Queensland Audit Office

Cloud computing

Report 13: 2015–16

Queensland Audit Office

Location Level 14, 53 Albert Street, Brisbane Qld 4000

PO Box 15396, City East Qld 4002

Telephone (07) 3149 6000

Email qao@qao.qld.gov.au

Online www.qao.qld.gov.au

Front cover image is an edited photograph of Queensland Parliament, taken by QAO.

ISSN 1834-1128

Your ref:
Our ref: 10675

Queensland Audit Office

February 2016

The Honourable P Wellington MP
Speaker of the Legislative Assembly
Parliament House
BRISBANE QLD 4000

Dear Mr Speaker

Report to Parliament

This report is prepared under Part 3 Division 3 of the *Auditor-General Act 2009*, and is titled Cloud computing.

In accordance with s.67 of the Act, would you please arrange for the report to be tabled in the Legislative Assembly.

Yours sincerely

Andrew Greaves
Auditor-General

Queensland Audit Office
Level 14, 53 Albert Street, Brisbane Qld 4000
PO Box 15396, City East Qld 4002

Phone 07 3149 6000
Email qao@qao.qld.gov.au
Web *www.qao.qld.gov.au*

Contents

Summary

The Queensland Government is using disruptive technology, such as cloud computing, to change the way it delivers Information and Communications Technology (ICT) and other government services. A recent scan of the Queensland Government gateway identified more than 2 000 instances of cloud solutions in use.

Cloud computing offers an alternative way for departments to deliver their services. It gives users the ability to access technology without significant upfront investment and to pay only for what they use. It gives them on-demand access to computing resources that third parties manage. Used with care, cloud technology means government can respond quickly to changing needs with affordable services.

The Queensland Government Chief Information Officer (QGCIO) developed a cloud computing strategy and implementation model in May 2014. This strategy positioned cloud computing at the centre of government ICT reform.

Departments are responsible for aligning their agency ICT strategies with the whole-of-government strategic directions set by QGCIO, including the cloud strategy, and for implementing ICT reforms. The Department of Science, Information Technology and Innovation (DSITI) and QGCIO are responsible for establishing frameworks, guidance and procurement panels to support departments in adopting cloud computing.

Cloud computing provides departments with the opportunity to reassess and optimise their ICT assets and services' portfolio, influencing the way they acquire, deliver and manage ICT. As with any new opportunity, departments need to balance the potential benefits with the challenges and risks when determining the suitability of cloud offerings. Implementing cloud has the potential to introduce new risks relating to information security, privacy and compliance with legislation.

In this audit, we examined how well departments are adopting the Queensland cloud computing strategy in modernising their ICT assets and services to deliver business value while managing risks.

Conclusions

DSITI, including QGCIO, took a positive step towards modernising Queensland government's ICT by releasing its 'cloud first' strategy and implementation plan—a first for the public sector in Australia. However, it does not assess how effective departments have been in implementing the strategy because it did not define expected benefits and is not monitoring and measuring departmental progress.

Queensland government departments are in early stages of adopting cloud, and in the main consider cloud solutions only when old systems require renewal or when they are purchasing new systems. Nevertheless, they are also not aware of all of the cloud solutions in use by their agencies as they do not have mechanisms to monitor user-initiated cloud computing. Without knowledge of all cloud solutions, they risk leaving government information insecure.

Departments now need to take a more strategic approach—to assess where cloud can add the most value, and to address the people, process or technology change activities that are required if the objectives of the ICT strategy are to be realised.

Failure to do so will limit their abilities to benefit from cloud and other emerging technologies and may result in higher cost ICT environments, more operational risks, an inability to keep up with citizen expectations of service delivery, and continued risk around ageing systems.

Central oversight and support of the strategy

Queensland was the first Australian state to adopt a cloud-first policy. QGCIO and DSITI established frameworks and procurement panels to support departments in adopting cloud computing.

The cloud computing strategy has created awareness amongst departments about the use of cloud technology. However, it has not driven the change needed in departments to develop mature frameworks within which to increase the levels of cloud adoption.

DSITI, including QGCIO, has not established processes for obtaining feedback and publishing lessons learnt from projects specifically relating to cloud computing. QGCIO has processes for departmental feedback for other aspects of the ICT landscape.

Guidance to support decision-making

QGCIO has provided guidance in the form of an example decision framework and risk assessments of cloud computing. These documents help departments assess the suitability of cloud computing.

The purchase of software and infrastructure is one of the first decisions that departments make when they consider using cloud computing. QGCIO does not provide guidance on choosing the type of products to purchase—either software or ICT infrastructure. This information can reduce the risk that departments select an unsuitable model.

DSITI, including QGCIO, provides limited guidance to departments about how to assess the suitability of cloud products in terms of technical standards, compliance, backup and disaster recovery capability, product and supply chain security, data centre locations, and legal jurisdiction of the service provider. Each department sources this type of information independently.

Procurement of cloud services

DSITI has established two panels to support departments to procure their cloud services, but cannot demonstrate that these panels are providing value for money. This is because they have not tracked the cost of establishing the panels, and do not have the data or processes to identify departments that use the panel for their cloud procurement. Consequently, DSITI is unable to identify the financial benefits of the panels or to forecast the usage for cloud services. Rather, it relies on the vendors to provide it with information about the use of the panels.

The changing ICT workforce

While QGCIO is delivering senior leadership programs for ICT, they have not developed a whole-of-government view of required workforce capability, or of gaps in capability and transition plans. Without this level of capability planning, there is a risk that at an overall level, the ICT workforce and capabilities will not align with the strategic direction.

Risk management

DSITI has not updated the framework for managing whole-of-government business continuity with cloud computing requirements. As a result, departments do not have guidance on how to evaluate the impact of cloud on their business continuity plans and how they will restore cloud-based services in the event of an incident or disaster.

Implementation by departments

To date departments have not planned and prioritised which of their ICT services will gain the most value from using cloud computing. Their focus remains on managing ICT assets whereas it needs to shift to transforming the overall ICT service delivery.

Departments are modifying their existing procurement processes to support cloud adoption. However, with easy and low cost cloud services, business can purchase these services directly from cloud providers, bypassing ICT governance and/or ICT due diligence process as shown in DSITI's recent scan of cloud services.

Most departments are in the early stages of adopting cloud computing and have not assessed how cloud fits into their overall portfolio of ICT assets and services.

Departments are using cloud computing mostly for their website and emails. They have not yet incorporated the insights from these transitions into their ICT planning.

A scan of Queensland government internet gateway by DSITI identified that there were 2 163 individual cloud services in use–significantly higher than the number of cloud services that departments have on record.

The departments have not yet determined whether all of these services relate to departmental business or are employees' personal use.

The scan also showed that around 75 per cent of 8 600 gigabytes of data is transferred to cloud services outside of Australia.

Most of the government ICT workforce is in the operational management area and in the survey, we conducted as part of this audit departments reported concerns about the lack of technical capability and expertise in managing cloud.

All the departments we audited have comprehensive risk management analysis in the pre-procurement phases of implementing cloud solutions. However, none is managing the operational risks introduced through cloud computing by implementing sufficient controls over:

- business units purchasing or using cloud computing without ICT due diligence
- business users transferring sensitive information outside the department
- access to administer the cloud computing solutions
- security incidents that result in data loss
- impact to the business from system outage.

They also do not obtain and review controls assurance reports from their cloud service providers.

Recommendations

We recommend that the Queensland Government Chief Information Officer (QGCIO):

1. reviews and updates the cloud strategy, implementation model and relevant documents including:
    - defining performance indicators and criteria for outcomes and benefits that meet the objective and vision of the cloud computing strategy and align with the Queensland Government Performance Management Framework
    - setting realistic timeframes with consideration of the resource and cost implications, and then adapting a flexible style of delivery to provide timely direction and guidance to government as the market and departments mature in adopting the technology
    - using existing whole-of-government ICT portfolio data to highlight to departments, services that represent maximum value and benefits at the lowest costs and risks for transitioning to cloud
    - improving formal feedback and consultation process targeted to the cloud strategy and publishing information on lessons learnt from projects relating to cloud computing.
2. reviews departmental cloud implementation roadmaps to identify whole-of-government risks and opportunities and inform decision-making, and completes key frameworks and guidelines including:
    - the ICT-as-a-service decision framework and guidelines
    - prioritise, in conjunction with departments, the pre-requisite activities required for cloud service brokerage

We recommend that Department of Science, Information Technology and Innovation (DSITI):

3. improves the cloud sourcing approach by:
    - working with departments and the whole-of-government procurement team to obtain relevant data on cloud usage
    - providing relevant due diligence information that it gathers when establishing panels.

We recommend that QGCIO and DSITI

4. identify whole-of-government ICT workforce target capability and gaps in capabilities, and make transition plans to address these gaps.
5. improve risk management practices by:
    - developing guidelines that departments can use to manage ICT services and operational risks in a cloud-computing environment
    - guiding departments on the types of assurance reports they need to obtain for various cloud deployment models
    - including any specific requirements relating to cloud computing services with the whole-of-government business continuity management and disaster recovery guide.

We recommend that all departments:

6. update their ICT strategies to articulate departmental drivers for adopting cloud and evaluate the current ICT assets and services portfolio to develop roadmaps and identified activities for transforming ICT service delivery incrementally
7. identify the impact of cloud computing on their ICT operations and workforce capability and develop transition plans
8. establish ICT due diligence and information management processes for user-initiated cloud solutions
9. evaluate the overall risks and control environment based on formal assurance reports from service providers, and implement controls and contingency plans where there are gaps
10. implement processes to detect and monitor user-initiated cloud services and a user awareness program relating to information on the risks of unapproved cloud services

Reference to comments

In accordance with s.64 of the *Auditor-General Act 2009*, a copy of this report was provided to Department of Science, Information Technology and Innovation, Department of Education and Training and Department of Housing and Public Works with a request for comments.

We have considered their views in reaching our audit conclusions and they are represented to the extent relevant and warranted in preparing this report.

The comments received are included in Appendix A of this report.

1. Context

The *Queensland Government ICT Audit Report*, October 2012, highlighted that Queensland government agencies had a significant number of heavily customised, high-cost information and communication technology (ICT) systems. It referred to a history of complex, long and costly ICT projects to implement systems and infrastructure. It showed that critical business systems used outdated technology with limited ICT disaster recovery capabilities. The report concluded that departments needed significant funding to maintain the ICT portfolio.

In response to the ICT Audit Report recommendations, the Queensland Government Chief Information Office (QGCIO) and the Department of Science, Information Technology and Innovation (DSITI) developed the *ICT strategy 2013–17*. QGCIO also developed the cloud computing strategy and cloud computing implementation model to facilitate ICT modernisation. These documents set the direction and approach for departments to deliver ICT services within their organisations.

ICT modernisation involves discovering and understanding the impact and benefits of new technologies and trends that disrupt the way business operates.

ICT strategy 2013–17

In June 2013, the Queensland Government published the *ICT strategy 2013–17*. This strategy contains three key objectives.

- To have effective digital services for clients to access government services and data when and where they want, with information security and privacy maintained.
- To have effective digital services, including departments consuming ICT as a service, using strategic sourcing and mitigating ICT risks with all significant systems having life cycle management.
- To have a transformed and capable workforce, focused on how to leverage digital services, understanding related commercial arrangements and aligning ICT projects with business objectives.

In addition, in May 2014 the QGCIO released the *Cloud Computing Strategy* as an addendum to the Queensland Government *ICT strategy 2013–17*. QGCIO is currently reviewing these strategies.

DSITI released the *ICT Strategy 2013–17 Action Plan* in August 2013. It aligned with the three objectives of the *ICT Strategy 2013–17*. DSITI developed the final draft of the next version*, ICT Renewal Action Plan*, in November 2014. In July 2015, DSITI published the *ICT Modernisation Action Plan*. The initiatives in this action plan relate to:

- connecting government for sharing and exchanging government information
- leveraging disruptive digital technology for improved services of the future
- innovating to simplify and procure products and services more efficiently
- adopting alternative service delivery models for government to deliver contemporary, value-for-money, ICT-enabled business solutions
- developing our workforce to support and enable digital-readiness within government.

Cloud computing strategy

The cloud computing strategy builds on objective two of the ICT strategy and positions cloud computing at the centre of government ICT reform.

It addresses the following key themes:

- Departments will take a 'cloud-first' approach and procure cloud-based ICT services as the default option for their ICT requirements, unless a sound business case exists for an alternative solution.
- The Queensland Government will:
  - develop an implementation model for cloud computing to minimise risk and maximise benefits
  - develop whole-of-government policies to adopt ICT-as-a-service, including cloud computing, and guide decisions on the appropriate use of offshore data storage and processing
  - develop appropriate legal and contractual artefacts for departments to use when procuring ICT-as-a-service
  - create procurement arrangements to streamline departments' adoption of ICT as a service, including cloud computing services
  - develop a cloud computing decision framework to provide departments with direction on selecting ICT workloads to be sourced from cloud providers.
- Departments will analyse their application portfolio and develop implementation plans (roadmaps) to adopt ICT as a service, including cloud computing.

Cloud technology has the potential to shift the way the Queensland Government uses information technology.

Definition of cloud

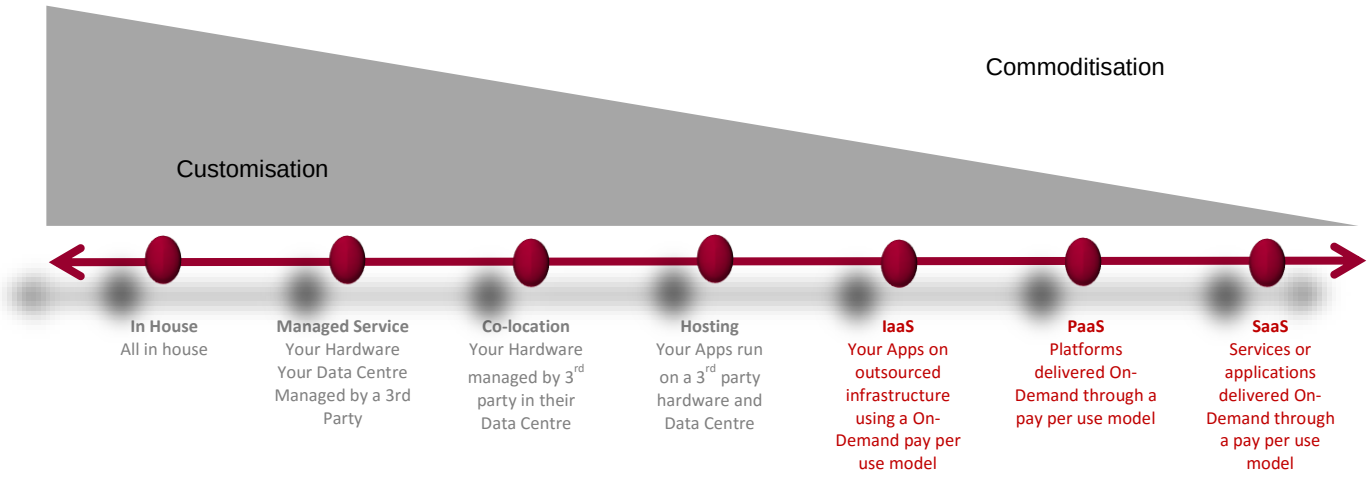
The Queensland Government has adopted the National Institute of Standards and Information Technology's (NISIT) definition of cloud computing, or 'the cloud':

> *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.*

The rationale for cloud computing is simple. Businesses can get the computing power, storage and software they need, when they need it, rather than having to set up the computing resources inside their offices. Businesses can pay for what they use, rather than paying to own information technology assets.

Traditionally, organisations have owned and managed all the ICT components required to deliver ICT services. We know this as 'in-house' ICT service delivery. Organisations adopt cloud computing in various ways, from accessing, rather than owning, some or all ICT components required to deliver ICT services. Figure 1A shows the range of ICT service delivery models from 'in-house' to full cloud computing.

Figure 1A
ICT service delivery models



Source: Queensland Audit Office

For an organisation's ICT service delivery to be in the cloud, it needs to comprise five essential characteristics:

- **On-demand self-service:** a department can provide computing capabilities as needed, automatically, without requiring human interaction with the service's provider.
- **Broad network access:** capabilities are available over the network and available through an interface on devices such as desktops, laptops, tablets and mobile phones.
- **Resource pooling:** providers pool computing resources in multi-tenant arrangements, with different resources assigned and reassigned according to demand.
- **Rapid elasticity:** according to demand, a department can provide capabilities rapidly, in some cases automatically, to increase and reduce the required computing capabilities in accordance to its need.
- **Measured service:** Cloud systems automatically control and optimise resources use by using a metre. This allows both the provider and consumers to keep track of what resources are used, enabling monitoring, control, reporting and charging of resources.

Cloud computing service models, namely *Infrastructure as a Service*, *Platform as a Service* and *Software as a Service,* have these essential characteristics and meet the definition of cloud computing. Figure 1B includes descriptions of these service models. The other models do not have on-demand self-service characteristics and therefore do not meet the definition.

Figure 1B
Cloud computing service models

Service model	Description
Software as a service	A user can access software over the internet rather than having it installed on a local computing device or in an internal data centre. This software allows minimal customisation. Therefore, business usually changes its processes to use the system.
Platform as a service	Users access online platforms to develop and run their own systems. The platform as a service model makes it relatively easy to create new online systems, within the constraints of the tools provided by the cloud-computing vendor.
Infrastructure as a service	Cloud computing vendor provides infrastructure for the users to store data, and develop and run any system that they want. This service allows organisations to move their programs and data into the cloud without having their own local servers and data centres.

Source: Queensland Audit Office

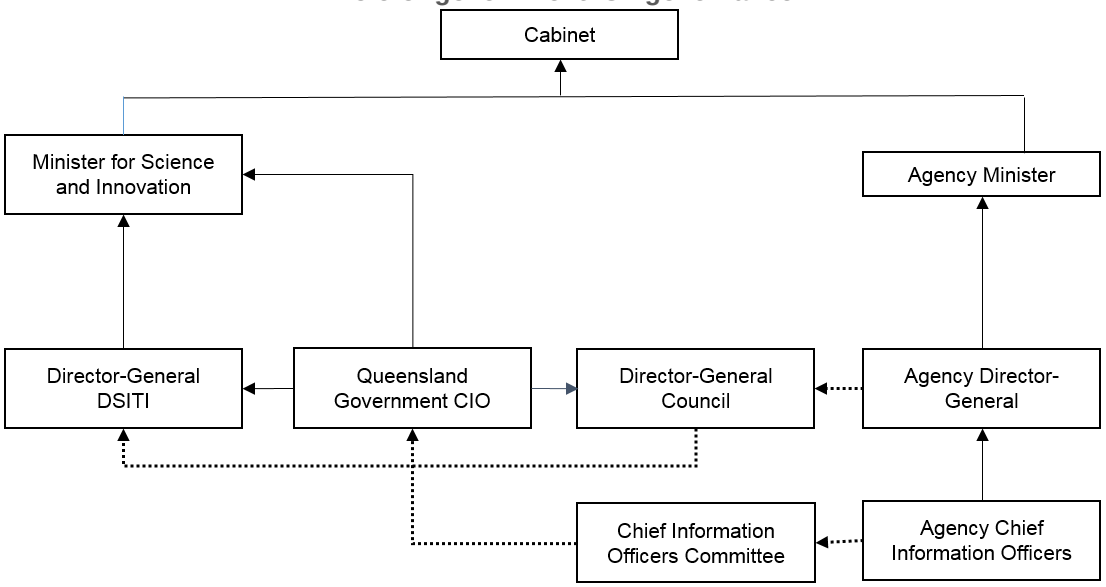
Roles and responsibilities

Technology is critical in connecting departments and the public with information and services they need. To align technology in departments with the government's strategic direction, DSITI developed a whole-of-government approach to directing and monitoring ICT services.

Governance structure for government ICT

Figure 1C shows the governance structure established for managing ICT strategic direction at the whole-of-government level. Parties within this structure collaborate to endorse the ICT strategic direction and monitor ICT initiatives to ensure they deliver value for money.

Figure 1C
Whole-of-government ICT governance



Source: Queensland Government ICT Strategy 2013–17 and Queensland Audit Office

Figure 1D shows key responsibilities and accountabilities for whole-of-government ICT.

Figure 1D
Responsibilities and accountabilities for whole-of-government ICT direction

Position in ICT governance	Responsibilities and accountabilities
Directors-General Council	Responsible for: ▪ endorsing critical and significant ICT investments ▪ monitoring ICT renewal portfolio ▪ monitoring risks relating to significant and at-risk ICT assets.
Director-General Science, Information Technology and Innovation	Accountable for: ▪ delivering the ICT renewal agenda as co-sponsor of the Directors-General Council ▪ delivering ICT risk management framework for implementation in all agencies ▪ reviewing agency performance so that government portfolio delivers on strategic investment objectives.
Queensland Government Chief Information Officer	Accountable for: ▪ setting whole-of-government ICT strategy and policies ▪ developing a government ICT workforce plan ▪ endorsing and monitoring significant ICT investments ▪ ensuring that the government's ICT investments support policy outcomes, represent value for money and are reliable.
Strategic ICT Division of DSITI	Accountable for: ▪ delivering whole-of-government projects and programs such as, ICT Modernisation and ICT for 1 William Street. Responsible for: ▪ strategic ICT procurement services ▪ assisting industry to access the Government ICT market ▪ providing ICT infrastructure, network and storage services to government agencies through CITEC.
Department Director-Generals	Accountable for: ▪ managing ICT risks of the Department ▪ evaluating, endorsing, and monitoring major ICT investments of the Department.
Chief Information Officers Committee	Responsible for: ▪ discussing collaboration opportunities ▪ sharing knowledge and experiences.
Departmental Chief Information Officers	Accountable to their Directors-General and responsible for: ▪ ICT business as usual operations ▪ ICT renewal and risk management in their departments.

Source: Queensland Audit Office

DSITI has specific responsibilities for whole-of-government ICT.

In accordance with the guiding principles articulated in the *ICT Strategic Plan 2013–17*, the Director-General of DSITI is accountable for the ICT reform agenda and whole-of-government strategic ICT initiatives through its Strategic ICT team.

The Queensland Government Chief Information Office is accountable for setting the strategic direction for ICT and the associated frameworks and policies that enable its implementation.

Directors-General for each department are accountable for their strategic ICT investment portfolio, realising intended business value and monitoring the ICT risks associated with the investments.

Vendor management and procurement

The strategic ICT sourcing team within DSITI establishes whole-of-government contracts and panel agreements with a range of suppliers. Departments can buy ICT products and services from the whole-of-government panel or establish their own arrangements.

The strategic ICT sourcing team has responsibility for accrediting vendors under the government information technology contract framework to enable them to engage in ICT contracts with departments.

Cloud computing implementation model

Department Chief Information Officers (CIOs) need to establish their cloud strategy and ensure their departments' overall ICT operating models support the use of cloud. They need to ensure that:

- cloud services integrate with internal services
- the organisation has the relevant skills and competencies to manage cloud vendors
- risks identified and risk management approaches reflect cloud solutions.

QGCIO provided context for departmental ICT cloud strategies through the cloud computing implementation model published in May 2014. The model sets out a Queensland Government vision for cloud computing and defines three enabling pillars summarised in Figure 1E that departments must collectively build to deliver the vision.

Figure 1E
Three pillars of the cloud computing implementation plan

	Pillar	Description
1	Service delivery enablement	Facilitating better interaction through user-centric design and information sharing with citizens and business.
2	Cloud service brokerage	Supporting government to become an efficient buyer and consumer of modern, contestable ICT services.
3	Trusted cloud services	The use of market-driven, innovative and ready-made services from well-credentialed providers.

Source: Cloud computing implementation plan

Timeframe to implement strategy

The strategy is a three-year strategy with a long-term goal of reorientating Queensland government agencies from developing and owning ICT assets in-house to that of a consumer of ICT services available from industry.

DSITI, including QGCIO, did not set a timeframe for departments to implement the cloud strategy. The move to cloud computing and 'as-a-service' will be partly dictated by the maturity of the market locally and globally and availability of the services departments need.

Risk management

There are new challenges in implementing cloud computing. Transitioning too quickly can introduce avoidable risks, while adopting too slowly can result in lost opportunities and benefits. Departments need a clear strategy to maintain the balance between risks and potential benefits.

Business users can generally set up a cloud account easily, upload documents and invite others (within or outside of the organisation) to collaborate. If information sharing is not managed or is on unapproved services, it may create records management, security and other risks for the departments. Consequently, departments need to assess privacy and security risks before collecting, processing, sharing, or storing government data in the cloud. In addition, departments need to assess the overall risk of the ICT portfolio and use this information to select target service delivery models through the department's enterprise architecture.

When departments move from in-house ICT service delivery to incorporating cloud computing it affects how they manage risk. The department CIO retains accountability for managing the risk of technology service provision to the department. ICT teams need to adopt a shared responsibility model with the cloud service provider to clarify the responsibilities of each party. The CIO must assure the department that the overall control environment is sufficient to manage inherent risk. Specific risks and challenges to consider include:

- data breaches and data loss
- departments' access to their own data
- legal issues associated with data sovereignty
- data transfer and ease of cloud provider changes
- cost escalation based on service throughput
- vendor transparency and inadequate or unclear service level agreement
- privacy and confidentiality of personal, sensitive, or regulated data and information
- legal and regulatory compliance
- cyber security and support for incident forensics
- maintaining adequate security across internal and external ICT services
- monitoring service levels across multiple cloud providers
- records preservation, access, and management
- service availability and reliability
- performance of geographically distributed systems
- workforce capability.

Standards and good practices

Guidelines that outline cloud technology good practices include:

- The Australian Government Information Management Office, 2012, *A guide to Implementing Cloud Services*—Better Practice Guide
- Cloud Security Alliance, *Security guidance for critical areas of focus in cloud computing v3.0*
- ISO/IEC 27001:2013, *Information technology—Security techniques—Information security management systems—Requirements*
- ISO/IEC 27005:2012, *Information technology—Security techniques—Information security risk management*
- ISO/IEC 27031:2011, *Information technology—Security techniques—Guidelines for information and communications technology readiness for business continuity*
- QGCIO, 2013, *Queensland Government Information Security Classification Framework*
- Australian Signals Directorate, Department of Defence, Intelligence and Security: *Cloud computing security consideration*
- Australian Government Information Management Office, *Better practice guide—privacy and cloud computing for Australian Government Agencies*
- ISACA.org, *Security considerations for cloud computing.*

We have used the principles outlined in these documents to assess the management of cloud risks and opportunities.

Audit objective, method and cost

The objective of the audit was to determine how well departments are adopting the Queensland cloud computing strategy to deliver business value while managing risks.

The audit addressed the objective through the following sub-objectives.

- Departments are giving due consideration to the use of cloud technology to deliver business benefit.
- Departments adopting cloud technology are realising expected benefits (financial or non-financial).
- Departments adopting cloud technology have effective on-going risk management processes in place.

The audit cost $348 000.

For the purposes of this audit, the scope of audit activities at selected agencies is limited to cloud computing services that fit the cloud computing essential characteristics and service models. We did not address other 'as-a-service' offerings.

In addition, the scope of the audit only includes the ICT Strategy 2013–17, its addendum, Cloud Computing Strategy, and whole of government actions as they relate to cloud computing. It does not include an audit of the ICT Action Plan, ICT Renewal Action Plan, ICT Modernisation Action Plan or any of the programs and projects relating to the action plans.

Entities subject to this audit

- Department of Science, Information Technology and Innovation— whole of government and departmental ICT and Queensland Government Chief Information Office
- Department of Education and Training
- Department of Housing and Public Works

We developed a questionnaire and interviewed departmental chief information officers to obtain information from all departments on their cloud strategies and implementation road maps.

Report structure

The structure for the remainder of this report is:

Chapter	
Chapter 2	Analyses whole-of-government ICT strategic direction
Chapter 3	Evaluates implementation of whole-of-government strategic direction and plans in three departments that we audited
Chapter 4	Results of our structured questionnaire relating to implementing cloud technology within all departments
Appendix A	Contains responses received on this report
Appendix B	Describes the audit methodology

2. Whole-of-government strategy

In brief

'Cloud first' continues to drive the government's ICT renewal program. We assessed the efficacy of the cloud computing strategy and its implementation model, and its impact on changing ICT service delivery and workforce. We also examined how well whole-of-government procurement and risk management guidelines are assisting departments in adopting this technology.

Conclusions

While the Queensland Government Chief Information Office (QGCIO) focuses on building policies, guidelines and foundational works for cloud implementation, it has not been as effective in leading and influencing departments to transform their ICT services and workforce to implement the cloud computing strategy. In addition, the strategy and its implementation model lack performance indicators for benefits and outcomes. This means that it is not possible to measure progress of departments in achieving the outcomes of the cloud strategy.

The whole-of-government procurement processes are in their early stages. Departments need to progressively develop their ICT architecture and build foundation capabilities to transition to, and manage, a cloud environment. Departments are opportunistically selecting cloud solutions without considering the long-term implications of managing a suite of standalone cloud applications. There are opportunities to improve guidance to departments on how they can incorporate cloud risks within their enterprise risk management.

Findings

- The strategic documents for cloud computing have clear intent to transform ICT services but do not define key performance indicators for outcomes. The cloud strategy is effective in creating awareness, but departments are yet to develop their overall ICT services portfolio to make the most of cloud computing.
- The QGCIO has not delivered the planned guideline for selecting service models. This may increase the risk that departments will select a cloud model that is not fit for purpose.
- The Department of Science, Information Technology and Innovation (DSITI) is unable to demonstrate that the panels it has established for cloud computing are providing value for money. This is because DSITI is unable to obtain timely and accurate data on how much departments are using the panels. In addition, DSITI can improve guidance to departments by sharing relevant information that it gathers during the due diligence.
- DSITI and QGCIO recognise the significant workforce and cultural change required in the adoption of cloud. However, the suite of cloud policies, frameworks and guidelines do not advise departments on how to plan for a workforce capability shift. This is one of the key concerns of departments implementing cloud.
- QGCIO has developed guidance for departments to manage risks during the pre-procurement and procurement phases, but not for ongoing operational cloud risk management.

Recommendations

We recommend that the Queensland Government Chief Information Office (QGCIO):

1. reviews and updates the cloud strategy and implementation model including key performance indicators for outcomes and benefits
2. reviews departmental cloud implementation roadmaps to identify whole-of-government risks and opportunities and inform decision-making, and complete frameworks and guidelines

We recommend that the Department of Science, Information Technology and Innovation (DSITI):

3. works with departments and whole-of-government procurement team to obtain relevant data on cloud usage and provide relevant due diligence information

We recommend that the QGCIO and DSITI:

4. identify whole-of-government ICT workforce target capabilities and make transition plans
5. guide departments in managing ICT services and operational risks for cloud computing.

Introduction

The Director-General of the Department of Science, Information Technology and Innovation (DSITI) leads Queensland government's Information and Communications Technology (ICT) reform agenda by developing whole-of government ICT strategies and initiatives. To this end, DSITI, including Queensland Government Chief Information Office (QGCIO), published the *Queensland Government ICT strategy 2013–17* in June 2013.

After releasing the strategy, DSITI published the *ICT strategy 2013–17* action plan, articulating a number of focus areas for each objective within the strategy. In particular, objective two: efficient digital services for government, focus area number eight relates to ICT-as-a-service.

All Directors-General are accountable for developing their strategic ICT investment portfolios, realising business value and monitoring ICT risks.

This chapter examines whether the implementation of the cloud computing strategy is delivering against the stated investment objectives. Specifically we assess:

- the efficacy of the cloud computing strategy and its implementation model
- adequacy of processes and guidance for procurement and capability uplift of ICT workforce
- adequacy of risk management guidance at a whole-of-government level.

This chapter also refers to the Strategic ICT team in DSITI as 'DSITI' for its role in implementing the whole-of-government ICT strategy and modernisation programs.

Conclusions

The cloud computing strategy aims to transform government ICT services and workforce, but implementation by departments has not resulted in whole-of-government reform. In the absence of effective leadership and focus, departments have so far implemented selected, standalone cloud solutions, using a piecemeal approach to cloud technology.

By not including outcome-focused objectives and performance indicators in the cloud computing implementation model, the planning process is inconsistent with the Queensland performance management standards. This also means that departments cannot measure their progress against achieving the outcomes of the cloud strategy.

Not addressing target workforce capability gaps increases the risk that departments will not train their existing ICT workforce and will be increasingly dependent on a finite pool of market resources.

The whole-of-government procurement processes are in their early stages. In a recent market analysis, DSITI, including QGCIO, concluded that the local market was not mature enough for DSITI to implement the cloud service brokerage. This is a fundamental part of the cloud implementation model. The cloud service brokerage would enable departments to access and manage cloud services from multiple vendors. DSITI and QGCIO have decided to defer implementing the brokerage until the local market matures.

DSITI also found that departmental practices are not standardised enough to be able to use the cloud service brokerage. However, DSITI has not prioritised activities to improve standardisation amongst departmental ICT services.

QGCIO and DSITI have a good understanding of risks presented from adopting cloud technology. However, QGCIO can improve its guidance to departments on how they can incorporate cloud risks within their operational risk management.

Efficacy of cloud computing strategy

The Queensland cloud computing strategy requires departments to purchase cloud based ICT services as the first option, unless there is a sound business case for an alternative solution. This strategy is similar to those of other jurisdictions, such as the Australian Federal, United States and United Kingdom governments.

The key difference with the United Kingdom and Unites States is that they set performance indicators within their strategies and publish regular reports on progress. The United Kingdom and United States are also more mature markets with significantly higher levels of demand.

As the cloud computing strategy originated from objective two, focus area eight of the Queensland *ICT strategy 2013–17*, we have examined whether completing action items of focus area eight has resulted in its intended outcomes identified in the ICT strategy.

Queensland Government ICT strategy 2013–2017

The ICT strategy identifies six business benefits targeted through investment in ICT as a service:

- Improve productivity and public value from digital services.
- Reduce overall expenditure on ICT infrastructure and maintenance.
- Improve organisational flexibility, agility and productivity.
- Increase predictability in cost structures.
- Decrease complexity in operational and support arrangements.
- Increase commoditisation of the services available from the cloud.

Figure 2A lists the action items and completion status for objective two, focus area eight of the Queensland ICT strategy.

Figure 2A
Action plans relating to objective 2, focus area 8: ICT-as-a-service

No.	Action plan	Estimated Completion	Actual delivery	Accountability
1.	Launch Queensland government cloud strategy and approach to adopting cloud	November 2013	May 2014	QGCIO
2.	Develop and implement government as-a-service policy	November 2013	February 2014	DSITI with Queensland Treasury and Trade support
3.	Develop and launch ICT-as-a-service tool kit	December 2013	Feb 2014 and ongoing	DSITI
4.	Revise and redefine commercial terms and conditions to support as-a-service options	December 2013	October 2015	DSITI with Department of Housing and Public Works Support
5.	Establish electronic communication and collaboration	October 2013	July 2015	DSITI
6.	A plan to divest CITEC including timeframes is developed	December 2014	Deferred	DSITI
7.	Develop one government one network business case	March 2014	Deferred	DSITI
8.	Establish market arrangements to transition commodity ICT-as-a-service	December 2013 and on-going	August 2014	DSITI
9.	Develop department as-a-service roadmaps to divest ICT systems and assets	March 2014	August 2014	DSITI and all departments

Source: Queensland Government ICT Strategy

DSITI released the cloud computing strategy in May 2014, six months later than its original estimated completion time of November 2013. QGCIO has not delivered frameworks and enabling technologies in line with the schedule and this has cumulative impact on the overall delivery of the implementation model.

While DSITI has completed tasks in the implementation plan, neither DSITI nor QGCIO have defined measures to assess the efficacy of the outputs of the action items in the cloud computing strategy or implementation model. As a result, there are no processes for measuring progress against the originally intended objectives and outcomes of the strategies.

Queensland Government performance management framework

DSITI's whole-of-government strategies and plans are integral components of the Queensland Government performance management framework.

This framework requires departments to develop performance indicators that show the extent to which the outcomes achieved are meeting the objectives in the plans.

It also requires that:

- Each objective must have one or more relevant and appropriate performance indicators, which should be outcome focused rather than output focused.
- Reporting actual results against the indicators should demonstrate the extent to which departments achieve the objective (reporting ends) and not performance with respect to services or activities (not reporting means).
- Departments develop and set specific and achievable targets for performance indicators where possible.

Knowing how well departments are performing against objectives is essential to determine if QGCIO and DSITI need to alter whole-of-government ICT strategies or policies, or revaluate its objectives.

While setting targets for performance indicators is complex, it aids accountability and challenges departments to progress their results in the desired direction. Without setting performance measures and targets, it is a 'best efforts' exercise and there is a risk that departments are not getting the best value for their ICT spends. The Queensland performance management framework provides detailed guidance on how departments can set targets.

In particular, DSITI, including QGCIO, needs to consult with departments to develop targets for objectives within the cloud computing strategy. DSITI and departments need to be clear about their roles and responsibilities and must acknowledge ownership and responsibility to deliver against the performance measures. DSITI and departments are accountable for meeting their respective performance measures through performance reporting.

Regular review of strategy

It is important to acknowledge that performance measures are subject to change. The pace of change for ICT strategies depend on the pace of change in the ICT industry, government priorities and users' and citizens' demand. To take advantage of the fast pace of technology changes, it is imperative that ICT strategies and related performance information are regularly reviewed and updated.

We acknowledge that the cloud computing strategy has a long-term goal of reorienting departments from owning ICT assets to that of a consumer of ICT services available from the market. However, DSITI, including QGCIO needs to have a regular review process to ascertain the efficacy of the strategy and to update it with respect to learnings from departments that are using the strategies.

Benefits of cloud computing

Transitioning from high cost, customised ICT applications to lower cost and standardised services is a driver of the Queensland cloud computing strategy.

However, DSITI, including QGCIO, has not defined measurable financial and non-financial benefits, such as ICT efficiency or faster and innovative service delivery. In addition, there is no assessment of whether and how cloud computing can address the challenges relating to the legacy ICT environment. In order to achieve these outcomes, DSITI, including QGCIO need departments to identify cloud benefits and provide baseline data to inform the strategic planning process.

DSITI maintains an aggregate view of ICT spend across government, however, departments allocate costs inconsistently which creates a barrier to analysing cost drivers, optimising efficiencies in ICT and measuring financial benefits.

While DSITI reports that the overall ICT spend at the whole-of-government level has reduced from $1.6 billion in 2012 to $1.2 billion in 2014–15, it is not possible to determine which factors have contributed to this reduction. This is because:

- Departments have not been consistent in reporting ICT costs in terms of cost of services delivered internally, versus those delivered through cloud computing.
- QGCIO did not define performance metrics to measure the success of the Queensland government cloud strategy. As a result, it is not clear whether the use of cloud computing in government is a result of effective cloud strategy or a result of market forces.

Cloud computing implementation model

QGCIO has developed a cloud computing implementation model to help departments move to standard, interchangeable cloud services. However, the model does not sufficiently address activities required to:

- assemble and integrate solutions from interchangeable components
- train the ICT workforce to use and manage cloud
- access cloud services to deliver innovative systems.

The model consists of a vision for the use of cloud. Three pillars that support the vision, three ICT-focused objectives, five delivery focus areas and 26 actions for delivery between 2014 and 2016.

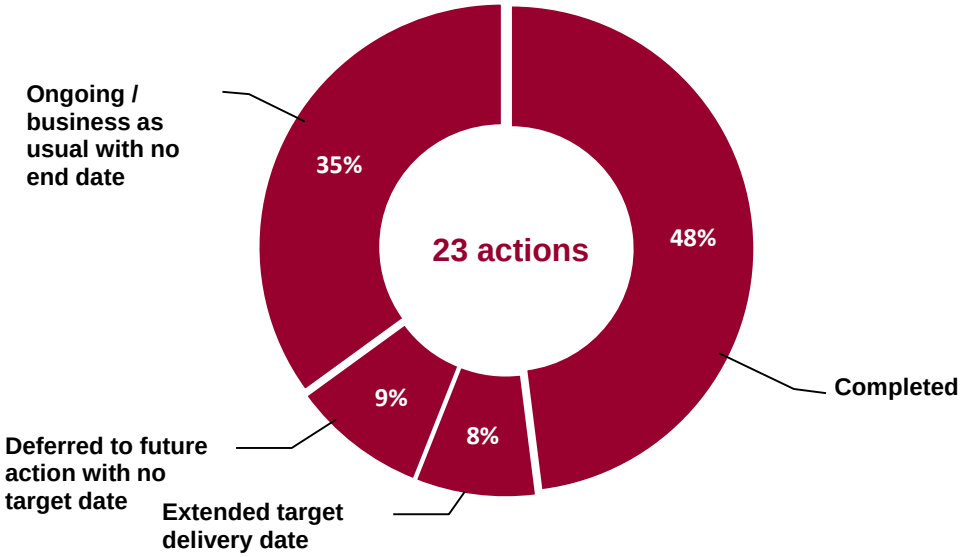
There is no clear link between the actions, the objectives and the pillars of the model. In addition, there are no success criteria or performance measures for the actions and objectives. Therefore, it is difficult to assess whether the 'in progress' and 'completed' actions have resulted in progress towards achieving the objectives and vision for cloud computing.

Status of action items within the implementation model

The implementation model outlined 23 actions for QGCIO and departments to deliver before July 2015. Figure 2B shows the status of each action as reported by QGCIO on 2 July 2015.

While QGCIO reports on the status of actions, it does not highlight progress against objectives of the implementation model. In addition, there is no weighting of actions to determine priorities in terms of their overall impact in achieving the vision.

Figure 2B
Status of action items of the implementation model



Source: Queensland Audit Office based on information provided by Queensland Government Chief Information Office

Forty-eight per cent of actions were those that QGCIO and DSITI completed. These actions are business-as-usual activities including developing policy, frameworks, panel arrangements and market analysis.

Eight actions moved to business as usual or ongoing category, which QGCIO considers as complete. However, these actions have not yet produced outcomes that contribute to the implementation model. We acknowledge that departments will submit these deliverables annually, together with other business-as-usual reports. However, moving these actions to business as usual means the QGCIO and DSITI will not be able to apply the same level of rigor to monitoring progress against the implementation model throughout the year.

Figure 2C lists activities transferred to business-as-usual with no dates for key milestones and deliverables.

Figure 2C
Activities transferred to business as usual

Action No	Action	Accountability
7	Departments start to transition from service provider to a service broker.	Departments
14	Government to take a leadership role in the promotion and encouragement of cloud services.	QGCIO with departments
15	Establish and foster a cloud community of practice across government.	QGCIO with departments
17	Departments to conduct an initial assessment of cloud service opportunities, and develop cloud migration plan.	Departments
23	Departments assess workloads for early cloud migration to gain experience from cloud. These include low risk candidates such as public cloud for website, testing and development environments.	Departments
24	Departments are discouraged from investment in private infrastructure as a service.	QGCIO with departments
25	Departments to consider cloud for new ICT procurement, refresh points and renewal or existing system where business case exists.	Departments
26.	QGCIO to provide advisory services for cloud design computing in Queensland government.	QGCIO

Source: Queensland Government Chief Information Office

ICT service delivery models

DSITI and QGCIO have developed the ICT-as-service decision framework that departments can use when planning to transition to new service models. In addition, DSITI facilitated workshops to support departments to develop their ICT-as-service implementation plans (roadmaps).

In this section, we examine how departments are using two of the ICT-as-service decision frameworks. We also examine how QGCIO and DSITI are using departmental ICT-as-a-service roadmaps to inform whole-of-government decisions and risk management.

ICT-as-service framework

The ICT-as-a-service decision framework released in February 2014 consists of three sequential processes:

- Choose a service model e.g. infrastructure as a service, platform as a service and software as a service.
- Choose a deployment model e.g. public cloud, private cloud, hybrid cloud and community cloud.
- Assess risks over the overall portfolio.

QGCIO has provided guidance on deployment models and risks but is still developing guidance on selecting a service model, the first process in the decision framework. Without this information, there is a risk that:

- departments may select a model that is not fit for purpose
- there is downstream impact on delivering the service delivery and system support
- implementation and support costs may escalate and departments may not realise expected benefits.

Departments are developing or sourcing their own decision frameworks and tools to support cloud implementation. Departments commented that the QGCIO framework is not detailed enough to support the department's requirements. There is consequently duplication of effort and inconsistencies in approaches across departments.

ICT-as-a-service roadmap

The data within departmental ICT-as-a-service roadmaps has varying levels of quality. As a result, QGCIO cannot use this information to develop a view of what the roadmap looks like at a whole-of-government level. They are therefore unable to use these roadmaps to assess risk or opportunities in cloud migration across departments. However, QGCIO has access to all departments' detailed ICT data through their annual ICT planning process. QGCIO could analyse this data to assist departments in identifying services that represent maximum value and benefits at the lowest costs and risks for transitioning to cloud.

It is evident from departmental roadmaps that departments have deferred their as-a-service transitions to as late as possible in the planning cycle. This creates risks that:

- departments will not develop incremental ICT-as-a-service capability
- departments will be competing for expertise from the market at the same time
- opportunity for leverage and shared learnings will be limited
- the concentration of activities will result in activities not being completed on time.

DSITI and QGCIO have marked this activity complete, with no further requirements for departments to report on progress against their ICT-as-a-service roadmap. Consequently, DSITI and QGCIO are not tracking whether departments are transitioning services to cloud as planned.

The changing ICT workforce

To take advantage of the new technologies and to move away from building and managing data centres and applications, it is important to broaden the capability of the ICT workforce to deliver services such as program, solution, supplier, and information management.

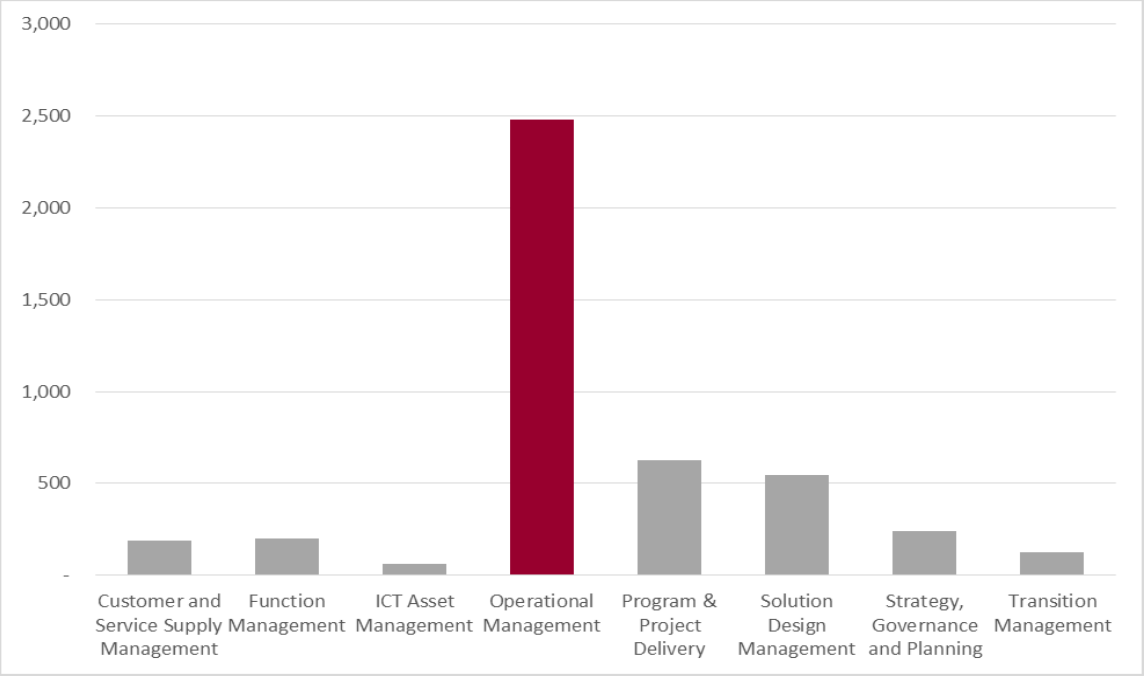
QGCIO identified senior ICT leadership skills development as the highest priority to support cloud implementation. To address this capability gap they are running a leadership program.

QGCIO also identified information security and enterprise architecture as the primary skills gaps for departments. DSITI and QGCIO have not developed further plans to address these technology-specific capability gaps, yet it is one of the top challenges for departments in using cloud computing.

While DSITI and QGCIO acknowledge that significant strategic workforce planning and cultural change is required, they have not developed a whole-of-government view of the target workforce capability, capability gaps and transition plans.

Figure 2D shows the composition of the whole-of-government ICT workforce. The majority of current ICT workforce is in the operational management area. To achieve the required level of uplift in technology skills, departments need sustained focus and investment in the medium term on its workforce.

Figure 2D
ICT workforce by function



Source: Queensland Audit Office based on Public Service Commission, Minimum Obligatory Human Resource Information data as at June 2015

Procurement processes and guidance

DSITI and QGCIO are accountable for delivering an ICT marketplace and a brokerage platform to enable departments to purchase trusted services from a variety of sources. In addition, DSITI implemented Office 365 (email and collaboration tool) as a pilot project to inform whole-of-government implementation.

In this section, we discuss DSITI's approach to the ICT marketplace and broker platforms, procurement panels, and the pilot Office 365 for email and collaboration.

ICT marketplace and broker platforms

DSITI and QGCIO have not yet delivered the ICT marketplace or cloud service brokerage. In their recent market analysis, DSITI and QGCIO concluded that the local market was not mature enough to provide cloud service brokerage. Additionally, DSITI and QGCIO identified a number of pre-requisites that departments need to address before implementing cloud service brokerage. These pre-requisites include common service levels, common procurement governance and terminology, familiarity with the cloud market as well as a strong understanding of which departmental services would benefit from cloud applications.

While DSITI and QGCIO decided to re-assess the local technology market when its maturity improves, they have not developed a plan to guide the departments to address the pre-requisites.

Case study 1 shows the United Kingdom (UK) government's statistics on their digital marketplace. It also shows the types of information that the digital marketplace has to assist departments to evaluate their options.

Case study 1

UK Government cloud adoption approach

The UK government's strategy included a cloud adoption target of 50 per cent by 2015. This Digital Marketplace enables public sector organisations to purchase trusted services from a variety of sources. The marketplace after four years of operation enables departments digital access to validated cloud services:

- 5 866 software-as-a-service products
- 971 platform-as-a-service products
- 1 369 infrastructure-as-a-service products
- 13 655 specialist cloud services.

The UK cloud marketplace publishes information about each service that supports their departments in assessing the suitability of the product, such as technical standards, compliance, backup and disaster recovery capability, product and supply chain security, data centre locations and legal jurisdiction of the service provider.

Source: Queensland Audit Office

The UK market is more mature and the UK government has invested in developing its digital marketplace. The Australian government has also committed funding to develop a digital marketplace and Queensland is seeking to align its efforts accordingly. Currently, Queensland departments have access to panels for:

- One software-as-a-service product (Office 365 email and collaboration software)
- 10 infrastructure-as-a-service products.

While the Queensland market is still developing, DSITI needs to provide guidance in assessing suitability of products in terms of technical standards, compliance, backup and disaster recovery capability, product and supply chain security, data centre locations and legal jurisdiction of the service provider. Currently, each department sources this type of information independently as part of its cloud assessment and decision frameworks, resulting in duplication of effort.

Procurement panels

DSITI is unable to demonstrate that the panels it has established for cloud computing are providing value for money. This is because DSITI does not:

- track the cost of establishing panels
- have processes in place to obtain data on how many departments use the panels and how much departments are spending through the panels.

There are times when departments negotiate directly with vendors to procure services that DSITI's panels do not cover. For example, DSITI's infrastructure-as-a-service panel agreement covers only the infrastructure-as-a-service subset of services available from large cloud providers. DSITI has no plans to extend the current arrangements to cover platform-as-a-service and software-as-a-service, which are available from the same cloud providers.

Departments that negotiate these offerings independently do not have central guidance on the additional contractual and due diligence requirements for different types of service models. In the absence of this guidance, departments may be unaware of any additional risks.

Third party assurance

DSITI does due diligence on vendors and their services when establishing a panel.

DSITI expects departments will do their own due diligence and risk assessments before entering into a contract with a panel supplier. However, there is some confusion over responsibilities, with some departments not completing due diligence and risk assessments, or duplicating the due diligence on the same service, paying multiple times.

QGCIO does not provide guidance to departments on the types of assurances required of their cloud service providers.

Office 365 pilot project

DSITI implemented Office 365, a cloud-based email and collaboration system. DSITI was also the lead agency for implementing cloud email services. Case study 2 describes key aspects of this enterprise-scale software-as-a-service solution.

During the implementation, DSITI experienced major issues with identity management, i.e. how the system will identify users and control their access levels. However, DSITI did not publish learnings that can support other departments when they implement Office 365. We acknowledge that there is a central community of practice for sharing knowledge and lessons from Office 365 implementation.

DSITI has re-aligned implementation of a federated identity platform (single sign-on to access multiple systems across departments) within the activities of the One William Street project. In the absence of a cloud-ready federated identity platform, some departments may experience similar challenges to DSITI's Office 365 experience with identity integration.

Other challenges of the project include:

- It is a technology project, without sufficient focus on business change, resulting in low user satisfaction and sub-optimal alignment between technology and business processes.
- DSITI chose not to implement Microsoft's recommended best practices, such as upgrading from Windows XP, due to time constraints, and this resulted in downstream technical problems and sub-optimal service outcomes.
- Business units were concerned that the cost was too high to achieve benefits, and that service levels were not commensurate with costs.

Case study 2

DSITI Office 365 implementation

DSITI implemented Office 365 at a cost of $3.2 million plus an ongoing licensing cost of $955 000 per year. The initial business case estimated benefits of $3.1 million over five years. DSITI did not assign accountability for monitoring and realising the benefits.

The implementation was a pilot of Office 365 and provided departments with a standing offer arrangement and implementation template approach.

DSITI sought external risk assurance on Office 365 and validated security controls for Office 365 through the Australian Signals Directorate. DSITI decided to implement some additional security controls based on this assurance and consequently encrypt data.

The implementation project ran for almost two years and the department finished the project early in phase 3 when the approved budget was exhausted. The department transitioned planned phase 3 activities such as change and benefits management to business as usual activities.

Source: Queensland Audit Office and Department of Science, Information Technology and Innovation

Risk management

Adopting cloud computing requires a balancing of risk and benefits. Transitioning too quickly will introduce risks and too slowly will delay benefits realisation.

In this section, we discuss whether departments have enough guidance from the whole-of-government level on managing risks, including business continuity management when using cloud solutions.

Queensland Government risk management guidelines

QGCIO has developed a document, *ICT as-a-service risk management guidelines,* and has not updated it since 2014. We acknowledge that the review date for this document is at an interval of two years.

However, with the rapid change in the ICT industry and with changes to department structures, the review interval of two years has resulted in the document not addressing current needs of the departments. In particular, these guidelines do not:

- guide departments on managing ongoing cloud risks
- clearly articulate risks specific to cloud computing
- address the inherent risk of sending and storing large amounts of data outside of the direct control of departments
- establish risk management strategies at the whole-of-government level.

Business continuity management and disaster recovery

In the event of a major incident, there is minimal assurance that government will deliver key cloud computing services within acceptable timeframes. Business continuity management is a key consideration when moving to cloud services and departments need to build it into architecture and operational support processes.

The QGCIO published the whole-of-government business continuity management and implementation guide on disaster recovery in September 2013. QGCIO is currently updating these documents.

Recommendations

We recommend that Queensland Government Chief Information Officer (QGCIO):

1. reviews and updates the cloud strategy, implementation model and relevant documents including:
   - defining performance indicators and criteria for outcomes and benefits that meet the objective and vision of the cloud computing strategy and align with the Queensland government performance management framework
   - setting realistic timeframes with consideration of the resource and cost implications, and then adapting a flexible style of delivery to provide timely direction and guidance to government as the market and departments mature in adopting cloud technology
   - using existing whole-of-government ICT portfolio data to highlight to departments, services that represent maximum value and benefits at the lowest costs and risks for transitioning to cloud
   - improving formal feedback and consultation process targeted to the cloud strategy and publishing information on lessons learnt from projects relating to cloud computing.
2. reviews departmental cloud implementation roadmaps to identify whole-of-government risks and opportunities and inform decision making, and completes key frameworks and guidelines including:
   - the ICT-as-a-service decision framework and guidelines
   - prioritise, in conjunction with departments, the pre-requisite activities required for cloud service brokerage.

We recommend that Department of Science, Information Technology and Innovation (DSITI):

3. improves the cloud sourcing approach by:
   - working with departments and the whole of government procurement team to obtain relevant data on cloud usage
   - providing relevant due diligence information that it gathers when establishing panels.

We recommend that QGCIO and DSITI:

4. identify whole-of-government ICT workforce target capability and gaps in capabilities, and make transition plans to address these gaps
5. improve risk management practices by:
   - developing guidelines that departments can use to manage ICT services and operational risks in a cloud-computing environment
   - guiding departments on the types of assurance reports they need to obtain for various cloud deployment models
   - including any specific requirements relating to cloud computing services with the whole-of-government business continuity management and disaster recovery guide.

3. Implementing the strategy in departments

In brief

One of the main reasons for using cloud technology is that departments can focus on transforming their service delivery rather than on owning and managing complex, highly customised IT systems. Departments can easily access technology and pay for only what they use. We evaluated how effectively three of the departments are using cloud computing to renew their Information and Communications Technology (ICT) environment and transform their service delivery.

Conclusions

The departments we audited are amongst the first to adopt cloud computing. They are using cloud to harness new opportunities or solve existing problems and have not yet planned for how they will equip their people, and transform processes and technology within their overall ICT architecture. They can improve the way they incorporate and manage cloud risk within their enterprise risk management processes.

Findings

- Two of the departments we audited have begun incorporating cloud computing within their ICT strategy. However, none of the departments have a roadmap to develop their overall ICT assets and services progressively. Departments are implementing cloud computing using customised department-specific architectures. This has resulted in duplication of effort and consultancy in areas such as privacy impact assessments.
- Departments are at different maturity levels in managing cloud operations. While all departments audited have had experience with cloud implementations, none of the departments actively equip their ICT workforce with the skills they need for managing cloud services.
- Each of the departments we audited undertook comprehensive risk assessments before they implemented the cloud services. However, departments are not formally monitoring ongoing operational risks of adopting cloud through their operational risk registers. In particular, the departments do not obtain and review formal controls assurance reports from the service providers, have not implemented sufficient controls over user access and have not reassessed business recovery goals (known as business impact analysis) as part of planning to transition to cloud services.
- Departments do not monitor user-initiated cloud computing. The departments do not have technology in place to prevent unauthorised data disclosure and cannot detect the transfer of sensitive information outside of the department.

Recommendations

We recommend that all departments:

1. update their ICT strategies to articulate any departmental drivers for cloud adoption and evaluate their current ICT assets and services portfolio to develop roadmaps and identify activities for transforming service delivery incrementally
2. identify the impact of cloud computing on ICT operations and workforce capability and develop transition plans
3. establish ICT due diligence and information management processes for user-initiated cloud solutions
4. evaluate overall risks and controls based on a formal assurance report from service providers, and implement controls and contingency plans where there are gaps
5. implement processes to detect and monitor user-initiated cloud services and a user awareness program relating to information on the risks of unapproved cloud services.

Introduction

We evaluated how effectively the whole-of-government direction translates into implementing cloud computing at three of the departments. In our sample of departments for detailed evaluation, we included the Department of Science, Information Technology and Innovation (DSITI), the Department of Education and Training (DET) and the Department of Housing and Public works (DHPW).

We specifically evaluated:

- How well departments are adopting the cloud computing strategy and whether they are adapting their Information and Communications Technology (ICT) operating model, architecture and workforce to managing the transition to new ways of delivering ICT services.
- Whether departments have changed their risk management processes to support cloud computing, evolving new security practices, access management, and business continuity.

Conclusion

DET and DHPW have set a cloud approach that they apply opportunistically. These departments are experimenting with cloud technology on a small scale when they are either purchasing a new solution or upgrading an existing system. Consequently, the departments have not planned for changes to their overall ICT assets and services portfolio. Both departments are at different stages in planning their workforce composition and capabilities.

DSITI is in the initial stages of adopting cloud computing, having implemented Office 365. DSITI does not have an enterprise view of its overall ICT assets and services and has not developed a cloud computing strategy or roadmap. This is partly due to DSITI having a fragmented ICT governance across a number of business units within the department. As a result, DSITI cannot demonstrate how it is implementing the 'cloud first strategy'.

All of the departments have comprehensive risk management analysis in pre-procurement phases of implementing cloud solutions. However, departments can improve the way they manage ongoing operational risks for cloud computing.

Developing cloud strategies

In implementing the Queensland cloud computing strategy, departments need to consider their overall ICT assets and services portfolio and create roadmaps to transform their ICT services. Ultimately, the strategies will result in mixed solutions of internally and externally managed systems, and cloud based services.

Two of the departments we audited, have developed strategies that include cloud computing. These departments consider cloud computing when implementing new systems or when upgrading existing systems. For example:

- DHPW is progressively addressing its at-risk systems and is planning to address people, process and technology changes for cloud through strategic planning. The department approved this plan in November 2015 and the next step will be for the department to demonstrate how it will execute the plan.
- DET has a digital strategy that includes cloud computing. The department’s information and innovation committee evaluates new opportunities for the use of cloud. DET invests in building cloud components that it can reuse for other implementations. However, DET has not assessed the value of cloud computing to its overall ICT assets and services portfolio. Therefore, it is difficult to determine whether investing in those components or initiatives offers the best value for the department.

DSITI has not developed a cloud computing strategy and roadmap. In addition, DSITI does not have an enterprise view of its overall ICT assets and services.

None of the departments audited uses benefits as a driver for transition to cloud computing. Two of the departments did not set targets for project benefits. These departments plan to harvest benefits as they arise. In particular, DHPW cannot demonstrate whether it has realised the benefits for the whole-of-government procurement system, QContracts.

DSITI's initial business case for implementing Office 365 included estimated benefits of $3.1 million over five years. However, DSITI did not quantify and assign accountability for realising the benefits. As a result, DSITI is not monitoring and reporting benefits from this project.

Re-designing ICT operating models

Being in the early stages of maturity, departments have roadmaps but these do not show how their ICT assets and services will evolve as they use cloud computing. In particular, departments are not updating their architecture blueprints to a level of detail that indicates target service models.

Without clearly articulating the design of the future ICT assets and services portfolio, the departments are not addressing how each of the people, process and technology components of their operating model will change. This also restricts the departments' ability to optimise timing for transitioning various services from in-house solutions to cloud computing solutions.

In addition, departments are not setting technical standards for integrating cloud-computing products within their existing ICT environment. This creates a risk that new cloud services will not integrate with existing environments and not operate effectively with other cloud services that departments purchase.

Adopting cloud

One of the key benefits of adopting cloud is to use commodity services available in the market to reduce the complexity and the need to customise IT systems. Departments are adopting the new commodity technology, but are implementing it in a similar way to traditional ICT. That is, they are using department-specific architectures and operating in isolation from other departments. Without standardising implementations wherever possible, departments are not setting up ICT architectures so that they can easily consolidate services in the event of major changes, such as machinery of government changes. In addition, inconsistent set ups may result in non-transferable staff skills across departments.

For example, the approach for software-as-a-service, Office 365 email, is different for each of the departments. While DSITI transitioned all business units within the department to the new system, DET and DHPW implemented this solution only for part of their businesses. As a result, DET and DHPW are managing a hybrid of on-premise and cloud solutions for emails. This increases the complexities in the transitional state, requiring different skill sets and resources to manage multiple modes of delivering the same service (email).

As DSITI's Office 365 is a pilot project for government, they identified benefits that they will achieve when implementing this solution, whereas, DET and DHPW did not see the need to identify the benefits upfront for their implementations. This is because DHPW needed an email system for a business unit that it acquired as part of the machinery of government changes. DET used its implementation of Office 365 for replacing an end-of-life system for schools.

Figure 3A outlines the different approaches across departments.

Figure 3A
Office 365 implementations

Topic	DET	DHPW	DSITI
In Scope	All schools. Moved from existing managed service arrangement at end-of-life.	Housing Services. Moved from Communities email due to machinery of government change.	All business units. Consolidated seven email systems.
Out of scope	Department of Education and Training corporate emails.	Other seven business units.	None.
Service model	Software-as-a-service, administered as a managed service.	Software-as-a-service, administered by department.	Software-as-a-service, administered by department.
Location	Singapore for O365 with Portal hosted at Azure Sydney.	Singapore.	Singapore.
Users	600 000	1 100	3 263
Delivery cost	$10 million total $5.25 mil: Office 365 $4.97 mil: Access portal	$340 000	$3.2 million
Technical delivery issues	Scale and identity management. DET commissioned a custom developed portal to handle access, identity and application delivery.	No significant issues.	Identity management. DSITI found maturity issues with the identity management tool.
Benefits	Not required—replaced end of life system.	Not required—machinery of government change.	$3.1 million over five years. Not yet realised.
Risk review including Privacy	External consultancy—same consultancy firm as DHPW.	External consultancy - same consultancy firm as DET.	External consultancy.
Encryption	Encrypted in transit and at rest.	Encrypted in transit but not at rest.	Encrypted in transit and at rest.
Recovery and backup	Amazon Web Services.	None.	None.

Source: Queensland Audit Office based on information provided by Department of Education and Training, Department of Housing and Public Works and Department of Science, Information Technology and Innovation.

Managing cloud operations

Of the three departments, DET has the most mature methods of managing cloud operations. However, DET has not addressed operational issues relating to the complexity of the continuous release of new features from cloud providers of QParents. This system uses six software-as-a-service components. For each component service, incremental change introduces business continuity risk to the department and complexity in change management and impact analysis.

DHPW has a clear process for the upfront procurement and provisioning of cloud infrastructure-as-a-service resources, but it will need to embed lifecycle management as its use increases.

DSITI does not have any significant cloud systems outside of Office 365 so it has only adapted operating practices for Office 365.

Building cloud capability

As departments move away from building and managing their own data centres and applications, the need for operational management skills will diminish. Therefore, departments need to broaden the capability of their current ICT workforce to deliver services such as program, solution, supplier, and information management.

Each of the departments has a formal workforce plan in place and is in a position to manage the re-skilling of its workforce.

DET has delivered two major projects and a number of minor initiatives using cloud technology. These experiences have placed DET in a good position to make informed assessments of how different service delivery models will affect its future ICT operating model and workforce needs.

DHPW has recognised the need for different skills to support cloud computing. Its ICT workforce transformation plan 2014–2019 positions cloud technical skills as a focus area in 2017–18. In the interim two years, the department is using a tactical approach to manage technical capability by including DHPW's 'business as usual' teams in cloud projects.

DSITI has undertaken workforce planning to profile its workforce. The department acknowledges that transforming the workforce will require more detailed planning. However, it has not begun this activity. Each business unit is responsible for its own workforce capability development and the department is not tracking or managing common capability gaps or skills surplus.

Managing vendors

Cloud computing provides departments with the ability to access technology without significant upfront investment and to pay only for what they use. Users can purchase or use applications without involving ICT. In these cases, business users may focus on solving their immediate problems and may not consider:

- ICT related due diligence such as security and adequate service level agreement when selecting the application
- compatibility and integration with department's existing systems.

Business units in DET can purchase ICT of up to $100 000 without engaging procurement or ICT teams. As most cloud solutions cost considerably less than $100 000, this practice is problematic because business users are not always aware of the ICT policies and practices. Consequently, the solutions they procure may not have sufficient security, backup, recovery, or reporting capabilities. In addition, the solutions may not integrate with existing ICT architecture.

Some of the business units that have whole-of-government responsibilities do not always involve the department's ICT governance processes. For example, at DHPW, the whole-of-government procurement team submitted a paper to the ICT steering committee in 2006 requesting approval to purchase software solution to manage whole-of-government supply arrangements. However, there is no evidence of the ICT steering committee being consulted leading up to the purchase of the software in 2009.

QContracts

The business area for whole-of-government procurement sits outside of DHPW's ICT governance process, as it does not relate to the internal DHPW business.

The business area did not:

- have the technical expertise within its team to assess:
  - the software technical risk profile
  - business continuity
  - data security
  - security testing requirements.
- have a formal process for managing the QContracts vendor since it purchased the system in 2010
- review the contract since its creation.

The solution has a number of implementation issues for which DHPW has established a recovery strategy in July 2015. As the business did not classify the data stored within the system, it cannot determine whether the security it has applied is appropriate.

Cloud decision tools

DET and DHPW used the whole-of-government cloud computing decision framework as a reference to develop their own decision tools. The decision tools in DET and DHPW serve as a guided discovery to the business units purchasing cloud solutions with a strong focus on information, privacy and security. The outputs from these tools inform decisions and, in DET, they inform contract negotiations.

While DET's decision tools provide useful input into the procurement and project processes, they do not provide a holistic view of whether the cloud solution or delivery model are a good fit for the departments. Specifically:

- The weight of criteria in the decision framework is unclear and there is no indication of whether criteria are optional or mandatory.
- There are gaps in technical considerations such as integration standards, access and identity management, backup and recovery and service management and this can result in complex and costly implementations.

Additionally, the departments do not provide guidance on the risks and benefits associated with different cloud service models or tools.

Managing risk

Cloud computing introduces different operating models and different risks to those experienced when using traditional ICT services. The more aware departments are about the risks and benefits of cloud computing, the more effectively they can prepare for future changes in the way ICT services operate.

When introducing any new systems, departments need to review and update existing ICT systems information and processes. With the introduction of cloud, departments are exposed to the risk of:

- compliance with legislation before purchasing cloud services
- third party service providers' controls not sufficient to address departmental risks relating to information security, data integrity and disaster recovery planning
- data leakage through user-initiated cloud services.

Pre-procurement risk assessment

Each of the departments we audited undertook comprehensive risk assessments and obtained consulting advice on compliance with legislation before they implemented the cloud services. However, departments are not formally managing ongoing operational risks of adopting cloud through their operational risk registers.

Cloud providers controls

None of the departments obtained and reviewed the formal lists of control activities available from cloud service providers. Therefore, the departments have not analysed whether the service provider has implemented sufficient controls.

Disaster recovery plans

As email systems were the main cloud implementations in all three departments, we assessed whether departments have updated their disaster recovery plans for email services.

The departments have not demonstrated that they can continue to operate effectively if there were a major disaster affecting a key component of their email services. This is because the departments have not defined continuity plans that outline how and when they will restore services if there is an extended downtime with email systems.

Departmental email services now rely both on department IT infrastructure services and cloud computing service providers. Therefore, continuity plans for the previous email systems are no longer relevant, as cloud computing has introduced additional complexities and dependencies on more sub-systems.

Security and incident management plans

None of the departments has updated its plans for security incident management to include the additional complexities when services depend on third parties. As a result, the departments may not gain sufficient access to technical systems and logs within the cloud service provider to investigate a suspected security breach within a reasonable period. Therefore, the departments may not be able to determine who committed the security breach.

Access controls to administer cloud services

For two of the departments, the strength of authentication for the system interface to administer the cloud email service is low. There is a risk of unauthorised access to the email system and its records.

User-initiated cloud services

Departments do not monitor user-initiated cloud computing. Each department audited permits staff to access most internet services, after first blocking access to websites known for inappropriate content. The departments do not have technology in place to prevent unauthorised data disclosure and therefore cannot detect the transfer of sensitive information outside of the department. This increases risks of security breaches.

Recommendations

We recommend that all departments:

6. update their ICT strategies to articulate reasons for adopting cloud and evaluate their current ICT assets and services portfolio to develop roadmaps and identify activities for transforming ICT service delivery incrementally
7. identify the impact of cloud computing on ICT operations and workforce capability and develop transition plans
8. establish ICT due diligence and information management processes for user-initiated cloud solutions
9. evaluate the overall risks and control environment based on formal assurance reports from service providers and implement controls and contingency plans where there are gaps
10. implement processes to detect and monitor user-initiated cloud services and a user awareness program relating to information on the risks of unapproved cloud services.

4. Using cloud computing across all departments

In brief

In this section, we analysed the results of our structured interviews with departmental Chief Information Officers (CIO) and provided insights on how departments applied the Queensland cloud computing strategy

Conclusion

All of the departments are in the initial stages of implementing cloud computing. The Queensland cloud computing strategy has prompted departments to consider using cloud services. However, departments are not evaluating their overall ICT services portfolio to ascertain where cloud computing can provide the best value. As a result, the implementation has been piecemeal, with limited longer-term planning or assessment of benefits.

General observations

- Seventy nine percent of departments indicated that they are adopting cloud services because of the whole-of-government strategy. However, most departments do not have a clear strategy or roadmap to integrate cloud services into their overall Information and Communications technology (ICT) architecture. This lack of planning for evolving the ICT infrastructure creates a risk that departments will implement systems and services that do not integrate with existing systems or interoperate amongst multiple-sourced cloud solutions.
- Departments report that they are transitioning mainly websites and email systems to cloud computing.
- The departments' key challenges in adopting the new technology include integration with existing systems, compliance with legislation and lack of appropriate skills and resources.
- Fifty five percent of the ICT workforce is in ICT operations. Therefore, departments need to plan for acquiring skills in the areas of enterprise architecture, ICT security and information management.
- The ICT teams within departments are not aware of a large number of user-initiated cloud services across government. DSITI's cloud discovery scan showed that a total of 8 600 GB of data is uploaded to cloud services and 75 per cent of the data is transferred to places outside of Australia.

Introduction

The intent of the Queensland cloud computing strategy is for departments to use cloud technology to transform the delivery of Information and Communications technology (ICT) services. Examples of cloud benefits include improved ICT capability, efficiency, and pace of delivering new and innovative ICT solutions to business. When used effectively, cloud computing can transform the way we do business and it can enable innovation.

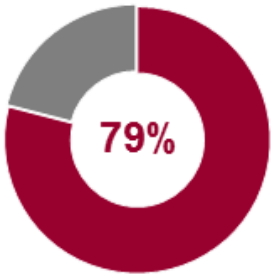
This chapter provides insights on how departments are applying the Queensland cloud computing strategy.

Conclusion

Overall, none of the departments has a planned approach to identifying and prioritising ICT services that will gain the most value from using cloud. As significant components of cloud implementation are for standalone software-as-a-service application, departments have achieved low levels of cloud benefits, which we expect will incrementally increase with more use of the technology.

Driver for adopting cloud computing

The Queensland cloud computing strategy has resulted in departments considering the use of cloud services.



79% of departments we surveyed stated that the primary driver for considering cloud computing is whole-of-government cloud computing strategy.

However, departments are using the strategy primarily as a sourcing decision when purchasing new systems or upgrading their existing systems. Departments have not evaluated their overall ICT services portfolio to ascertain which services are ready and will have the highest value in transitioning to cloud computing.

This has resulted in departments:

- Selecting standalone applications for cloud implementation (81 per cent of departments), contributing to a piecemeal approach.
- Not considering the long-term impact of cloud computing on their overall ICT architecture blueprint.
- Not explicitly considering benefits of cloud computing in business cases.

As a critical aspect of the ICT strategy, departments need to design, implement and continually optimise the way they operate their ICT services. Their operating models need to support the risks of managing new ICT services and complex multi-source cloud computing environments.

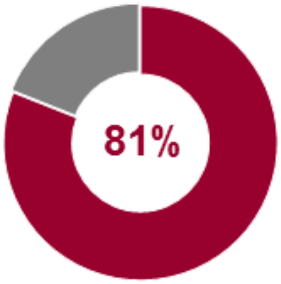
However, only nine departments have included cloud computing within their ICT strategies. Five of these departments have developed a cloud-specific strategy. If this lack of planning for evolving the ICT infrastructure continues, there is a risk that departments will have integration and interoperability issues amongst multiple-sourced systems.

Cloud adoption

Overall, departments have transitioned a low number of information assets to cloud. Currently departments' record of cloud system is less than one per cent of the overall whole of government systems portfolio.

Types of systems migrated to cloud

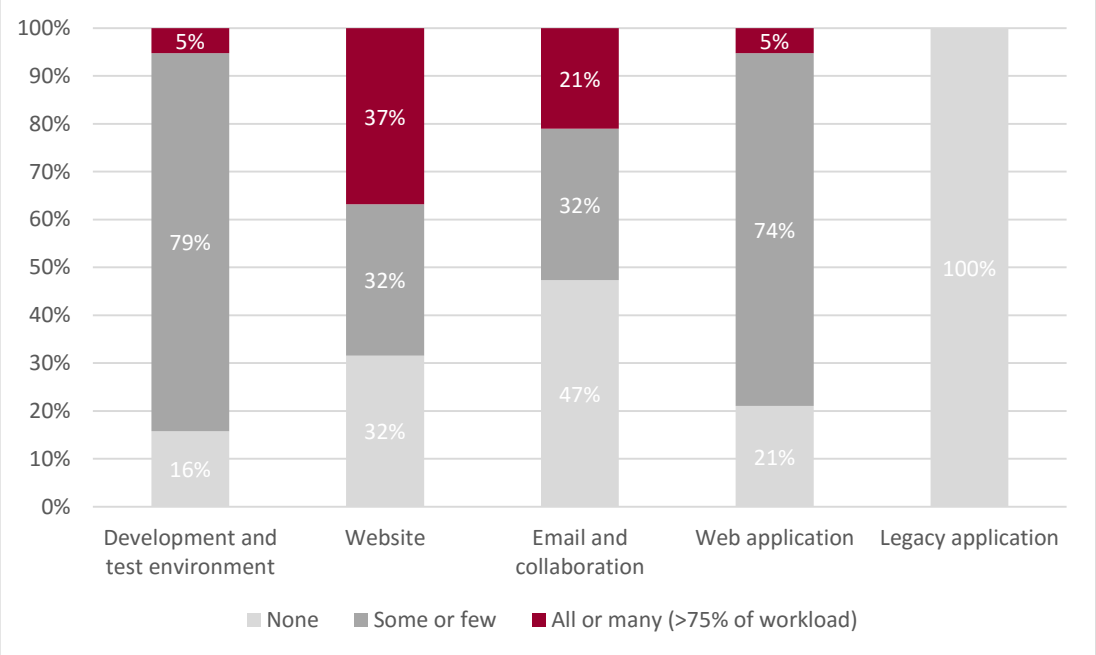
There is limited use of infrastructure and platform-as-a-service. This means that departments have not shifted their focus from managing ICT assets to transforming the overall ICT service delivery platform and procuring cloud-computing services from the market where there is value.



About 81% of the cloud solutions are standalone, software-as-a-service applications. Departments also use cloud computing mostly for their website and emails.

Figure 4A shows that 37 per cent of departments use cloud for website hosting and 21 per cent of departments use cloud for their email. A significant number of departments are managing their emails in-house (47 per cent or nine departments) or using a hybrid of in-house and cloud email solutions (32 per cent or six departments). This is despite email and collaboration systems being strong candidates for cloud computing.

Figure 4A
Department migration to the cloud - by type of application



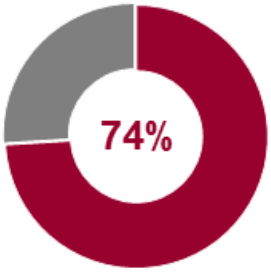
Source: Queensland Audit Office based on information provided by departments

A standard pattern for implementing cloud computing is to start with development and test environments that are less mission critical than the production environment. While 79 per cent of departments have started to use cloud for development and test environments, they are not using this technology for the majority of their test and development activities.

Maturity levels

In ascertaining the level of cloud adoption across government, we assessed:

- each departments' maturity level, using the Open Data Centre Alliance Cloud Maturity Model, which we have described in Figure 4B
- the types of information assets departments have migrated to cloud.



About 74% of the departments are in the 'initial level' of maturity in their cloud implementation. While these departments have started to implement cloud, they do not have a plan or a roadmap for their approach.

None of the departments has reached a 'defined level' maturity. This means that none of the departments has a planned approach to identifying and prioritising ICT services that will gain the most value from using cloud computing. Therefore, departments have achieved low levels of cloud benefits, which we expect will incrementally increase with higher levels of maturity.

While these departments have started to implement cloud, they do not have a plan or a roadmap for their approach.

Figure 4B describes each of the maturity levels from a baseline of no cloud use through five progressive levels of maturity.

Figure 4B
Cloud maturity model

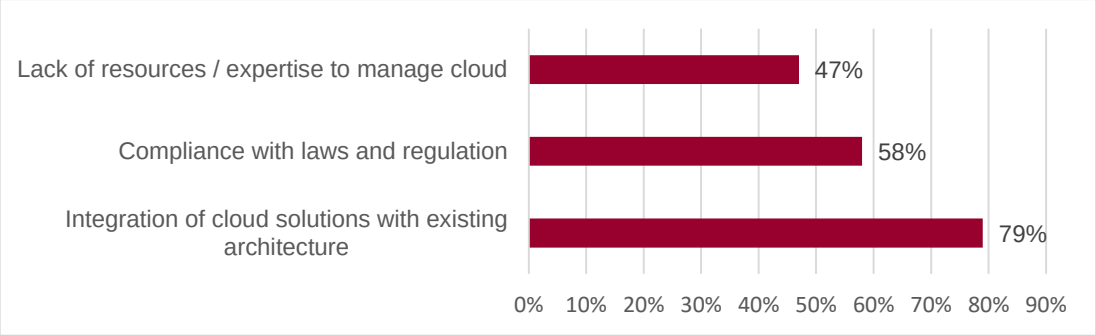
Level	Title	Description
0.	None	The department hosts legacy applications on dedicated infrastructure. No elements of cloud are being implemented.
1.	Initial, Ad Hoc	Some groups within the department have started to implement cloud. There is awareness of cloud computing. There is no cohesive cloud-computing plan.
2.	Repeatable, Opportunistic	The department has set a cloud approach that it applies opportunistically. The approach may overlap existing processes. The ICT organisation achieves capability gains from cloud.
3.	Defined, Systematic	The department governance bodies have formally endorsed a cloud approach. There is a formal approach to transitioning the ICT architecture blueprint to cloud. The ICT organisation achieves efficiency gains from cloud.
4.	Measured, Measurable	The department deploys cloud-aware applications according to business requirements on public, private and hybrid platforms. They measure cloud capability quantitatively via some type of governance structure. Appropriate metrics are gathered and reported.
5.	Optimised	The department manages a federated, interoperable and open cloud. They consistently gather metrics and use these to improve the capability. The department has established multi-cloud operations. The ICT organisation proactively enables business strategy.

Source: Cloud Maturity Model, Open Data Center Alliance, Inc. adapted by Queensland Audit Office

Challenges in implementing cloud computing

Departments identified key challenges in implementing cloud computing as described in Figure 4C.

Figure 4C
Challenges in implementing cloud computing



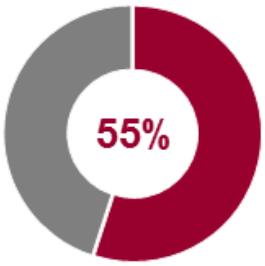
Source: Queensland Audit Office based on information from departments

Departments report that legacy systems complicate integrating cloud solutions with the existing ICT environment. This is mainly because legacy applications frequently cannot transition to cloud unless the system vendor provides a transition pathway. Legacy applications can transition to a managed service or departments may need to replace these with cloud-enabled systems at end of life.

The lack of resources and expertise to manage cloud exists for departments that have not implemented cloud or are at the initial stage of their cloud journey. It is therefore critical that, as departments progressively develop their method of delivering services, they consider their ICT workforce skills and competencies' profile.

The changing ICT workforce

As departments move away from building and managing their own data centres and applications, the need for operational management skills will diminish. Therefore, departments need to broaden the capability of their current ICT workforce to deliver services such as program, solution, supplier, and information management.

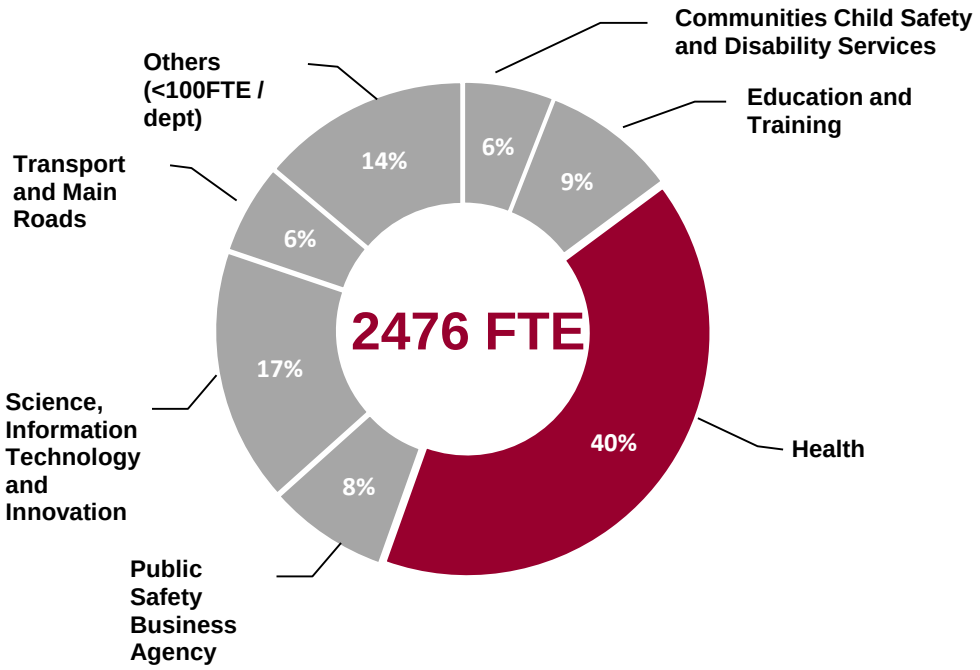


55% of whole-of-government ICT workforce are for ICT operational management function.

With such a large component of the ICT workforce involved in operating and managing ICT services, departments need sustained focus and investment in the medium term to achieve the uplift in technology skills for new service models.

Departments with large ICT operations workforce will have the highest change requirement when implementing cloud computing. Figure 4D shows the distribution of full time equivalents (FTE) in ICT operations management across departments. Without planning, departments will increasingly depend on the market to provide skills for designing and operating ICT services using cloud computing. Adequate workforce planning will also enable staff to incrementally transition into the new way of delivering ICT services.

Figure 4D
ICT Operational Management FTE breakdown by department

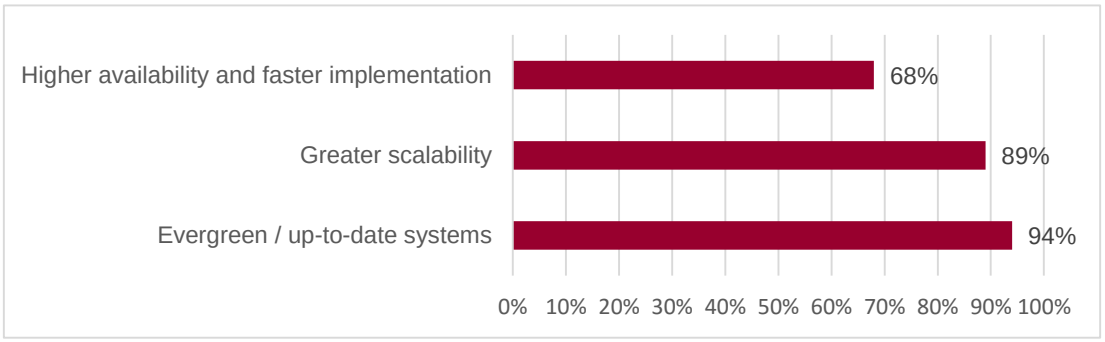


Source: Queensland Audit Office based on Public Service Commission, Minimum Obligatory Human Resource Information (MOHRI) data as at June 2015

Benefits from implementing cloud computing

Departments identified key benefits from implementing cloud computing as described in Figure 4E.

Figure 4E
Benefits from implementing cloud computing



Source: Queensland Audit Office based on information from departments

Departments who have implemented several cloud solutions found the following factors to be both a benefit and a challenge in adopting cloud computing:

- 'Evergreen' or up-to-date systems: cloud providers continuously and automatically update the systems. The challenge occurs when a department uses a system, which incorporates a number of cloud components from different service providers. When a service provider automatically updates one component, this change may have an impact to the overall integrity of the system.
- Changing the ICT funding model from capital to operating expenditure: purchasing cloud solutions means that departments need to change their funding model from capital expenditure requirements to operating expense. As departments are only in the initial stage of cloud use, departments have not yet experienced the impact of changing the funding model.

The role of ICT

Departments identified the following roles of the ICT team in promoting and implementing cloud computing:

- broker cloud services for the business
- decide or advise which systems to go to cloud
- manage cloud deployment
- set policies for how and when cloud can be used.

All the departments indicated that ICT teams and/or information steering committees have made or influenced the purchasing decisions for significant cloud computing implementations to date.

User initiated cloud computing

While departments may involve ICT when procuring significant cloud solutions, users can now easily use or purchase cloud solutions available over the internet for free or at a low cost. This requires departments to consider the risks of users purchasing cloud computing services without appropriate ICT due diligence.

Departments indicated that they do not have processes or mechanisms to monitor the use of user-initiated cloud computing in their departments. Only 20 per cent of the departments reported that they have started to purchase or pilot some tools to identify user initiated cloud computing.

Results of the Department of Science, Information Technology and Innovation's cloud discovery scan

The Department of Science, Information Technology and Innovation (DSITI) recently conducted a scan of the Queensland government internet gateway and identified that there were 2 163 individual cloud services in use. This is significantly higher than the cloud services that departments have on record and have supplied to us during our audit.

DSITI's cloud discovery scan also showed that a total of 8 600 GB of data is uploaded to cloud services and 75 per cent of the data is transferred to places outside of Australia.

User awareness program

The majority of departments surveyed (63 per cent), indicated they have cloud awareness programs. However, these programs do not include key considerations, such as, the importance of ICT due diligence when purchasing low cost applications, and whether storing business information online needs to be approved. Only 50 per cent of the departments surveyed believe that a user awareness program is important.

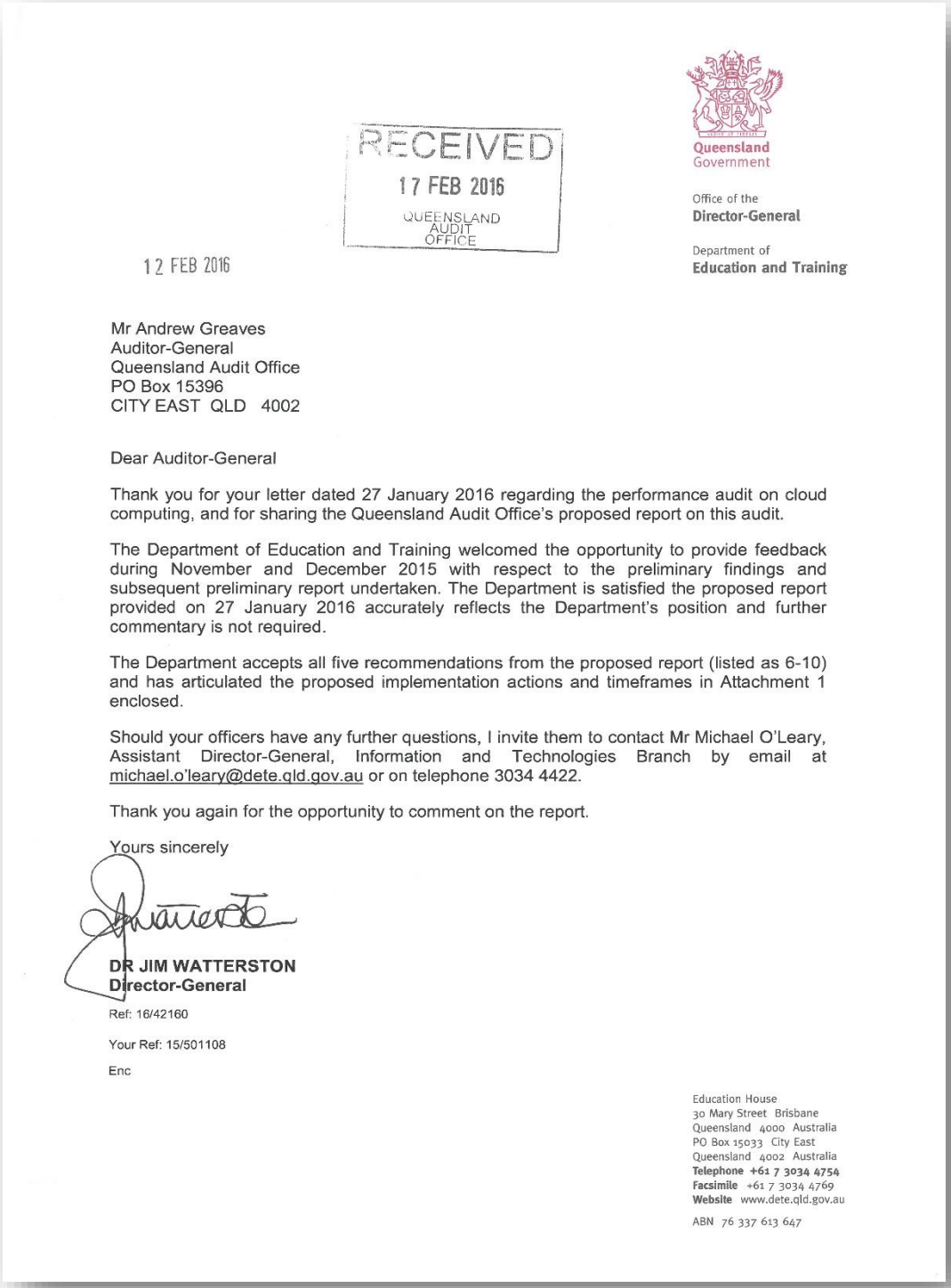
Appendices

Appendix A—Comments

In accordance with s.64 of the *Auditor-General Act 2009*, a copy of this report was provided to the Department of Education and Training, the Department of Housing and Public Works and the Department of Science, Technology and Innovation with a request for comment.

Responsibility for the accuracy, fairness and balance of the comments rests with the head of these agencies.

Comments received from Director-General, Department of Education and Training



RECEIVED
17 FEB 2016
QUEENSLAND AUDIT OFFICE

12 FEB 2016

Queensland Government

Office of the
Director-General

Department of
Education and Training

Mr Andrew Greaves
Auditor-General
Queensland Audit Office
PO Box 15396
CITY EAST QLD 4002

Dear Auditor-General

Thank you for your letter dated 27 January 2016 regarding the performance audit on cloud computing, and for sharing the Queensland Audit Office's proposed report on this audit.

The Department of Education and Training welcomed the opportunity to provide feedback during November and December 2015 with respect to the preliminary findings and subsequent preliminary report undertaken. The Department is satisfied the proposed report provided on 27 January 2016 accurately reflects the Department's position and further commentary is not required.

The Department accepts all five recommendations from the proposed report (listed as 6-10) and has articulated the proposed implementation actions and timeframes in Attachment 1 enclosed.

Should your officers have any further questions, I invite them to contact Mr Michael O'Leary, Assistant Director-General, Information and Technologies Branch by email at michael.o'leary@dete.qld.gov.au or on telephone 3034 4422.

Thank you again for the opportunity to comment on the report.

Yours sincerely

DR JIM WATTERSTON
Director-General

Ref: 16/42160

Your Ref: 15/501108

Enc

Education House
30 Mary Street Brisbane
Queensland 4000 Australia
PO Box 15033 City East
Queensland 4002 Australia
Telephone +61 7 3034 4754
Facsimile +61 7 3034 4769
Website www.dete.qld.gov.au

ABN 76 337 613 647

Response to recommendations

Queensland Audit Office
better public services

Department of Education and Training, Cloud Computing (Report No. 13: 2015–16)

Response to recommendations provided by Mr Michael O'Leary, Assistant Director-General, Information and Technologies Branch, Department of Education and Training on 3 February 2016

Recommendation	Agree / Disagree	Timeframe for Implementation (Quarter and Year)	Additional Comments
We recommend that all departments:			
6. update their ICT strategies to articulate departmental drivers for adopting cloud and evaluate the current ICT assets and services portfolio to develop roadmaps and identified activities for transforming ICT service delivery incrementally	Agree	Quarter 2, 2016	Action 6.1 - Update Strategic Planning documents to articulate the specific drivers to adopt cloud services
		Quarter 2, 2016	Action 6.2 - Develop and deliver an ICT Cloud roadmap to engage and consume cloud based services that is driven by business requirements and a considered risk approach
		Quarter 4, 2016	Action 6.3 - Update ICT Asset and Services Portfolio Strategic Management Plan focusing on an enterprise architecture approach to incorporate a transition to cloud services
7. identify the impact of cloud computing on their ICT operations and workforce capability and develop transition plans	Agree	Quarter 4, 2016	Action 7.1 - Update the ITB Workforce Management Plan to incorporate training, skilling and hiring of required workforce to accommodate any move to cloud services
8. establish ICT due diligence and information management processes for user-initiated cloud solutions	Agree	Quarter 2, 2016	Action 8.1 - Update departmental procedures to inform and guide the cloud decision making process
	Agree	Quarter 2, 2016	Action 8.2 - Provide a tailored/targeted Cloud Decision Framework for schools and business units

1

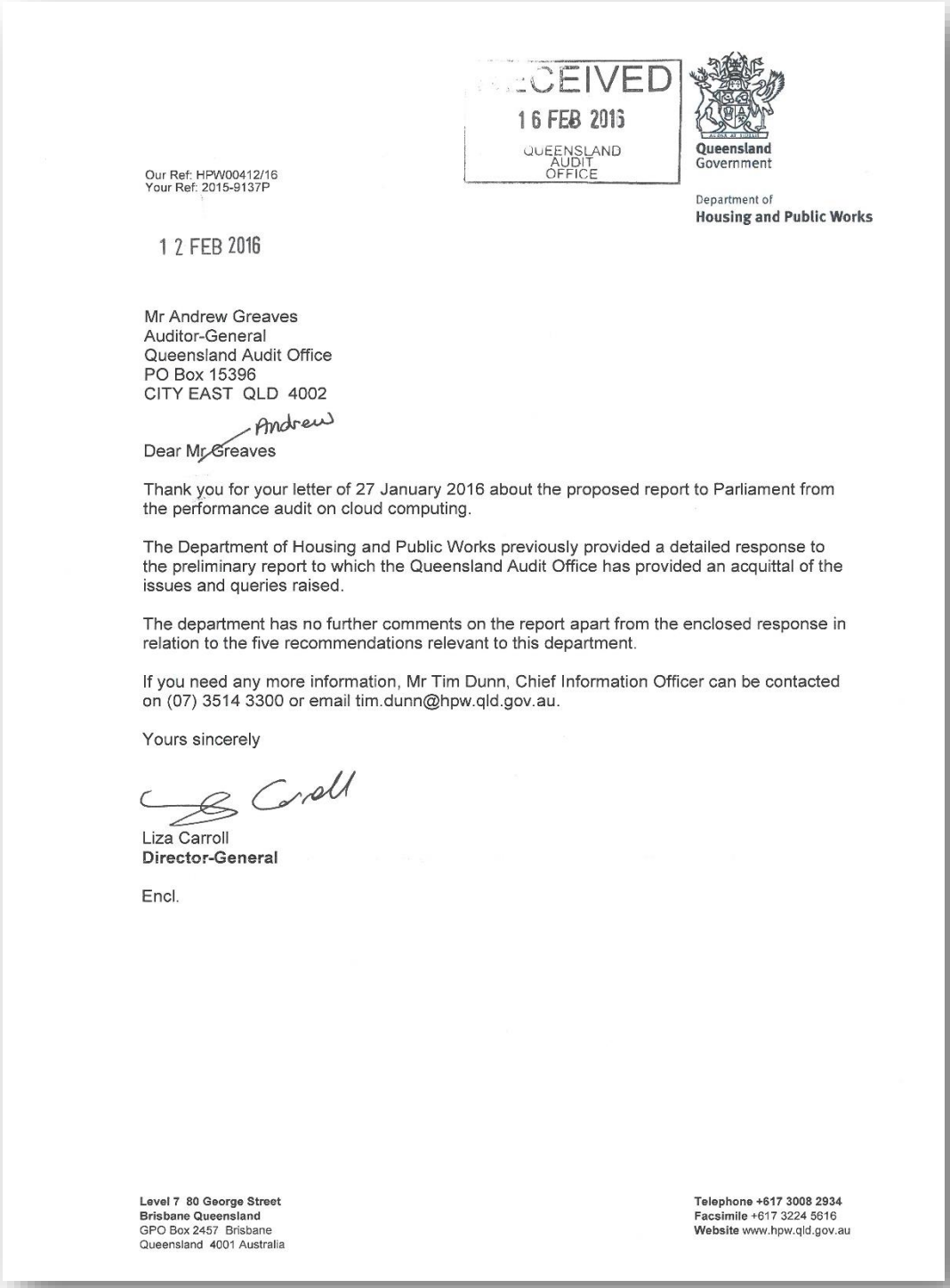
Response to recommendations

Queensland Audit Office
better public services

Recommendation	Agree / Disagree	Timeframe for Implementation (Quarter and Year)	Additional Comments
9. evaluate the overall risks and control environment based on formal assurance reports from service providers, and implement controls and contingency plans where there are gaps	Agree	Quarter 2, 2016	Action 9.1 - Update the ICT Operational and departmental Risk Register framework to include cloud based risks
		Quarter 4, 2016	Action 9.2 - Create an assurance framework and process to assess cloud service providers, including appropriate consideration of information management to implement controls and contingency plans
		Quarter 4, 2016	Action 9.3 – Update Disaster Recovery documentation to incorporate cloud services contingency planning and controls
10. implement processes to detect and monitor user-initiated cloud services and a user awareness program relating to information on the risks of unapproved cloud services	Agree	Quarter 4, 2016	Action 10.1 - Update training and resource material for schools and business units to inform on risks and risk mitigation strategies for the uptake of cloud services, including user education and awareness programs
		Quarter 4, 2016	Action 10.2 - Work with cloud service vendors and through appropriate channels implement detection, monitoring, reporting and escalation of cloud service usage within the department
		Quarter 4, 2016	Action 10.3 - Assess and promote a service catalogue of approved cloud service solutions

2

Comments received from Director-General, Department of Housing and Public Works



RECEIVED
16 FEB 2016
QUEENSLAND AUDIT OFFICE

Queensland Government

Department of
Housing and Public Works

Our Ref: HPW00412/16
Your Ref: 2015-9137P

12 FEB 2016

Mr Andrew Greaves
Auditor-General
Queensland Audit Office
PO Box 15396
CITY EAST QLD 4002

Dear Mr ~~Greaves~~ Andrew

Thank you for your letter of 27 January 2016 about the proposed report to Parliament from the performance audit on cloud computing.

The Department of Housing and Public Works previously provided a detailed response to the preliminary report to which the Queensland Audit Office has provided an acquittal of the issues and queries raised.

The department has no further comments on the report apart from the enclosed response in relation to the five recommendations relevant to this department.

If you need any more information, Mr Tim Dunn, Chief Information Officer can be contacted on (07) 3514 3300 or email tim.dunn@hpw.qld.gov.au.

Yours sincerely

Liza Carroll
Director-General

Encl.

Level 7 80 George Street
Brisbane Queensland
GPO Box 2457 Brisbane
Queensland 4001 Australia

Telephone +617 3008 2934
Facsimile +617 3224 5616
Website www.hpw.qld.gov.au

Response to recommendations

Queensland Audit Office
better public services

Department of Housing and Public Works, Cloud Computing (Report No. 13: 2015–16)

Response to recommendations provided by Liza Carroll, Director-General, Department of Housing and Public Works on 10 February 2016.

Recommendation	Agree / Disagree	Timeframe for Implementation (Quarter and Year)	Additional Comments
We recommend that all departments:			
6. update their ICT strategies to articulate departmental drivers for adopting cloud and evaluate the current ICT assets and services portfolio to develop roadmaps and identified activities for transforming ICT service delivery incrementally	Agree	Dec 2016	HPW already operates on a cloud-like infrastructure-as-a-service model. All ICT strategic planning activities assume the consideration of adopting appropriate industry delivery models in order to incrementally transform ICT service delivery.
7. identify the impact of cloud computing on their ICT operations and workforce capability and develop transition plans	Agree	Complete	HPW has an approved ICT Workforce Transformation Plan.
8. establish ICT due diligence and information management processes for user-initiated cloud solutions	Agree	Dec 2016	
9. evaluate the overall risks and control environment based on formal assurance reports from service providers, and implement controls and contingency plans where there are gaps	Agree	Dec 2016	
10. implement processes to detect and monitor user-initiated cloud services and a user awareness program relating to information on the risks of unapproved cloud services	Agree	Dec 2016	HPW has a project underway to identify and plan for the introduction of the technology to detect user initiated cloud services – this will then be subject to the usual project approval consideration.

1

Comments received from Director-General, Department of Science, Information Technology and Innovation and the Queensland Government Chief Information Officer

Emailed
15.02.16.

Queensland Government

Department of
Science, Information Technology and Innovation

Ref: 00232-2016
Your ref: 2015-9137P

RECEIVED
15 FEB 2016
QUEENSLAND AUDIT OFFICE

Mr Andrew Greaves
Auditor-General
Queensland Audit Office
PO Box 15396
CITY EAST QLD 4002

Dear Mr Greaves

Thank you for your letters of 27 January 2016 requesting comment on the preliminary draft report, including recommendations, to Parliament on the performance audit on cloud computing.

Thank you for consideration of previous commentary on the previous draft report and the acquittal provided. Both the Department of Science, Information Technology and Innovation (DSITI) and the Queensland Government Chief Information Office (QGCIO) have reviewed the draft report and have no further issues to raise.

With respect to the ten recommendations, related to both DSITI and QGCIO, both agencies agree with the recommendations put forward. Work has already commenced on a number of the recommendations, with timeframes for completion included in the attached return.

Should your officers require any further information, they may contact Evan Hill, Chief Change and Operations Officer, Department of Science, Information Technology and Innovation by email at evan.hill@dsiti.qld.gov.au or on telephone 3719 7800 or Andrew Mills, Queensland Government Chief Information Office by email at andrew.mills@qgcio.qld.gov.au or on telephone 3215 3927.

Yours sincerely

Jamie Merrick
Acting Director-General
15/2/16

Andrew Mills
Queensland Government Chief Information Officer
15/2/16.

Encl. (1)

Level 26, 111 George Street
Brisbane 4000

GPO Box 5078 Brisbane
Queensland 4001 Australia

Telephone +61 7 3215 3700
Website www.qld.gov.au

Response to recommendations

Queensland Audit Office
better public services

Department of Science, Information Technology and Innovation (DSITI), Cloud Computing (Report No. 13: 2015–16)

Response to recommendations provided by the Acting Director-General, Department of Science, Information Technology and Innovation and the Queensland Government Chief Information Officer on 16 February 2016.

Recommendation	Agree / Disagree	Timeframe for Implementation (Quarter and Year)	Additional Comments
We recommend that Queensland Chief Information Officer (QGCIO):			
1. reviews and updates the cloud strategy, implementation model and relevant documents including:	Agree	2nd Qtr, 2016 – Policy 3rd Qtr, 2016 – Guidance 4th Qtr, 2016 – CCIM and Cloud Strategy	QGCIO has a standard process for reviewing QGEA artefacts and is progressing these recommendations as part of its normal agency consultation process.
• defining performance indicators and criteria for outcomes and benefits that meet the objective and vision of the cloud computing strategy and align with the Queensland Government Performance Management Framework	Agree	2nd Qtr 2016	One of the key dependencies for defining performance indicators is to have an established baseline of the current ICT landscape on which to set realistic, measurable and achievable indicators. QGCIO and DSITI are progressing two initiatives to establish baseline measures of cloud adoption.
• setting realistic timeframes with consideration of the resource and cost implications, and then adapting a flexible style of delivery to provide timely direction and guidance to government as the market and departments mature in adopting the technology	Agree	4th Qtr, 2016	The setting of timeframes and operational responsibility must be led by each agency CIO. QGCIO will incorporate requirements into the standard ICT baseline and profiling actions that happen across a number of activities.
• using existing whole-of-government ICT portfolio data to highlight to departments, services that represent maximum value and benefits at the lowest costs and risks for transitioning to cloud	Agree	4th Qtr, 2016	QGCIO notes that the value in moving to cloud services is best determined by agencies and should align with procurement policy and broader government policy objectives.

1

Response to recommendations

Queensland Audit Office
better public services

Recommendation	Agree / Disagree	Timeframe for Implementation (Quarter and Year)	Additional Comments
• improving formal feedback and consultation process targeted to the cloud strategy and publishing information on lessons learnt from projects relating to cloud computing.	Agree	1st Qtr, 2016	In addition to QGCIO's existing formal consultation process for reviewing QGEA policies and strategies, a formal Community of Practice is being established (complementing existing informal working groups) to capture and share lessons as well as identifying priority areas of support.
2. reviews departmental cloud implementation roadmaps to identify whole-of-government risks and opportunities and inform decision making, and completes key frameworks and guidelines including: • the ICT-as-a-service decision framework and guidelines • prioritise, in conjunction with departments, the pre-requisite activities required for cloud service brokerage	Agree	4th Qtr, 2016	QGCIO will review and analyse roadmaps as they become available to capture potential risks and opportunities.
We recommend that Department of Science, Information Technology and Innovation (DSITI):			
3. improves the cloud sourcing approach by: • working with departments and the whole of government procurement team to obtain relevant data on cloud usage	Agree	2nd Qtr, 2016	
• providing relevant due diligence information that it gathers when establishing panels.	Agree	As required	
We recommend that QGCIO and DSITI			
4. identify whole-of-government ICT workforce target capability and gaps in capabilities, and make transition plans to address those gaps.	Agree	3rd Qtr, 2016	The draft QG ICT Workforce Capability Plan will be further developed to support these requirements. QGCIO and DSITI will focus on identifying and providing strategic advice and guidance on target

2

Response to recommendations

Queensland Audit Office
better public services

Recommendation	Agree / Disagree	Timeframe for Implementation (Quarter and Year)	Additional Comments
			capabilities, transitioning capabilities and the cultural changes required. Planning and operational responsibility must be led by each Agency CIO (as per Recommendation 7) as each department's strategy will ultimately result in a mixed solution of internally and externally managed systems for which their workforce requirements must align.
5. improve risk management practices by:			
• developing guidelines that departments can use to manage ICT services and operational risks in a cloud-computing environment	Agree	4th Qtr, 2016	
• guiding departments on the types of assurance reports they need to obtain for various cloud deployment models	Agree	4th Qtr, 2016	
• including any specific requirements relating to cloud computing services with the whole-of-government business continuity management and disaster recovery guide.	Agree	3rd Qtr, 2016	Consultation for the review of the whole-of-government business continuity management and disaster recovery guide has progressed. Based on the consultation, the current guide will be replaced with an implementation factsheet that will expand on existing policies and guidelines, reference widely recognised standards and include a focus on understanding dependencies. Agencies are obligated to have effective BCP and ICT DR regardless of the deployment model, including cloud.
We recommend that all departments:			
6. update their ICT strategies to articulate departmental drivers for adopting cloud and evaluate the current ICT assets and services portfolio to develop roadmaps and identified activities for	Agree	2nd Qtr, 2016	DSITI is currently developing a Departmental ICT Strategy that will incorporate drivers for cloud.

3

Response to recommendations

Queensland Audit Office
better public services

	Recommendation	Agree / Disagree	Timeframe for Implementation (Quarter and Year)	Additional Comments
	transforming ICT service delivery incrementally			
7.	identify the impact of cloud computing on their ICT operations and workforce capability and develop transition plans	Agree	3rd Qtr, 2016	DSITI will work with QGCIO (in their workforce leadership capacity) to support the undertaking of this recommendation.
8.	establish ICT due diligence and information management processes for user-initiated cloud solutions	Agree	4th Qtr, 2016	DSITI will collaborate across government with respect to developing these processes.
9.	evaluate the overall risks and control environment based on formal assurance reports from service providers, and implement controls and contingency plans where there are gaps	Agree	1st Qtr, 2017	Negotiation with service providers will be required to obtain their standard assurance report.
10.	implement processes to detect and monitor user-initiated cloud services and a user awareness program relating to information on the risks of unapproved cloud services	Agree	2nd Qtr, 2016	

4

Appendix B—Audit methodology

Audit Objective

The objective of this audit is to determine how well departments are using cloud technology to deliver business value while managing risks.

The audit addressed the objective through the following sub-objectives and lines of inquiry set out in Figure B1.

Figure B1
Audit scope

Sub-objectives		Lines of inquiry	
1	Departments are giving due consideration to the use of cloud technology to deliver business benefit.	1.1	The department has a fit for purpose strategy and decision-making structure that considers cloud adoption where it aligns to business needs.
		1.2	The ICT operating model, including workforce capability, supports the adoption of cloud.
		1.3	Frameworks, policies and processes support market engagement, procurement, vendor due diligence and financial management of modern technology solutions, such as cloud.
2	Departments adopting cloud technology are realising expected benefits (financial or non-financial).	2.1	There are processes in place to assess whether cloud implementations are fit for purpose (there is value for money including financial and non-financial business benefits).
		2.2	There are benefit realisation processes in place to monitor and ensure cloud technology delivers business value.
		2.3	There is performance management of vendors through service level agreements, key performance indicators and governance structures.
3	Departments adopting cloud technology have effective on-going risk management processes in place.	3.1	There is an effective approach to managing risks associated with cloud technology, including information security, data privacy and sovereignty.
		3.2	There are processes in place to monitor adherence to departmental policies and legislation, including information security and data privacy.
		3.3	There is effective user education and awareness programs on cloud risk, including those related to using individual cloud services.

Source: Queensland Audit Office

Reason for the audit

The Queensland Government ICT Audit Report, October 2012, highlighted that Queensland government agencies had a significant number of heavily customised and high-cost information and communication technology (ICT) systems. In addition, there was a history of complex, long and costly ICT projects to implement systems and infrastructure. The audit report also noted that business critical systems were on outdated technology with limited disaster recovery capabilities and that departments would need significant funding to maintain the ICT portfolio.

The government developed the Queensland Government ICT Strategy 2013–17 to address the recommendations within the audit report. In addition, it developed the Queensland Government Cloud Computing Strategy and the Cloud Computing Implementation Model to facilitate ICT modernisation.

This audit provided insights on the rate and type of cloud adoption within departments and how well departments are managing the associated risks.

Performance audit approach

We conducted the audit in accordance with the Auditor-General of Queensland Auditing Standards-September 2012, which incorporate the requirements of standards issued by the Australian Auditing and Assurance Standards Board.

We conducted the audit between June and October 2015 and entities included in this audit are:

- Department of Science, Information Technology and Innovation
- Department of Education and Training
- Department of Housing and Public Works.

We also interviewed the chief information officers of all government departments to gain an understanding of the level of cloud use and/or road maps for all departments.

Auditor-General Reports to Parliament

Reports tabled in 2015–16

Number	Title	Date tabled in Legislative Assembly
1.	Results of audit: Internal control systems 2014-15	July 2015
2.	Road safety – traffic cameras	October 2015
3.	Agricultural research, development and extension programs and projects	November 2015
4.	Royalties for the regions	December 2015
5.	Hospital and Health Services: 2014-15 financial statements	December 2015
6.	State public sector entities: 2014-15 financial statements	December 2015
7.	Public non-financial corporations: 2014-15 financial statements	December 2015
8.	Transport infrastructure projects	December 2015
9.	Provision of court recording and transcription services	December 2015
10.	Queensland state government: 2014–15 financial statements	December 2015
11.	Management of privately operated prisons	February 2016
12.	Follow up Report 12: 2012-13 Community Benefits Funds: Grant Management	February 2016
13.	Cloud computing	February 2016