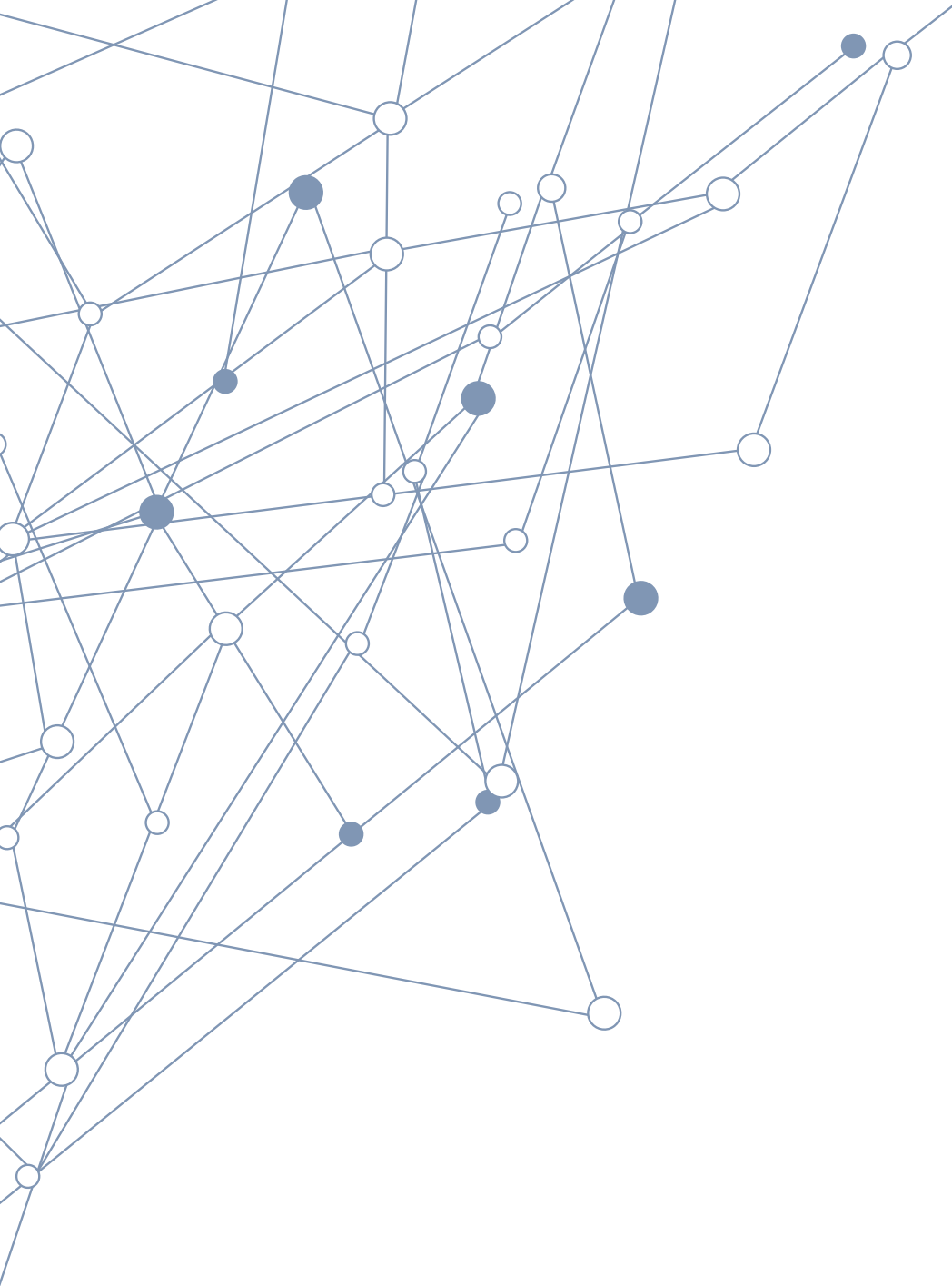


Queensland Government

# Cloud Computing Implementation Model

Supporting Queensland Government ICT reform

CLASSIFICATION: PUBLIC



Queensland Government Cloud Computing Implementation Model, © State of Queensland (Department of Science, Information Technology, Innovation and the Arts 2014

Published February 2014



This document is licensed under a Creative Commons Attribution 3.0 Australia licence. To view the terms of this licence, visit <http://creativecommons.org/licenses/by/3.0/au>. For permissions beyond the scope of this licence, contact [qgcio@qgcio.qld.gov.au](mailto:qgcio@qgcio.qld.gov.au)

To attribute this material, cite the Queensland Government Chief Information Office

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.

All enquiries regarding this document should be directed in the first instance to the Queensland Government Chief Information Office at [qgcio@qgcio.qld.gov.au](mailto:qgcio@qgcio.qld.gov.au)

An electronic version of this document is available at [www.qld.gov.au/dsitia](http://www.qld.gov.au/dsitia)

# Contents

Executive summary .....	1
1. Introduction .....	5
2. Definitions .....	7
3. Vision .....	8
4. Key objectives .....	13
1. ICT capabilities will be sourced cloud-first. ....	13
2. Cloud service brokerage platforms will be used to aggregate, simplify, secure and integrate a diverse range of cloud services. ....	15
3. Cloud brokers will be appointed for SaaS, PaaS and IaaS services and engaged first to orchestrate other providers .....	19
4. Agency ICT divisions will transition from a service provider to a service broker role. ....	23
5. An ICT marketplace and storefront will support the sourcing of a wide range of mass-market ICT services from industry .....	24
6. A federated identity model will underpin sharing of commodity and common services, multi-vendor sourcing strategies and support the establishment of a new cloud security perimeter .....	28
7. Trusted cloud services will be pre-enlisted from multiple providers .....	32
8. Information security will be improved through the use of mature, well-credentialed cloud services providers .....	33
9. A Queensland Government community cloud for IaaS will be established to support common government and enterprise-grade ICT requirements. ....	34
10. ICT services will become more accessible at any time, any location and preferably on any device. ....	36
11. A cloud-educated workforce will exploit new cloud capabilities to deliver innovative solutions and cost efficiencies. ....	37
12. A hybrid ICT delivery model where cloud and traditional ICT environments co-exist will become the new steady state .....	37
13. Maintaining an evergreen cloud environment will become the new benchmark. ....	38
14. Rapid access to cloud services will enable innovative, next-generation applications and service delivery .....	39
5. Cloud considerations. ....	40
6. Implementation model .....	44
6.1 Focus area 1: Cloud ready .....	46
6.2 Focus area 2: Cloud foundations .....	50
6.3 Focus area 3: Cloud engagement .....	54
6.4 Focus area 4: Cloud accelerate .....	58
6.5 Focus area 5: Cloud governance. ....	63
6.6 Recommendation timeline .....	65

Appendix A: Definition of cloud computing.....	66
Appendix B: Glossary of terms .....	69
Appendix C: Related documents .....	72
Appendix D: References .....	73

**Figures**

Figure 1: ICT commodity services versus core business focus.....	6
Figure 2: NIST cloud computing definition .....	7
Figure 3: Queensland Government cloud enablement blueprint.....	12
Figure 4: Contrast between a cloud service brokerage (CSB) vs ad hoc approach ....	16
Figure 5: Three architectural brokerage roles .....	16
Figure 6: Example brokerage integration platform concept.....	18
Figure 7: Multiple cloud brokers participating in a common ICT marketplace .....	22
Figure 8: Agency shift from service provider to service broker .....	23
Figure 9: Queensland Government ICT marketplace and CloudStore.....	26
Figure 10: Federated identity broker concept .....	30
Figure 11: Unified access portal/cloud desktop concept .....	31
Figure 12: Five key focus areas .....	44
Figure 13: Cloud ready implementation approach.....	46
Figure 14: Cloud foundations implementation approach .....	51
Figure 15: Cloud engagement implementation approach.....	55
Figure 16: Cloud accelerate implementation approach .....	59
Figure 17: Cloud governance implementation strategy .....	63
Figure 18: Recommendation implementation timeline.....	65
Figure 19: NIST cloud computing definition.....	66

## Executive summary

The Queensland Government will look to place cloud computing at the centre of government ICT reform by taking 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. The United States of America, United Kingdom and New Zealand governments have previously implemented similar cloud-first policies.

The Queensland Government's adoption of cloud-based services will enable it to transition from mainly internal, high-cost customised ICT applications and solutions to lower-cost, standard, interchangeable services where quality improvements and cost reductions are driven by highly-competitive market forces. Simultaneously, cloud services present the opportunity to reduce vendor lock-in, enable self-service and accelerate innovation and productivity in the delivery of contemporary public services to Queensland's citizens.

The Independent Commission of Audit report, published in February 2013 recommended government:

- adopt an ICT-as-a-service strategy
- utilise appropriate cloud-based computing and other emerging technologies
- discontinue ownership and management of significant ICT assets and systems.

The ICT Audit also identified cloud services as a key service delivery transformation that will help address several of the challenges being faced by the legacy ICT environment.

Cloud computing provides the opportunity to meet the future demands on ICT through:

- **cost reduction:** changing to an on-demand model for ICT where we only consume and purchase what infrastructure and software services are needed from a competitive marketplace
- **debt reduction:** reducing future capital costs and requirement for borrowings by moving to a fee-for-service based model
- **sustainability:** lifecycle management becomes the responsibility of the service provider
- **innovation:** new functions are driven by market competition with the potential to take advantage of new innovative functions without necessarily investing in start-up research and innovation processes
- **value sooner:** realisation of business benefits are achieved sooner as commoditised ICT functions can be more quickly procured, tested and deployed
- **business agility:** ICT is able to respond more quickly to changing business needs and priorities as ICT services can be provisioned, scaled up or scaled down in very short timeframes
- **improved security:** relative to current security capabilities within Queensland Government, most agencies will benefit from an improvement in security when delivered by mature and certified cloud providers
- **improved information sharing:** facilitating better interaction and information sharing to improve collaboration, cross-agency case management, decision making and policy development.

The following table contrasts the current state ICT environment against the corresponding shift to the future cloud model:

Current state	Future cloud model
High-cost and bespoke ICT solutions	Consumption of well-defined, standardised and highly-configurable shared services which continue to evolve and innovate based upon the needs of a large and diverse customer base and are paid for by many customers
Aging technology requiring continual refresh and upgrades	An evergreen model where lifecycle management is predominantly the responsibility of the service provider and quality improvements and cost reductions are driven by highly-competitive market forces.
Limited security-focused resources and funding	Information security will be improved through the use of mature cloud services providers that hold extensive security accreditations and implement well-established security management processes which undergo regular external audit
Complex and long projects to provision (design, build and test) commodity ICT solutions and infrastructure	Rapid business value derived through the consumption of ready-made ICT services which are available for near immediate use ( <b>excluding organisational change and business transition</b> )
Rigid and inflexible systems	More flexible, responsive and innovative services which were inherently built to be both enduring and flexible to service changing business needs
Low agility and resource intensive management	Self-service ICT models and automated just-in-time fulfilment without human intervention by the service supplier
Long lead times to increase or reduce ICT capacity of services	On-demand increases and reductions in ICT capacity
Low utilisation of assets	Greater sharing of resources, improved economies of scale and the ability to closely match allocated resources to demand
Capex intensive investment and assets centric model	A more financially sustainable Opex model on pay-for-what-you-consume basis
Limited disaster capabilities and preparedness	The ability to take advantage of highly available and fault tolerant services which are cost-effective due to economies of scale and their shared nature

The *Queensland Government Cloud Computing Strategy* outlines a future state vision which seeks to create a trusted cloud ecosystem through provision of a ‘storefront’, marketplace and technical brokerage platforms, in which a community of cloud service providers, consultants, integrators and partners operate.



The key strategies to achieve this vision are:

- The establishment of a whole-of-government cloud marketplace and storefront to streamline procurement of accredited cloud software, platform and infrastructure services.
- The establishment of commercial arrangements for external brokers of cloud services to support agencies in value-for-money procurement, management and integration of cloud services.
- The establishment of a Queensland Government private community cloud to support common government requirements and workloads unsuitable for public cloud.
- The establishment of a whole-of-government identity federation platform to support the secure sharing of common ICT services across government.
- The transformation of agency ICT divisions from a service provider role responsible for building and managing ICT assets and systems to acting as a trusted broker of ICT services from external suppliers.

These strategies support a hybrid ICT delivery model, combining both cloud and traditional ICT approaches. Queensland Government will need to continue maintaining legacy ICT environments and delivery models in parallel during transition and to accommodate systems unsuitable for cloud.

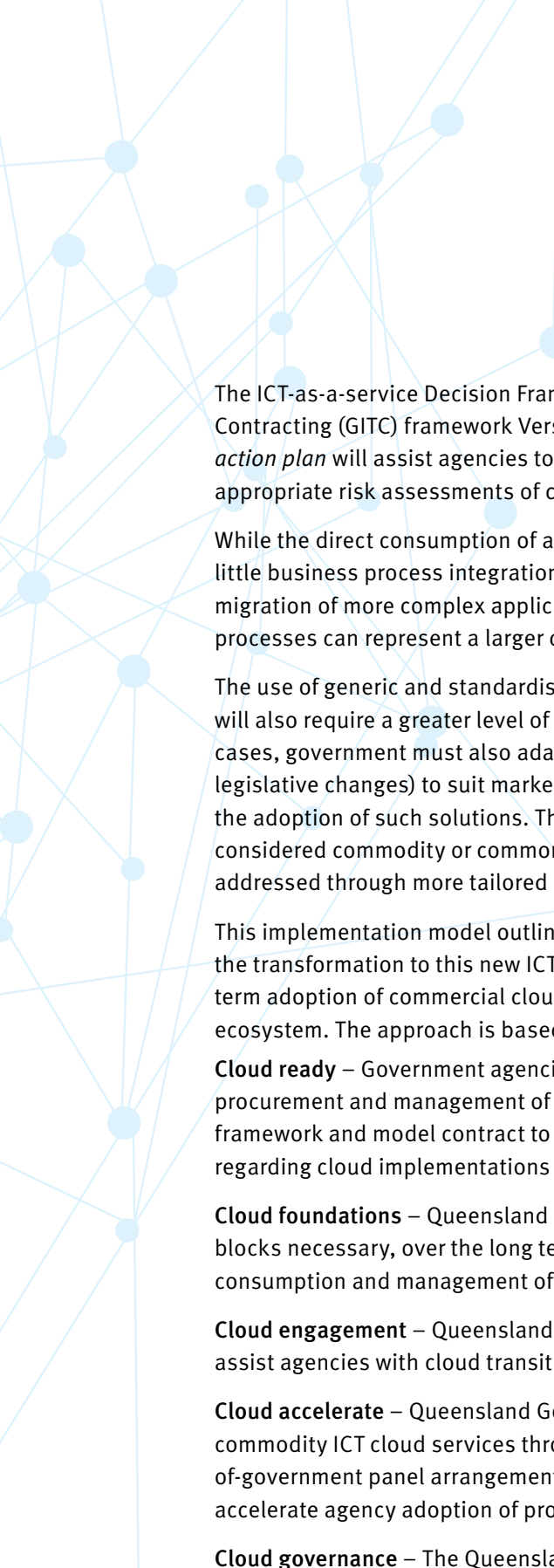
Over time the consumption of many different types of cloud services from multiple suppliers may lead to a highly-heterogeneous and distributed ICT environment. Should this diversity not be carefully managed the potential benefits of adopting cloud services may be slowed or not realised and limit the benefits government could achieve.

This implementation model outlines a coordinated service brokerage approach consisting of both technical brokerage/integration platforms and the use of external organisations (cloud brokers) to aggregate, simplify, secure and integrate a diverse range of cloud services.

A transformed and capable workforce is also required to support the transition to cloud-based services. ICT procurement, contract and performance management, organisational change management, information security and service integration will become key strategic skill sets requiring further development with government.

Information security, privacy and data sovereignty are key risks pertaining to the use of cloud services. Cloud computing provides an opportunity to improve information security (relative to current security practice) through the use of mature and well-credentialed cloud service providers. This does not negate the need for government to maintain in-house information security management expertise.

While the majority of these risks are equally valid for traditional architectures, the transfer and potential off-shoring of data introduces additional risks pertaining to data sovereignty and privacy. In most cases, these risks can be addressed or mitigated through appropriate contractual arrangements and technical controls. There still remains an element of trust, as a customer has little visibility of a provider's internal operation. Government will need to rely upon regular external audits as sufficient evidence of assurance.



The ICT-as-a-service Decision Framework and model Government Information Technology Contracting (GITC) framework Version 5 contractual terms developed through the *ICT action plan* will assist agencies to develop suitable contractual arrangements and conduct appropriate risk assessments of cloud service options.

While the direct consumption of a single cloud service for a single business function with little business process integration can be achieved in a relatively simplistic manner, the migration of more complex applications that support many highly-integrated business processes can represent a larger challenge and involve longer and more costly transitions.

The use of generic and standardised cloud solutions for these more complex systems will also require a greater level of business process and organisational change. In these cases, government must also adapt business practices (potentially including policy and legislative changes) to suit market offerings and avoid undue customisation which inhibit the adoption of such solutions. The cloud-first approach targets those systems which are considered commodity or common, and allows for niche government requirements to be addressed through more tailored solutions built upon common cloud infrastructure.

This implementation model outlines an approach for Queensland Government to begin the transformation to this new ICT delivery paradigm and a blueprint for the long-term adoption of commercial cloud services by government in a multi-cloud provider ecosystem. The approach is based around five key focus areas:

**Cloud ready** – Government agencies will be better educated and informed on best practice procurement and management of cloud services. Cloud computing policies, a decision framework and model contract to assist agencies to make well-informed decisions regarding cloud implementations will be developed.

**Cloud foundations** – Queensland Government will establish the key foundational building blocks necessary, over the long term, to address a holistic approach to acquisition, secure consumption and management of a multi-provider cloud ecosystem.

**Cloud engagement** – Queensland Government will make available trusted advisers to assist agencies with cloud transition and migration plans.

**Cloud accelerate** – Queensland Government will initially look to adopt common and commodity ICT cloud services through accredited (pre-qualified) arrangements. Whole-of-government panel arrangements for cloud email and infrastructure-as-a-service will accelerate agency adoption of proven cloud solutions from trusted suppliers.

**Cloud governance** – The Queensland Government will leverage existing governance arrangements such as the Directors-General Council Gateway Review to ensure alignment with a ‘cloud-first enterprise’ vision.

The implementation model outlines 26 recommendations to progress Queensland Government’s transition to a cloud-first enterprise. Upon acceptance of this implementation model recommendations the Queensland Government ICT action plan will be updated to incorporate those recommendations that are to be progressed.



# 1. Introduction

In March 2012, the Queensland Government established an Independent Commission of Audit to provide advice on Queensland's current and forecast financial position and to recommend strategies to strengthen the economy, restore the state's financial position and to ensure value for money in service delivery. The Independent Commission of Audit report, published in February 2013, recommended ways in which the quality and quantity of front-line services could be improved, including models that made better use of the skills, capacity and innovation of the private and not-for-profit sectors.

The report recommended adopting an ICT-as-a-service strategy and the desire to utilise, as appropriate, cloud-based computing and other emerging technologies. The Independent Commission of Audit also described the need to discontinue ownership and management of significant ICT assets and systems.

On 8 May 2012, Cabinet approved that the Queensland Government Chief Information Office (QGCIO) lead an audit of ICT management practices (ICT Audit) and prepare a report for Cabinet. The focus of the audit was to discover risks as well as opportunities for savings, increased performance and reduction of waste through more effective ICT management. The report identified a number of key issues and challenges that impede the government's ability to maintain sustainable, effective and efficient ICT services to support service delivery to the public.

Like the Independent Commission of Audit, the ICT Audit identified cloud computing as one of the key service delivery transformations that will assist in addressing several of the challenges being faced by the legacy ICT environment.

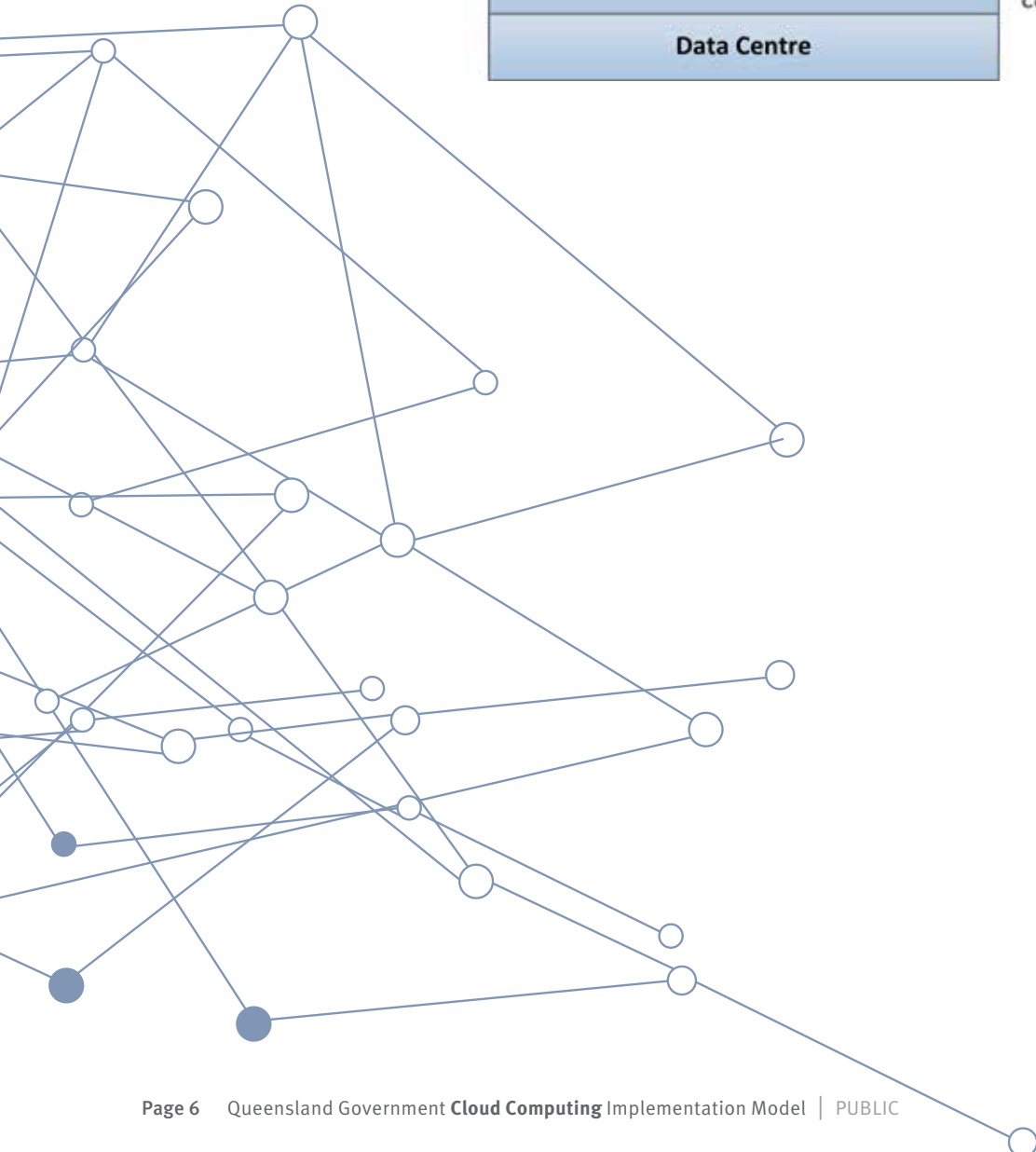
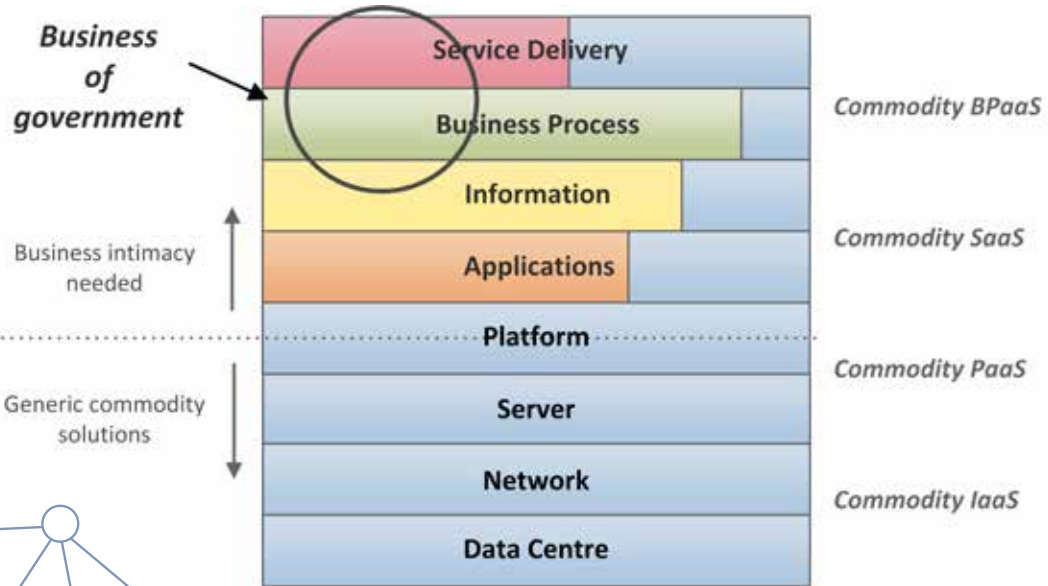
The issues and challenges identified by the ICT Audit are compounded by the current-state ICT landscape is an information technology industry that is evolving rapidly in the areas of mobility, ubiquitous broadband connectivity, the consumerisation of information services and applications and the use of ICT to support collaboration between government workers, industry and the public. This is driving change in the requirements of government workplaces to meet the service delivery expectations and behaviour of employees and citizens. At the same time, the requirement for optimal efficiency, cost effectiveness and lower environmental impact has never been stronger.

The adoption of cloud computing will provide the necessary step change in ICT service delivery.

Figure 1 is a representation of ICT domains that illustrates how agencies should focus on core business, and the opportunity presented by cloud computing to release agencies from performing the more commoditised functions of the ICT stack.

By consuming ready-made ICT services from the cloud, agencies can better focus on their core missions and ministerial responsibilities. It is proposed that in general, agencies should not build internal ICT services when these are available as generic commodity or common solutions from industry. This will likely require government agencies to transform business process in order to avoid undue customisation which can inhibit the adoption of market offerings.

Figure 1: ICT commodity services versus core business focus



## 2. Definitions

### Cloud computing

The US National Institute of Standards and Technology (NIST) definition of cloud computing is commonly used throughout the ICT industry, and it is the definition adopted by the Queensland Government:

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

This model is composed of five essential characteristics, three service models and four deployment models as depicted in Figure 2.

**Figure 2: NIST cloud computing definition**



It should be noted, both the service consumer and provider have an equal responsibility to ensure these essential characteristics are delivered.

Refer to Appendix A for an expanded definition of the various characteristics, service and deployment models.

### Cloud services

There is a difference between cloud computing and cloud services. A cloud service is an established bundle of processes, people, organisations and technology which has been assembled by a cloud provider to deliver a well-defined, shared service to many customers. Cloud computing refers to the suite of technology innovations, including scalable infrastructure, multi-tenant infrastructure, virtualisation, automation and self-service provisioning portals which underpin cloud services.

This implementation model supports government's adoption of readily available cloud services as a form of outsourced shared service.

## 3. Vision

### Vision statement

Cloud computing is a model of ICT service provision that enables the simple, convenient and on-demand access to shared pools of computing resources designed to maximise economies of scale. This disruptive technology provides a significant opportunity for improved outcomes and increased satisfaction with government services through the delivery of innovative and more cost-effective services.

Queensland Government will be a 'cloud-first enterprise'. This will provide improved service delivery to Queenslanders as agencies maximise value for money from the transition of internal ICT service provision to the consumption of cost-effective commodity ICT services and innovative market capabilities that improve flexibility and agility to meet the rapidly changing service delivery expectations.

A cloud-first vision advocates that cloud-based provision of ICT-enabled business solutions and services will, over time, become the default approach.

However, simply sourcing cloud technology as the first option will not in itself provide the required ICT reform—the greatest benefit will be derived from re-orienting the focus, culture, skill sets and enterprise architecture of government to change the way ICT is delivered, operated and consumed.

### A CLOUD-FIRST ENTERPRISE CHARTER

The behaviour and principles needed to support a cloud-first enterprise:

- take a cloud-first approach to sourcing ICT capabilities over traditional delivery
- act as a broker of ICT services from external suppliers to satisfy business needs
- take advantage of the market capabilities, rather than unnecessarily building high-cost and bespoke ICT solutions
- look to re-engineer business processes to enable the consumption of standard offering, rather than customising solutions to fit current practice
- integrates multiple services to compose a business solution
- unify ICT delivery across multiple suppliers and delivery channels
- promote automated and self-service access to ICT services
- prefer web delivery of systems to enable device agnostic, anywhere and anytime access
- acquire resources on-demand and releases them when no longer required
- exploit innovations in cloud technology to deliver next generation business applications, and more cost-effective services
- leverage innovative solutions from the market to derive rapid business value
- embrace an evergreen mindset to continually incorporate small evolutionary changes to the business and avoid the creation of complex legacy solutions and associated costs
- assemble tailored business solutions out of standard components and services
- embrace agile principles of modular and iterative design to deliver more flexible, responsive and innovative services
- realign the ICT workforce skills and capability to best leverage the benefits and potential risks of adopting cloud services.



## Vision blueprint

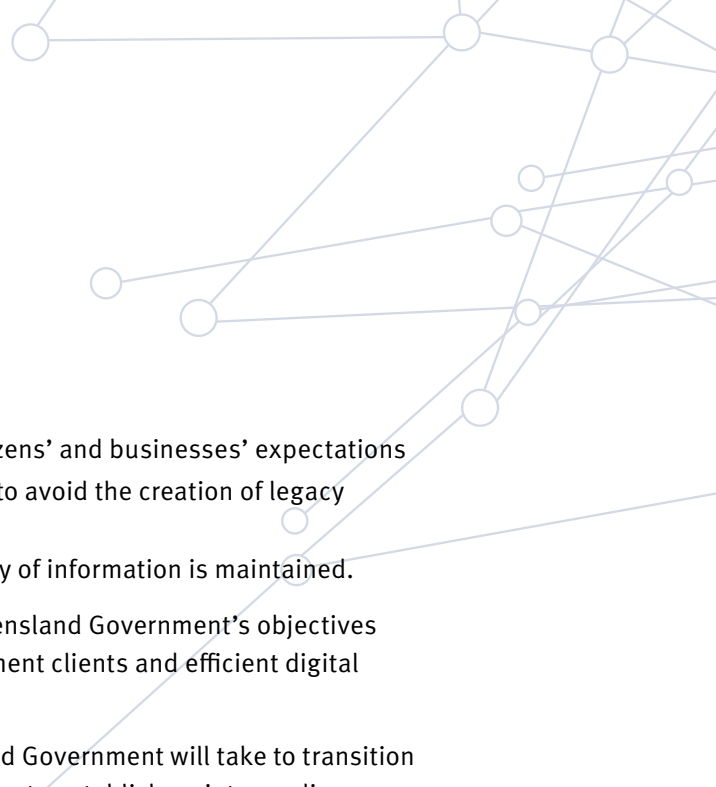
Queensland Government's cloud-first enterprise vision seeks to create a trusted cloud ecosystem through provision of a storefront, ICT marketplace and technical brokerage platform to cultivate and develop a business ecosystem and community of cloud service providers, consultants, integrators and partners.

This approach aims to:

- enable and accelerate government's cloud adoption
- efficiently manage risk to maximise derived value
- streamline procurement and leverage one-government economies
- partner with industry through an ICT marketplace to:
  - create an efficient and easy channel to government
  - lower barriers to entry to increase opportunities for small to medium enterprises (SMEs)
  - provide a means for government to quickly discover and utilise evolving technology
  - support the development of innovative solutions.

This vision is built around three key pillars:

- 1. Service delivery enablement**—facilitating better interaction through user-centric design and information sharing with:
  - citizens: irrespective of the time of day, location, device or preferred channel
  - businesses, partners and non-government organisations to:
    - support co-production and efficient joint-service delivery
    - enhance information access to enable high-quality services
  - government agencies to improve collaboration, cross-agency case management, support decision making and policy development.
- 2. Cloud service brokerage**—supporting government to become an efficient buyer and user of modern, contestable ICT services to:
  - reduce asset ownership/operation and improve value for money
  - take advantage of market capabilities which continue to improve due to competitive forces
  - assemble solutions from standard interchangeable components, rather than unnecessarily building high cost and bespoke solutions
  - streamline procurement through an ICT marketplace and efficient partnering with industry
  - maintain cloud service and vendor abstraction to foster competition and choice.
- 3. Trusted cloud services**—the use of market-driven, innovative and ready-made services from well-credentialed providers to:
  - deliver better, simpler and more cost-effective government services
  - deliver new ICT-enabled solutions to service delivery challenges
  - respond more rapidly to community needs

- 
- enable new delivery channels which meet citizens’ and businesses’ expectations
  - transition towards an evergreen environment to avoid the creation of legacy complexities and cost
  - ensure the confidentiality, security and privacy of information is maintained.

The first and third pillars align closely with the Queensland Government’s objectives of effective digital services for Queensland Government clients and efficient digital services for government.

The second pillar is core to the approach Queensland Government will take to transition to a cloud-based delivery model. The approach seeks to establish an intermediary (brokerage layer) between cloud service providers (CSPs) and government consumers to reduce the risk of consuming cloud services and assist government and agencies to maintain a level of strategic control and governance over a diverse and rapidly evolving outsourced, multi-cloud and multi-vendor environment.

Learnings from other government jurisdictions have proven that without a coordinated and structured approach to cloud acquisition and consumption, large-scale government-wide cloud adoption will quickly be slowed by issues such as complexity of integration, acquisition and security<sup>1</sup>. Furthermore, the propagation of siloed acquisition models and duplication will limit the amount of savings that could otherwise be achieved through cloud<sup>2</sup>.

The conceptual blueprint on page 12 depicts the future implementation of Queensland Government’s cloud-first enterprise vision encompassing the three key pillars of service delivery enablement, cloud services brokerage and trusted cloud services. The blueprint is also supported through internal and external cloud brokers which procure and curate cloud offerings for the ICT marketplace. Under this model, the internal agency ICT divisions also act as a broker of services across existing traditional and new cloud environments.

The implementation of this blueprint will see the establishment of a number of key capabilities and roles:

1. Cloud service brokerage platforms to assist with aggregating, securing, integrating and simplifying the consumption of a diverse range of cloud services.

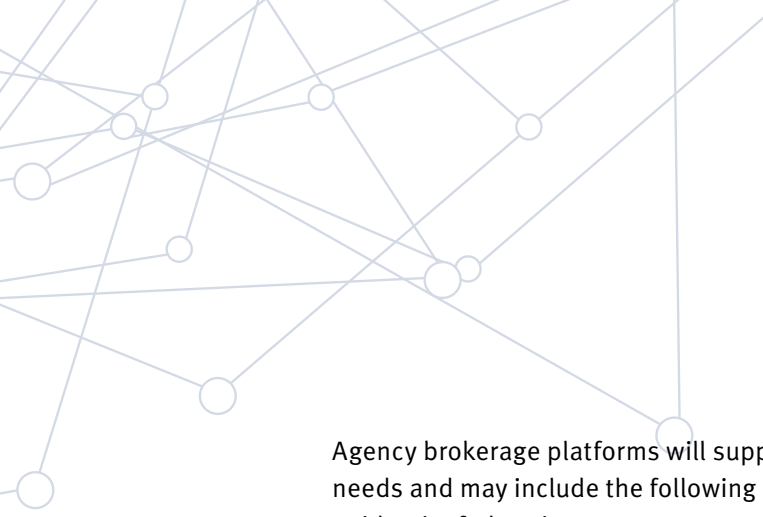
A common government brokerage platform will provide:

- a. SaaS brokerage capability including:
  - a ICT marketplace and storefront (CloudStore)
  - an identity federation capability for shared, cross-agency and non-government organisation delivered services
- b. IaaS brokerage capability to deliver a brokered cloud management interface across a whole-of-government community IaaS cloud and multiple connected public IaaS clouds.

---

<sup>1</sup> US Government General Services Administration (GSA) IAC NT SIG Presentation—Helping Agencies Move to Cloud, 2013

<sup>2</sup> ibid



Agency brokerage platforms will support agency-specific SaaS and line of business needs and may include the following capabilities:

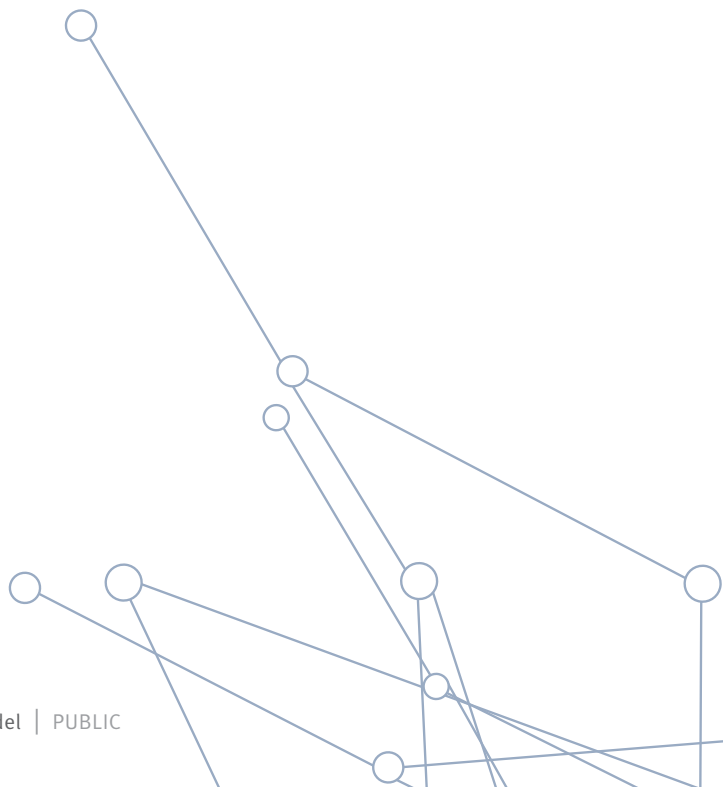
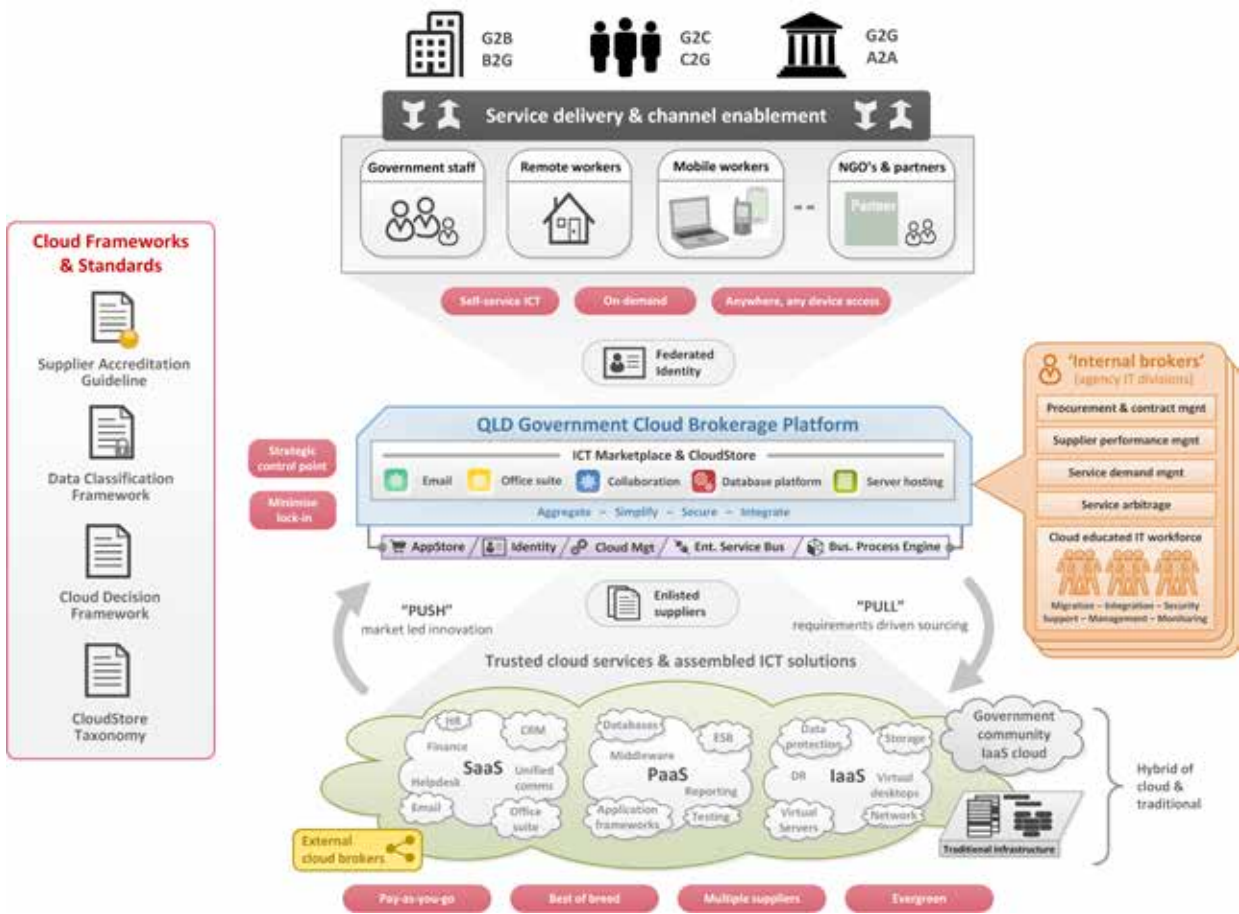
- a. identity federation
  - b. an enterprise/cloud service bus
  - c. business process orchestration and management.
2. Appointment of cloud brokers to negotiate supplier relationships and manage the use, performance and delivery of cloud services. This may be performed by either:
    - a. internal agency brokers (the agency ICT division)
    - b. lead agency brokers within a given cluster or for common whole-of-government services
    - c. trusted external cloud brokers (commercial agents) acting on behalf of government/agencies.
  3. Cloud standards framework to support consistent governance across the ICT marketplace and multiple cloud brokers.

Within the context of this approach, the term ‘cloud service brokerage platform’ refers to a technical implementation of integration (middleware) software, whereas the term ‘cloud broker’ refers to a human resources (people and process) function.

The individual brokerage platform technologies depicted in Figure 3 specifically address control, governance, compliance and visibility requirements to ensure government retains these key control points within an outsourced relationship to minimise the risk of technology and vendor lock-in. Specifically:

- maintaining control of technical diversity, baseline standards, supplier assurance and accreditation through an applications store
- ensuring enterprise-grade, contextual and risk-based security policy and controls for authentication and authorisation are applied consistently across all connected cloud environments through identity management
- brokering interfaces to cloud infrastructure (IaaS) providers through a cloud management platform (CMP) to enforce security policy and preserve the ability to migrate workloads between suppliers
- securely brokering and mediating data and information exchange through an enterprise/cloud service bus (ESB)
- enabling orchestration and business process innovation across standardised commodity components through business process management (BPM) and automation.

Figure 3: Queensland Government cloud enablement blueprint





## 4. Key objectives

There are 14 key strategic objectives to transform Queensland Government to this future state. These are:

1. ICT capabilities will be sourced cloud-first.
2. Cloud service brokerage platforms will be used to aggregate, simplify, secure and integrate a diverse range of cloud services.
3. Cloud brokers will be appointed for SaaS, PaaS and IaaS services and engaged first to orchestrate other providers.
4. Agency ICT divisions will transition from a service provider to a service broker role.
5. A ICT marketplace and storefront will support the sourcing of a wide range of mass-market ICT services from industry.
6. A federated identity model will underpin sharing of commodity and common services, multi-vendor sourcing strategies and support the establishment of a new cloud security perimeter.
7. Trusted cloud services will be pre-enlisted from multiple providers.
8. Information security will be improved through the use of mature, well-credentialed cloud services providers.
9. A Queensland Government community cloud for IaaS will be established to support common government and enterprise-grade ICT requirements.
10. ICT services will become more accessible at any time, any location and preferably on any device.
11. A cloud service-educated workforce will exploit new cloud capabilities to deliver innovate solutions and cost efficiencies.
12. A hybrid ICT delivery model where cloud and traditional ICT environments co-exist will become the new steady state.
13. Maintaining an evergreen cloud environment will become the new benchmark.
14. Rapid access to cloud services will enable innovative, next-generation applications and service delivery.

### 1. ICT capabilities will be sourced cloud-first

Queensland Government will take a cloud-first approach to the sourcing of external ICT functions, requiring agencies to first consider cloud-based solutions in preference to traditional ICT investments where cloud services demonstrate value for money and are fit for purpose.

The evaluation of alternate sourcing models for ICT-enabled functions will be driven through contestability processes and assessments as recommended by the Independent Commission of Audit.

It is recommended all ICT functions, particularly those considered commodity or common across agencies, be selectively sourced as-a-service from entities for which those services form core competencies and can be delivered more cost effectively and efficiently.

The consumption of ICT-as-a-service will allow government to re-align its resources and investments to focus on strategic planning, innovation, and the transformation of front-line service delivery. This will also serve as a strategic lever to assist in changing the culture of government to adapt to the market solutions and not build unnecessary high-cost bespoke solutions.

There should be an initial focus on ICT functions which will have the highest near-term positive impact from a shift to a cloud model. All new workloads should first consider cloud options and all existing workloads should be assessed, particularly at the key refresh points or contractual renewals within the ICT lifecycle. All attempts should be made to avoid ownership and operation of traditional licensed software in preference to acquiring ICT functions in the form of SaaS or business process-as-a-service (BPaaS).

Cloud services present a compelling alternative to traditional outsourced models, particularly for commodity ICT requirements. These ready-made services are available for near immediate use and offer a set of capabilities and reliability superior to what a single organisation could build themselves. Cloud services also continue to evolve and innovate based upon the needs of a large and diverse customer base and are paid for by many customers<sup>3</sup>.

## CLOUD-FIRST POLICY

- Agencies **must** consider first cloud-based solutions in preference to traditional ICT investments (in-house or managed services).
- Applies to **all** ICT functions, particularly those which are considered:
  - commodity or
  - common.
- First preference should be given to the use of:
  - established and well-credentialed public cloud services
  - SaaS and BPaaS models to:
    - avoid ownership of assets, including traditional licensed software
    - rationalise, standardise and re-engineer business processes.
- Supported by a decision framework that:
  - ensures the safe, secure and effective use of public cloud services—directs high-risk workloads and datasets to alternative delivery models.

A cloud decision framework will be developed to support the safe, secure and effective use of external cloud services, while directing workloads and datasets that are higher risk to alternative delivery models.

<sup>3</sup> Why government agencies need the cloud, Ovum, February 2012 (0100190-009)



## 2. Cloud service brokerage platforms will be used to aggregate, simplify, secure and integrate a diverse range of cloud services

While the direct consumption of a single cloud service by a single agency or individual line-of-business group (within an agency) can be achieved in a simplistic manner, as consumption expands to include multiple services across multiple suppliers, the following activities become a substantial challenge and do not scale efficiently, for example:

- managing the various commercial agreements (e.g. service level agreements (SLAs), billing and support arrangements)
- managing technical aspects such as security, management, integration and migration
- unifying end-user consumption across multiple services and suppliers.

Consuming many different types of cloud services from multiple suppliers in an ad hoc fashion will create a highly heterogeneous and distributed ICT environment as each cloud service is inherently different in terms of its:

- contract, SLA, billing and licensing models
- security (identity sources, credentials, access control and audit capabilities)
- data integration interfaces and use of standards
- provisioning mechanisms.

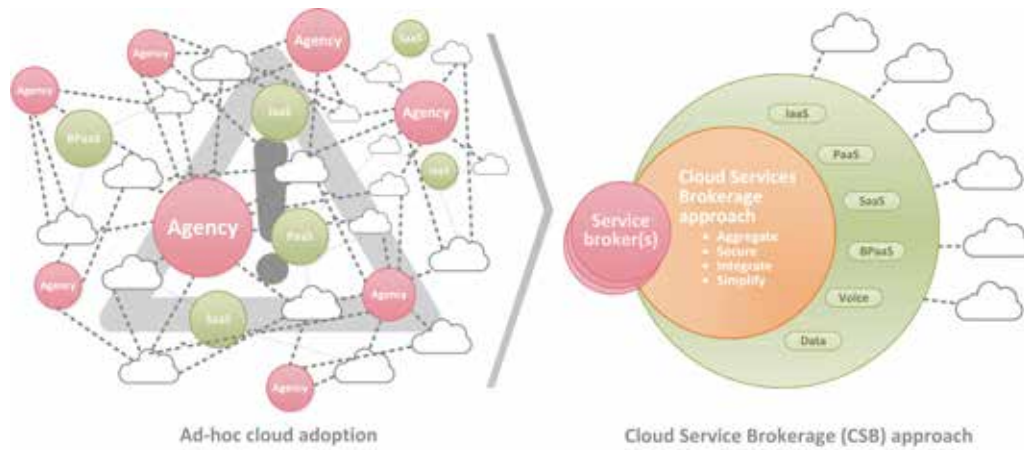
If such diversity is not carefully managed, the potential benefits of adopting cloud services may be slowed or not realised and limit the benefits government cloud could achieve.

Many governments including the United States of America, United Kingdom and Singapore as well as large enterprises have recognised the need for a more systemic and coordinated approach, referred to as cloud service brokerage (CSB). CSB is increasingly recognised as an important foundation and proven to be critical to the successful adoption of a multi-cloud ecosystem.

Gartner defines the CSB model as an architectural, business and ICT operations model for enabling, delivering and managing different cloud services in a consistent framework. It provides a single point of entry into multiple clouds, eliminating complex management of multiple providers and integration.

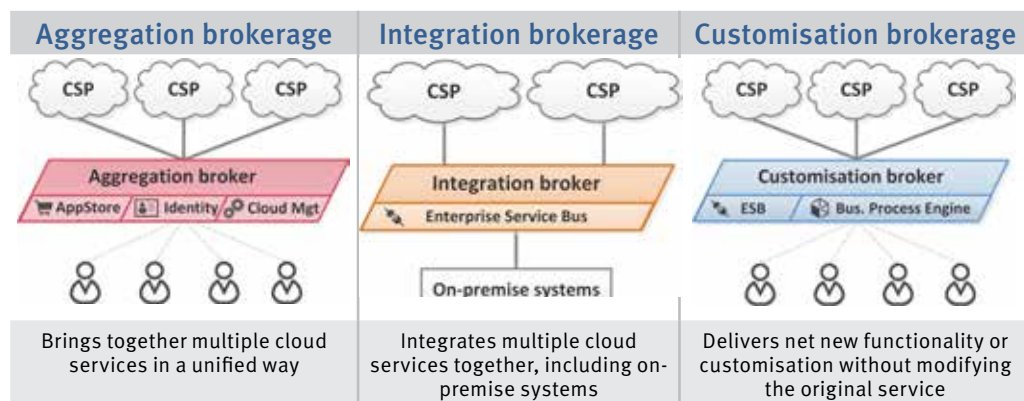
Figure 4 contrasts the difference between taking a coordinated brokerage approach to cloud adoption versus an ad hoc approach which would result in a disjointed and fragmented environment.

**Figure 4: Contrast between a cloud service brokerage (CSB) vs ad hoc approach**



Gartner defines three key architectural and brokerage roles (Figure 5) with each role typically incorporating a number of supporting technologies.

**Figure 5: Three architectural brokerage roles**





## Brokerage technologies

The associated brokerage technologies are designed to be deployed in a manner that assists Queensland Government agencies to maintain a level of strategic control and consistency over multiple outsourced relationships while hiding complexity for end users through:



### **An applications store/ICT marketplace capability**

provides control over technical diversity, standards, assurance and accreditation, including a brokered interface to multiple SaaS providers to abstract and normalise provisioning and billing complexity.



### **An identity federation/management capability**

enables centralised, contextual, risk-based and enterprise-grade security policy and controls to be consistently enforced across all connected cloud environments regardless of an individual provider's capability. Identity federation allows Queensland Government to act as the identity provider to ensure appropriate levels of identity registration, authentication (credential strength), authorisation and compliance.



### **A cloud management platform capability**

provides a brokered interface to multiple cloud infrastructure (IaaS) providers with embedded policy controls to determine workload placement and improve workload portability between suppliers.



### **An enterprise service bus/cloud integration platform capability**

provides control over the exchange of information and datasets, including the brokering of data between cloud services and traditional on-premise systems. This proactive decoupling aids a staged migration to cloud services and facilitates better interoperability and migration between clouds.



### **A business process management capability**

provides the ability to externalise business process logic to support modifications to cloud services in a structured way that preserves the original cloud service, including the ability to orchestrate and drive innovation in business process across standardised commodity components.

These technical brokerage capabilities embed standard integration interfaces (or application programming interfaces (APIs)) which will normalise integration requirements and provide a common way to integrate cloud services (and suppliers). This allows:

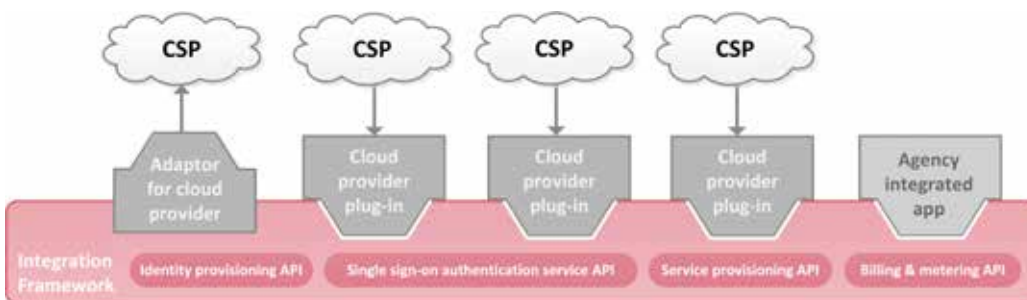
- Queensland Government to:
  - consistently authenticate and authorise users, including single sign-on
  - automate the activation of new services or service changes (click-to-buy)
  - electronically receive metered billing information from suppliers
  - secure and broker data and information interchange
  - automate chargeback and spending analysis.

- industry to:
  - quickly implement and integrate services to government
  - offer richer functionality and integration through improved data sharing and process integrations
  - become familiar with government requirements
  - leverage integration efforts across multiple services and/or multiple agencies.

Figure 6 depicts an example of a conceptual integration framework providing capabilities at an authentication, identity (user) provisioning, service provisioning and billing/metering layer. Integration is achieved by:

- out-of-the-box plug-ins to connect to standards-based cloud service interfaces
- pre-developed custom adaptors to connect to propriety interfaces of cloud services
- the ability to integrate custom solutions via a software development kit.

**Figure 6: Example brokerage integration platform concept**



Given the maturity of brokerage platforms, a single brokerage platform to support government’s parallel adoption of both SaaS and IaaS services is not available in the market. Where possible, Queensland Government and agency brokerage platform implementations will look to utilise pre-existing, well-established and industry-accepted platforms to:

- avoid the need to develop and maintain integration platforms
- minimise the need for suppliers to integrate with a Queensland Government-specific framework
- provide access to a ‘network’ and large portfolio of pre-integrated services and suppliers.

By default, all procured cloud services should be intermediated through a suitable brokerage platform:

- At a minimum, all SaaS services (and hosted IaaS or platform-as-a-service (PaaS) applications) are required to integrate for:
  - delegated or single sign-on authentication
  - identity provisioning and/or de-provisioning (where required).
- It is highly preferable all data interchange (cloud-to-cloud and cloud-to-on-premise) for SaaS and PaaS services be brokered and abstracted through an enterprise/cloud service bus.

- Richer and more functional levels of integration and automation can be gained for select services through integration with the CloudStore for automated service provisioning and billing of reoccurring acquisitions.
- All IaaS services will be integrated to a common cloud management platform (CMP).

### **3. Cloud brokers will be appointed for SaaS, PaaS and IaaS services and engaged first to orchestrate other providers**

A cloud broker as defined by Gartner is an entity which manages the use, performance and delivery of cloud services, and negotiates supplier relationships<sup>4</sup>. Under this model, a cloud broker may be:

- an internal agency broker (the agency ICT division)
- a lead agency broker with responsibility for a given agency cluster or for common whole-of-government services
- an external broker (commercial agent/business entity) acting on behalf of government or an agency.

By default, given the outsourcing of ICT functions, the ICT division within an agency will transition to act as a broker between the internal services delivered and new services delivered by external providers. This organisational change is described further in objective 4—agency ICT divisions will transition from a service provider to a service broker role.

The cloud brokerage model also lends itself to the use of external cloud brokers which, in some cases, may be better positioned to more efficiently perform the core business process functions of a broker. These being market research, negotiation and other ancillary support services to on-board, integrate and manage services. The appointment of cloud brokers and brokerage responsibility will be determined and governed based on contestability processes.

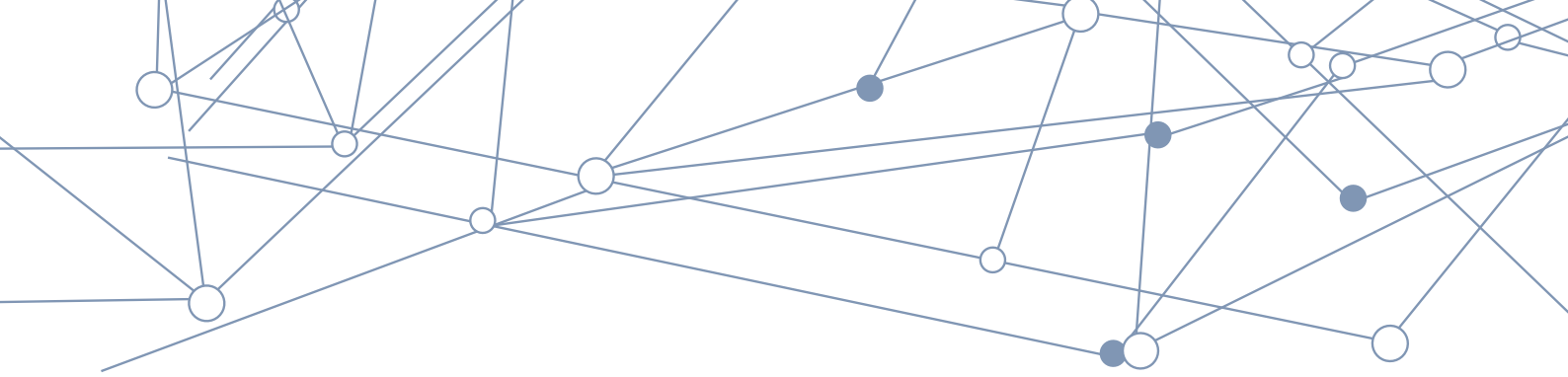
A given broker (internal or external) may also elect to utilise other brokers to provide access and aggregation across other ‘long tail’ cloud services, negating the need to manage each relationship.

While agency brokers are uniquely positioned to broker and manage the transition from legacy to cloud environments, external brokers should be used to complement this approach.

External cloud brokers will be appointed by Queensland Government to cover SaaS, IaaS and PaaS markets. Agencies are encouraged to engage a broker first to orchestrate other providers where this delivers added value.

---

<sup>4</sup> A CIO Primer on Cloud Services Brokerage, Gartner 2012 (G00245329)



Brokerage responsibility between external brokers may be segmented based upon:

- service model (SaaS, IaaS and PaaS)
- service classification/category
- architectural brokerage role performed (e.g. aggregation vs integration)
- services offered by the broker (market research, negotiation, migration, integration or management services)
- level of neutrality required.

Over time, competition between brokers will provide the government with the ability to source the same product or service from multiple brokers, providing contestability to the services while maintaining competitive tension in the market. This will require brokers to add value to the re-selling of existing commodity services and source new and innovative products to broker to the market. It is also essential that a broker is capable of managing a range of service providers from SMBs to large transnational corporations.

While multiple brokers can assist government to find the best services mix, the added increase in supply chain complexity must be managed. It is expected agencies will strategically partner with one or two key brokers and develop a close business understanding and relationship.

### Role of a broker

An agency may engage a broker to perform one or more of services (or sub-services). These services have been broadly categorised as market research, negotiation or ancillary services. The notable client control points are:

- acceptance of the selection of services provided by the broker
- acceptance of the commercial terms, information security assurance process, and, risk and business impact assessment.

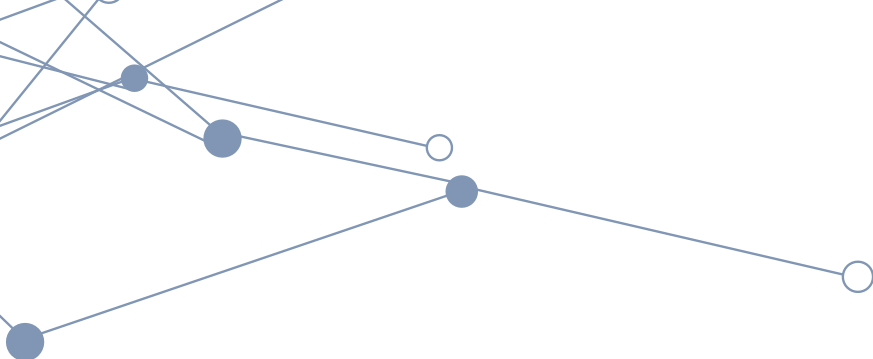
### Market research services

- **Research:** The broker works with the agency to understand their business requirements, researches cloud options and models available for the agency to make informed business decisions.
- **Qualification:** The broker based on agency criteria presents matching services.
- **Assessment:** The broker assesses the agency's business and ICT environment to gauge suitability.
- **Selection:** The agency selects services through the broker.

### Negotiation and assurance services

- **Negotiation:** The broker supports the ability for agencies and CSPs to negotiate business terms, either by facilitating direct communication or via some level of automated intermediation.
- **Assurance:** The broker may take a limited or active role. The broker follows the agencies and Queensland Government's information assurance and risk management frameworks. However, the broker's involvement doesn't absolve the CSP or the agency from performing their own due diligence in meeting respective security and compliance objectives, including risk acceptance and ongoing risk management.





- **Acceptance:** The agency must accept the business terms it selects via the broker including the outcomes from risk, business impact and information assurance assessments.

#### Ancillary support services

- **On-boarding:** The broker may support the agency transition, migration and provision of cloud resources.
- **Management/integration:** The broker manages the relationships between both the CSP and agency throughout the lifecycle (both business and technical).
- **Integration –** Optionally, the broker may assist with integration via an integration hub or bus.
- **Failover:** The broker may also handle and provide support with switching providers. Such failover may occur as the result of a technical problem (e.g. a denial of service incident or a business problem where the primary CSP is no longer competitive or operating).
- **Off-boarding:** The broker may facilitate transition out, extraction of data, including confirming data no longer resides in the CSP and contractual termination.
- **Help desk support:** The broker may be engaged to provide help desk (level 1 or level 2 support) and assist with incident management, problem management and change management processes.

#### Standards

The following standards and procedures will be developed to support the operation of the ICT marketplace and multiple cloud brokers:

- standard guidelines for supplier accreditation to ensure consistent vetting of suppliers and assurance levels, including matching the level of certification based on the data classification/sensitivity
- a standard data classification framework to ensure a consistent approach to dealing with the sensitivity and confidentiality of information assets
- an as-a-service decision framework and methodology to ensure informed and evidence-based decisions surrounding placement and orchestration of workloads across cloud services, including selection of appropriate service and deployment models
- a common CloudStore taxonomy to assist with categorising and comparing cloud service offerings against desirable business and non-functional service attributes and characteristics. For example, the contract jurisdiction, data storage location, data extraction ability, cloud deployment model and recognised security certifications held by a provider.

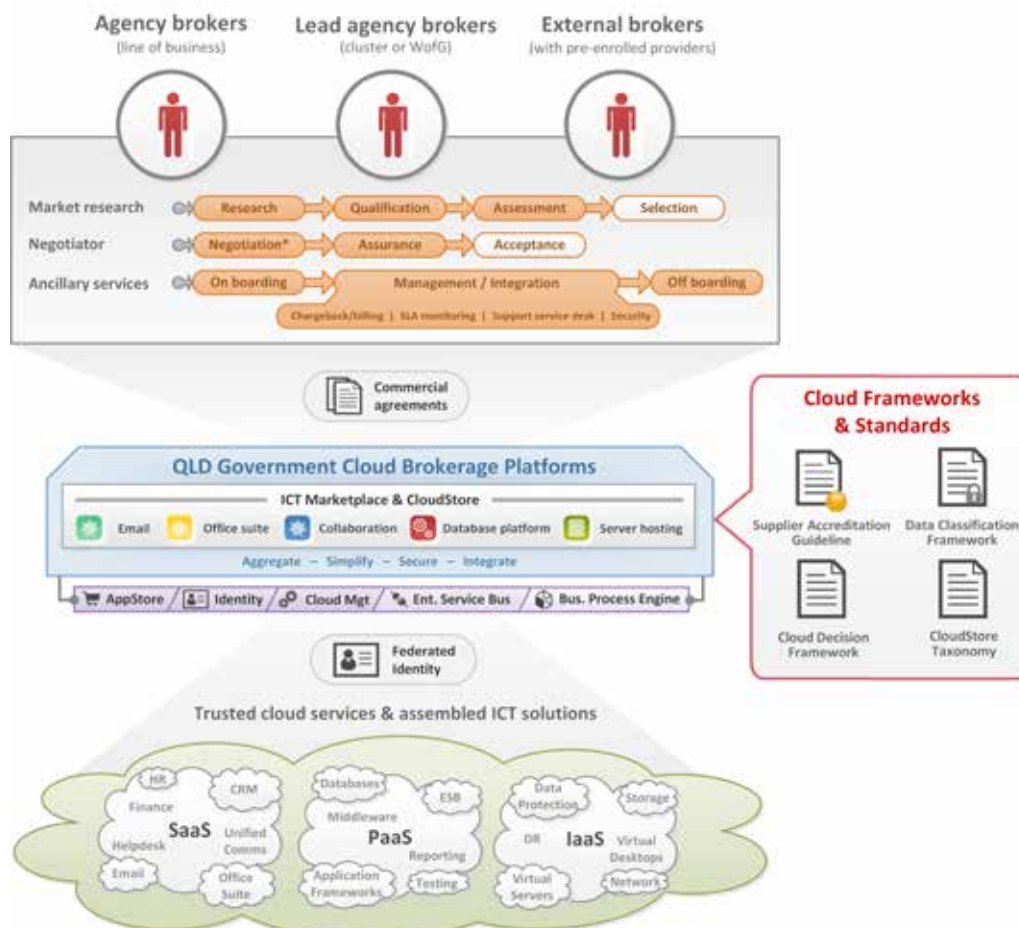
Cloud brokers (internal or external) will be required to:

1. operate under a common governance model
2. participate in a common ICT marketplace for Queensland Government
3. integrate and utilise the government's brokerage platform/s to consistently aggregate, secure, integrate their service offerings. The brokerage platforms will provide a common:
  - storefront to offer, provision, manage and meter services
  - identity and authentication framework for individual agency or shared agency SaaS services

- cloud management interface for IaaS services
- integration bus for data interchange and integration for SaaS services with government information systems.

As depicted in Figure 7, multiple cloud brokers will establish commercial agreements for cloud services, which in turn, are added to a common government-wide storefront (or agency sub-store) for reuse. Brokers utilise common data classification, supplier accreditation frameworks and taxonomies to profile and describe offerings.

**Figure 7: Multiple cloud brokers participating in a common ICT marketplace**



The concept of brokerage will vary across providers, with some offering simple links to manual service provisioning functions, to fully integrated and orchestrated service provisioning (click-to-buy).



## Commercial role

Given the maturity of the cloud market, the number of potential external cloud brokers is currently limited. The commercial arrangements which govern external broker models are also still relatively untested globally and continue to be developed and evolve. As the maturity of these models improve and become more streamlined, external cloud brokers should be engaged where there is clear value. By default, an agency will inherit brokerage responsibility and may engage external procurement services or legal advisers for assistance.

Commercial obligations and contractual commitments for cloud services may be held and/or negotiated directly by Queensland Government with a CSP or by the external broker on government's behalf. However, the exact model is likely to vary on a case-by-case basis, given the nature of the commercial agreement and where the majority of the risk sits for the required service outcome.

The level of accountability placed on a broker for SLAs and end-to-end service management will become particularly important in circumstances where the broker bundles or integrates multiple underlying services together.

## 4. Agency ICT divisions will transition from a service provider to a service broker role

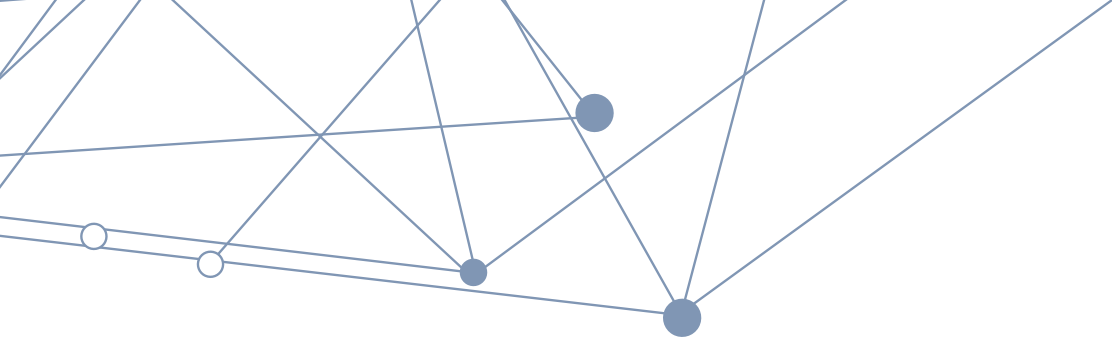
Traditionally, agency ICT divisions have been the in-house provider of ICT services. However, with cloud adoption and the corresponding sourcing ICT capabilities as-a-service, their role and mindset will shift from producing and managing assets to acting as a broker of ICT services from external suppliers or utilising other brokers to satisfy business needs. This paradigm shift is depicted below:

**Figure 8: Agency shift from service provider to service broker**



Agencies are to have a minimal asset ownership, and should be brokering, investing in and leveraging a network of ready-made capabilities to assemble and deliver innovative business-led ICT solutions. Notwithstanding this shift in role, there will still be a need to continue maintaining traditional ICT delivery components in a hybrid ICT model.

This change represents a significant organisational, cultural and technological shift for the agency ICT division, and for agencies as a whole. Strong organisational change management, governance and leadership is required to facilitate and manage this interdependent commercial, cultural and technological shift.



The agency or service broker's primary role will be to:

- facilitate the acquisition of cloud capabilities (e.g. procurement and contract management)
- assess the benefits, risks and costs of business requirements against cloud offerings
- orchestrate workloads and capabilities across a portfolio of service providers
- manage service demand, optimise consumption, licenses and associated costs
- monitor and manage service quality and supplier performance
- understand the wider cloud market to optimise financials and manage service lifecycles.

Value in this new model is delivered through a broker's ability to consume and orchestrate multiple pre-packaged services in a structured way that:

- unifies delivery across multiple suppliers and delivery channels
- enables anywhere, anytime and self-service access to ICT capabilities
- assembles custom-fit ICT solutions using standard and interchangeable cloud components
- exploits new disruptive cloud patterns and benefits to deliver more cost-effective services
- continually brokers and enables new and innovative services and solutions.

## **5. An ICT marketplace and storefront will support the sourcing of a wide range of mass-market ICT services from industry**

Establishment of a ICT marketplace and associated storefront (CloudStore) for government will support the sourcing of a wide range of mass-market ICT services from industry which continues to improve and innovate due to high competitive market forces. The government ICT marketplace will serve as the first point of call for agency ICT requirements and aims to:

- create a vibrant marketplace/ecosystem enabling the best product at the best possible price
- simplify and standardise the adoption of commodity ICT services
- promote the sharing and re-use of common ICT services, solutions and components.

The ICT marketplace will offer an interactive storefront, providing agencies with the information, tools and community to discover the best ICT solutions which meet their needs at the best possible price (i.e. value for money). This concept is similar to that of a travel search engine, where users can input specific requirements or criteria to discover available options including cost.

Catalogue offerings will be categorised against a standard taxonomy which embeds the appropriate cloud decision and policy points to support comparing cloud service offerings against desirable business and non-functional service attributes and characteristics of unity and tariff.

The taxonomy will also support a linkage to the:

- inputs and outputs of the Queensland Government Enterprise Architecture (QGEA) ICT-as-a-service Decision Framework
- the supplier accreditation guideline to describe industry-recognised certifications held by a provider.

When standardising a given taxonomy, there is a need to balance homogenising all cloud services to a lowest common denominator (to promote price comparison and competition) and supporting a sufficiently diverse range of catalogue items for differentiation and innovation. Consideration will be given to the degree of control over each catalogue class to ensure the large volume savings opportunities (e.g. email, office productivity, IaaS etc.) are well represented without stifling the niche and innovative cloud-sourced capabilities.

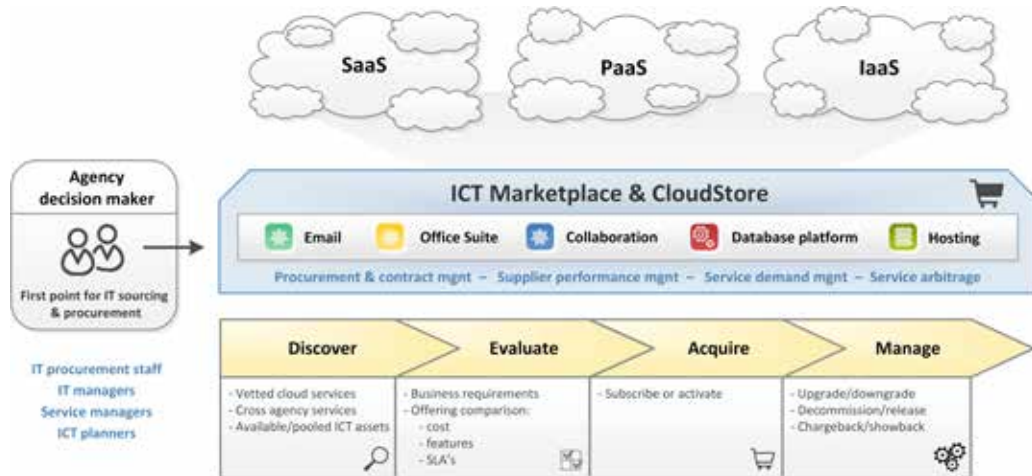
The ICT marketplace seeks to drive the best product at the best possible price by:

- encouraging suppliers to provide innovative solutions
- broadening competition to encourage SME and niche suppliers
- leveraging whole-of-government purchasing economies of scale
- providing transparency of cost and comparative performance indicators
- providing a framework/channel for industry to easily interface with government
- streamlining procurement through simplifying recurring acquisitions of products and services
- reducing duplication of cloud procurement and redundant security assessments
- offering mechanisms for agencies to quickly discover and use evolving technology
- contracting cloud services on a short-term basis
- enabling continual competition and higher flexibility, including options for dynamic services.

The conceptual schematic (Figure 9) depicts a common ICT marketplace that institutes consistent acquisition processes and provides a tangible means for agency ICT procurement managers, ICT architects and strategists, and service delivery managers to:

- discover cloud services and facilitate choice and cost comparisons across services
- evaluate offerings against business needs and determine suitability/availability of cloud alternatives
- provision new services in an automated fashion—upgrade, scale up or down or switch services
- manage consumption, business demand and ICT supply processes and relationships
- manage associated costs through a common financial model for IaaS, PaaS, SaaS across community and public clouds.

**Figure 9: Queensland Government ICT marketplace and CloudStore**



Easy access to multiple best-in-class offerings will also provide greater choice, flexibility and reduce vendor lock-in by minimising costs associated with switching suppliers through efficient on-boarding and off-boarding. Government suppliers will be able to offer new service releases and product improvements as they become available—the applications store concept and product lifecycle approach allows for new and existing consumers to readily discover new services, options and innovations. The ability to quickly and easily take advantage of these new market capabilities is underpinned by a no lock-in strategy and the ability to contract cloud services on a short-term basis. There is also benefit in an ICT marketplace that can support more rapid access to innovative services which do not require the same level of accreditation (for certain categories of services).

## Benefits

The CloudStore will streamline procurement by providing:



### **A catalogue of trusted cloud services for agencies**

A catalogue of trusted cloud services will be available from accredited suppliers, with assurances that the terms and conditions have been vetted, surety of security controls and a contract and rate schedule has been agreed to in advance. This catalogue will expand as brokers establish commercial arrangements with cloud providers and add those offerings to the ICT marketplace.



### **A common service description framework**

A common taxonomy will assist with categorising and comparing cloud service offerings against desirable business and non-functional service attributes/ characteristics. For example:

- contract jurisdiction
- data storage location
- data extraction ability
- cloud deployment model
- industry-recognised security certifications held by providers.

The standard attributes support the QGEA ICT-as-a-service Decision Framework.



### **Whole-of-government and agency storefronts**

The CloudStore will support a tiered model, with agency sub-stores and a common storefront for whole-of-government services.



### **Improved visibility of government ICT consumption**

The applications store will provide better visibility into government ICT consumption and outsourced arrangements to:

- compare value to cost
- better plan ICT investments
- manage supplier performance
- aggregate demand
- allow agencies to better understand and adjust their consumption.

## 6. A federated identity model will underpin sharing of commodity and common services, multi-vendor sourcing strategies and support the establishment of a new cloud security perimeter

Large scale cloud adoption will see Queensland Government's ICT environment become more fragmented, distributed and more of a virtual concept. Current government business applications service a defined set of local users, reside in tightly controlled and segmented local area networks and often have limited points of remote access.

The adoption of cloud services and other changes in work practices (e.g. greater mobility) will see government's application portfolio become part of a wider network of services running across the internet, servicing a more distributed set of users and be accessible anywhere at any time from multiple devices.

Protecting information stored across this extended network, combined with an increasingly mobile enterprise (where end-users often manage their own devices) requires a new approach to security. Traditional approaches to security include a heavy reliance on network-based perimeters that will increasingly prove difficult and less effective with cloud-based services.

Furthermore, as each cloud service has its own disparate authentication and authorisation model, it will prove increasingly difficult to:

- consistently apply security controls across multiple services and providers
- enforce policy consistent with current enterprise controls
- strengthen the security of particular applications and data
- gain visibility and control of government data
- demonstrate compliance.

A degree of integration (at an identity level) is required to connect multiple disparate cloud services into a consistent federated framework that allows for centralised, contextual and risk-based authentication and authorisation security controls to be enforced consistently, regardless of an individual provider's capabilities or technology.

The implementation of such models often represents a major undertaking for agencies, given most current identity architectures are positioned to support inward identity propagation for on-premise enterprise applications, compared to an outwards (or federated) model in support of externally-hosted services and business partnerships.

It is also difficult and expensive for an individual organisation's in-house resources to implement and manage such a high level of integration given continually changing APIs, the maturity of the standards and the varying vendor support.

Identity brokerage services assist by providing access to large portfolios of pre-integrated services and cloud service connectors, including extensible integration points.





## Business drivers

An integrated view of identity is required to:



### Secure cloud services

Provide a secure authentication and authorisation framework to ensure government security policies can be applied consistently across providers, including the ability to leverage and integrate existing identity investments.



### Integrate cloud services

The ability to facilitate integration (system/data/process/interface) between multiple cloud services (or providers) including the ability to facilitate cloud migrations.



### Share cloud services

Allow multiple agencies to share a single cloud service (fit within one organisational tenant context) to provide an enhanced level of collaboration, for example, a shared customer relationship or travel management system.

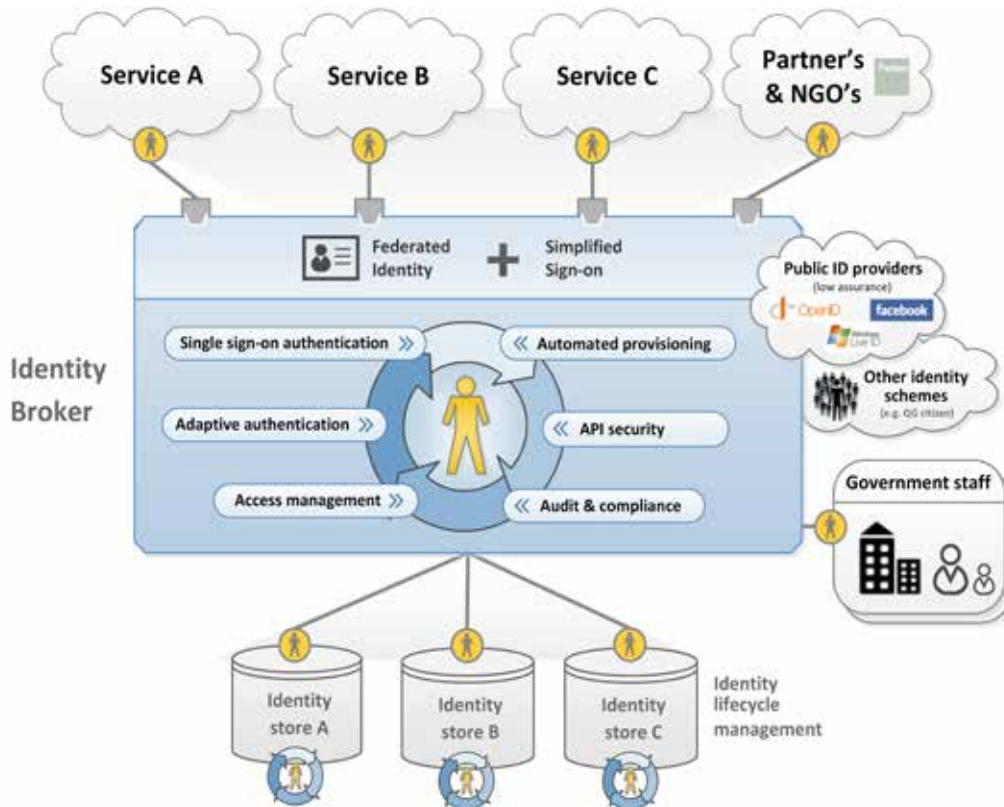
To support the first two drivers, agencies will be enabled and supported through the adoption of cloud identity federation capabilities (delivered as a service) for direct federation with their line of business cloud services.

A whole-of-government federated identity broker will also be established to support the sharing of cloud services and applications across agencies and whole of government. Federation with non-government organisations and partners should occur using the central broker where there is benefit in standardising and abstracting government integration requirements for providers.

Baseline requirements will be established to ensure procured cloud services will be capable of federating with whole-of-government or individual agency-based identity providers.

Figure 10 depicts the concept of an identity broker which integrates with an agency's existing identity management environment to leverage existing investments (enrolment processes, credentials and directories). An identity broker also facilitates federation with partners and non-government organisations, public identity providers and other identity schemes such as the Queensland Government Citizen Identity Management Scheme.

Figure 10: Federated identity broker concept

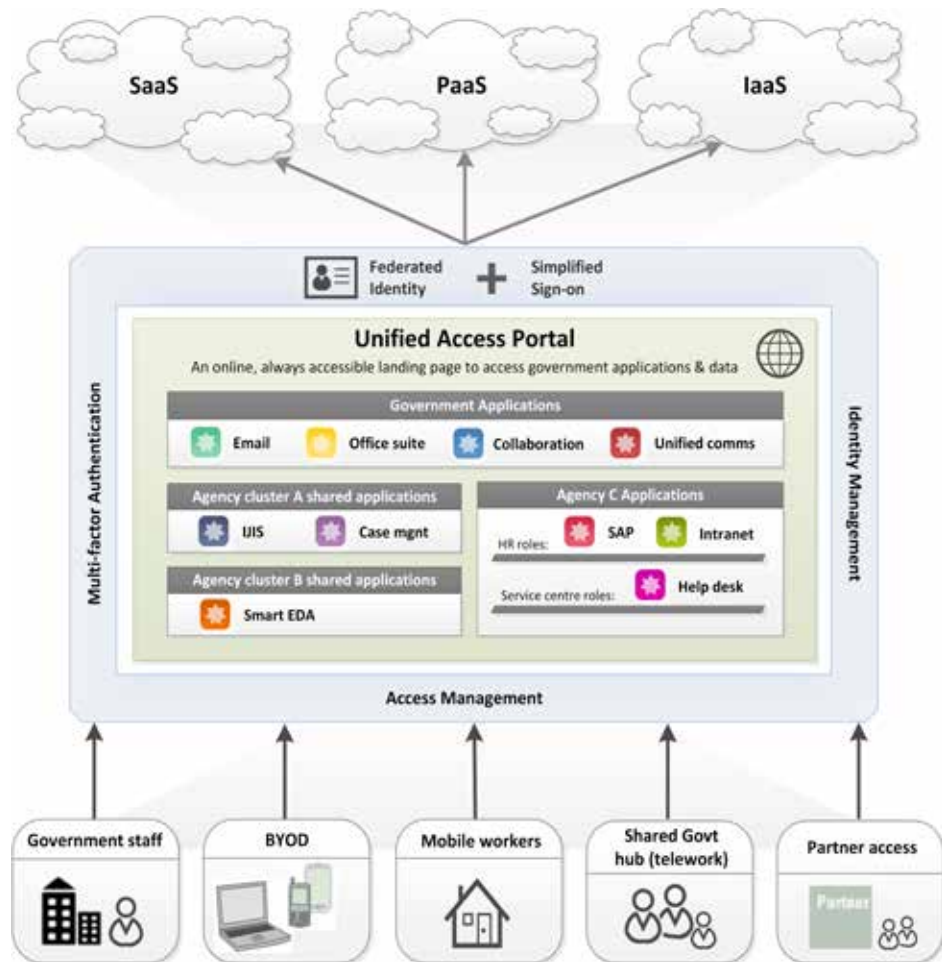


The identity broker’s access portal will provide a single landing page for users to securely and transparently access the brokered cloud services from anywhere, at any time from a wide range of devices. This consistent and managed access point provides:

- the ability to control access based on user/role, device, location, time etc. including authentication strength
- single sign-on capabilities to provide one secure password for all services, ensure government credentials are never known or stored repeatedly by external providers and that compromised credentials can be changed in one place
- self-service administration and delegation of entitlement management
- automated provisioning and revocation of access
- a central point for audit and compliance.

Figure 11 depicts the concept of a unified access portal (or cloud desktop) and portrays the grouping of applications based on a user’s role.

Figure 11: Unified access portal/cloud desktop concept





## 7. Trusted cloud services will be pre-enlisted from multiple providers

Government will move away from mandated central agreements, to pre-qualified and accredited providers where commodities can be bought on short-term contracts. Services will be available from multiple cloud providers, to minimise lock-in and provide competitive tension that creates an environment for improving service quality and price competitiveness.

Agreed exit strategies will form part of cloud service contracts to streamline the process of switching providers should a provider fail to deliver on its SLA, exit the market or fall behind the capabilities of its competitors. Such conditions will stipulate certain pre-conditions and caveats for data management (e.g. allowance for data migration upon contract exit) to reserve rights to enable alternative sourcing.

There will be an increased importance placed on the use of open standards to reduce the risk of vendor lock-in, provide data portability and/or facilitate interoperability between different vendor clouds. The inadvertent creation of islands of cloud technologies and data would otherwise lock government into solutions that may become rapidly out-of-date or be difficult or expensive to change. Current solutions are typically vertically coupled into single vendor contracts or technology silos.

New ICT solution components should also be loosely coupled to preserve options for the government to transparently source capabilities at each layer of service from multiple providers where the added complexity is outweighed by additional business value.

It is expected government's cloud portfolio will consist of specific SaaS clouds for line of business applications, a smaller number of PaaS clouds aligned with the mainstream application development frameworks and an even smaller number of enlisted IaaS clouds. It will be important the cloud brokerage platform/s can continuously support a dynamic and changing cloud services mix.

IaaS and PaaS service arrangements will be required to support a hybrid framework/model to provide workload portability across different cloud deployment models and zones (community and public) to cater for different data classifications. Open PaaS and commercial versions of open PaaS platforms can also support a hybrid model which reduces lock-in associated with vendor specific offerings and provides a consistent management framework across different service providers and deployment models.

Each best-in-class cloud offering will provide for varying degrees of security, availability, scalability, performance and price to support different government workload requirements. Over time, it will be possible for highly-commoditised functions (e.g. IaaS computer services) to be rapidly switched between suppliers based on policy variables such as cost-effectiveness, performance and availability through an arbitrage brokerage capability.



## 8. Information security will be improved through the use of mature, well-credentialed cloud services providers

Mature cloud service providers hold extensive security accreditations, and implement well-established security management processes which undergo regular audits, and provide monitoring and reporting mechanisms. The reputation of major cloud providers rests on their security practices and compliance with the data sovereignty requirements of their customers. Significant breaches can impact their business severely and precipitously with major events and incidents often being disclosed in the public arena.

In many cases, information security will be enhanced by moving an ICT system to a mature, well-credentialed cloud services provider. The relative risk of cloud-based services can be lower than what government agencies have been able to achieve internally in the past with limited security-focused resources and funding<sup>5</sup>. There is a potential risk in not adopting appropriate cloud services where it confers improvements in service delivery, cost reduction, and information security.

While the use of cloud-based services will see a reduction of risk in certain areas, the level of risk may increase in other aspects of cloud-based services. Understanding the risk/reward value proposition and changed risk profile of a particular cloud opportunity is key to determining its suitability. One of the primary changes and challenges with cloud environments is that governance, compliance and risk management responsibilities are typically shared between the customer and cloud service provider.

There are a number of specific risks/issues/challenges that need to be considered when utilising cloud services. Although most risks are shared with the traditional ICT outsourcing model, the transfer and potentially off-shoring of data to a cloud service provider (particularly public cloud services) can introduce additional risk relating to data sovereignty, privacy and portability<sup>6</sup>.

### Data classification and risk assessment

Agencies are required to conduct risk assessments for the particular ICT workloads they wish to move to a cloud environment. The existing QGEA and methodologies for data classification and threat and risk assessment are as equally valid for cloud services as they are for traditional architectures. Use of these methodologies is, however, generally at a low level of maturity across the sector.

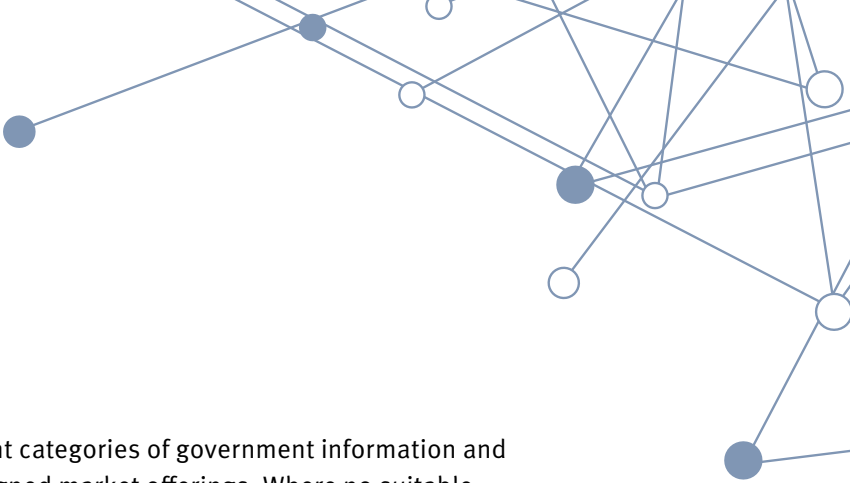
Classification of agency data (using the government's data classification scheme<sup>7</sup>) remains critical and will assist agencies to identify data that is sensitive or confidential, and data that may require specific security needs. This will allow agencies to identify a desired cloud delivery model<sup>8</sup> (e.g. private, public, hybrid, on-shore, off-shore,

5 The Auditor-General's reports to Parliament on information security in government agencies have raised issues of inadequate security capability over the last 3 years.

6 The Queensland Government Cloud Computing Guideline Annexe – Risk/Considerations document is focused on providing further guidance regarding the key risks dimensions of cloud services that agencies should consider.

7 The Queensland Government Information Security Classification Framework (QGISCF) provides a framework for agencies to consistently classify their information in order to manage risks associated with confidentiality, integrity and availability.

8 The QGEA Cloud Decision Framework – Deployment Model Selection guideline outlines the potential suitability of the various deployment models with respect to data classification.



on-premise, off-premise etc.) for different categories of government information and systems and to subsequently assess aligned market offerings. Where no suitable market offering exists, agencies may need to reconsider their initial requirements and deployment model preferences.

### Supplier accreditation

Queensland Government will look to utilise well-known industry-recognised accreditations (e.g. ISO 27001, SOC2 Type 2 or SOC3 etc.) as evidence of assurance. Qualified cloud service providers will be required to comply to these industry-recognised security standards, certifications, and require regular audit commensurate with the sensitivity of the information being processed on their systems.

Leveraging the use of third-party accredited assessors and assessments will avoid the need for Queensland Government to audit and individually certify cloud providers. For most public cloud services, an individual client will not have the right to audit.

A supplier accreditation guideline will be developed to assist agencies to understand the equivalence of Queensland Government security requirements (e.g. Information Standard 18) to industry-recognised accreditations and the value of those accreditations as to what constitutes sufficient assurance.

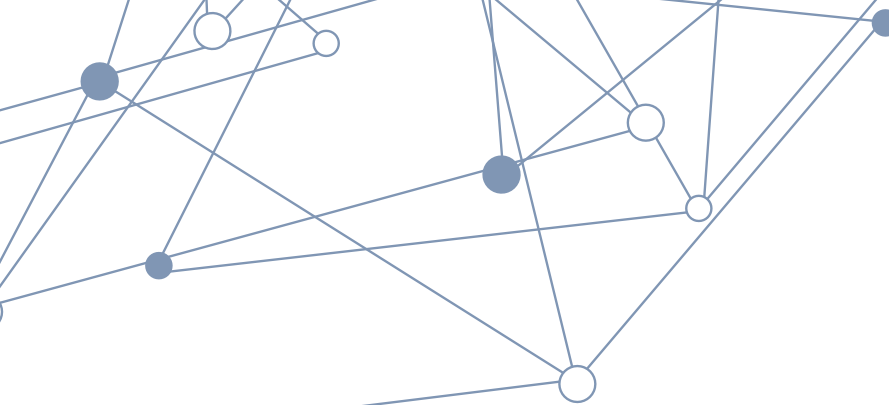
Self-assessment options such as enrolment on the CSA Security Trust and Assurance Registry with a completed CSA Consensus Assessments Initiative Questionnaire may be valid for lower levels of assurance for certain systems.

## 9. A Queensland Government community cloud for IaaS will be established to support common government and enterprise-grade ICT requirements

Public and private cloud computing are considered two extremes. Community hybrid clouds offer a blend of public and private cloud benefits and challenges which address a specific set of organisations or individual's needs (e.g. government, the healthcare industry, universities etc). Community clouds, unlike public cloud, service substantially fewer users and can more extensively address the privacy, compliance, security, availability and performance needs or risk tolerance of its community.

Establishment of a Queensland Government Community IaaS cloud will better support agencies' enterprise-grade ICT requirements and accommodate a wider range of existing traditional computing workloads not immediately suitable for public cloud.

Community cloud in the short term serves as an intermediate stage between the current agency private only models and public cloud computing. A more controlled computing environment with limited membership may assist to build trust in cloud models for highly-sensitive workloads as resources are not shared with non-government users. Due to Queensland Government's existing investment in data centre facilities, both options for on-premise and off-premise models delivered as-a-service will be considered.



The community cloud service will provide:

- a local in-country location to efficiently address government security and privacy requirements, including latency considerations
- a more controlled environment with greater ability to support government or agency-specific compliance and legal requirements
- a higher assurance environment which is not shared with non-government users to host sensitive data
- a more isolated environment with greater ability to guarantee resources for critical applications or reallocate resources in support of wider government priorities
- the capability to support a wider range of enterprise-grade ICT requirements and workloads, including higher guarantees for business critical applications and data
- potentially a higher level of flexibility to accommodate functions required outside of a provider's standard core services
- government-wide pooling of demand.

The community cloud model aligns well with services offered by the local ICT industry. Gartner states: 'most cloud providers in Asia do not pitch themselves as public cloud providers. They believe they lack the scale or innovation to compete with large disruptive players such as Amazon. As such, they are focused on offering 'private' or 'virtual private cloud' services to large enterprises looking for enterprise-grade services<sup>9</sup>.

Local cloud providers also differentiate themselves by in-country data centres and providing local support. If similar community cloud initiatives are undertaken at federal, state or local levels, this may present opportunities to further pool resources.

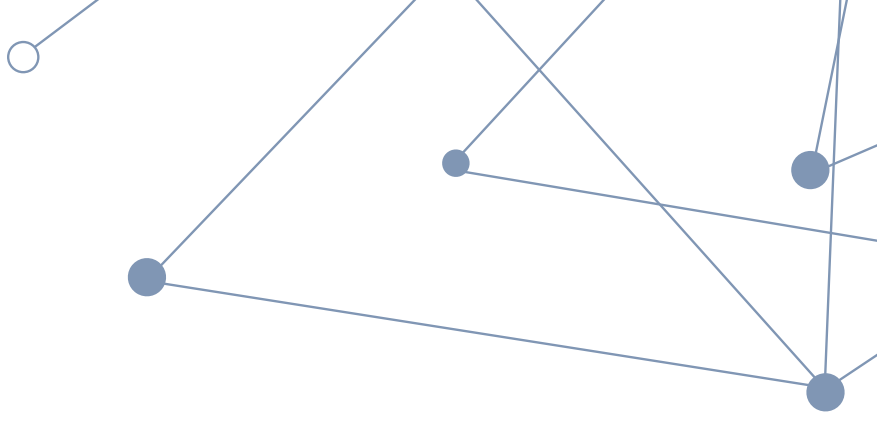
In alignment with the cloud-first strategy, agency IaaS workloads will be transitioned into public or community clouds where possible. To drive transformation, agencies will be actively discouraged from building or acquiring private cloud computing infrastructure within their organisations and expansion of existing virtualisation infrastructure will be actively discouraged and subject to contestability.

Where an agency identifies new infrastructure requirements for applications that cannot be hosted outside their organisation for valid reasons, it is proposed that other existing workloads be considered for relocation to the public or community clouds to release internal capacity instead of expanding or acquiring additional localised capacity.

Public cloud IaaS is considered the default position for hosting workloads. The community cloud delivery model represents a transitional stage to full public cloud adoption to support workloads which are not immediately suitable for public cloud or are cost prohibitive. The QGEA ICT-as-a-service Decision Framework will guide agency workload placement.

---

9 Key Considerations for Selecting Cloud Providers for Enterprise Requirements in Asia/Pacific, Gartner 2012 (G00236073)



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.) has been resolved. Additionally, the suitability of potential cloud candidates should be reviewed in line with major infrastructure and application refresh cycles.

It should be noted, IaaS itself is only a transitional state for functions not able to be accommodated by SaaS, BPaaS or PaaS service models. However, the transition to community or public IaaS arrangements may in some circumstances deliver specific business outcomes (e.g. cost reduction, reassignment of resource and expertise) for certain workloads (e.g. migrating platforms for legacy systems) in the short term while reducing the cost and risks associated with more complex transformation programs.

A hybrid cloud sourcing approach for IaaS will see the internal community cloud resources be augmented with other connected public clouds. Workloads may be migrated between connected public clouds or brought back into the community cloud based on market pricing, capacity requirements or quality of service attributes (e.g. performance or availability). IaaS integration brokerage software (a CMP) will provide visibility, consistent management and policy across the multiple connected clouds.

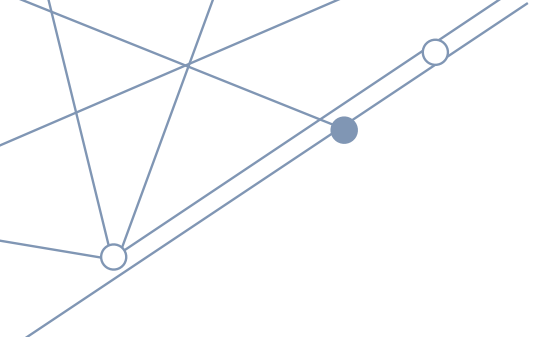
## **10. ICT services will become more accessible at any time, any location and preferably on any device**

Core systems and data should be accessible by staff remotely via a wide range of computing devices. Most current government ICT application resources are premises-based, along with the access to them. The adoption of appropriate cloud-based services will see government applications and data more accessible from the internet and web-enabled devices such as smartphones, laptops and notebooks. Associated end-user applications from consumer app stores (such as Apple iTunes® and Google Play™) will also improve the front-end usage experience through native device support.

The transition towards cloud-based services will also support future mobility and bring-your-own-device (BYOD) strategies, including the Queensland Government's one network vision.

To support this objective, Queensland Government will need to adapt security models to suit cloud environments and consider end-to-end security. The information that agencies have traditionally believed to be protected within the perimeter of their own networks will be shifted to the cloud. A new data-centric security approach which focuses on securing the data as opposed to the end-computing device (which constrains accessibility) is required. This dictates a security paradigm shift from network-based perimeter security models, which are increasingly challenged for effectiveness, to a user (identity) and data centric model.





The consumption of modern cloud-based services also provides the ability and opportunity to re-architect and address security at the application layer or application delivery channel to deliver a step-change in security over that available in legacy systems.

## **11. A cloud-educated workforce will exploit new cloud capabilities to deliver innovative solutions and cost efficiencies**

Queensland Government requires a cloud-educated workforce to readily consume and exploit new cloud capabilities and value sources. Persisting with traditional ICT practices and thinking will hinder the agility, innovation and cost-saving benefits delivered by cloud computing. ICT personnel will need to recognise new cloud patterns, skills and thinking to be able to fully leverage cloud capabilities, ensure efficient use, and support a cloud-first approach. Due consideration must also be given to cloud computing experience when hiring new ICT employees.

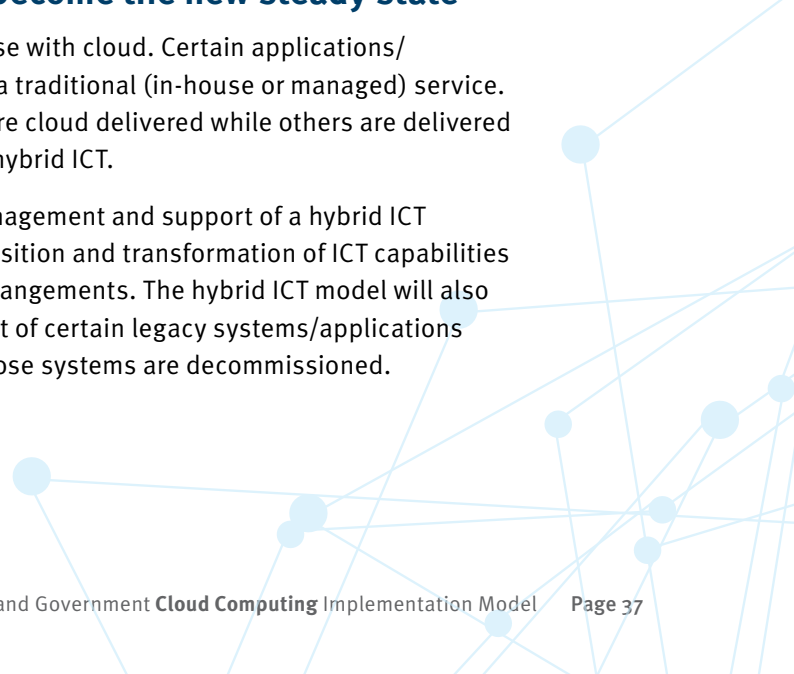
Cloud-educated ICT personnel will be able to:

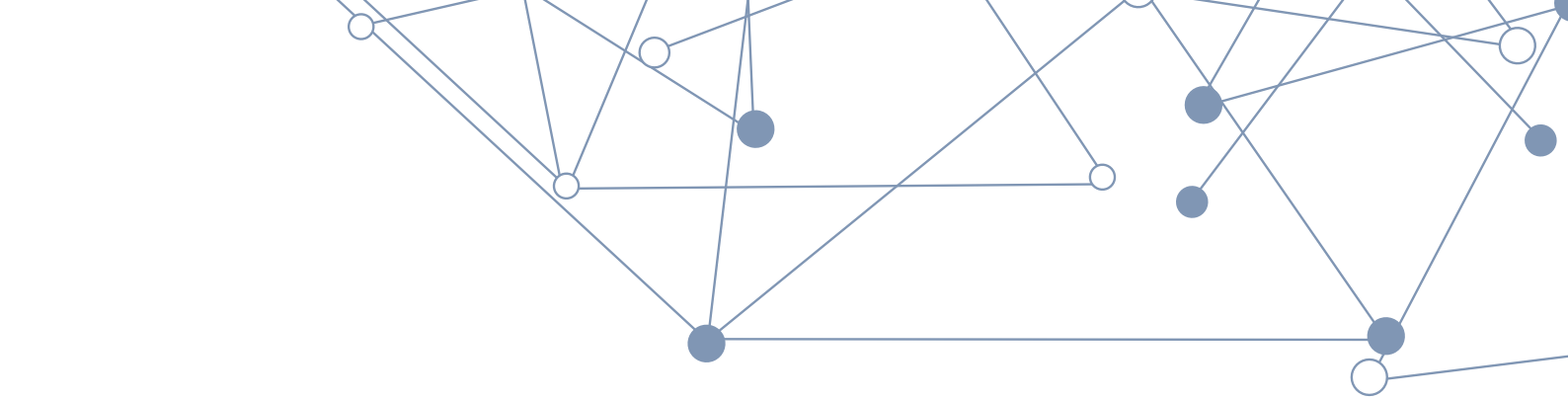
- design cloud-optimised solutions exploiting the scale, elasticity, multi-tenancy and high-availability benefits of cloud, with consideration for cloud sensitivities such as latency, performance and security
- manage cloud solutions efficiently to keep charges to a minimum
- integrate cloud services and other on-premise systems using modern web-based and API-driven integration technologies
- customise cloud services to deliver new functionality using modular cloud SaaS platforms or other workflow technologies to externalise business logic
- engage collaboratively with the consumer and provider communities in translating requirements and capabilities across both groups
- analyse cloud-based services financial benefits to prove business cases.

## **12. A hybrid ICT delivery model where cloud and traditional ICT environments co-exist will become the new steady state**

Legacy/traditional ICT delivery will not cease with cloud. Certain applications/workloads will continue to be delivered as a traditional (in-house or managed) service. The resultant state, where some services are cloud delivered while others are delivered under traditional models, is referred to as hybrid ICT.

Agencies will need to contend with the management and support of a hybrid ICT environment driven by the progressive transition and transformation of ICT capabilities to new cloud and as-a-service managed arrangements. The hybrid ICT model will also exist to support the continued management of certain legacy systems/applications unable to operate in a cloud model until those systems are decommissioned.





While the first preference is to source new capabilities and replacements for existing systems from the cloud, for a sub-set of operations, government will still have a continued dependency on licensed, on-premise, enterprise applications. This may be attributed to:

- market availability of suitable cloud alternatives
- leveraging existing return on investment
- technical constraints (such as software licensing, throughput or latency)
- requirements for greater levels of security, privacy or trust for critical data and applications.

In these cases, the ownership and management of such dedicated government infrastructure can be outsourced to trusted providers. Over time only the systems most unsuitable for cloud provisioning will remain.

The QGEA ICT-as-a-service Decision Framework provides a structured methodology for agency workload readiness assessment.

### **13. Maintaining an evergreen cloud environment will become the new benchmark**

The evergreen ICT vision is a pattern of ICT provisioning, architecture, and operational management designed to deliver loose coupling between logically distinct layers of the ICT stack such that every layer can be continually refreshed with reduced interdependencies between layers.

While the acquisition of evergreen<sup>10</sup> cloud services which are managed, maintained and upgraded transparently and automatically by external parties is a key enabler, this in itself does not guarantee a legacy-free environment. Achieving and sustaining an evergreen cloud environment requires a concerted effort and a set of new thinking, design practices and architectural patterns.

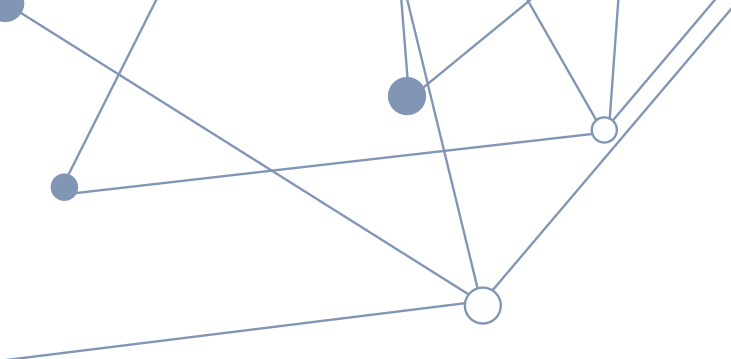
Adopting practices and patterns which aim to deliver loose coupling between logically distinct layers within the ICT stack, will allow components to be interchanged and continually refreshed relatively simply with minimal consideration for the interdependencies between layers. This provides an efficient and effective way of avoiding the creation of legacy complexities and cost with continued incremental investment.

The current close coupling of systems and all layers within their operating stack, including vendor-introduced lock-in means replacing one component often dictates the modification or replacement of other dependant components. The forced upgrade of inter-related components often imposes unnecessary costs, as those components could continue to be functional, meet business requirements and operate cost effectively.

Government agencies should have a constant emphasis on reducing dependencies

---

<sup>10</sup> Enabling Evergreen IT, Technology Forecast, Summer 09, PricewaterhouseCoopers, March 2009.



between components to allow components to be swapped out, upgraded or replaced when required and driven by genuine business need with minimal impact.

#### **14. Rapid access to cloud services will enable innovative, next-generation applications and service delivery**

Rapid access to large-scale global cloud service platforms will allow agencies to take advantage of leading-edge technology advances to assemble next-generation applications and innovative solutions to contemporary service delivery challenges.

Cloud development platforms will provide the opportunity to quickly prototype, test concepts and rapidly assemble new innovative business applications that respond to community needs. On-demand access to cloud resources provides the ability to investigate opportunities quickly with little or no upfront infrastructure or long-term commitment.

Examples of next-generation applications may be:

- social-ready applications which expose and capture events, data and activity streams
- citizen-focused applications exploiting new online channels, portals and interaction patterns
- mobile-first approaches and context-rich services which exploit new device technology and sensors
- composite applications which present and orchestrate together multiple separate application components or co-designed applications, potentially for multi-party/ multi-organisation transactions
- API-centric applications which leverage third-party API services and datasets for enhanced functionality and integration and expose APIs to improve interoperability, re-use opportunities and extensibility
- big data analytics and business intelligence based applications storing and processing large data sets and event streams.

## 5. Cloud considerations

While the potential benefits of cloud-based services are significant, adoption must be carefully considered. A cloud model represents a significant shift in the sourcing approach of ICT services to that which has historically existed in Queensland Government.

This shift brings with it a number of challenges and potential constraints that need to be considered. Each challenge will have a varying degree of difficulty, importance and influence over the ICT architecture and cloud-delivery model.

Both holistic and detailed planning is required for risk mitigation to ensure successful business outcomes. The following considerations outline the key risk dimensions pertaining to cloud services which agencies should consider using existing risk management frameworks. The QGEA ICT-as-a-service Decision Framework—Risk Assessment Guideline document expands upon each of the considerations below and suggests possible mitigations.

Challenges/ constraints	Description
<b>Market availability</b>	There are varying levels of maturity within the cloud market across service provider capabilities and cloud brokerage business models. While the market continues to evolve, the availability of cloud services which meet Queensland Government service assurance, confidentiality, security and privacy requirements in certain domains, may be limited or not available. This constraint mostly applies to the availability and maturity of ready-made SaaS solutions to replace traditional software services in parity for certain domains. In the short term, this may see an increased adoption of IaaS or traditional application management services for packaged products.
<b>Organisational change management</b>	The adoption of cloud services will involve significant business and cultural change to agency business practice, business operations, people and processes. Additionally staff skill sets, roles and responsibilities, contractual and financial operating models will need to be considered.

Challenges/ constraints	Description
<b>Business practice and processes</b>	<p>The transitioning of ICT functions to cloud solutions will 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 will require follow-on changes to interrelated and interdependent business processes, policies and practices. Cloud services are often highly standardised and therefore cannot accommodate the same level of customisation and integration possible (subject to cost) within traditional software packages. In some cases legislative changes may be required to facilitate changing business processes to suit commercially-supplied cloud software.</p> <p>In all cases, this presents an opportunity or challenge for agencies to consider opportunities for:</p> <ul style="list-style-type: none"> <li>• rationalisation, re-engineering, re-modelling business processes</li> <li>• simplification and standardisation of business processes</li> <li>• enable new business models.</li> </ul>
<b>Workforce capability</b>	<p>The adoption of cloud services will require agencies to build new skills and capabilities into their workforce. In particular, agencies will require a high level of proficiency in procurement, contract negotiation and management, and supplier performance management to ensure value for money is realised.</p>
<b>Impact and relationship with the ICT industry</b>	<p>The market shift towards cloud services will have a significant impact on the ICT industry throughout the world and see a reduction in capital investment in on-premise ICT infrastructure and applications. Ongoing consultation will be required to examine strategies/ approaches that progress the government’s requirement to move to cloud services while still ensuring a viable ICT industry in Queensland.</p>

Challenges/ constraints	Description
<b>Information, data and records management</b>	<p>There are a number of issues relating to information management and governance that need to be considered when utilising cloud services:</p> <ul style="list-style-type: none"> <li>• <b>data classification</b>—consistent classification of information to guide consistent approaches to dealing with the sensitivity and confidentiality of information assets</li> <li>• <b>data location/retrieval</b>—agencies will need to ensure that data is portable between providers and can only be stored in agreed locations, and be retrievable inside agreed timeframes</li> <li>• <b>data ownership and protection</b>—the Queensland Government will need to retain control over any data or information that is placed in a cloud service and ensure it is adequately protected from loss</li> <li>• <b>privacy, confidentiality and retention</b>—privacy of any data stored on a cloud computing service must be maintained in accordance with statutory/regulatory obligations</li> <li>• <b>data integrity and authenticity</b>—the Queensland Government will need the ability to prove records and other data 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 are not in place</li> <li>• <b>deletion/retirement</b>—agencies will need data permanently deleted from a provider’s storage media</li> <li>• <b>legislation and regulation</b>—agencies will need to be aware of Queensland and Australian legislative and regulatory requirements when storing personal data (e.g. the <i>Queensland Information Privacy Act 2009</i> and the <i>Public Records Act 2002</i> will apply).</li> </ul>
<b>Security management</b>	<p>Much of the information that agencies have traditionally believed to be protected within the perimeter of their own networks will be shifted to the cloud. Queensland Government will need to adapt security models to suit cloud environments and consider end-to-end security. One of the primary changes and challenges with cloud environments is that governance, compliance and risk management responsibilities are typically shared between the customer and cloud service provider.</p>
<b>Service integration</b>	<p>Using services from the cloud could present challenges to agencies when those services need to integrate with agency systems that are not in the cloud, or alternatively when data integration/migration is required between multiple services from different cloud providers.</p>

Challenges/ constraints	Description
<b>Service level/ performance management</b>	<p>Ensuring adequate service performance and reliability in cloud environments needs to be carefully considered. 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 key performance indicators.</p> <p>Certain cloud solution offerings will be dependent on internet connectivity and cloud providers may not commit to service performance (quality of service, latency, reliability) for the internet component since it is not within their control. IaaS services will be more dependent on performance characteristics of virtual private networks between end users and application hosting providers. Consideration may need to be given to wide area network application acceleration technologies to improve end-user experience.</p> <p>Application and network architecture changes and/or business process contingencies may be required in some circumstances to ensure satisfactory service levels in a cloud environment.</p>
<b>Financial and fiscal management</b>	<p>As Queensland Government moves to consume more pay-as-you-go service, utilising a cloud-based service delivery more, a proportion of capital expenditure (Capex) will need to be translated into operational expenditure (Opex).</p>
<b>Existing investments</b>	<p>The government has a significant existing investment in ICT applications and infrastructure that will need to be considered as services are moved to the cloud. It will be important to understand which infrastructure/applications should be maintained and leveraged, but also any instances where the current contractual models (e.g. software licensing) may present a potential impediment to cloud services that needs to be addressed.</p>
<b>Procurement and contractual management</b>	<p>A shift to pay-as-you-go cloud services introduces new contractual challenges that will require agencies to revise ICT legal contracts to cater for cloud providers and to cover issues such as: protection of information, liability, ending the arrangement, dispute resolution, early warning of bankruptcy (or similar), introduction of harmful code, compensation for data loss/misuse, change of control and assignment/novation, change of terms at the discretion of the provider, and information privacy.</p>

## 6. Implementation model

The Queensland Government will undertake a program of work to progressively transform into a cloud-first enterprise. Five key focus areas and work streams have been identified to progress this strategy:

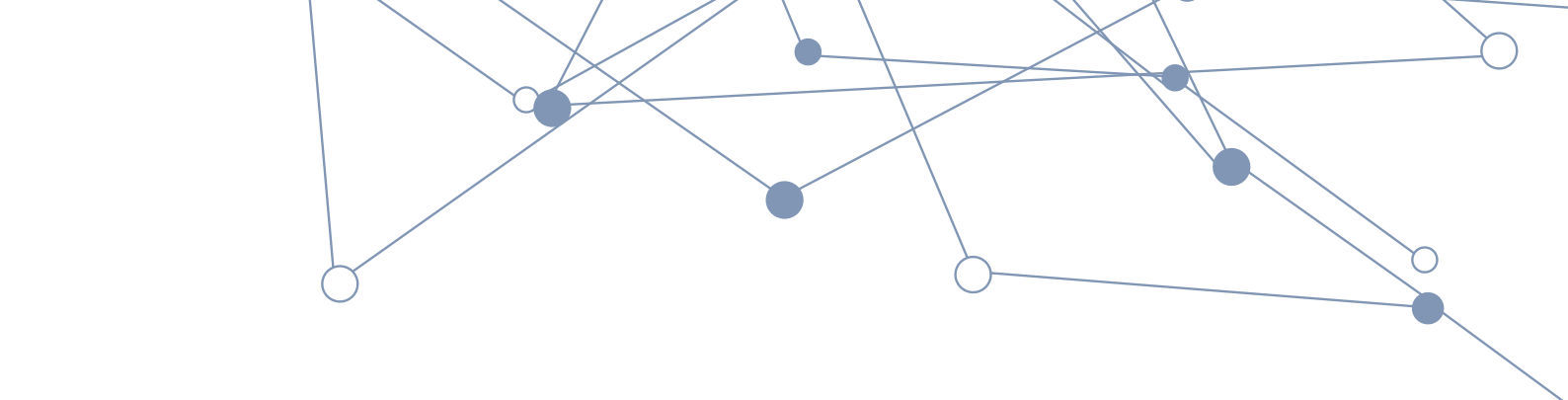
**Figure 12: Five key focus areas**



Focus area	Objective
Cloud ready	Set the necessary policy, standards, tools and frameworks to facilitate the adoption of cloud services across government.
Cloud foundations	Implement the commercial and technical brokerage foundations of a ICT marketplace and federated identity enablement.
Cloud engagement	Engage with agencies and industry to prepare for and assist with the take-up of cloud services.
Cloud accelerate	Encourage and transform government ICT through accelerated adoption of cloud services.
Cloud governance	Set in place the necessary oversight and guidance mechanisms to ensure Queensland Government can realise continued benefit.

The implementation approach across the five work streams seeks to balance the cloud-first imperative, with the recognition that substantial activity, as described in the cloud ready focus area, is required to provide the foundations necessary to ensure the successful and earliest adoption of cloud services.





The focus areas present a balanced approach allowing government to adopt services progressively in a managed risk way and to develop maturity/appetite for managing cloud services over time, recognising that not all current systems can or should be migrated to the cloud. There will be a focus on mature cloud commodity services initially as early wins and then a prioritised program of work to progressively identify and transition other services over time.

Recommendations are focused on providing the necessary support, sourcing arrangements, architectures and education which will ease the introduction of cloud computing services to agencies, while ensuring that government's transition to a cloud-first enterprise occurs in a timely manner.

The establishment of the ICT marketplace and brokerage approach are key to ensuring the continued success and sustainability of a vibrant cloud ecosystem. However, agencies in the meantime are encouraged to pursue opportunistic cloud investments which can be realised quickly, deliver initial savings and provide opportunities for hands-on learnings that will inform the future evolution of the other work streams.

There are significant benefits that the government can realise quickly through beginning the transition of workloads to an initial set of common cloud services. The adoption of individual cloud solutions early in the cloud maturity journey is supported; where such adoption poses a low level of incremental complexity and later integration with the brokerage and governance framework is possible.

Observations of the early cloud adopters indicates the most successful cloud implementations were achieved by those organisations that adopt an incremental and iterative approach to cloud adoption. The greatest successes to date have come from small, sharply-focused cloud projects, where business stakeholders and ICT staff worked co-operatively to drive business cases to success.

While the approach below outlines an intended implementation model to achieve the cloud-first enterprise vision, the execution path may differ while the market continues to evolve and mature. There are varying levels of maturity in the market across cloud brokerage business models, brokerage platforms, software vendor licencing models and service provider capabilities to meet the service assurance, confidentiality, security and privacy requirements of Queensland Government.

It should be noted, several of the initiatives target specific focus areas and stages within wider ICT strategies (e.g. identity federation within a broader identity management approach). These interdependent stages are leveraged as part of a singular cloud strategy to enable the progression and synchronised delivery of key building blocks required to support the cloud-first imperative.

A number of QGEA policy documents (outlined below) will be developed to provide guidance to support agency cloud adoption. The model cloud contract and cloud decision framework documents will undergo regular review to reflect lessons learnt and best practice.

## 6.1 Focus area 1: Cloud ready

### Outcome

Queensland Government agencies are educated and informed regarding best practice procurement and management approaches for cloud services, and are well positioned to successfully use cloud services to cost-effectively meet their business requirements.

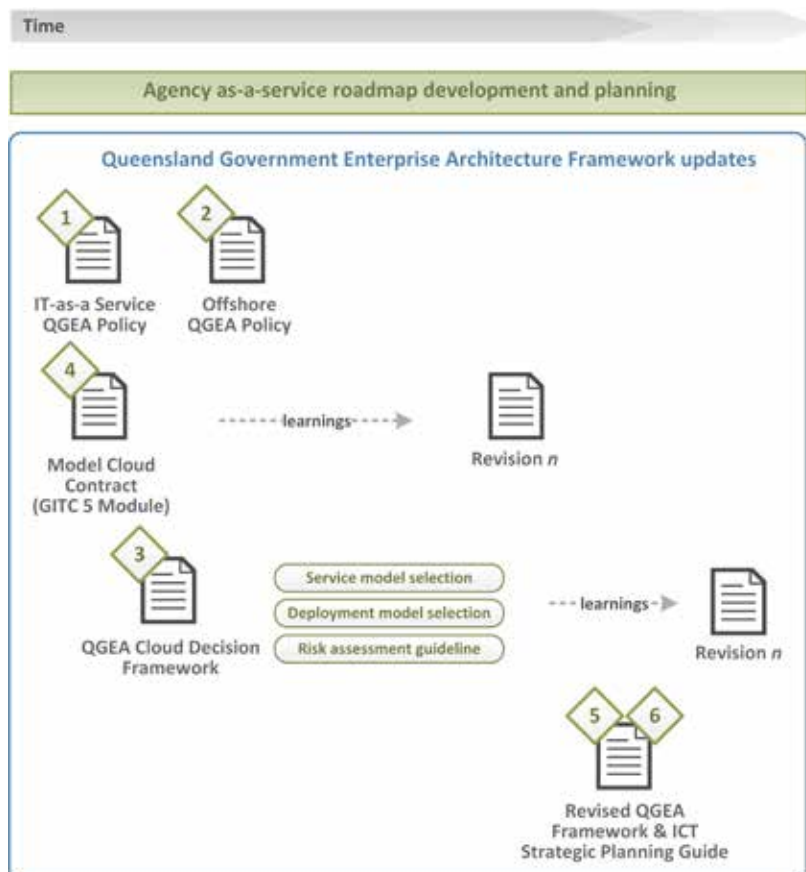
### Approach

The Queensland Government needs to develop and update existing policies, principles, frameworks and tools to guide agencies on the path to planning, implementing and managing cloud services.

A number of QGEA policy documents (outlined below) will be developed to provide guidance to support agency cloud adoption. The model cloud contract and cloud decision framework documents will undergo regular review to reflect lessons learnt and best practice.

As per the ICT action plan, agencies are required to develop as-a-service roadmaps to divest ICT systems and assets. Agencies will assess their ICT portfolio to prioritise early candidates for transition, identify timeframes and ensure alignment with contestability and their department's investment priorities.

Figure 13: Cloud ready implementation approach





## Description

### Cloud ICT-as-a-service Decision Framework

The QGEA ICT-as-a-service Decision Framework will be established to augment the existing QGEA ICT planning and portfolio management processes. The decision framework will provide a common planning framework that assists agencies in assessing the suitability of different cloud service options for particular circumstances. Key areas that the QGEA ICT-as-a-service Decision Framework will address include:

- policy/standards guidance regarding the use of cloud services
- architectural guidance regarding choice of cloud service model (BPaaS, IaaS, PaaS, SaaS) and deployment model (public, private, community) for particular ICT workloads
- tools to support risk and security assessment of cloud service options.

There are a number of areas of policy and legislation to be considered which do not fall under the umbrella of the QGEA. Key areas include:

- Queensland Government procurement instruments (e.g. State Purchasing Policy, GITC).
- state/federal statutory/legislative requirements (e.g. *Public Records Act 2002*, *Information Privacy Act 2009*, IS31—Retention and disposal of public records, IS40—Recordkeeping)
- legislative and regulatory requirements in other geographic regions
- funding arrangements
- workforce skills and capability<sup>11</sup>.

The decision framework will identify these touch points and highlight key considerations to address, however agencies themselves will also need to ensure compliance with any expectations specified in these instruments. Some or all of these instruments may need to evolve to support effective cloud sourcing.

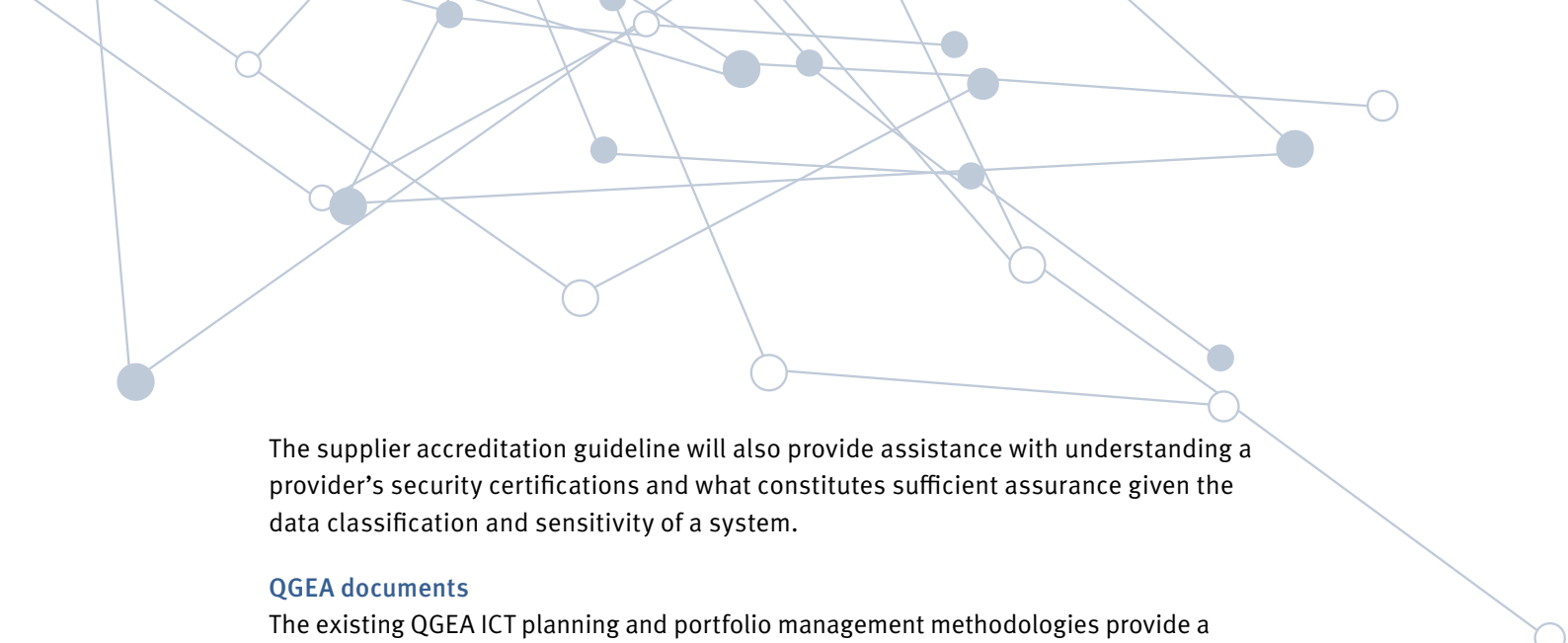
### Model cloud contract

A standard model contractual agreement and SLA for cloud services (SaaS through to IaaS service models) will be defined by government in the form of a GITC 5 module (10—Cloud services). However, in many cases, a cloud provider's contractual terms may be pre-defined and not malleable given the highly commoditised and standard nature of public cloud services.

To support public cloud adoption, the model contract will serve as a basis to understand a desired and agreed position to appropriately inform negotiation and risk trade-off assessments. Agencies may also need to seek further education and legal assistance to adequately understand the SLA and contractual elements offered by the provider.

---

<sup>11</sup> ICT workforce transformation is addressed as a topic within the Queensland Government ICT Audit



The supplier accreditation guideline will also provide assistance with understanding a provider's security certifications and what constitutes sufficient assurance given the data classification and sensitivity of a system.

#### **QGEA documents**

The existing QGEA ICT planning and portfolio management methodologies provide a robust framework to support agency business and ICT planning. These methodologies provide investment management guidance for ICT workloads in general terms, however consideration needs to be given to incorporating additional dimensions/tools relating to cloud sourcing. In particular, existing processes for establishing ICT inventory, demand aggregation and prioritisation need to be updated to better support the cloud-first enterprise vision.



## Recommendations

<p>1) Develop a QGEA cloud computing and ICT-as-a-service policy that reflects the cloud-first enterprise approach considering ICT strategic planning, capital investment, systems acquisition, development and integration.</p> <p>ICT action plan alignment:</p> <ul style="list-style-type: none"> <li>• Action [8.02]: Develop and implement government as-a-service policy (including cloud).</li> </ul>	<p><b>QGCI0</b></p>
<p>2) Develop a QGEA offshore data processing and storage policy to provide guidance and a process for the use of off-shore cloud services.</p> <p>ICT action plan alignment:</p> <ul style="list-style-type: none"> <li>• Action [5.01]: Develop security and privacy guidance, risk assessment and business impact assessment tools.</li> </ul>	<p><b>QGCI0</b></p>
<p>3) Develop a QGEA Cloud Computing Decision Framework to assist agencies in making well-informed and strategically-aligned placements of their application portfolio into cloud-based services.</p> <p>ICT action plan alignment:</p> <ul style="list-style-type: none"> <li>• Action [8.03]: Develop and launch the ICT as-a-service toolkit.</li> </ul>	<p><b>QGCI0</b></p>
<p>4) Review current ICT procurement arrangements with a view to developing an agile procurement process, supplier accreditation guideline, including the development of GITC 5 module reflecting standardised SLAs and model form of contract requirements for cloud services.</p> <p>ICT action plan alignment:</p> <ul style="list-style-type: none"> <li>• Action [8.04]: Revise and redefine commercial terms and conditions to support as-a-service options.</li> <li>• Action [7.06]: Deliver ICT procurement reform (short term).</li> <li>• Action [7.07]: Deliver ICT procurement reform (medium term).</li> </ul>	<p><b>DSITIA ICT Strategic Sourcing with QGCI0</b></p>
<p>5) Review and update the QGEA ICT strategic planning methodology, ICT baseline processes to improve decision process for cloud adoption and lifecycle management.</p>	<p><b>QGCI0</b></p>
<p>6) Review and update the QGEA framework to reflect treatment of cloud computing.</p>	<p><b>QGCI0</b></p>

## 6.2 Focus area 2: Cloud foundations

### Outcome

The key foundational building blocks are in place for Queensland Government to consume cloud services and manage the use, performance and synchronised delivery of a multi-provider cloud ecosystem.

### Approach

Department of Science, Information Technology, Innovation and the Arts (DSITIA) will lead establishment of the core cloud aggregation brokerage capability at a whole-of-government level including the:

- CloudStore and ICT marketplace (multi-tenant)
- identity federation platform for shared and cross-agency services
- IaaS brokerage/cloud management platform (multi-tenant).

By default, agencies are required to utilise the above centrally-provided and multi-tenant brokerage capabilities unless there are suitable grounds for exemption.

Agencies are also required to establish suitable brokerage and intermediation capabilities (delivered as-a-service) for services specific to a given agency (e.g. line of business). Required capabilities include:

- aggregation brokerage—identity management for direct federation with line of business services
- integration brokerage—enterprise service bus/cloud integration platform capabilities to facilitate and intermediate data interchange and interoperability between cloud services and agencies
- customisation brokerage—a business process management capability to orchestrate agency business processes across multiple cloud services and agencies.

DSITIA will continue to:

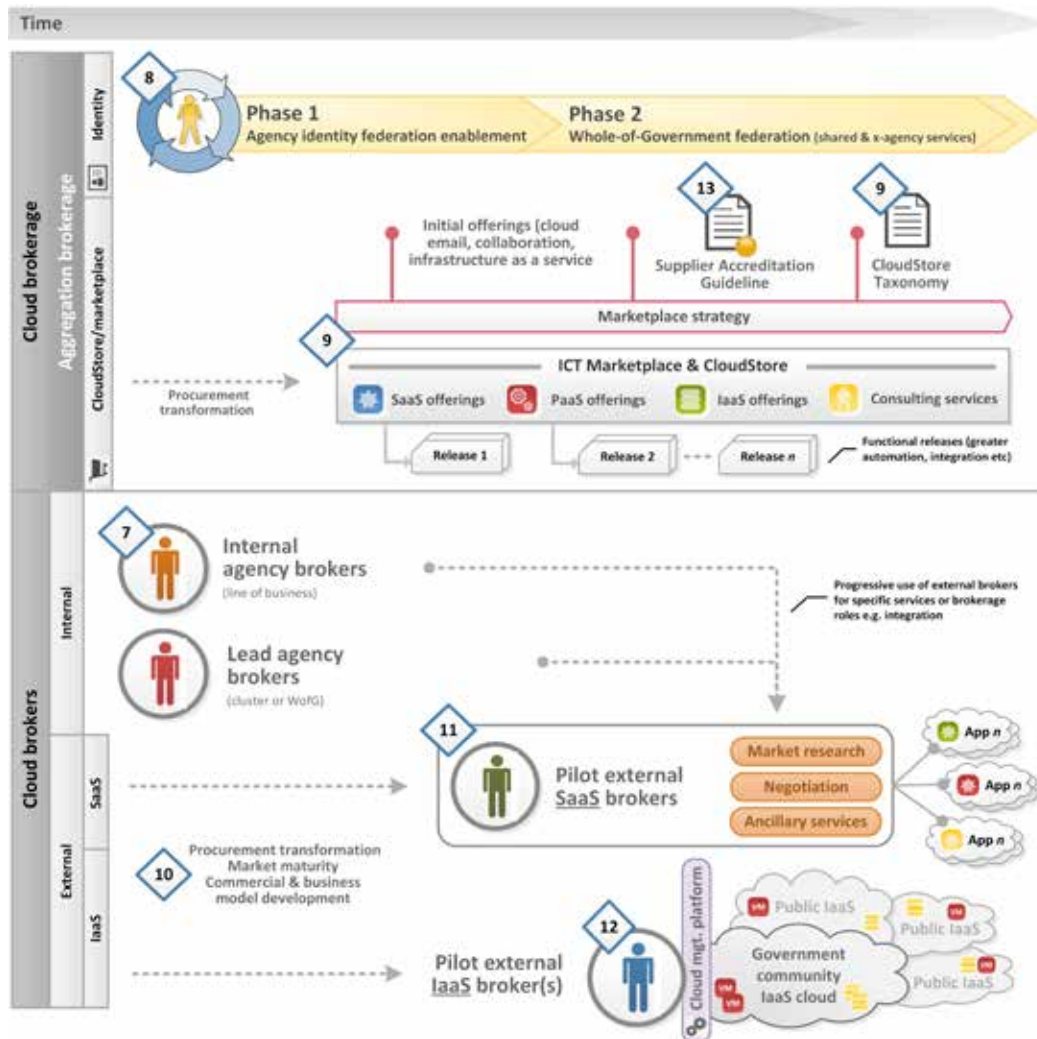
- develop standards, interoperability frameworks and maturity models to guide agency-centric implementations
- assess the merits of centralised and shared brokerage capabilities to drive transformation and maximise benefit.

Agencies will begin the transition to act as internal brokers between current in-house ICT delivery and the use of external cloud services. Lead agency brokers for a given agency cluster or for whole-of-government services will be formed. Commercial, business and operational models for the use of external cloud brokers will be investigated and developed, prior to piloting external brokers for IaaS and SaaS services.

IaaS brokerage models will be progressed prior to SaaS brokerage, given the availability of mature cloud management platforms. The number of IaaS suppliers to be brokered will also be smaller and more static compared to SaaS services. SaaS brokers must have an efficient process and robust commercial model to support ongoing procurements covering a diverse range of services.

A whole-of-government ICT marketplace and CloudStore when established will embody a transformed and simpler procurement process. The functionality of the CloudStore will improve over time to include additional levels of integration and automation.

**Figure 14: Cloud foundations implementation approach**

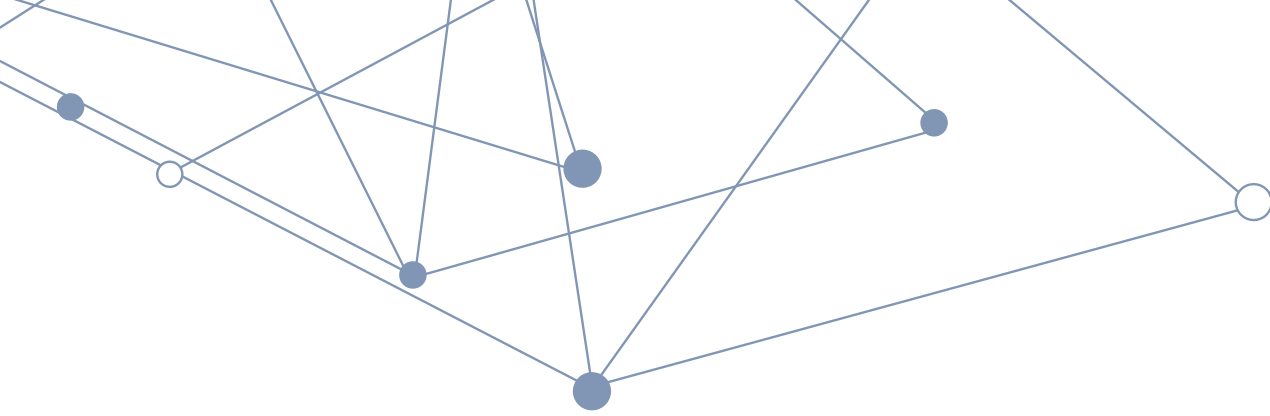


### Description

#### Whole-of-government ICT marketplace and storefront for SaaS, PaaS and IaaS

Queensland Government will look to establish a commercial arrangement for the supply of a ICT marketplace and storefront for SaaS, PaaS and IaaS services.

Queensland Government Chief Information Office will develop a CloudStore taxonomy and supplier accreditation guideline to govern the ICT marketplace. Delegated access to the ICT marketplace will be provided to cloud brokers where there is benefit to be gained by government.



### **Whole-of-government identity federation platform**

Queensland Government will look to establish a commercial arrangement for the supply of a trusted and managed federated identity broker to enable the sharing of cloud and cross-agency services. A business case will assess implementation options, including the supply of cloud-based identity federation capabilities for agencies.

### **Pilot an external SaaS broker**

Queensland Government will look to investigate and pilot commercial arrangements with an independent external cloud broker to streamline procurement of SaaS services. Broker services may include market research, negotiation, accreditation and other ancillary services such as migration and integration services. Additional SaaS brokers will be appointed where there is clear value to government based on the established model.

A framework to manage broker segmentation and responsibility (e.g. based on service classification, architectural brokerage roles and functions etc.) will be determined.

### **Pilot an external IaaS broker**

The Queensland Government will look to investigate and pilot commercial arrangements with an external cloud broker for IaaS services, including the:

1. supply of a brokered interface (cloud management platform) to a whole-of-government community IaaS cloud and multiple-connected public IaaS clouds
2. supply of a community IaaS cloud for Queensland Government
3. commercial arrangements with multiple public IaaS providers.

Note: While the above acquisition method aligns to the desired brokerage model, item 2 above is subject to business case justification (recommendation 21—Cloud Accelerate). Item 3 above will also be subject to the prior establishment of a Queensland Government standing offer arrangement (SOA) for public IaaS services (recommendation 20—Cloud Accelerate).



## Recommendations

<p>7) Agencies' ICT divisions are to begin the transition from service provider to a service broker to:</p> <ul style="list-style-type: none"> <li>• support the uptake of cloud services</li> <li>• continued delivery of traditional services in a hybrid model</li> <li>• reduce ownership and operation of major ICT assets.</li> </ul> <p>This represents a significant organisational, cultural and technology shift and will require strong organisational change management, governance and leadership.</p>	<p><b>Agencies</b></p>
<p>8) Establish a managed identity federation platform for Queensland Government commencing with a pilot.</p> <p>ICT action plan alignment:</p> <ul style="list-style-type: none"> <li>• Action [3.06]: Pilot a single federated public service identity.</li> </ul>	<p><b>DSITIA ICT Strategic Sourcing with QGCIO</b></p>
<p>9) Establish a commercial arrangement for the supply of a ICT marketplace and storefront and develop a supporting policy to ensure agencies utilise, as appropriate, centralised multi-tenanted brokerage capabilities.</p>	<p><b>DSITIA ICT Strategic Sourcing with QGCIO</b></p>
<p>10) Investigate commercial, business and operational models that suitably inform the piloting of external cloud brokers for IaaS and SaaS service arrangements.</p>	<p><b>DSITIA ICT Strategic Sourcing with QGCIO</b></p>
<p>11) Pilot opportunities for commercial arrangements with external brokers for SaaS services.</p>	<p><b>DSITIA ICT Strategic Sourcing with QGCIO</b></p>
<p>12) Pilot opportunities for commercial arrangements with external broker/s for IaaS services including an IaaS brokerage platform.</p>	<p><b>DSITIA ICT Strategic Sourcing with QGCIO</b></p>
<p>13) Develop a supplier accreditation guideline to ensure consistent vetting of suppliers and assurance levels.</p> <p>ICT action plan alignment:</p> <ul style="list-style-type: none"> <li>• Action [5.03]: Security assessment requirements established.</li> </ul>	<p><b>DSITIA ICT Strategic Sourcing with QGCIO</b></p>

## 6.3 Focus area 3: Cloud engagement

### Outcome

Through a shared vision and a coordinated approach, Queensland Government and its ICT providers will be best positioned to leverage and realise the benefits of cloud-based services.

### Approach

A cloud-first enterprise approach will foster an environment that is collaborative across government and industry, where participants openly engage to help educate, promote, encourage and mature a ICT marketplace that establishes trusted relationships.

This approach is principally about addressing the cultural change needed to transform Queensland Government from the traditionally siloed ICT service delivery approach to a more coordinated, unified and integrated environment that leverages commoditised and innovative services in the market.

Agencies' efforts in general will be directed to reduce reliance in non-sharable, dedicated infrastructures, and look to meet their business needs through shared computing capabilities in the cloud. To achieve this goal, strong leadership and vision is required across government.

The following will be established to support the cultural shift and transition to, and use of cloud services.

- A panel of trusted advisers to assist agencies with the development of cloud migration plans. The QGEA ICT-as-a-service Decision Framework will provide a consistent framework for the assessment of cloud workload candidates.
- A panel of solutions integrators (SIs) to assist with cloud migration, integration, training, support and legacy application remediation where required to support cloud migration.
- A cloud community of practice (CoP) to share knowledge, learnings, best practises across government and look to further develop standards to support cloud uptake.

### Description

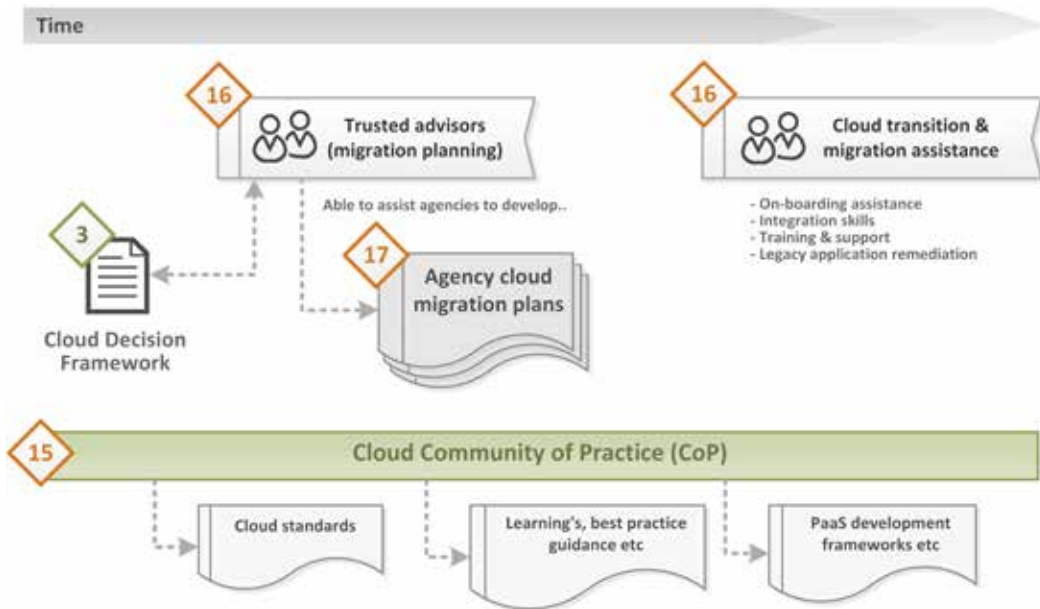
#### Trusted advisers

Due to the rapidly evolving and disruptive nature of the cloud services landscape, Queensland Government will need to ensure agencies have the ability to access expertise and collaborate with the ICT industry to assist in the adoption of cloud-based services by Queensland Government.

A panel of trusted cloud advisers, sourced from industry will be engaged to provide agencies the skills and resources to undertake an initial assessment of their ICT portfolios for cloud service opportunities.

The trusted advisers will need to be equipped to deal with cloud migration challenges which will not only require strong consulting and planning expertise, but also the capability to draw upon a large range of technical skills during planning and execution.

**Figure 15: Cloud engagement implementation approach**



A consistent methodology will be applied across all agencies to ensure that approaches are aligned across whole-of-government. Each existing workload (cloud candidate) will be assessed against the QGEA ICT-as-a-service Decision Framework developed in focus area 1. Trusted advisers will also be invited to assist in the ongoing development and improvement of the decision framework.

**Migration and transformation assistance**

To ensure agencies are well supported in their adoption of cloud services, access to a panel of pre-approved system integrators (or technical consultants) that have the competencies to assist agencies to activate, on-board, migrate, integrate and support cloud services will be made available.

Access to application remediation services, technical expertise and intellectual property to assist with modernising (refactoring, re-architecting, re-platforming) legacy applications for cloud environments may also be required.

**Cloud migration plans**

Following the initial assessment of cloud service opportunities each agency will develop a cloud migration plan for their organisation that outlines the identified cloud candidates and prioritises migration investment. This plan will also be used to identify common capability and demand requirements across the sector. Subsequent planning activities will be incorporated as part of the normal ICT strategic planning processes.



### Cloud community of practice

A cloud community of practice working group will be facilitated by QGCIO using a combination of online collaboration forums and in-person meetings. The working group will look to:

- educate by way of knowledge sharing and developing awareness campaigns for agencies in areas relating to opportunities and best practices in the use of cloud services
- consider the value of establishing guidelines such as cloud technical standards, PaaS development frameworks and/or interoperability approaches
- collate and share lessons learned among agencies to facilitate continual learning, better practice approaches and practical lessons learned
- encourage the sharing of end-user customisations to services, e.g. business workflow assets across agencies to balance the drive for standardisation with the need for configuration
- identify opportunities for cloud services trials.

### Local ICT industry involvement

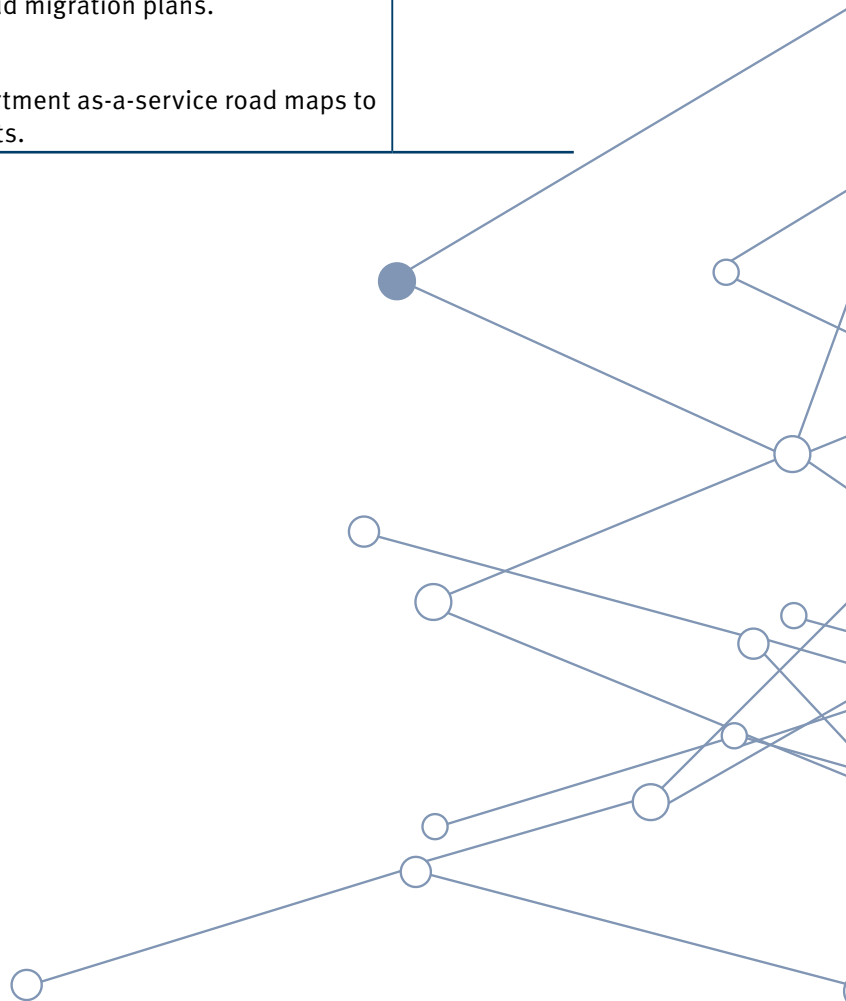
General feedback and initial consultation with industry representatives from the Australian Industry Association Australia (AIIA) and IT Queensland on the Queensland Government's adoption of cloud-based ICT services has been both positive and supportive.

The Queensland Government's commitment to a cloud-first and ICT-as-a-service approach will see many opportunities for the local ICT industry to:

- offer differentiated cloud and managed service offerings
- partner with cloud service providers to resell or bundle valued-added services
- assist with cloud opportunity analysis and business case development
- provide local support, implementation, migration and training services
- assist with business process rationalisation, re-engineering and re-modelling
- assist to transform and modernise legacy applications and data to a cloud stack
- assist with the development of innovative next-generation cloud applications.

## Recommendations

<p>14) Government to take a leadership role in the promotion and encouragement of cloud services.</p>	<p><b>QGCIO with agencies</b></p>
<p>15) Establish and foster a cloud community of practice with representatives across agencies to help educate and inform on areas of cloud maturity, challenges, lessons learned and general experiences with cloud adoption and management.</p>	<p><b>QGCIO with agencies</b></p>
<p>16) Establish a panel of:</p> <ul style="list-style-type: none"> <li>• trusted advisers comprising of representatives from ICT consulting organisations to assist in identifying cloud opportunities for agencies</li> <li>• pre-approved system integrators (or technical consultants) that have the appropriate skills and experience to assist with cloud migration and application remediation for agencies.</li> </ul> <p>ICT action plan alignment:</p> <ul style="list-style-type: none"> <li>• Action [7.08]: Implement the ICT services panel arrangement.</li> </ul>	<p><b>DSITIA ICT Strategic Sourcing with QGCIO</b></p>
<p>17) Agencies to conduct an initial assessment of cloud service opportunities, and develop cloud migration plans.</p> <p>ICT action plan alignment:</p> <ul style="list-style-type: none"> <li>• Action [8.09]: Develop department as-a-service road maps to divest ICT systems and assets.</li> </ul>	<p><b>Agencies</b></p>



## 6.4 Focus area 4: Cloud accelerate

### Outcome

Queensland Government has reformed its ICT service delivery model by adopting a cloud-first enterprise strategy, through the use of accredited cloud service arrangements for common and commodity ICT services.

### Approach

Queensland Government will peruse the adoption of SaaS, PaaS and IaaS cloud service opportunities in parallel. To accelerate this journey:

- investments in private IaaS will be actively discouraged
- a whole-of-government procurement panel of public IaaS providers will be established as a low barrier to entry for agencies to migrate existing workloads
- agency public-facing websites and development/test workloads will be assessed as early cloud candidates for migration to develop learnings
- a business case will be developed to assess demand for a Queensland Government community IaaS cloud to host workloads unsuitable for public cloud
- DSITIA will pilot and migrate to a cloud-based email service
- a whole-of-government procurement panel for electronic collaboration and communication SaaS solutions will be established
- lines of supply will be established for commodity and common SaaS and PaaS needs to replace line of business applications and systems of record.

### Description

To develop an environment where agencies are motivated to move forward towards the cloud-first enterprise vision, Queensland Government will encourage and transform cloud usage across the sector.

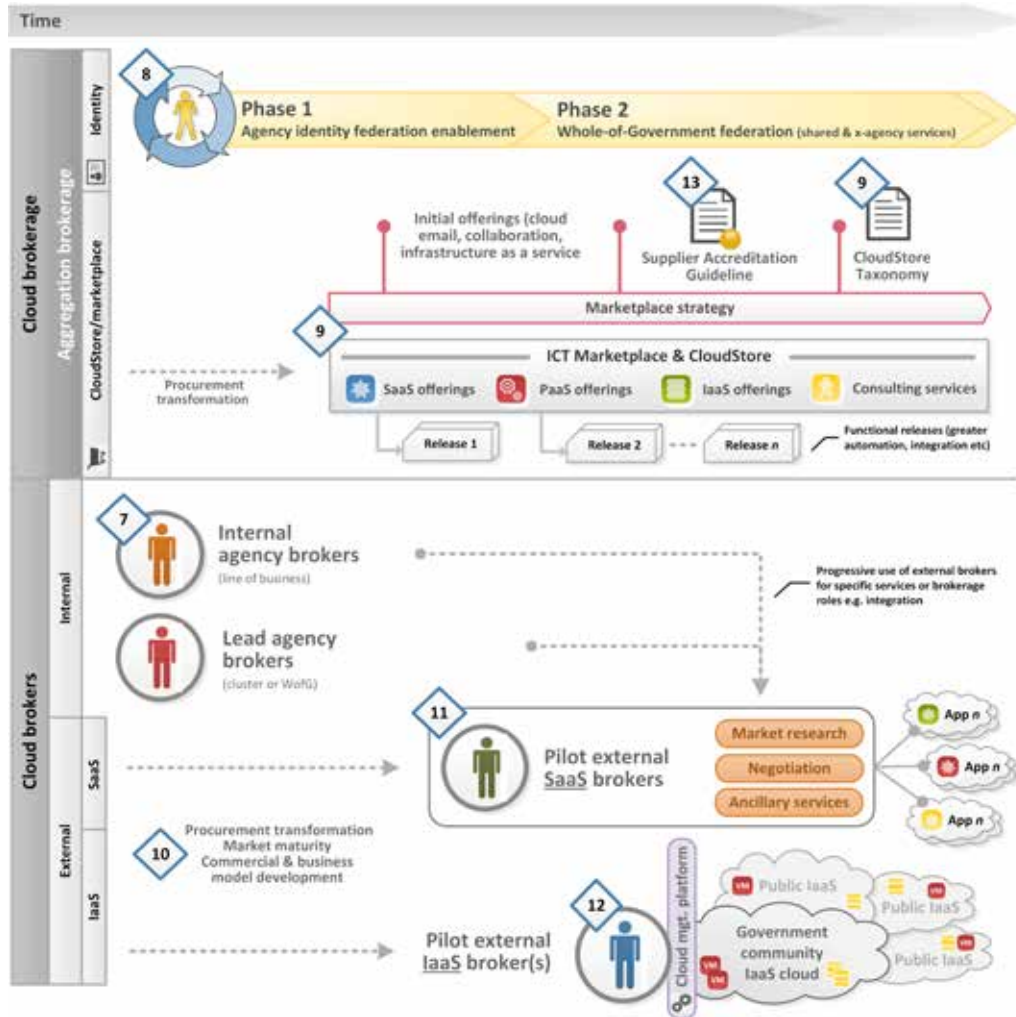
### Encourage

Queensland Government aims to actively encourage agency innovation and efficiency through take up of cloud services. To achieve this, agencies should adopt a commodity-first approach to cloud.

Agencies should look to first adopt cloud services for those areas where the market has already achieved an acceptable level of maturity. Typically, this is where multiple established providers exist with some track record of reliability and have established a solid user base. Mature areas typically have begun to extend their focus from delivery pure functionality to additional attributes like security, availability, performance and interoperability. Commoditisation of cloud services will see downward pressure on unit prices which cause market players to extend their products to try and maintain attractiveness with their current and future customers.

Functions that are most generic and commoditised will often be the best candidates for transition and may offer significant savings to current delivery methods. By outsourcing these commodity services, focus can be realigned to supporting the real business needs of government.

Figure 16: Cloud accelerate implementation approach



Cloud services should also be actively considered in situations where new or changing business needs can be rapidly met by innovative market offerings.

While agencies must have the flexibility to acquire ICT capabilities that suit their business needs, it is essential that acquisitions be governed properly to ensure strategic alignment. The QGEA principle of 'share, before buy, before build' should be forefront in the evolution of ICT.

Opportunities in all three cloud service models (SaaS, PaaS and IaaS) should be actively sought out to drive innovation and efficiencies.

## SaaS

The industry has seen rapid development of innovative cloud solutions that may bring significant value to Queensland Government. Agencies should give consideration to the following examples of business and commodity ICT applications when considering alternatives:

- project and portfolio management
- business intelligence and data warehouse
- training and learning management
- travel management
- event management
- grants management
- geospatial information systems
- mobile device management
- electronic records management
- enterprise resource planning
- finance management
- human capital management
- supply chain management
- case management
- ICT service management
- managed/secure file transfer.

The ICT 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
- office productivity suite
- collaboration including IP telephony
- customer relationship management.

Opportunities in these and other areas will be sought through the ICT marketplace.

## PaaS

For the exception where new bespoke application development is required and sanctioned by government, it is recommended that preference be given to utilising PaaS architectures. New applications can leverage platform services from multiple providers and deployed in a mix of public or community models depending on requirements.


PaaS services support a broad range of software development frameworks and may also provide middleware services such as databases, messaging, reporting, business intelligence and data warehousing. A range of PaaS services will be offered through the ICT marketplace.

## IaaS

Infrastructure workloads will still be required to support existing bespoke and packaged off-the-shelf applications. Agencies will be encouraged to migrate workloads off their internal infrastructure and onto infrastructure that is provided as a service. Significant demand for IaaS is expected in the short to medium term. As more applications are acquired through SaaS and PaaS architectures demand for IaaS is expected to soften overtime.

A hybrid approach will see a combination of community and public cloud services used. Public cloud IaaS will typically offer the lowest price point and greatest access to innovation, but may not be suitable for all use cases. Careful placement of





workloads will be required to ensure the necessary service attributes are obtained. Key considerations of security, availability and performance should be used to differentiate each service offering when making placement decisions.

## **Transform**

In line with the recommendations of the ICT Audit, a number of identified ICT service areas will be transformed through the adoption of cloud services. DSITIA will lead the establishment of procurement arrangements to simulate the ICT marketplace and transform agency adoption in the following areas:

### **Email and collaboration**

Enterprise class cloud email and collaboration solutions have evolved into a largely commoditised product, which is readily available in the market from a number of vendors. Several local organisations, Australian and state governments, overseas government agencies and commercial organisations have recently adopted cloud email services from industry, showing the maturation this market has now achieved. The ICT Audit identified opportunity for savings through adoption of cloud-based email services. Cloud email also offers a rapid mechanism to consolidate email for newly-formed agencies like DSITIA which is dispersed across multiple providers and disparate email systems.

### **Infrastructure-as-a-service**

Queensland Government will acquire a range of IaaS cloud services to address the cost and duplication of running isolated virtualised infrastructure environments. Key attributes of these services are performance, availability, security, location and connectivity (latency, bandwidth, etc.).

There is a distinction in the IaaS market between web/commodity-oriented and enterprise-oriented offerings. Web-oriented services are designed to best optimise the scalability and availability of large distributed cloud-native web applications. These modern cloud-native applications are designed from the ground-up to be fault tolerant and distributed in a stateless manner across multiple isolated commodity components. Web-oriented clouds are often built on a paradigm of massively scalable and global data centres filled with large containers of commodity ICT infrastructure to minimise costs.

Enterprise-oriented clouds are designed (and often certified) to host a diverse mix of typical enterprise business applications and legacy workloads. These application workloads were architected with the assumption that the underlying infrastructure is resilient. Therefore, it would be difficult to transition these workloads as-is to a modern web-oriented cloud without a level of transformation to improve availability/resiliency at an application layer. This may not be possible in all cases due to the original application's architecture or licensing costs associated with a scale-out model.

Enterprise-oriented clouds are likely to provide a more comparable hosting environment in the short to medium term for the diverse range of existing agency business

applications. Adoption of web-oriented cloud services will be driven through new application workloads or the transformation of existing strategic application assets into a cloud-native format to maximise the attributes and benefits of a cloud platform.

## Recommendations

18)	DSITIA to pilot, adopt and migrate to a cloud-based email service.	DSITIA
19)	Establish a standing offer arrangement for a panel of cloud-based email and collaboration providers. ICT action plan alignment: <ul style="list-style-type: none"> <li>• Action [8.05]: Establish electronic communication and collaboration including email.</li> </ul>	DSITIA ICT Strategic Sourcing with QGCIO
20)	Establish a standing offer arrangement for a panel of commodity public IaaS cloud services. ICT Action Plan alignment: <ul style="list-style-type: none"> <li>• Action [8.08]: Establish market arrangements to transition to commodity ICT as-a-service.</li> </ul>	DSITIA ICT Strategic Sourcing with QGCIO
21)	Explore the feasibility and develop a business case for the provision of a Queensland Government community IaaS cloud. ICT action plan alignment: <ul style="list-style-type: none"> <li>• Action [8.08]: Establish market arrangements to transition to commodity ICT as-a-service.</li> </ul>	DSITIA ICT Strategic Sourcing with QGCIO
22)	Establish lines of supply for in-demand commodity SaaS and PaaS services. ICT action plan alignment: <ul style="list-style-type: none"> <li>• Action [8.08]: Establish market arrangements to transition to commodity ICT as-a-service.</li> </ul>	DSITIA ICT Strategic Sourcing with QGCIO
23)	Agencies are to assess the following workloads for early cloud migration as low-risk candidates to assist in developing cloud experience and learnings (where cloud services demonstrate value for money and are fit for purpose): <ul style="list-style-type: none"> <li>• public-facing websites to public cloud hosting services</li> <li>• testing and development environments (where suitable).</li> </ul>	Agencies
24)	Agencies are actively discouraged from investment in private IaaS.	QGCIO and agencies

## 6.5 Focus area 5: Cloud governance

### Outcome

Queensland Government has implemented a range of effective governance measures to ensure successful cloud adoption and continued alignment with the cloud-first enterprise vision.

### Approach

This focus area looks to provide the necessary oversight and governance to ensure Queensland Government can realise continued benefit from its cloud initiatives.

Fostering a cloud-first enterprise environment will require strong governance over the funding, acquisition, deployment, management and use of cloud services for Queensland Government to harvest the intended benefits and outcomes with minimal risk to operations and information assets. Existing governance methodologies, frameworks, and processes should be leveraged. This includes:

- operations of contestability units within agencies
- ICT management framework, including assurance and investment review processes
- Directors-General Council for Procurement and ICT
- relevant project, program and portfolio frameworks

**Figure 17: Cloud governance implementation strategy**



### Description

#### Design authority

Agencies should consult with the QGCIO as the design authority for cloud computing across Queensland Government.

The QGCIO, as the design authority, is responsible for:

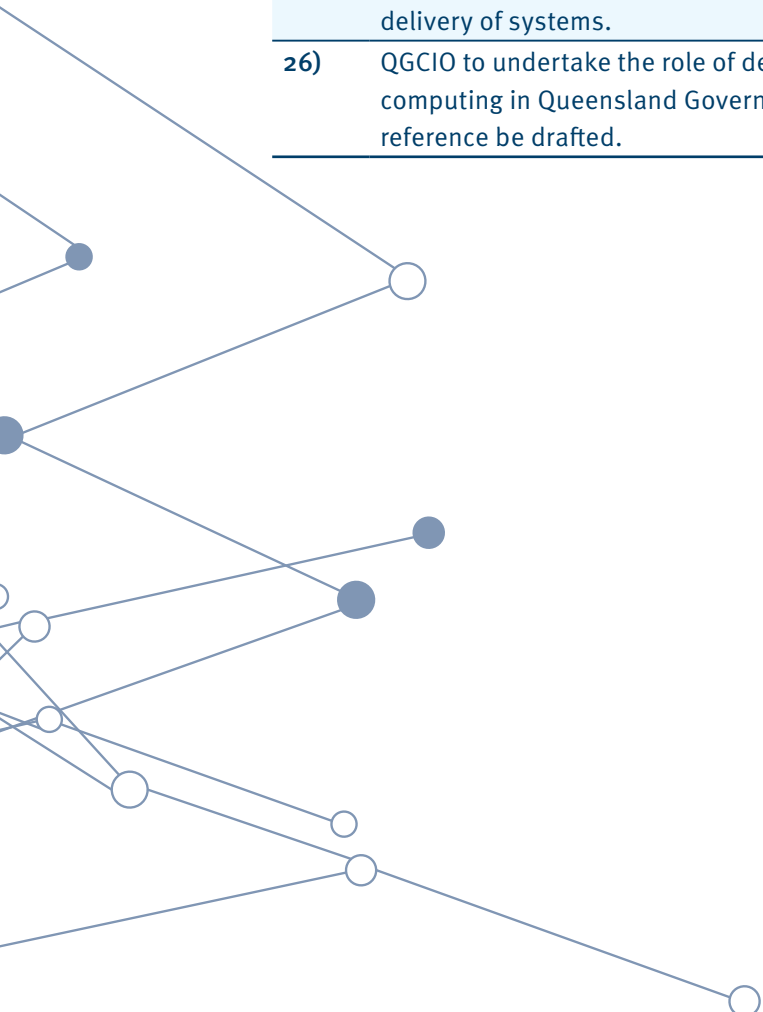
- defining, reviewing and monitoring the overall architecture and approach adopted across Queensland Government with regards to cloud services
- ensuring a consistent, coordinated and optimised approach is taken
- coordinating the synchronised delivery of foundational cloud building blocks across agencies and stakeholders
- reviewing whether additional tools are necessary to assist agencies to self-assess their own cloud computing needs
- reporting on the use and effectiveness of cloud services.

### Cloud anti-patterns

There is a need to ensure agencies align to a cloud-first enterprise strategy and are not continuing to invest in traditional services for ICT commodities. Agencies will be discouraged from pursuing architectures that are not cloud aligned.

### Recommendations

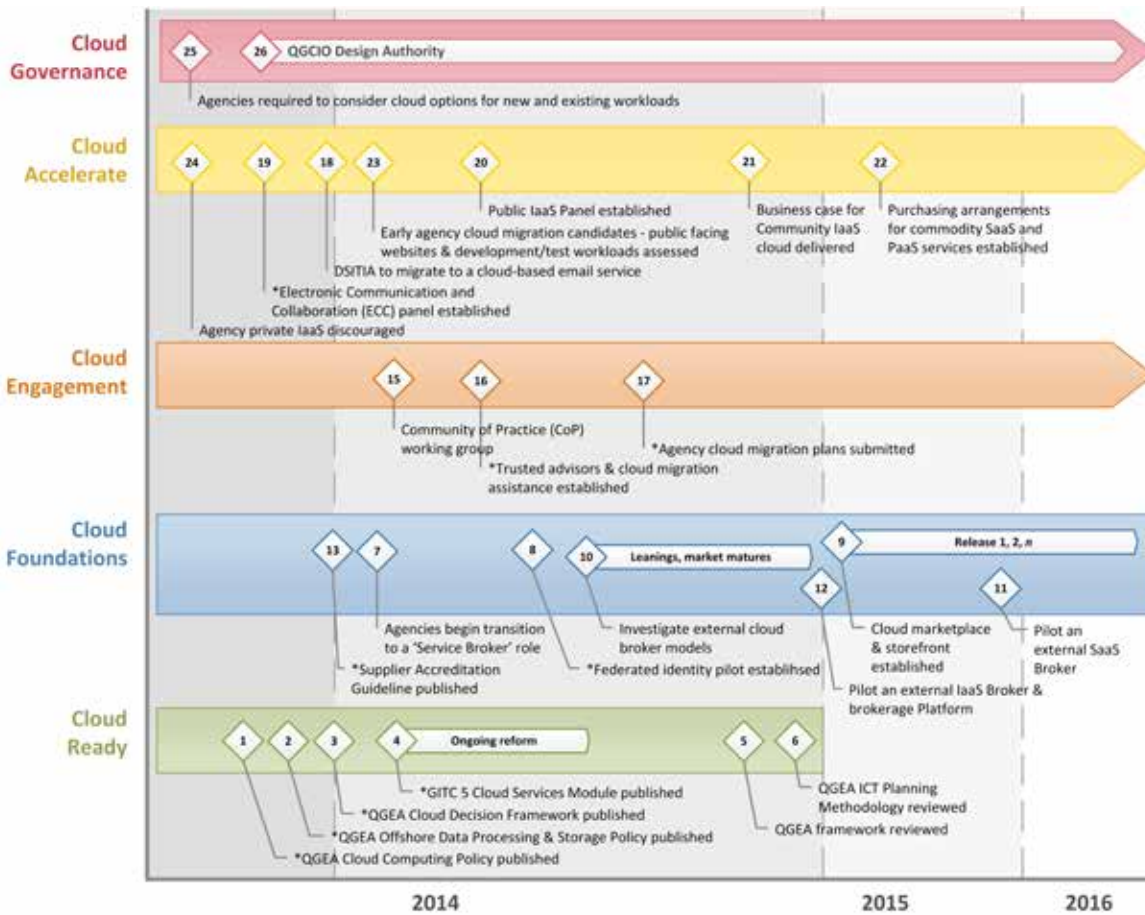
<p>25) Agencies are required to consider cloud service options (including public cloud services) as per the cloud-first enterprise policy for:</p> <ul style="list-style-type: none"><li>• new ICT procurements</li><li>• existing ICT systems at natural ICT refresh points and contractual renewal</li><li>• existing ICT systems where early cloud migration presents a compelling business case.</li></ul> <p>Agency cloud assessments should align with an agency's broader contestability framework. The risk of cloud service options must be considered relative to the current in-house delivery of systems.</p>	<b>Agencies</b>
<p>26) QGCIO to undertake the role of design authority for cloud computing in Queensland Government with a terms of reference be drafted.</p>	<b>QGCIO</b>



## 6.6 Recommendation timeline

Proposed priority and staged delivery of the above recommendations is presented in Figure 18.

Figure 18: Recommendation implementation timeline



Key: \* Indicates timeframe aligned with ICT action plan

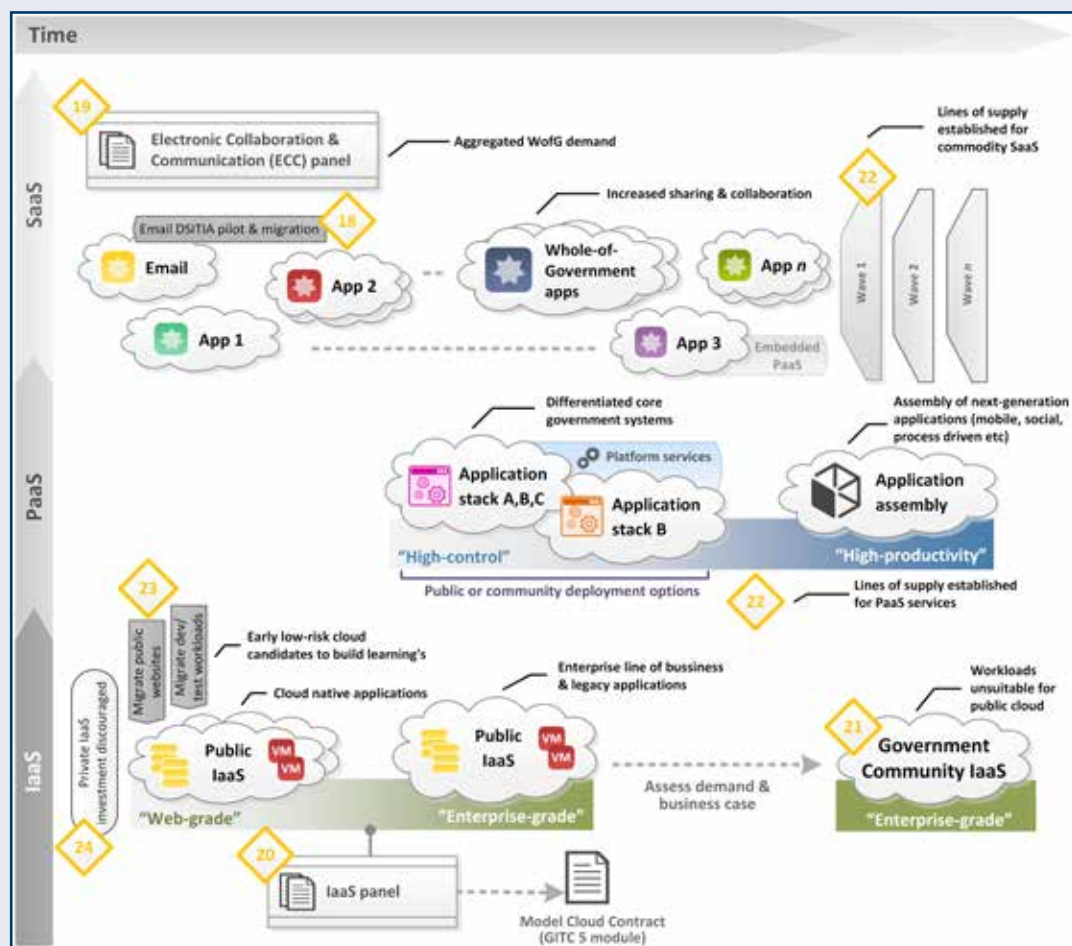
# Appendix A: Definition of cloud computing

The US National Institute of Standards and Technology (NIST) definition of cloud computing is commonly used throughout the ICT industry, and it is the definition adopted by the Queensland Government:

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

This cloud model is composed of five essential characteristics, three service models, and four deployment models as depicted.

Figure 19: NIST cloud computing definition



## Essential cloud characteristics

**On-demand self-service:** A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

**Broad network access:** Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g. mobile phones, tablets, laptops, and workstations).

**Resource pooling:** The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g. country, state, or data centre). Examples of resources include storage, processing, memory, and network bandwidth.

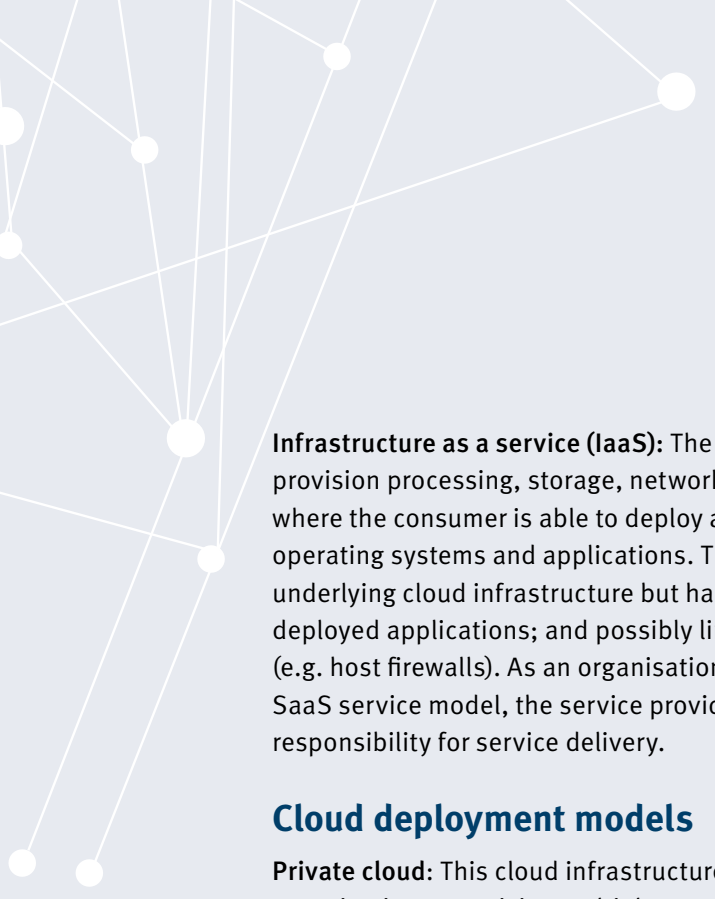
**Rapid elasticity:** Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appears to be unlimited and can be appropriated in any quantity at any time.

**Measured service:** Cloud systems automatically control and optimise resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled and reported, providing transparency for both the provider and consumer of the service.

## Cloud service models

**Software as a service (SaaS):** The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g. web-based email) or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

**Platform as a service (PaaS):** The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.



**Infrastructure as a service (IaaS):** The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g. host firewalls). As an organisation transitions from the traditional model to a SaaS service model, the service provider assumes a greater level of ownership and responsibility for service delivery.

## Cloud deployment models

**Private cloud:** This cloud infrastructure is provisioned for exclusive use by a single organisation comprising multiple consumers (e.g. business units). It may be owned, managed, and operated by the organisation, a third party, or some combination of them, and it may exist on or off premises.

**Community cloud:** This cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organisations that have shared concerns (e.g. mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organisations in the community, a third party, or some combination of them, and it may exist on or off premises.

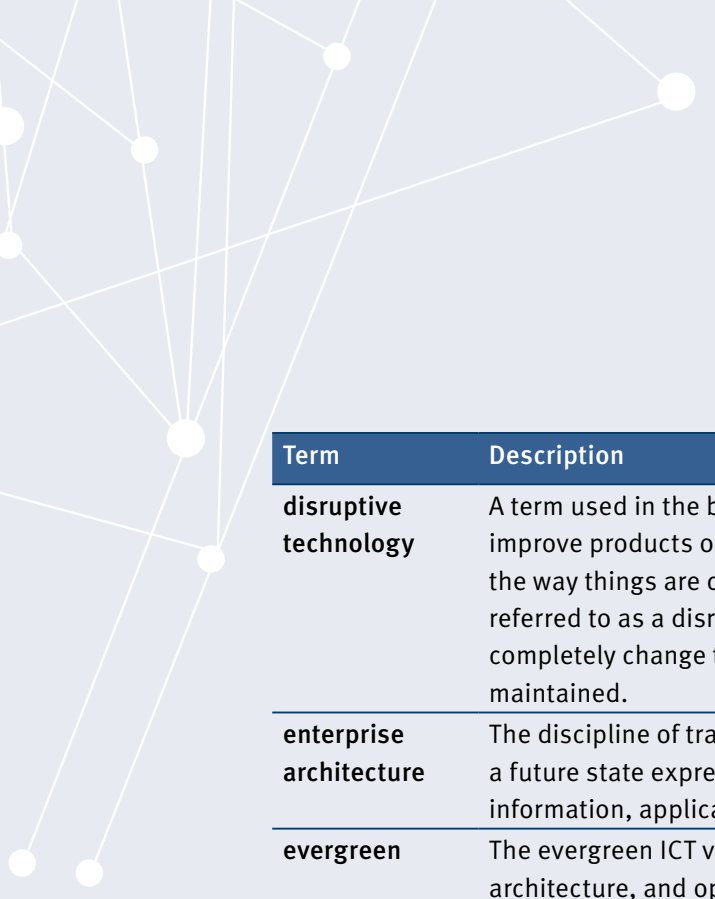
**Public cloud:** This cloud infrastructure is provisioned for open use by the general public. It may be owned, managed and operated by a business, academic or government organisation, or some combination of them. It exists on the premises of the cloud provider.

**Hybrid cloud:** This cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardised or proprietary technology that enables data and application portability (e.g. cloud bursting for load balancing between clouds).



## Appendix B: Glossary of terms

Term	Description
<b>A2A</b>	Agency to agency
<b>administrative arrangements</b>	Administrative arrangements set out the principal ministerial responsibilities of Ministers and the Acts that they administer. The arrangements are determined solely by the Premier and are made by Order in Council in accordance with section 44 of the <i>Constitution of Queensland 2001</i> .
<b>business process-as-a-service (BPaaS)</b>	Business processes that are delivered based on the cloud services model their own devices to access corporate systems and resources.
<b>BYOD</b>	Bring your own device – allowing employees to bring their own devices to access corporate systems and resources.
<b>B2G</b>	Business to government.
<b>C2G</b>	Citizen to government.
<b>capital expenditure (Capex)</b>	Funds used by an organisation to acquire or upgrade physical assets such as property, industrial buildings or equipment. This expenditure is depreciated over the life of the asset. Within the context of ICT spend, this could relate to major plant and equipment (including ICT systems and technologies) greater than \$5,000 (servers, storage, and networking) and software purchased or internally generated that amount to greater than \$100,000.
<b>cloud computing</b>	Refer to Appendix A – Definition of cloud computing.
<b>commodity</b>	ICT services and products which are common to most if not all agencies. Examples: desktop, networks, data centres, commercial off the shelf business software and business systems that support common business functions across government. These commodities can be procured directly or as services through software as a service, hardware as a service or infrastructure-as-a-service arrangement.
<b>community cloud</b>	Refer to Appendix A – Definition of cloud computing.
<b>CSP</b>	cloud service provider
<b>data centre</b>	Manages the operation of secure and controlled facilities supporting information technology and telecommunications equipment operations that store, process and transmit government information.



Term	Description
<b>disruptive technology</b>	A term used in the business world to describe innovations that improve products or services in unexpected ways and change both the way things are done and the market. Cloud computing is often referred to as a disruptive technology because it has the potential to completely change the way ICT services are procured, deployed, and maintained.
<b>enterprise architecture</b>	The discipline of translating the enterprise's vision and strategy into a future state expressed in terms of services, business process, information, applications and technologies.
<b>evergreen</b>	The evergreen ICT vision is a pattern of ICT provisioning, architecture, and operational management designed to deliver loose coupling between logically distinct layers of the ICT stack. The result is an approach where incremental ICT investment no longer creates legacy systems. Instead, each layer of the ICT stack can be continually refreshed without worrying about interdependencies between layers.
<b>Gartner</b>	Gartner, Inc. is a leading information technology research and advisory company that delivers the technology-related insight necessary to making the decisions.
<b>G2B</b>	Government to business
<b>G2C</b>	Government to citizen
<b>G2G</b>	Government to government
<b>hybrid cloud</b>	Refer to Appendix A – Definition of cloud computing.
<b>infrastructure-as-a-service (IaaS)</b>	Refer to Appendix A – Definition of cloud computing.
<b>innovation</b>	The successful application of new ideas to bring about change and continuously reinvent products, services, ways of doing business and the nature of the business itself. Innovation is an important contributor to increased productivity and performance.
<b>legacy</b>	A legacy system or technology is classified as having one of the following attributes: <ol style="list-style-type: none"> <li>1) an age greater than the average age of all government systems</li> <li>2) past its end-date of use or</li> <li>3) is classified as 'retire' or 'streamline' as part of the ICT planning methodology.</li> </ol>
<b>platform-as-a-service (PaaS)</b>	Refer to Appendix A – Definition of cloud computing.
<b>public cloud</b>	Refer to Appendix A – Definition of cloud computing.

Term	Description
<b>private cloud</b>	Refer to Appendix A – Definition of cloud computing.
<b>portability</b>	How readily an information, application or technology asset can be used in a different technology environment other than the one in which it was created without requiring major rework.
<b>on-demand self-service</b>	Refer to Appendix A – Definition of cloud computing.
<b>operational expenditure (Opex)</b>	An ongoing cost for maintaining or running a business. This could represent a fixed duration of on-going costs for initiatives or for maintaining currently owned ICT assets.
<b>risk management</b>	The identification, selection and adoption of countermeasures justified by the identified risks to assets in terms of their potential impact upon services if failure occurs, and the reduction of those risks to an acceptable level.
<b>self service</b>	A feature that allows customers to provision, manage, and terminate services themselves, without involving the service provider, via a web interface or programmatic calls to service APIs.
<b>service level agreement (SLA)</b>	A written agreement between a service provider and customer/s that documents agreed service levels for a service.
<b>service provider</b>	The company or organisation that provides a public or private cloud service.
<b>subscription-based pricing model</b>	A pricing model that lets customers pay a fee to use the service for a particular time period often used for SaaS services. See also consumption-based pricing model.
<b>Queensland Government Enterprise Architecture (QGEA)</b>	The collection of ICT policies and associated documents that guides agency ICT initiatives and investments to improve the compatibility and cost-effectiveness of ICT across the government.
<b>software-as-a-service (SaaS)</b>	Refer to Appendix A – Definition of cloud computing.
<b>whole-of-government</b>	Defines scope of context to all of the Queensland Government.
<b>workload (or ICT workload)</b>	This term generically refers to an ICT application/infrastructure component, typically in the context of migration of a particular component to the cloud.

## Appendix C: Related documents

The following QGEA-related documents will be available to assist agencies in cloud decision making:

Document title
ICT-as-a-service Decision Framework Overview
ICT as-a-service Model Selection
ICT as-a-service Deployment Model Selection
ICT as-a-service Risk Assessment Guideline
ICT as-a-service Risk Assessment Guideline Annexe—Risks Considerations
ICT as-a-service policy
ICT as-a-service offshore data storage and processing policy
Supplier Accreditation Guideline

Refer to the QGCIO website ([www.qgcio.qld.gov.au](http://www.qgcio.qld.gov.au)) to obtain the most recent versions.

# Appendix D: References

## Queensland Government

- Information Privacy Act 2009
- Information security (IS18) November 2010
- Information security external party governance guideline
- Internet (IS26) December 2010
- Procurement and Disposal of ICT Products and Services (IS13) November 2009
- Queensland Government Enterprise Architecture 2.0
- Recordkeeping (IS40) June 09
- Retention and Disposal of Public Records (IS31) November 2010
- Public Records Brief: Managing the Recordkeeping Risks Associated with Cloud Computing October 2010
- Office of the Information Commissioner Queensland – Cloud computing and the privacy principles
- Cloud Computing Guidelines May 2012
- Office of Information Commissioner – Contracted Service Providers April 2012
- Queensland Commission of Audit, Final Report February 2013
- Queensland Government ICT Audit October 2012

## Australian Government

- Better Practice Checklist – Privacy and Cloud Computing for Australian Government Agencies February 2012
- Better Practice Guide – Financial Considerations for Government use of Cloud Computing February 2012
- Better Practice Guide – Negotiating the cloud – legal issues in cloud computing agreements February 2012
- Cloud Computing Security Considerations (Department of Defence) April 2011
- Cloud Computing Strategic Direction Paper April 2011
- Information Privacy Principles April 2008
- Information Security Management Guidelines July 2011



## Other government strategies and reports

European Union Cloud Strategy

New Zealand Government Whole of Government Cloud Approach

Hong Kong Government Cloud Strategy

Singapore Government Cloud Approach

United Kingdom Government Cloud Strategy

United States of America (USA) Federal Government Cloud Computing Strategy

United States Government Accountability Office Report – Progress Made but Future Cloud Computing Efforts Should be Better Planned

Advice on managing the recordkeeping risks associated with cloud computing – Victorian Government

Risk assessment for cloud computing – Victorian Government

A Code of Practice for Cloud Computing – New Zealand Computer Society

## Industry analysts

Why government agencies need the cloud, Ovum, February 2012 (O100190-009)

Gartner 2011 Cloud Computing Planning Guide: The Shift to Hybrid IT, March 2011 (G00210316)

Gartner Migrating Applications to the Cloud: Rehost, Refactor, Revise, Rebuild, or Replace? , December 2010 (G00207162)

Cloud Computing in AP and why enterprises focus on private cloud, 23 October 2012 (G00239563)

Five Roles for Government in Cloud Computing, 16 July 2010 (G00201496)

Key Considerations for Selecting Cloud Providers for Enterprise Requirements in Asia-Pacific, 22 June 2012 (G00236073)

Five Cloud Computing Trends That Will Affect Your Cloud Strategy Through 2015, 10 February 2012 (G00230221)

Hype Cycle for Cloud Services Brokerage, 30 July 2012 (G00234256)

A Logical Reference Model for Cloud Services Brokerage, 13 October 2010 (G00206188)

Cloud Computing Journal: Adopting a Cloud First Mindset

Telco 2.0 Guest Post: How can CSPs become Cloud Services Brokers

Cloudwashing the Cloud Brokerage

Enabling Evergreen IT, Technology Forecast Summer 09, PricewaterhouseCoopers, March 2009

## **Industry standards bodies**

NIST SP800-145 The NIST Definition of Cloud Computing

Cloud Security Alliance— Cloud Control Matrix

Cloud Security Alliance—Security Guidance

