Queensland Government Enterprise Architecture

ICT-as-a-service risk assessment - guideline

Final

February 2014

v1.0.2

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* 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

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

Figures

1 Introduction

1.1 Purpose

A Queensland Government Enterprise Architecture (QGEA) guideline provides information for Queensland Government agencies on the recommended practices for a given topic area. Guidelines are generally for information only and agencies are not required to comply. They are intended to help agencies understand the appropriate approach to addressing a particular issue or doing a particular task.

This document provides guidance to support an agency in making informed and evidence-based decisions to either transition an ICT workload (system/application/data) to an as-a-service model (cloud, managed service) or to deliver via an in-house traditional approach.

1.2 Background

The Queensland Government has identified[1] that it will adopt an ICT-as-a-service strategy and source ICT services, especially commodity ICT services, from private providers in a contestable market. Cloud computing is a key enabler of this ICT-as-a-service vision.

Queensland Government will take a 'Cloud-First' approach to the sourcing of ICT functions, requiring agencies to consider cloud-based solutions in preference to traditional ICT investments wherever feasible and cost-effective.

While the first preference is to source new capabilities and replacements for existing systems from the cloud, it is expected that some business services may not be able to be met by cloud services at this time. The resultant state, where some services are cloud delivered while others are delivered by traditional IT is referred to as hybrid IT.

Cloud computing is an emerging way to deliver ICT services. While it presents many opportunities, there are many challenges. Cloud computing standards and practices are still developing. It is highly recommended that a risk-based approach be followed when considering cloud computing services. This guideline provides such an approach allowing for business requirements and user-base, information security classification, legal and privacy requirements.

1.3 Audience

This document is primarily intended for:

- Business system owners
- ICT systems managers
- ICT security managers
- ICT network managers
- ICT strategic managers
- ICT investment and planning managers
- ICT architects
- Financial and procurement managers
- Information management specialists

[1] In the *ICT Audit, Cloud Computing Strategy, Commission of Audit report* and *Qld ICT Strategy*

- Legal officers

1.4 Scope

1.4.1 In scope

This guideline applies to all Queensland Government departments and agencies.

This guideline applies generally to domains within the technology, business, information and application layers of the QGEA.

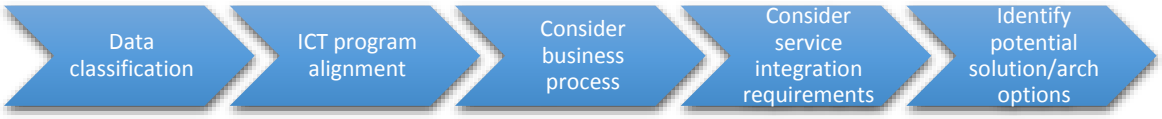
1.5 Related documents

The *ICT-as-a-Service risk assessment annexe – risks/considerations* provides supporting detail for this guideline. The annexe is focussed on providing further details regarding key as-service risks, and potential mitigations, that agencies should consider during their risk assessment of as-a-service service options.

This guideline (and the annexe) is part of a broader set of artefacts which collectively form the ICT-as-a-service Decision Framework. Refer to the *ICT-as-a-service Decision Framework – Overview* for details of all related documents.

2 Pre-requisites

Agencies need to consider and address a number of prerequisites before they are in a position to properly consider as-a-service sourcing options.



2.1 Classify Data according to QGISCF

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

Prerequisite - Data must be classified according to the QGISCF

2.2 Ascertain relevant current ICT portfolio

The complexity of planning for transitioning to as-a-service sourcing options will be alleviated if agencies have already collated ICT portfolio and enterprise architecture details of the current state of the system/s under consideration including

- inventory of information assets, applications and technologies
- understanding of the application integration, information exchanged and data flows between applications, including formats, volume, and ownership of information
- assessments of business criticality and significance of information assets, applications and technologies, and the organisation's maturity in business continuity planning
- operational costs of ICT assets in the portfolio
- existing resources and skillsets for ICT support, vendor and contract performance management.

Much of this information is typically collected by agencies as part of existing ICT baseline activities.

Prerequisite – Agencies should use the existing details of their current ICT portfolio and enterprise architecture as input to the analysis of as-a-service sourcing options.

2.3 Ensure ICT program alignment

Agencies will need to ensure that their individual ICT sourcing decisions do not inhibit or overly complicate the ability for government to achieve outcomes in other key programs. Agencies need to maintain an awareness of government vision and directions and consult with other agencies where necessary to verify whether:

- They should proceed to source the workload independently; or
- They should proceed to source the workload independently but modify certain attributes regarding the application/infrastructure to support integration with other programs; or
- They should not proceed to source the workload independently, but instead work with other agencies to define requirements and consider sourcing options collectively.

Prerequisite – Agencies need to ensure that their sourcing approach is aligned with broader agency and Queensland Government programs.

2.4 Consider business process

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. Challenging/changing a business process may:

- enable a workload to be cloud-sourced that might otherwise have been considered unsuitable for cloud
- enable a more cost-effective outcome – for example, instead of sourcing an IaaS solution to support a customised application, an agency might instead modify business processes and acquire an SaaS solution.

Prerequisite – Agencies should be open to the possibility of challenging existing business processes in order to maximise the possibility of using cloud services.

2.5 Consider service integration requirements

Using services from the cloud presents challenges to agencies when those services need to integrate with agency systems that are not in the cloud, or alternatively when integration is required between multiple services from different cloud providers. The potential exists for inadvertent creation of ‘islands’ of cloud technologies or solutions that will reduce interoperability across cloud types and associated implementations.

Prerequisite – Agencies need to be mindful **up front** of how they spit application/ workload sourcing. For example, splitting collaboration components into multiple separate sourced solutions may not provide as feature rich an experience as sourcing these as a bundle.

2.6 Identify potential solution/architecture option/s

This guideline can be used by an agency to help assess the risk of their preferred solution or architecture. It can also provide guidance on other sourcing approaches that an agency should consider in the event that the risk of their preferred approach is found to be unacceptable. Agencies must however have some idea up front of potential solution/architecture approaches in order to undertake a risk assessment.

It is assumed that agencies using this guideline will have identified either

a) a preferred solution (e.g. public cloud email system – Office 365, Gmail etc.) or
b) a preferred service model (e.g. SaaS, PaaS, IaaS) and deployment model (public cloud, community cloud, private cloud, Traditional IT).

Agencies that require guidance selecting the right architecture for their ICT workload should refer to the following artefacts:

- *ICT-as-a-service service model selection* and/or
- *ICT-as-a-service deployment model selection*

Prerequisite – Agencies should have an initial idea of preferred solution and/or architecture (service/deployment model) prior to using this guideline.

2.7 Consider existing and emerging sourcing alternatives

The ICT Commission of Audit identified priority applications within the Queensland Government application portfolio that are commoditised sufficiently for urgent consideration as candidates for public SaaS cloud. These are:

- email
- Collaboration including IP telephony
- office productivity suite
- customer relationship management

Other areas identified for cloud sourcing include:

- finance/payroll systems also identified in the ICT Commission of Audit for outsourcing
- trusted community IaaS panel

Some of these cloud opportunities (and others) may be pursued at a whole-of-government level. In other cases, individual agencies may pursue the opportunity. In such circumstances these agencies could potentially act as lead agency in establishing contracts/procurement arrangements on behalf of the Queensland Government.

Over time as cloud services are adopted across the Queensland Government, the potential for re-using existing cloud services or leveraging off existing sourcing arrangements becomes possible. Cloud services could be re-used as a whole or in part as a direct fit or with minor changes or with some business process changes.

Prerequisite – Agencies should consider use of existing and emerging cloud sourcing arrangements via the Queensland Government CloudStore[2] wherever possible.

[2] Refer to the *Queensland Government Cloud Computing Implementation Model* for further details about the CloudStore

3 Risk assessment[3]

ICT workloads will need to be subjected to a formal risk assessment to determine the preferred sourcing approach.

Agencies are required[4] to establish and maintain appropriate systems of internal control and risk management and should already have well established risk management frameworks in place. The *Australian Standard AS/NZS ISO 31000:2009: Risk Management – Principles and Guidelines* typically forms the basis for agency risk management frameworks. The figure below depicts the key process steps.

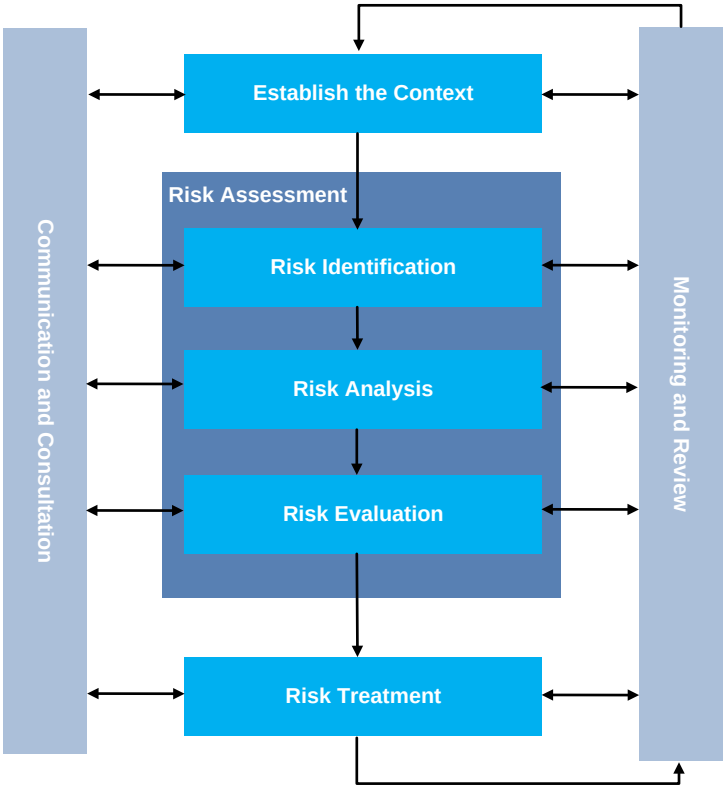


Figure 1: Overview of the risk assessment framework.

It is important to involve a wide range of stakeholders, from different disciplines within the agency - such as business, finance, security, business continuity planning, legal and IT, and ensure that the business owners of the information assets, application and associated technologies are included during the process and at final sign-off on conclusion.

The ICT-as-a-service provider, all subcontractors in the service provision supply chain and components of the agency business area providing the business service which will be using the service provider, must be subject to the risk assessment.

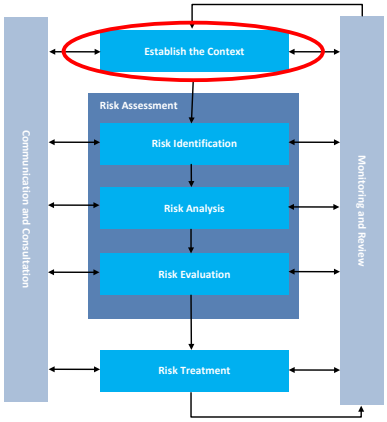
The aim of this guideline is to assist agencies in developing a risk assessment when considering an ICT-as-a-service sourcing approach. It outlines the key **ICT-as-a-service** considerations/risks that agencies should address as part of their existing risk management framework processes.

[3] Generic (i.e. non-cloud) content in this section is extracted, for the most part, from the DSITIA Risk Management Guideline and A Guide to Risk Management developed by Queensland Treasury and

[4] Under the *Financial Accountability Act 2009*

3.1 Establish the context

The purpose of this phase is to define the parameters within which risks will be managed and set the scope for the rest of the process. This phase is concerned with developing an understanding of the internal and external context within which the department or business area operates and the factors that may influence the achievement of objectives. It also establishes the risk management context (i.e. the organisation and parameters of the risk management task itself) and scope of the target system being assessed.



3.1.1 Understand the internal and external environment

Understanding the internal and external environment is part of a broader scanning activity and provides the platform for building strategic, business and operational objectives and understanding how the agency operates.

The primary influences on the **external environment** relate to the social, cultural, political, legal, regulatory, financial, technological and economic environments within which the agency operates. Agencies should consider what external factors are relevant to their situation, and factor these into their risk assessment process. Some examples include:

- Queensland Government information standards/policies/frameworks
- State/Federal Statutory/Legislative Requirements e.g. *Public Records Act 2002*, *Information Privacy Act 2009*
- foreign laws and potential jusisdictional access to information, and
- The expectations and strategic direction of the Queensland Government (eg. as-a-Service, cloud-first philosophy)
- the need to integrate solutions with the Queensland Government CloudStore
- community and industry expectations
- product roadmaps and the stability of the cloud vendor marketplace and offerings.

Influences on the **internal environment** may include:

- the agencies governance and accountability structures
- policies, standards and guidelines (and the extent to which they facilitate or impede cloud service take-up)
- resources availability with the agency (for example, information systems, staffing and funding)
- organisational readiness (in terms of ability to support/manage cloud services)
- nature and extent of contractual relationships (and the extent to which these may impede transition to cloud services)
- the agency culture, including the security culture
- existing risk management expertise and practices
- budget/financial/timing constraints
- ICT architecture and technical constraints.

3.1.2 Risk management context

The risk management context refers to the organisation and parameters of the risk management task itself. Key considerations include:

- risk appetite
- risk tolerance
- risk impact and likelihood
- risk matrix and responsibilities
- risk rating responses
- risk management maturity

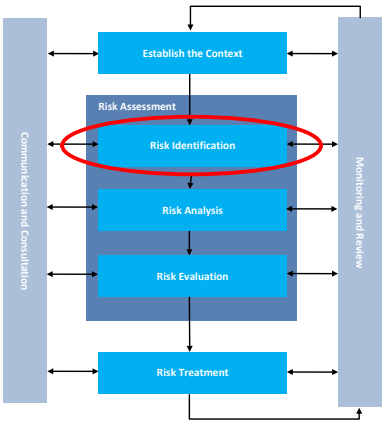
The agency's risk management framework will outline the preferred treatment/tools in these areas.

3.1.3 Scope of the target system

It is necessary to clarify the boundaries/scope of the system being targeted (e.g.- what it contains and what it entails, integration points with associated upstream and downstream systems). It is also important to ensure that the context identifies what is NOT part of the scope of the evaluation.

3.2 Risk identification

Risk identification involves identifying the possible risk events that may impact on the agency, the most likely cause, and the consequence and impact of the event. The risk identification process should be broad and comprehensive, since the risks identified will form the basis of the assessment process.



Agencies need to identify risks associated with the proposed sourcing approach for the ICT workload. As depicted below, the risks that need to be identified will depend on the focus of the overall assessment. Risks may need to be identified for a cloud solution, managed service solution or agency supported solution.

The table below list some suggested risks for consideration (agencies may choose to add others). The list has primarily been developed with *Cloud sourcing* in mind. However it is also applicable (for the most part) to managed service arrangements.

Risk domain	Risk control area	Risk/s
Business	Workforce capability and organisational change management	The agency may not have the capacity and capability to support the cloud solutions in their target operating environment.
	Data classification maturity	Incorrect classification could lead to incorrect controls
	Business models and processes	The cloud service may impact interrelated and inter-dependent business processes, policies, practices and systems.

Risk domain	Risk control area	Risk/s
	Procurement and contract management	The agency may not have suitable expertise/ maturity to establish legal contracts for Cloud services and to manage ongoing contract performance
Technical	Service management tools	The agency may not have suitable tools and/or access to properly monitor and manage the service provider.
	Service integration and interfaces	Unable to make business applications interoperate effectively between different cloud providers, or between cloud providers and traditional IT systems hosted on agency networks.
		There is potential for increased security risk and/or data leakage if interfaces and data exchanges are ill-defined.
Strategic	Industry/vendor maturity	The service provider may not have the capacity and capability to support the cloud solution in line with business expectations.
	Reputation/political	Damage to Queensland Governments reputation resulting from a privacy or security breach.
	Portability	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.
	Financial	Cloud service for the workload may not represent value-for-money for the Queensland Government.
Information, data and recordkeeping management	Privacy and confidentiality	Risk of compromise to confidential information through third party access to sensitive information. This can pose a threat to ensuring the protection of intellectual property, and personal information.
		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 Cloud Service Provider (CSP) 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.
	Data ownership	Agency will be unable to meet its statutory/regulatory requirements for retention, maintenance and preservation of data/records.
		Records not being disposed of in a timely way, once authorised by the State Archivist.
	Data integrity and authenticity	If an organisation 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

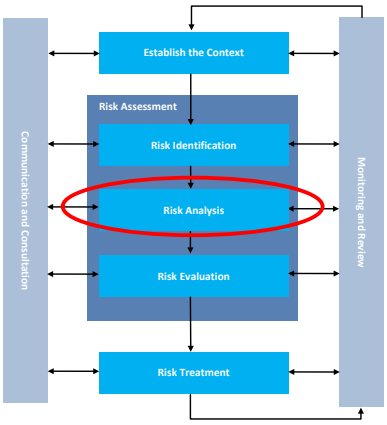
Risk domain	Risk control area	Risk/s
		value as evidence. In addition the evidential value of records may be affected if appropriate audit trails and descriptions of management processes performed on records while they are kept in cloud computing systems are not maintained.
Operational	Business continuity and disaster recovery	Access to information or records may be lost, or not provided in a timely way.
	Service performance	Service performance of the application/system may not meet business requirements.
	SLA/incident management	Service provider will not respond to incidents (security or otherwise) in an effective and timely manner.
	Security	Unauthorised access by a third party, the service provider's employees, the service provider's customers or an unidentified party.

Further details about the risks listed above can be found in the *ICT-as-a-service risk assessment guideline annexe – risks/considerations* document

3.3 Risk analysis, evaluation and treatment

The risk analysis, evaluation and treatment steps are not typically considered separately. They are interrelated processes which need to be considered by the agency simultaneously.

3.3.1 Risk analysis



Risk analysis is about developing an understanding of the risk in order to determine the level of risk and make decisions about how the risk should be treated. Risk analysis will result in determining the risk level or risk rating for each identified risk. It involves developing an understanding of each risk, its consequences and the likelihood of the risk occurring. The risk analysis will inform the evaluation of risks, whether risks need to be treated and the selection of the most appropriate risk treatment strategy.

Agencies will need to assess the likelihood and consequence of each risk occurring (taking into account existing controls). The process for analysing risk will differ from agency to agency. All agencies will utilise some sort of risk matrix mapping and 'dashboard' representation similar to that depicted below to identify a rating (e.g. low, medium, high, extreme) for each risk.

	CONSEQUENCE				
LIKELIHOOD	Insignificant	Minor	Moderate	Major	Critical
Rare	LOW Accept the risk Routine management	LOW Accept the risk Routine management	LOW Accept the risk Routine management	MEDIUM Specify responsibility and treatment	HIGH Quarterly senior management review
Unlikely	LOW Accept the risk Routine management	LOW Accept the risk Routine management	MEDIUM Specify responsibility and treatment	MEDIUM Specify responsibility and treatment	HIGH Quarterly senior management review
Possible	LOW Accept the risk Routine management	MEDIUM Specify responsibility and treatment	MEDIUM Specify responsibility and treatment	HIGH Quarterly senior management review	HIGH Quarterly senior management review
Likely	MEDIUM Specify responsibility and treatment	MEDIUM Specify responsibility and treatment	HIGH Quarterly senior management review	HIGH Quarterly senior management review	EXTREME Monthly senior management review
Almost Certain	MEDIUM Specify responsibility and treatment	MEDIUM Specify responsibility and treatment	HIGH Quarterly senior management review	EXTREME Monthly senior management review	EXTREME Monthly senior management review

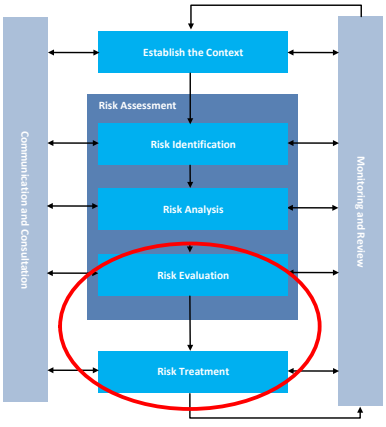
Agencies may use different categories for likelihood/consequence, or have differing criteria/thresholds for each category, or even have different risk ratings than those shown above. These variations do not matter. The point is that agencies will arrive at a per risk assessment as follows[5]:

Risk	Likelihood	Consequence	Rating	Risk Owner
Risk 1	…	…	…	…
Risk 2	…	…	…	…
..etc	…	…	…	…

Agencies will often expand on the table above to outline the variation in likelihood/ consequence based on *inherent* risk versus *residual* risk (refer to your agency's risk management framework to determine if this approach is applicable).

3.3.2 Risk evaluation/treatment

The purpose of *risk evaluation* is to make decisions based on the outcomes of risk analysis about which risks are acceptable, which risks need treatment and the treatment priorities. The highest priority should be given to those risks that are evaluated as being the least acceptable. To treat unacceptable risks, agencies may improve existing controls or develop and implement new controls.



The risk evaluation stage involves the following key steps:

1. determine treatment actions using risk rating responses (refer to your agency risk management framework for details)
2. determine the risk target (refer to your agency risk management framework for details)

[5] The risks in this table will be those identified during the risk identification step. Note - A

3. determine the treatment decision

The decision about how to treat a risk is based on the relationship between their current risk rating and the target risk rating.

- Where the current risk rating is higher than the target risk rating, risk treatment options should be undertaken to reduce the risk to the required target.
- Where the current risk rating is the same or lower than the target risk rating, the risk can be accepted and monitored.

It is important that risks are treated appropriately to reduce the risk to a level that is tolerable to the agency. It is also important that mitigation efforts are focussed on priority risk areas. In some instances the risk target may be high despite the risk tolerance of the agency. This could occur in situations where no amount of reasonable mitigation treatment will effectively reduce the risk to a normally tolerable level.

When determining the treatment decision consider:

- The causes of the risk and whether they are within the agency's ability to manage
- The effectiveness of existing controls to manage the causes of the risk
- What resources would be required to implement treatment actions and what is the expected change to risk level?
- The cost of implementing each treatment option against the benefits derived from it
- The impact should the risk still occur despite the treatments applied
- The gap between the current risk rating and the risk target.

The following treatment options are possible:

Treatment	Definition
Reduce	The agency can apply risk treatments/mitigations that reduce either the likelihood or consequence of the risk/s occurring to enable deployment of the preferred service. In many cases this will involve 'contracting in' provisions in the service provider contract to reduce overall solution risk. The *ICT-as-a-service risk assessment annexe – risks/considerations* document outlines potential mitigation options that agencies may wish to consider for different risks. The list is not exhaustive - agencies will need to consider a range of different mitigation options on a case-by-case basis.
Avoid	Agency makes an informed decision not to proceed with deployment of a particular solution/architecture in order to not be exposed to a particular risk. There are numerous possible 'avoid' scenarios depending on the context and outcome of the evaluation. Scenarios include: • Avoid solution/vendor – Risk assessment might determine that although the proposed cloud sourcing approach is valid, the risks associated with a particular solution/vendor might be unacceptable. In this case other solutions/vendors offering similar solution/architecture would be assessed. • Avoid sourcing approach - It may be determined that risk associated with the

Treatment	Definition
	intended sourcing approach might be unacceptable, and that a change in overall approach is required, i.e. ○ workload is not suitable for *cloud*, consider a managed service, or ○ workload is not suitable for *managed service;* consider agency supported traditional IT deployment instead. • Avoid cloud service model – cloud sourcing might be valid but service model may need to be modified, for example change from BPaaS to SaaS, SaaS to IaaS etc. • Avoid cloud deployment model – cloud sourcing might be valid but deployment model may need to be modified, for example change from public to community cloud, community cloud to private. Note – In practice, Agencies may undertake a risk analysis for several potential options simultaneously as part of an overall options analysis (as opposed to doing risk assessment for one option at a time, finding out it was unsuitable and then starting all over)
Share/ transfer	Agency distributes risk with other parties. Potential options could include: • cloud insurance (this is an emerging field that enables some transfer of risk to a third party) • in certain circumstances, and for certain risk types, sharing risk at a whole-of-government level may be acceptable in those cases where doing so at an agency level had been deemed unacceptable. • shifting/sharing risk with the service provider may be an option for certain risk types. However it is more likely that this approach would be to *reduce risk* only since government agencies cannot 'outsource' risk for their regulatory/statutory requirements. Agencies are still ultimately responsible.
Accept	Determine that the agency can tolerate the risks introduced by the solution.

There may be a mixture of risk treatments applied – for example a combination of *reduce*, *share* and *accept* treatments could be applied across the range of individual risks to achieve an overall acceptable level of risk for a solution.

4 Practical application of this guideline

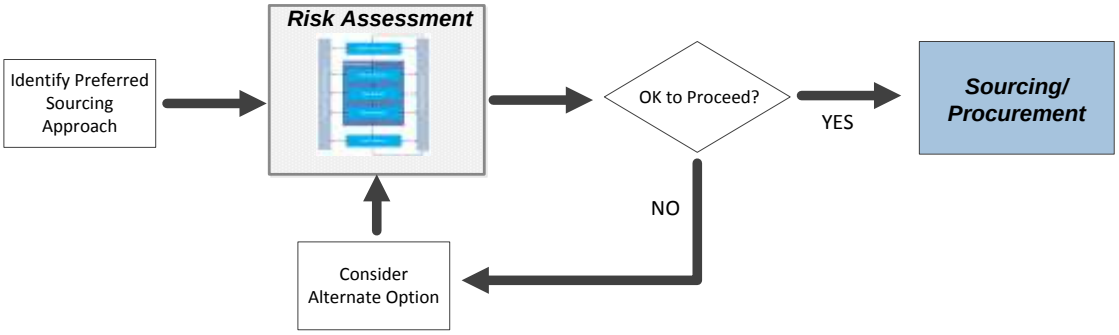
The way in which the risk assessment process is undertaken can vary depending on different situations.

4.1 Hybrid scenarios

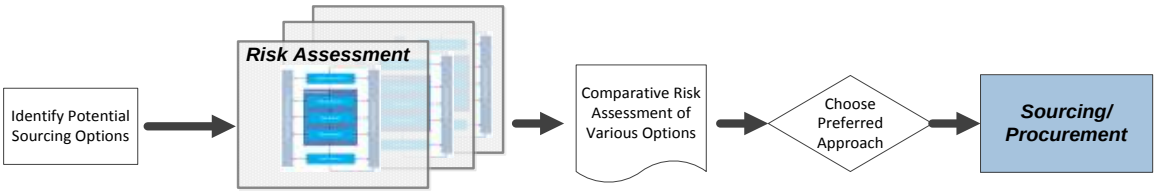
The process described in section 3 is focused on models where an entire workload is being sourced in one way. Hybrid models where some parts of a system are sourced in one way and other parts sourced in another way are not directly covered. However, an agency could in this instance still use this guideline by assessing each component separately. For example, an agency could do a risk assessment of two separate cloud components and then view results collectively to make an overall decision.

4.2 Assessing multiple options simultaneously

The risk assessment process outlined in section 3 has been described from the perspective of an agency having a single preferred solution/architecture that it wishes to assess. In the event that the solution/architecture is deemed to not be suitable then alternative options would need to be identified and risk-assessed separately. A high-level depiction of this process is provided below:



The process above was chosen because it makes it easier to focus on, and describe, the steps required for assessing a specific solution. In practice, an agency may not be as clear on their preferred solution/architecture and in this case they may instead choose an approach whereby multiple potential options are assessed simultaneously. Such an approach is depicted below:



4.3 Two-phase risk assessment

In practice, there may be a requirement to undertake two phases of risk assessment:

- Phase 1 : Pre-procurement
- Phase 2 : Procurement

Figure 2 depicts the process flow and key decision points associated with the traversal of an ICT workload through the risk assessment in this scenario.

Some workloads will have attributes that enable them to be filtered out during the pre-procurement phase while others will need to go through both phases before a preferred solution can be identified.

The depth of consideration in each risk area will vary for each phase. Some risk areas can be mostly assessed during the pre-procurement phase whilst others, particularly operational risks, cannot be properly assessed until vendor specific engagement occurs in the procurement phase.

4.3.1 Pre-procurement phase

The risk assessment undertaken during this phase will usually be part of a broader business case (/options analysis) activity with the focus on identifying the preferred sourcing approach and getting stakeholder 'buy-in' to proceed to procurement.

Typically during this phase, the agency would gather detailed information regarding agency capability/requirements and combine this with a generic market assessment of cloud service providers (CSP's) or managed service providers (MSP's). The CSP/MSP assessment would use publicly available information, preliminary vendor feedback, industry analyst reports etc. to make a decision; basically the idea is to gather as much research as possible to help inform risk assessment, short of going to a formal tender.

There are two primary decision paths that a workload follows from this point:

- not Suitable for cloud
- suitable for cloud

Not suitable for cloud

Risk analysis identifies that cloud sourcing would introduce an unacceptable level of risk (that cannot be satisfactorily treated/mitigated) across one or more of the risk control areas. In this circumstance the agency would need to examine *traditional IT* alternatives. The ICT-as-a-service philosophy of government should see agencies favour *managed service* options ahead of an *agency supported* approach; nonetheless a risk assessment of each approach is required. Potential outcomes are summarised below:

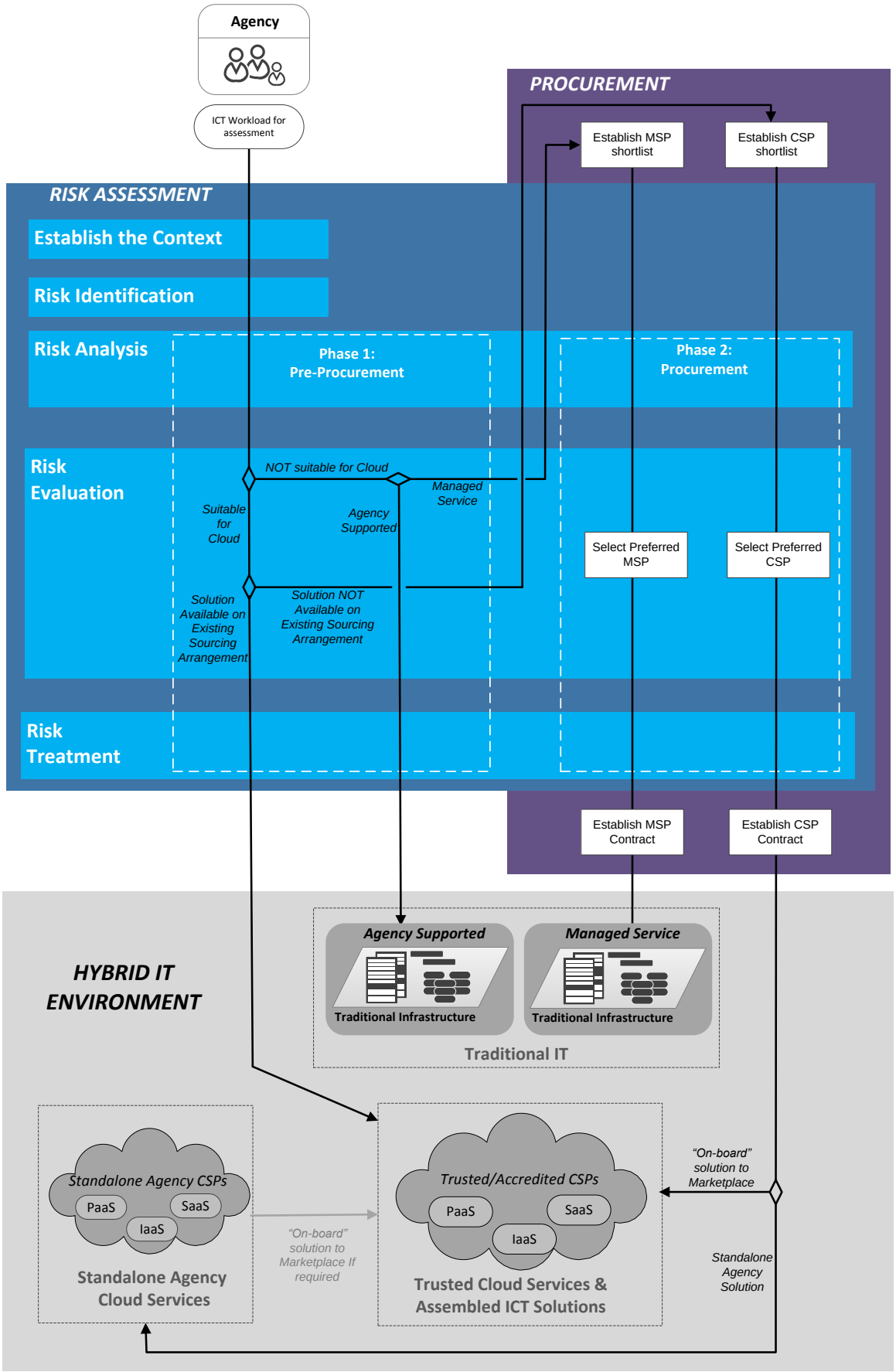


Figure 2: Two-phase risk assessment process

Option	Explanation	Next step (subject to approval)
Managed service	Risk analysis has identified that managed service risks are acceptable	Procurement phase – managed service provider (MSP)
Agency supported – traditional IT	Risk analysis has identified that an agency-supported approach is the only viable option for delivery of the ICT workload.	As depicted in Figure 2, It is assumed that agencies will not acquire additional localised capacity. Agencies should seek to reuse capacity that has been released via relocation of other workloads to the Cloud.

Suitable for cloud

Risk analysis has identified that cloud sourcing risks are acceptable, or can be mitigated sufficiently to proceed. Potential paths are summarised in the table below:

Option	Explanation	Next Step (Subject to approval)
Solution available via QG CloudStore	The preferred solution is available on an existing Queensland Government sourcing arrangement.	Source the solution from the Queensland Government CloudStore. The agency will need to treat any identified risks as part of the implementation.
No existing sourcing arrangement	There is no suitable solution available on an existing sourcing arrangement.	Procurement phase - CSP

At this point, information should exist to enable a decision to be made about the way forward. The outcome of the pre-procurement risk assessment would be compiled into a report for senior management consideration and approval[6]. Subject to signoff, sourcing/procurement of the preferred solution could proceed.

In certain risk/cost situations the Investment Review Committee (IRC) would need to review and approve the proposed approach/expenditure. The IRC will pay particular attention to any proposed expenditure on *traditional IT* systems since this approach is counter to the 'as-a-service' and 'cloud-first' philosophy of government. Key areas that the IRC will look for in such circumstances include the following:

- Agencies are able to demonstrate an evidence-based approach in support of their decision. This will include details of the options that were considered in reaching this decision (including consideration of business process changes) and the reasons these options were not feasible.
- Impediments/barriers identified through this process are often temporary in nature (e.g. industry maturity, agency maturity). In situations where impediments / barriers to adopting cloud servers have been identified, plans and timeframes for overcoming these obstacles should be provided. Agencies should endeavour to

[6] The process/templates for doing this will vary from one agency to the next.

resolve these impediments within the timeframes to facilitate cloud adoption as soon as possible. If no such timeframe is provided, the Investment Review Committee will set an appropriate timeframe

4.3.2 Procurement phase

The risk assessment undertaken during this phase will be part of a broader procurement activity often involving an invitation to offer (ITO). This phase allows specific assessment of vendor capability.

The vendor of the proposed cloud/managed service 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. If the system being analysed already has mitigating controls in place, the risk analysis should incorporate these and, therefore, the result found in the risk map should be the ‘residual risks’.

Note – A decision to avoid cloud/managed service could still occur as part of the risk analysis in the procurement phase. However, this should be rare since agencies will not typically go through the expense of an ITO without a high degree of confidence that at least one suitable provider exists in the market.

5 Guideline review

Cloud computing is a relatively new discipline in the ICT arena. The standards, legalities and work practices are rapidly developing. This guideline should be reviewed yearly until, at least, 2015.

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 –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
- Data Sovereignty and the Cloud report - Cyberspace Law and Policy Centre, UNSW