]: ○ the nature of legal powers to access or restrict data ○ the lack of transparency ○ the prevailing culture of some countries ○ complications from data being simultaneously subject to multiple jurisdictions. • At any given point in time, agencies must abide by the statutory/regulatory requirements that exist. It is important to realise that the cloud computing paradigm is rapidly evolving and gaining widespread acceptance. This is driving a need for statutory/regulatory controls to be reconsidered to support greater user of cloud services. Agencies should consider whether there may be an opportunity to drive statutory/regulatory changes to facilitate migration to the cloud or whether in fact such changes may already be being progressed.

[3] Refer to the Australian Government paper *'Australian Government Policy and Risk management guidelines for the storage and processing of Australian Government information in outsourced of offshore ICT arrangements'* for details regarding the points listed.

	• For each risk identified or requirement to be met, agencies should wherever possible look to establish a binding contract clause/s to ensure the cloud provider meets their obligation - as noted above however, cloud providers will not always be able to (or prepared to) put such contract provisions in place; or even if they are prepared to do so, such provisions may have limited value depending on the broader political/legal framework of the parent country of the company and the country where data resides. Agencies will need to consider all these factors as part of their decision process.

5.2 Data ownership

Obligations relating to the creation, maintenance and preservation of public records including compliance with the *Public Records Act 2002*, *Information Standard 40: Recordkeeping*, apply to all public records including those stored in an ICT-as-a-service delivered application.

Agencies must also meet any statutory requirements around data retention that may apply to data stored in cloud applications. For example, *Information Standard 31: Retention and Disposal of Public Records* prohibits the disposal of public records (including information stored in a cloud computing application) without the authorisation of the State Archivist, which is generally provided in a Retention and Disposal Schedule.

Agencies must also consider the impact of the Information Privacy Principles (Information Privacy Act 2009) on data ownership. According to the Office of the Information Commissioner[4]:

> *'If an agency's agreement with a cloud provider allows the agency to retain control over and sole access to its information, then the transfer of information from the agency computer to the cloud provider's computer will be a 'use' and not a 'disclosure'.*
>
> *However, if the agreement does not allow the agency to retain control over the information, or it allows the cloud provider to access the information—for example, it permits scanning of the information for marketing purposes—this will be a disclosure. Disclosure is only permitted in the circumstances set out in the privacy principles.'*

Risk	Agency will be unable to meet its statutory/regulatory requirements for maintenance and preservation of data/records.
Questions for agency to address	• Can you maintain control/ownership of information in accordance with Information Privacy Principles (Refer *to Cloud Computing and the Privacy Principles* for guidance)? • Can you meet your obligations around recordkeeping (including compliance with the *Public Records Act 2002*, *Information Standard 40: Recordkeeping*) that public records stored in cloud applications will remain accessible and useable, preserving their evidential integrity for as long as they are required?

[4] Cloud Computing and the Privacy Principles (Section : 'Use and Disclosure')

	• Can you meet your statutory requirements around data retention (e.g. IS31) that may apply to data stored in cloud applications? • Can you confirm that the agency's records are not to be disposed of without the authorisation of the State Archivist? • Does the service provider demonstrate an understanding that the ownership of all public records stored in cloud applications is vested in the State of Queensland? • Does the service provider demonstrate an understanding of the copyright ownership of the data that the agency wishes to store? (Not all agency data will be copyrighted to the State of Queensland, although much of it will be.) • What are the intellectual property ownership rights that relates to stored customer data?
Mitigation considerations	For each risk identified or requirement to be met, agencies should wherever possible look to establish a binding contract clause/s to ensure the cloud provider meets their obligation - as noted above however, cloud providers will not always be able to (or prepared to) put such contract provisions in place; or even if they are prepared to do so, such provisions may have limited value depending on the broader political/legal framework of the parent country of the company and the country where data resides. Agencies will need to consider all these factors as part of their decision process.

Risk	Records not being disposed of in a timely way, once authorised by the State Archivist.
Questions for agency to address	• Can you obtain an assurance that no copy of your agency's records or information is retained by the service provider when lawfully disposed of when authorised by the State Archivist? • Can you obtain an assurance that no copy of your agency's records or information is retained by the service provider after the termination of the contract? • Can you confirm that at the conclusion of the agency's use of the services of the service provider that all specified records and associated metadata are removed permanently from the service providers systems? (*Note – Consideration needs to be given to all copies of data - it is common for service providers to replicate records for multiple backup, sending copies to sites in different locations or even different jurisdictions. This can mean that time-expired records are not properly deleted from every server held in every site. This can be a serious risk where there is a specific requirement for information to be destroyed, such as personal or sensitive information in records*[5]) • Can you confirm that the agency's records are not to be disposed of without the authorisation of the State Archivist?

[5] Source : ADRI – *'Advice on managing the recordkeeping risks associated with cloud computing*'

	• Does the Service provider demonstrate an understanding that the ownership of all public records stored in ICT-as-a-service applications is vested in the State of Queensland? • Does the service provider demonstrate an understanding of the copyright ownership of the data that the agency wishes to store? (not all agency data will be copyrighted to the State of Queensland, although much of it will be) • Does the service provider allow for recovery of data and associated metadata when required?
Mitigation considerations	For each risk identified or requirement to be met there should be a binding contract clause/s to ensure the service provider meets their obligation.

5.3 Data integrity and authenticity

Government records need to be managed in such a way that they can be shown to be authentic and reliable.

Risk	If an agency is not able to prove that records could not or have not been altered or tampered with in anyway, this will reduce or negate their value as evidence. In addition the evidential value of records may be affected if appropriate audit trails and descriptions of management processes performed on records while they are kept in *ICT-as-a-service* systems are not maintained.
Questions for agency to address	• How does the vendor implement mechanisms such as redundancy and offsite backups to prevent corruption or loss of my data, and guarantee both the integrity and the availability of my data for as long as it is required? • Can you meet your statutory requirements around recordkeeping (e.g. IS40) that public records stored in ICT-as-a-service applications will remain accessible and useable, preserving their evidential integrity for as long as they are required? • Does the service provider have the capacity to protect the evidentiary integrity of data? • Can the service provider effectively guarantee the cessation/ prevention of data and meta-data deletion in the case of a legal hold order? • What audit and logging facilities does the service or environment provide? • How adequate are these facilities to demonstrate the integrity of data? • How audit logs are provided and made available to you? • Are logs easily downloadable when moving data off service?
Mitigation considerations	For each risk identified or requirement to be met there must be a binding contract clause/s to ensure the service provider meets their obligation. In situations where it is not possible to mitigate risks satisfactorily through contract clauses, the agency should consider whether there are any business process changes or continuities that could be put enacted to cover the risk.

6 Operational

6.1 Business continuity and disaster recovery

Agencies will have business continuity and disaster recovery plans for their critical business processes and systems. When transitioning workloads to an ICT-as-a-service model, agencies will need to ensure that the SLAs meet or exceed the BCP/DR requirements for maintaining services and protecting data.

Risk	Access to records/system may be lost, or not provided in a timely way.

Questions for agency to address	• Is the network connectivity (between your agency users and the vendor's network) adequate in terms of availability? Is it designed to be suitably fault tolerant?
	• Is the service provider's business continuity and disaster recovery plan acceptable?
	  ○ Does the service provider have adequate mechanisms in place for protecting data from loss by machine fault and human error?
	  ○ Can I ensure the availability of data in the event of any and all types of outage including disaster events? (e.g. through off site backup data that is accessible to your agency)
	  ○ How much time does it take for my data and the services that I use to be recovered after a disaster and do the vendor's other customers that are larger and pay more money than me get prioritisation?
	  ○ If I accidentally delete a file, email or other data, how much time does it take for my data to be partially or fully restored from backup, and is the maximum acceptable time captured in the SLA?
	• The Australian Department of Defence paper *Cloud Computing Security Considerations* provides a range of questions to identify the service performance risks associated with cloud computing. It is suggested that agencies pay particular attention to the following:
	  ○ (19f) Vendors guarantee of availability
	  ○ (19g) Impact of outages
	  ○ (19h) SLA inclusion of scheduled outages
	  ○ (19i) SLA compensation
	• Is there a risk that upgrade to cloud hardware and/or software by the CSP could introduce an incompatibility with the agency's hardware/software, meaning there is a risk of data loss or of records not being readable on return?
	• Will I incur additional costs to ensure adequate availability of my data?
	  ○ Do I need to consider the use of multiple cloud computing providers depending on the business criticality of the system deployed to the cloud, and if so how will this affect to overall TCO and risk profile of my sourcing decision?
	  ○ Will I spend additional money to replicate my data or business functionality with a second vendor that uses a different data centre and ideally has no common points of failure with the first vendor? This replication should preferably be configured to automatically 'failover'

	• When restoring records, can the service provider ensure that the structure of records (not just the content) and associated metadata is maintained?
Mitigation considerations	• Develop a suitable overall solution architecture that aligns with the business outcomes required. • For each risk identified or requirement to be met there must be a binding contract clause/s to ensure the service provider meets their obligation. In situations where it is not possible to mitigate risks satisfactorily through contract clauses, the agency should consider whether there are any business process changes or continuities that could be put enacted to cover the risk.

6.2 Service performance

Queensland Government agencies typically have mature processes in place to ensure the effective performance of ICT systems deployed on their own networks. Agencies have developed application and infrastructure architectures which deliver optimal performance to end users. However, agency experience is comparatively immature with regards to performance management of ICT services from cloud providers. There are a number of challenges that can come into play:

- Certain cloud solution offerings will be dependent on internet connectivity and cloud providers cannot commit to service performance (quality of service, latency, reliability) for the internet component since it is not within their control.
- If an existing application has very stringent service levels and low latency requirements (that cannot be cost-effectively resolved by re-architecting the application) then it may be difficult to accommodate in the cloud.
- Sourcing database, application and presentation layers from different cloud providers could introduce network latency issues that adversely affect user performance.

Risk	Service performance of the application/system 'in the cloud' may not meet business requirements

Questions for agency to address	• Is the network connectivity (between your agency users and the vendor's network) adequate in terms of traffic throughput (bandwidth), delays (latency) and packet loss?
	• Do you need to consider changes to your applications/architecture to achieve satisfactory service levels?
	• Does your application have extremely stringent service levels and low latency requirements? Can these requirements be relaxed/addressed by cost-effectively modifying the application prior to cloud deployment?
	• Does the SLA provide suitable performance guarantees? Is there adequate compensation for not meeting these guarantees?
	• Does the contract offer audit rights so customer can ensure compliance to terms and conditions including but not limited to:
	  ○ Right to audit provider's compliance to the agreement including rights of access to the providers premise where relevant records and customer data is being held
	  ○ Audit rights for the customer or its nominee, Auditor General, Privacy/Information Commissioner

	○ Right to appoint a commercial auditor or its nominee ○ Where possible the right to remote monitor access to its data and where not that the provider maintains an audit log that is available upon request ○ Right to review provider standards certification audit results where relevant.
Mitigation considerations	Agencies may need to consider whether changes to their applications/architecture would be necessary to achieve satisfactory service levels in a cloud environment. Business process contingencies may be required to ensure business continuity can be maintained in situations where service levels of certain components cannot be guaranteed. Agencies will need to ensure that contracts established with cloud providers contain prescriptive requirements regarding performance and that compliance with these requirements can be accurately measured by KPIs. Agencies will need to actively track SLAs and hold vendors accountable for failures.

6.3 SLA/incident management

Risk	Service provider will not respond to incidents (security or otherwise) in an effective and timely manner.
Questions for agency to address	The Australian Department of Defence paper *Cloud Computing Security Considerations* provides a range of questions (to ask cloud service providers) regarding the handling of security incidents. Many of these questions can also be modified to apply to any type of incident (not just security). It is suggested that agencies consider the following both from a security perspective and more generally in terms of other incidents: • (23a) timely vendor support • (23b) vendor's incident response plan • (23c) training of vendor's employees • (23d) notification of security incidents • (23e) extent of vendor support • (23e) extent of vendor support • (23f) my access to logs • (23g) security incident compensation • (23h) data spills.
Mitigation considerations	Agencies will need to ensure that service provider practices and contract satisfactorily address the questions highlighted above.

6.4 Security

The best practice security approaches for traditional on-premises IT delivery are relatively mature and well understood. Cloud computing, by contrast is a rapidly evolving area and represents a new challenge for security professionals who are more familiar with traditional environments.

Much of the information that agencies have traditionally been able to protect within the perimeter of their own networks will be shifted to the cloud. Agencies may have limited ability to prescribe the security controls employed within cloud environments but they will nonetheless remain responsible for the information that is stored and processed in the cloud. Agencies will need to adapt security models to suit cloud computing environments and consider end-to-end security.

A primary consideration for moving applications and data to the cloud is that a level of trust needs to be established (and contracted) through verification of cloud providers operating procedures and governance controls. Agencies will need to ensure that cloud computing service providers are sufficiently transparent, have adequate security and management controls, and provide the information necessary for the agency to assess and monitor the effectiveness of those controls.

The Office of the Information Commissioner advises[6] that:

> *'Agencies are required to ensure that personal information is properly protected against loss and unauthorised access, use and disclosure. This means agencies will have to consider the security a cloud provider will apply to their information and whether this complies with the privacy principles. Agencies might also wish to consider whether the agreement obliges the provider to notify the agency if the security is breached'*

There is a significant amount of freely available collateral (from vendors, analysts, governments, end users etc.) regarding security risks. Agencies are free to utilise whatever resources/research they see fit in assessing security risks, however the following two resources in particular are recommended for consideration:

(1) The Australian Department of Defence (DSD) paper *Cloud Computing Security Considerations*	This document provides a range of questions to identify the security risks associated with cloud computing. It also provides advice in other areas such as business continuity and incident management. Relevant questions (for agencies to consider) from this document are noted throughout this guideline When referencing the DSD paper, agencies will note that some of the questions are contextual to the Australia Government (e.g. reference federal artefacts). Agencies should use those parts of the questions that are relevant to their situation.
(2) Cloud Security Alliance	Key references/tools Here include: Cloud Security Guidance > Refer to Security Guidance for Critical Areas of Focus in Cloud Computing GRC Stack Refer to https://cloudsecurityalliance.org/research/grc-stack/ for details. There are four primary artefacts in the GRC stack, however the two that are most relevant to agencies are the Cloud Controls Matrix (CCM) and the Consensus Assessments Initiative Questionnaire (CAIQ). These tools are designed to support both consumers and providers: • Consumers - as an assessment tool • Providers - As a public assertion of control maturity via the STAR certification program (https://cloudsecurityalliance.org/star/certification/)

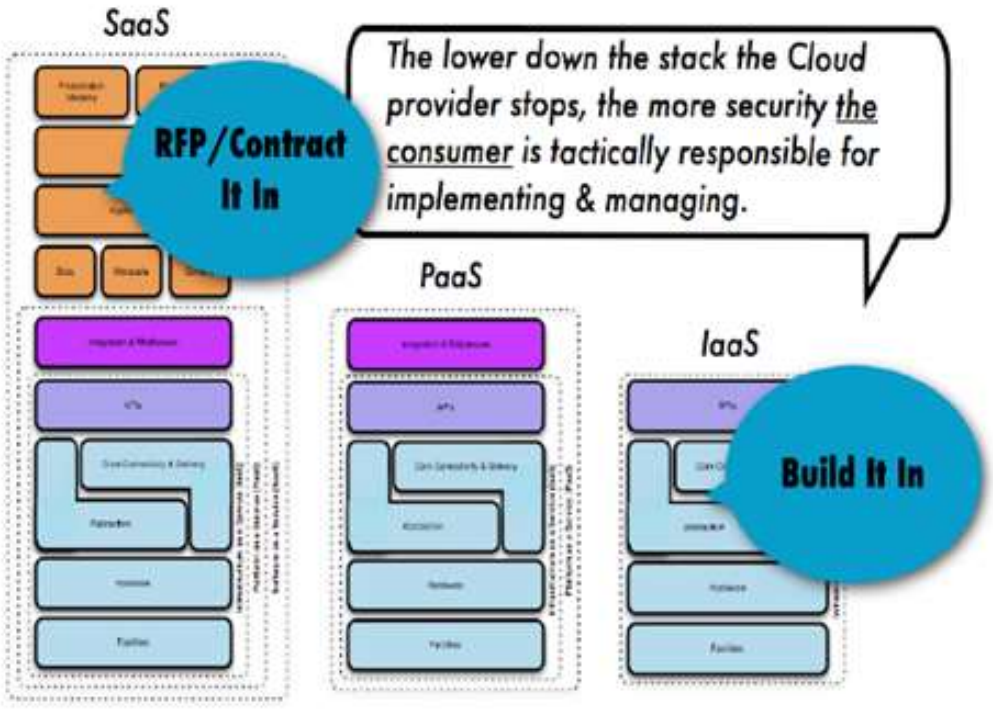
[6] Cloud Computing and the Privacy Principles (Section : 'Protection and Security')

It is important to realise that security risks, treatments and responsibilities will vary depending on the service model (SaaS, PaaS, IaaS) and deployment model (public, community, private, traditional) used.

The Cloud Security Alliance paper notes the following –

> *'In SaaS environments the security controls and their scope are negotiated in the contracts for service; service levels, privacy and compliance are all issues to be dealt with legally in contracts. In IaaS offering, whilst the responsibility for securing the underlying infrastructure and abstraction layers belongs to the provider, the remainder of the stack is the consumer's responsibility. PaaS offers a balance somewhere in between, where securing the platform falls onto the provider, but both securing the applications developed against the platform and developing them securely, belong to the consumer. Understanding the impact of these differences between service models and how they are deployed is critical to managing the risk posture of an organisation.'*

The figure below[7] depicts the different security responsibilities/approaches required for different service models:



The primary risk areas to consider are outlined below. As noted above, the depth and breadth to which agencies need to consider these risks will vary depending on service/deployment model. Agencies should exercise their judgement on depth of analysis required on a case by case basis.

The higher the classification of information the greater emphasis agencies need to place on assuring themselves that adequate controls are being implemented and maintained in line with the risk assessment. For Protected and Highly Protected data in particular, Agencies should ensure that all of the questions below and suggested mitigations are addressed.

[7] Security Guidance for Critical Areas of Focus in Cloud Computing

Risk	Unauthorised access by a third party.
Questions for agency to address	The Australian Department of Defence paper *Cloud Computing Security Considerations* provides a range of questions to identify the security risks associated with cloud computing. It is suggested that agencies pay particular attention to the following: • (21a) Customer segregation • (21b) Weakening my security posture • (21c) Dedicated servers • (21d) Media sanitisation • (20e) Data encryption technologies • (20g) Vendor's remote monitoring and management • (20j) Gateway technologies • (20k) Gateway certification • (20m) Policies and processes supporting the vendor's IT security posture • (20n) Technologies supporting the vendor's IT security posture • (20o) Auditing the vendor's IT security posture • (20p) User authentication • (20q) Centralised control of data • (20r) Vendor's physical security posture • (20s) Software and hardware procurement.
Mitigation considerations	• The vendor of the proposed cloud solution should be asked to provide information about any compensating controls or means by which they will mitigate any identified risk as part of the analysis phase. • An increasing number of vendors will have their service assessed/ described against industry benchmarks. An agency could for example ask their service provider to describe how their controls align to those of the Cloud Security Alliance[8]. • Is the cloud service provider compliant with or certified against industry best practise standards: (ISO 27001, PCI-DSS, FedRAMP, NIST 800-53 etc.). It may be cost prohibitive for agencies to conduct these assessments themselves even if the CSP is willing to allow client security audits. Independent accreditations provide greater assurance over CSP self-assessment however the agency needs to diligent to understand the scope and validity that the assessment provides (e.g. PCI-DSS accreditation may be for a small subset of the CSPs infrastructure and operations and it may not apply to the services that the agency is receiving). Certifications of this nature are particularly relevant for *Protected* and *Highly Protected* workloads. • Agencies can use contractual arrangements to mitigate/minimise security risks associated with cloud sourcing, by : ○ specifying the necessary protective security requirements in the terms and conditions of any contractual documentation (including sub-contractual arrangements), and

[8] Cloud Security Alliance, Cloud Controls Matrix: https://cloudsecurityalliance.org/research/ccm/

	○ verifying that the contracted service provider complies with the terms and conditions of any contractual documentation. • Agencies should consider including a mandatory breach notification clause in all agreements with cloud providers. This will oblige the cloud provider to tell the agency in a timely manner if there has been an incident which may have impacted on the security of its data; this, in turn, will let the agency take steps to minimise the negative impacts of such a breach. • For each risk identified or requirement to be met there must be a binding contract clause/s to ensure the cloud provider meets their obligation. In situations where it is not possible to mitigate risks satisfactorily through contract clauses, the agency should consider whether there are any business process changes or continuities that could be put enacted to cover the risk.

Risk	Unauthorised access by the service provider's employees.
Questions for agency to address	The Australian Department of Defence paper *Cloud Computing Security Considerations* provides a range of questions to identify the security risks associated with cloud computing. It is suggested that agencies pay particular attention to the following: • (22a) Data encryption key management • (22b) Vetting of vendor's employees • (22c) Auditing vendor's employees • (22d) Visitors to data centre • (22e) Physical tampering by vendor's employee's • (22f) Vendors subcontractors.
Mitigation considerations	• The vendor of the proposed cloud solution should be asked to provide information about any compensating controls or means by which they will mitigate any identified risk as part of the analysis phase. • An increasing number of vendors will have their service assessed/ described against industry benchmarks. An agency could for example ask their service provider to describe how their controls align to those of the Cloud Security Alliance[9]. • Is the cloud service provider compliant with or certified against industry best practise standards: (ISO 27001, PCI-DSS, FedRAMP, NIST 800-53 etc). It may be cost prohibitive for agencies to conduct these assessments themselves even if the CSP is willing to allow client security audits. Independent accreditations provide greater assurance over CSP self-assessment however the agency needs to diligent to understand the scope and validity that the assessment provides (e.g. PCI-DSS accreditation may be for a small subset of the CSPs infrastructure and operations and it may not apply to the services that the agency is receiving).

[9] Cloud Security Alliance, Cloud Controls Matrix: https://cloudsecurityalliance.org/research/ccm/

	• Agencies can use contractual arrangements to mitigate/minimise security risks associated with cloud sourcing, by:
	  ○ specifying the necessary protective security requirements in the terms and conditions of any contractual documentation (including sub-contractual arrangements), and
	  ○ verifying that the contracted service provider complies with the terms and conditions of any contractual documentation.
	• Agencies should consider including a mandatory breach notification clause in all agreements with cloud providers. This will oblige the cloud provider to tell the agency if there has been an incident which may have impacted on the security of its data; this, in turn, will let the agency take steps to minimise the negative impacts of such a breach.
	• For each risk identified or requirement to be met there must be a binding contract clause/s to ensure the cloud provider meets their obligation. In situations where it is not possible to mitigate risks satisfactorily through contract clauses, the agency should consider whether there are any business process changes or continuities that could be put enacted to cover the risk.

Appendix A References

A.1 Queensland Government

- Public Records Act 2002
- Financial Accountability Act 2009
- Information Privacy Act 2009
- Cloud Computing and the Privacy Principles
- Procurement and disposal of ICT products and services (IS13)
- Information Security (IS18)
- Information security external party governance guideline
- Internet (IS26)
- Information Standard 31: Retention and disposal of public records (IS31)
- Information access and use policy (IS33)
- Information Standard 40: Recordkeeping (IS40)
- Public Records Brief : Managing the Recordkeeping Risks associated with Cloud Computing
- Queensland Government Enterprise Architecture 2.0
- Government Informational Technology Contracting Framework
- Queensland Government Information Security Classification Framework
- Risk Management Guideline - DSITIA
- A guide to risk management - Queensland Treasury

A.2 Australian Government

- Australian Government Cloud Computing Policy – July 2013, AGIMO
- Better Practice Checklist - Privacy and Cloud Computing for Australian Government Agencies - February 2012, AGIMO
- Better Practice Guide - Financial Considerations for Government use of Cloud Computing - February 2012, AGIMO
- Better Practice Guide - Negotiating the cloud - legal issues in cloud computing agreements - February 2012, AGIMO
- Australian Government Policy and Risk Management guidelines for the storage and processing of Australian Government information in outsourced or offshore ICT arrangements – July 2013, Attorney General's Department
- Cloud Computing Security Considerations – updated Sept 2012, Australian Department of Defence (Defence Signals Directorate)
- Information Privacy Principles – Office of the Australian Information Commissioner
- Information Security Management Guidelines – July 2011, Attorney General's Department

A.3 Other

- Advice on managing the recordkeeping risks associated with cloud computing – CAARA : Council of Australasian Archives and Record Authorities
- Victorian Cloud Computing standards, policy and guidelines – June 2013, Public Record Office Victoria
- Cloud Risk Decision Framework – Microsoft Australia Pty Ltd
- Cloud Computing Code of Practice – Institute of IT Professionals New Zealand

- Security Guidance for Critical Areas of Focus in Cloud Computing – Cloud Security Alliance
- GRC Stack – Cloud Security Alliance