Queensland Government Enterprise Architecture

ICT-as-a-service deployment model selection - guideline

Final | February 2014 | v1.0.0 | PUBLIC

Purpose

This Queensland Government Enterprise Architecture (QGEA) guideline outlines key principles that agencies should consider when selecting their preferred deployment model for an ICT workload. This guideline is part of the *ICT-as-a-Service Decision Framework.*

Introduction

The Queensland Government has committed to a 'cloud-first' approach. This will require agencies to first consider cloud-based solutions in preference to traditional ICT investments, where those cloud services demonstrate value for money, are trustworthy and fit for purpose.

Cloud services provide a number of deployment model options that will suit different situations. The most common of these deployment models are:

- public cloud
- community cloud
- private cloud.

In situations where none of the models above are suitable then an agency may be required to consider a *Traditional IT* approach, i.e. where the ICT services are owned and operated by the Queensland Government or a contracted third party (managed service).

A *Hybrid* approach may be required in some circumstances where a combination of multiple cloud deployment models, or cloud in conjunction with Traditional IT, is required to achieve the desired outcome

ICT-as-a-service decision guidance

Agencies need to consider the following principles when choosing a deployment model:

1 Public cloud should be preferred where key considerations of security, availability and performance are satisfactorily met by standard offerings

Public cloud models will typically offer the lowest price point due to the economies of scale but it may not suitable for all use cases. Careful placement of workloads will be required to ensure the necessary service attributes (e.g. security, performance and availability) are obtained. Key considerations of these attributes should be used to differentiate each service offering when making placement decisions.

While a hybrid cloud delivery model comprising of public and community clouds may need to exist in the short to medium term, the long term strategic objective is to migrate as much of the Government's ICT portfolio as is possible to public cloud.

Public cloud solutions may be provided by companies that are not based in Australia. Agencies will need to balance this principle with industry development/SME support expectations specified the Queensland Procurement Policy.

2 Community cloud services should be explored where standard public cloud options are not suitable

The community cloud delivery model can represent a transitionary stage to full public cloud adoption. Agencies will be required to periodically re-assess their application portfolio as part of the annual ICT strategic planning process to determine whether the criteria that may have prevented workloads moving to a public cloud (e.g. legislative constraints, security, data privacy, performance characteristics, etc.) have been resolved. The trigger for review could also be an infrastructure re-fresh cycle, re-hosting, re-factoring, rebuilding or replacing of applications.

Community cloud scenarios could include:

- whole-of-government on-shore community cloud (e.g. IaaS) architected to meet Queensland government performance, availability and security requirements
- community-of-interest based clouds that are established for state, national, federal, or even international collaboration in certain areas. Examples could include health, law enforcement amongst others.

3 Agency ownership and support of ICT infrastructure is discouraged

The Independent Commission of Audit report, published in February 2013 recommended (#150) that government:

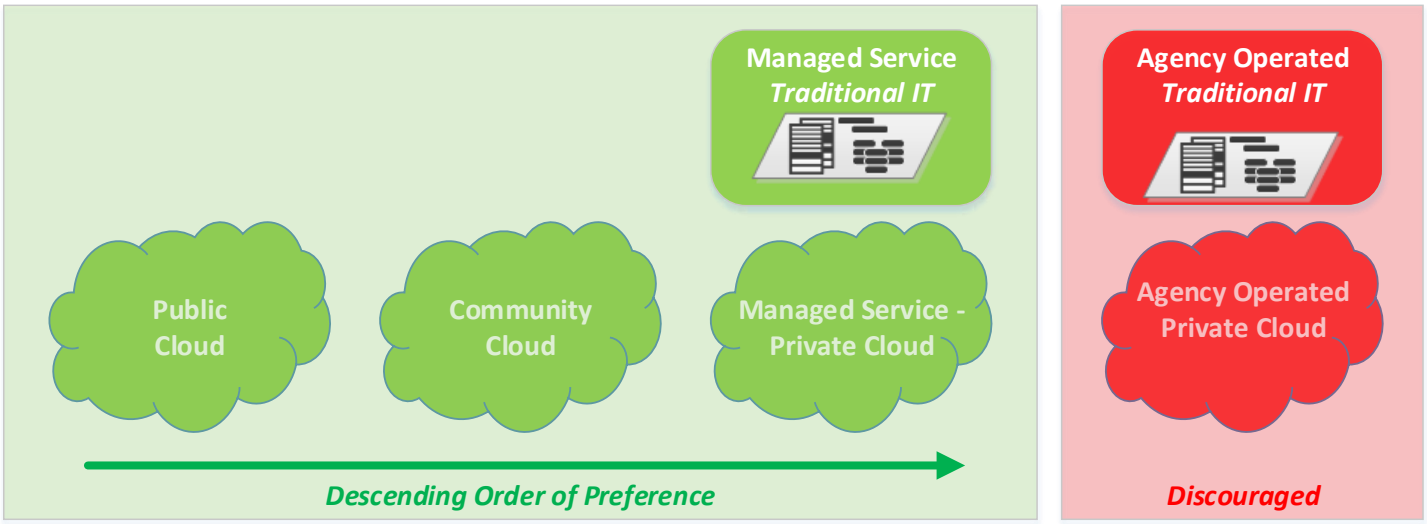
- adopt an ICT-as-a-service strategy
- use appropriate cloud-based computing and other emerging technologies
- discontinue its role as an owner and manager of significant ICT assets and systems
- implement a program to divest ICT assets and systems, with required ICT services to be purchased under contractual arrangements with private providers.

The Queensland Government accepted these recommendations.

Agencies will be actively discouraged from building private cloud computing infrastructure or traditional IT within their organisations and expansion of existing virtualisation infrastructure will be capped. Agency-operated (as opposed to managed service) *traditional IT* should only be considered for workloads with a classification of Protected or Highly Protected, or where market analysis has determined there is no suitable 'As-a-service' offering available.

Deployment model considerations

Based on the principles above, the high-level preference for ICT-as-a-service deployment models can be depicted as follows:



The philosophy depicted above is based on a value-for-money perspective. Generally speaking public cloud solutions will provide the lowest price point, whilst agency operated solutions will typically be the most expensive to operate. Clearly there are other factors besides cost which must be considered, and which will influence the selection of the preferred deployment model. These include:

Functional requirements

Agency functional requirements will be a primary factor in determining the most appropriate deployment model. Agency requirements in areas such as security, performance and availability may not be adequately met by certain cloud models. For example, If the ICT system/application has very stringent service levels and low latency requirements (that cannot be cost-effectively resolved by re-architecting the application) then it may not be an ideal candidate for an offshore public cloud solution.

Industry 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 certain deployment models may not be cost-effective for certain workloads. Agencies need to be comfortable that the market options are sufficiently mature (with proven track record) to meet their business requirements.

Service model selection

The deployment model options need to be considered in light of the desired cloud service model (See *ICT-as-a-service: Service model selection* document for further discussion on this). For example, while the public cloud deployment model applies to all service models (SaaS, PaaS, IaaS), the community cloud deployment model may be more likely to apply to IaaS (or hosted PaaS appliances).

Information security classification

As stated in the *ICT-as-a-service offshore data storage and processing policy*, departments must use the Queensland Government information security classification framework (QGISCF) to determine the information security classification of the ICT system/application/data being considered.

Information security classification provides a coarse-grain filter to further narrow down the deployment options that an agency should consider. The table below shows potential deployment models for each information security classification.

Cell colours are used to indicate the following:

- Red – Deployment models that are not permitted - Offshoring of Highly-Protected data is not permissible as per the ICT-as-a-service offshore data storage and processing policy
- Yellow - Deployment models where compliance with expected controls may be challenging. ICT workloads with a higher security classification will require controls and assurance that are often more achievable in non-public, onshore environments. The security/jurisdictional challenges posed by (public cloud) solutions in overseas environments for example may present compliance challenges for the expected controls relating to protected/highly protected data.

Blue –Blue is used in the above table to indicate deployment models that are considered more likely to be suitable for the information security classification in question. This is not a hard and fast rule. There may be individual market solutions where the security controls implemented in a public cloud for example may in fact be superior to those in a private cloud solution. These colours are just intended as “rule of thumb” guidance.

		ICT-as-a-service deployment models							
		Public cloud		Community cloud		Managed service-private cloud		Managed service – traditional IT	
		Offshore	Onshore	Offshore	Onshore	Offshore	Onshore	Offshore	Onshore
Information security classification	Public								
	Unclassified								
	X-In-Confidence								
	Protected			*	*				
	Highly Protected				*				

Note (*) – The highlighted community cloud scenarios **are** potentially acceptable where the nature of the community is such that the community has common trust, compliance, jurisdiction and security needs relative to the information in question. Also subject to restrictions by the information originator and their acceptance of the community cloud. For instance, Australian Government information at protected level may only be allowed in selected onshore community clouds.

Hybrid models

Hybrid Cloud options may also be applicable in certain cases - A particular cloud workload may be partitioned and split between one or more deployment models where the sub-components or sub-systems are assessed to different security classification levels. In such cases, the additional business value of partitioning the workload outweighs the additional complexity. For example, hosting the front-end of a multi-tier web application in a public cloud to benefit from highly scalable, global internet content distribution networks, while ensuring the more sensitive data processing and repositories reside in a community or managed arrangement.

Risk Assessment

The guidance provided above is intended to help guide agencies on narrowing down the range of potential deployment options that they may wish to consider for their particular ICT workload. Ultimately however agencies need to choose the option that they believe best meets their business requirements, and which satisfactorily balances requirements for security, availability and performance. The *ICT-as-a-service risk assessment guideline* should be used by agencies to assist in this determination