Australian Government
Department of Finance

Australian Government Cloud Computing Policy

Smarter ICT Investment

Archived

Contents

This document supersedes *Australian Government Cloud Computing Policy, Version 2.1* July 2013.

Foreword

When we talk about Information and Communications Technology (ICT), we increasingly talk about how ICT is supporting innovation, driving change and transforming the way we work. This is as true for the public sector as it is for the private sector.

The Australian Government recognises that the community expects government services to be responsive to their needs and available where and when they want them. Key to realising this vision is the effective use of ICT by government, including the adoption of cloud services.

To do this, government agencies need to think and act smarter when it comes to investing in ICT. The availability of cloud services offers an opportunity for government to deliver services more efficiently, as well as providing services that are more responsive to business and community needs.

This policy aims to drive a greater take up of cloud services by federal government agencies by adopting a 'cloud first' approach.

Under the Government's Cloud Policy agencies now *must* adopt cloud where it is fit for purpose, provides adequate protection of data and delivers value for money.

The Australian Government procures approximately $6 billion of ICT services annually and combined with state and territory governments, public sector expenditure on ICT accounts for approximately 30 per cent of the domestic market.

We are committed to leading by example, demonstrating the benefits of investing in and using cloud services.

The Departments of Finance and Communications will continue to work together, updating this policy as elements of the ICT Investment Framework are developed.

Mathias Cormann   Malcolm Turnbull

Minister for Finance   Minister for Communications

Policy

Goal

The Australian Government will reduce the cost of government ICT by eliminating duplication and fragmentation and will lead by example in using cloud services to reduce costs, lift productivity and develop better services.

Statement

Non-corporate commonwealth entities[1] are required to use cloud services for new ICT services and when replacing any existing ICT services, whenever the cloud services:

- are fit for purpose;
- offer the best value for money, as defined by the *Commonwealth Procurement Rules*[2]; and
- provide adequate management of risk to information and ICT assets as defined by the *Protective Security Policy Framework*[3];

Practical Considerations

In using cloud services to reduce costs, lift productivity and develop better services, non-corporate commonwealth entities (entities) are to:

- use ICT refresh points as a trigger for evaluating cloud services;
- adopt public cloud services for testing and development needs and for hosting public facing websites;
- evaluate private, community, public or hybrid cloud services for operational systems as defined by information requirements;
- consider opportunities to develop/adopt cross entity or portfolio cloud services and/or build on initiatives established by other entities;
- comply with relevant legislative and regulatory requirements and to select cloud services commensurate with the requirements of the information;
- update the Agency Solutions Database[4] after acquiring a cloud service; and
- use the extensive guidance, detailed on page 11, to assist in the evaluation process.

---

[1] non-corporate commonwealth entities are as defined in the *Public Governance, Performance and Accountability Act 2013. Chapter 2, Division 2 – Accountable authorities, Subdivision C – Application of government policy.*

[2] http://www.finance.gov.au/procurement/procurement-policy-and-guidance/commonwealth-procurement-rules/

[3] http://www.protectivesecurity.gov.au/pspf/Pages/default.aspx

[4] Located in the GovShare repository: https://www.govshare.gov.au/information-on-using-agency-solutions/

Examples of refresh points include:

- business and IT systems scheduled for replacement;
- planned system implementations/upgrades;
- requirements for system development/testing where cloud infrastructure could be used;
- pilots, time-bound or short lifespan projects; and
- capabilities used only periodically.

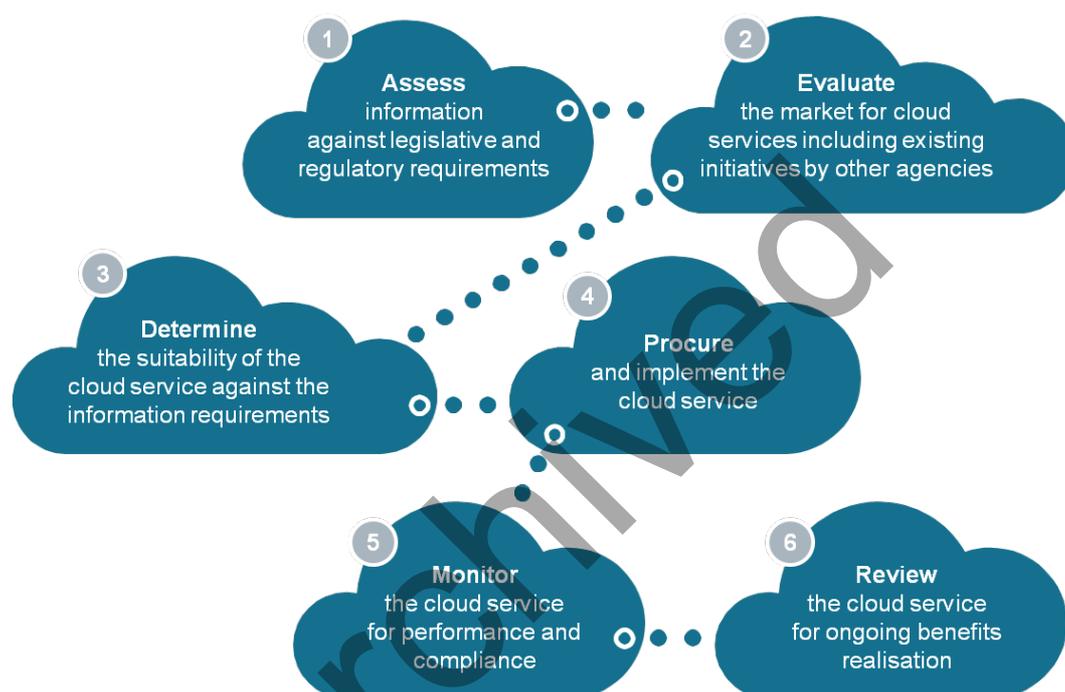Figure 1 provides a suggested high level approach to the process of evaluating cloud services.

Figure 1.

Progress to date

Data shows there has been only modest use of cloud services by government agencies to date. Cloud procurements in AusTender have totalled approximately $4.7 million since July 2010, and the Data Centre as a Service multi-use list has reported cloud contracts totalling approximately $1.5m since October 2012.

To put this in context, the Australian Government spends approximately $6 billion a year on ICT.[5] These figures demonstrate that agencies have made limited progress in adopting cloud. A significant opportunity exists for agencies to increase their use of cloud services through the Australian Government Cloud Computing Policy.

There is also an important flow-on effect to the broader economy. Combined with states and territories, government expenditure on ICT makes up approximately 30 per cent of the domestic ICT market. Improved adoption of cloud services by the

---

[5] $5.97 billion in FY2011-12 according to the Australian Government ICT Expenditure Report 2008-09 to 2011-12

government sends an important signal to the private sector. If government agencies were perceived to be treating cloud services as risky, this could reduce the adoption in the economy more generally.

Despite an overall lack of progress, some government agencies have begun to take advantage of cloud services.

As early as 2009, the Australian Maritime Safety Authority (AMSA) developed a cloud based application tool to track the compliance of international ships to safety standards across 14 geographically separated ports. This cloud based approach enabled AMSA to:

- acquire a solution that was significantly cheaper and faster to deploy compared to non-cloud solutions;
- increase user satisfaction through improved functionality and remote access on mobile devices; and
- accelerate organisational learning and maturity in using and procuring cloud services.

It is still in operation today.

More recently, the Department of Finance has undertaken an options analysis to move AusTender to a cloud based service. This analysis has recommended that a cloud pilot be undertaken for AusTender for a period of one year (with an additional 12 months available, if required), on the basis that cloud would provide superior value for money, provide greater confidence and has implementation advantages.

State governments have also taken advantage of cloud services. For example, the Queensland Government recently deployed a cloud based mail service across the state. The move will reportedly save Queensland taxpayers $13.7 million over three years in IT expenses.[6]

---

[6] See http://statements.qld.gov.au/Statement/2014/4/10/new-microsoft-deal-delivers-137million-in-savings, The Hon Ian Walker, Queensland Minister for Science, Information Technology, Innovation and the Arts.

Actions

In providing leadership on the digital economy and making more effective use of ICT across government, the following key actions are intended to assist in maintaining and growing the adoption of cloud services by entities.

#	Action	Implementation
1	Evaluate cloud services for new ICT services and when replacing existing ICT services at ICT refresh points. To support the effective adoption of cloud services, Finance will release a Resource Management Guide (RMG) to reflect this policy.	Finance to issue RMG in October/November 2014 non-corporate commonwealth entities ongoing
2	Update the Agency Solutions Database[7] after acquiring a cloud service	non-corporate commonwealth entities ongoing
3	Trial the relocation of critical data to a secure government cloud using automated tools from 2014.	Finance to complete by December 2014/January 2015
4	Review the Data Centre as a Service Multi-Use-List during 2014	Finance to complete by December 2014
5	Establish a Cloud Services Panel.	Finance to establish by January 2015
6	Streamline obligations on entities relating to the storage and processing of Australian Government information.	Attorney-General's Department (in consultation with Finance and the Department of Communications) completed
7	Update information sharing to facilitate continual learning and establish a repository of case studies, better practice guides, practical lessons learned and information on entity solutions. Interested State and Local Government organisations will be invited to participate.	Finance ongoing
8	The Government will assist entities to share experiences and best practice in developing contracts to successfully acquire cloud services.	Finance ongoing
9	The Government will report on the use of cloud services across Federal Government entities.	Finance ongoing
10	The government will continue to contribute to regional and international standards institutions and technical committees.	Finance ongoing

---

[7] Located in the GovShare repository: https://www.govshare.gov.au/information-on-using-agency-solutions/

What is cloud computing?

Australian Government definition of cloud computing

The Australian Government has adopted the US Government's National Institute of Standards and Technology (NIST) Definition of Cloud Computing[8].

The following is an excerpt from the current NIST Definition of Cloud Computing, Special Publication 800-145 September 2011.

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

Essential Characteristics:

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

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

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

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

---

[8] http://www.nist.gov/itl/cloud/

Measured service. Cloud systems automatically control and optimize resource use by leveraging a metering capability[9] at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

Service Models:

Software as a Service (SaaS). The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure[10]. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

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

Infrastructure as a Service (IaaS). The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

Deployment Models:

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

---

[9] Typically this is done on a pay-per-use or charge-per-use basis.

[10] A cloud infrastructure is the collection of hardware and software that enables the five essential characteristics of cloud computing. The cloud infrastructure can be viewed as containing both a physical layer and an abstraction layer. The physical layer consists of the hardware resources that are necessary to support the cloud services being provided, and typically includes server, storage and network components. The abstraction layer consists of the software deployed across the physical layer, which manifests the essential cloud characteristics. Conceptually the abstraction layer sits above the physical layer.

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

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

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

Guidance

Related strategies, policies, guidance and standards

A range of strategies, policies, guidance and standards are related to the decision making process when evaluating cloud services. Entities are urged to review, and incorporate where appropriate, the following:

Strategies

Australian Government Data Centre Strategy 2010-2025

The *Australian Government Data Centre Strategy 2010-2025*[11] aims to improve and optimise government use of data centre facilities over a fifteen year period through the aggregation and standardisation of entities data centre requirements via the Data Centre Facilities Panel.

The strategy identifies a number of trigger points such as asset refresh cycles, end of outsourcing contracts, end of life for data centre, or expansion of data centre capacity that place mandatory obligations on entities to use the Data Centre Facilities Panel.

Entities considering infrastructure cloud services such as Infrastructure and Platform as a Service (IaaS and PaaS) are advised to contact the Data Centres team at datacentres@finance.gov.au

Australian Government Big Data Strategy

The *Australian Government Big Data Strategy*[12] investigates the use of big data analytics as a tool to improve productivity through better service delivery and policy development. The *Australian Government Big Data* Strategy is scheduled for review in late 2014.

Policy

Protective Security Policy Framework

The *Protective Security Policy Framework*[13] provides a whole-of-government approach for the way the Australian Government protects its people, information and physical assets. The policy is the Government's principle document outlining entities mandatory obligations for the protection of information including the

---

[11] http://agimo.gov.au/policy-guides-procurement/data-centres/data-centre-strategy/

[12] http://www.finance.gov.au/big-data

[13] http://www.protectivesecurity.gov.au/pspf/Pages/default.aspx

management of security risks associated with electronic data transmission, aggregation and storage.

Information Security Manual

The *Information Security Manual[14]* is a part of the Protective Security Policy Framework providing a principles and risk-based approach to the security of government information and communications technology systems.

The manual articulates mitigating strategies and processes for entities to reduce the security risks to the Government's information assets.

Commonwealth Procurement Rules

The *Commonwealth Procurement Rules[15]* are the keystone of the Government's procurement policy framework. The rules enable entities to design procurement processes that are robust and transparent while permitting innovative solutions that reflect the scale, scope and risk of the desired outcome.

Officials must achieve value for money in procurement. Recognising that best value for money may be attained through aggregating buying power, the *Commonwealth Procurement Rules* mandate coordinated procurements, for non-corporate Commonwealth entities, and promote cooperative procurements for relevant entities.

In conducting procurements, officials are expected to appropriately manage risk. This requires considering the approach to procurement, evaluating available courses of action and recording and documenting relevant decisions. When making decisions, officials should be aware of their responsibilities to make proper use of public resources under the PGPA Act[16].

ICT Customisation and Bespoke Development Policy

The *ICT Customisation and Bespoke Development Policy[17]* aims to reduce the percentage of customised and bespoke ICT solutions across government. The policy places a mandatory obligation on entities to consider existing government or commercial off-the-shelf ICT solutions, such as cloud services.

Better Practice Guides and Frameworks

Cloud Computing Regulatory Stock Take

The *Cloud Computing Regulatory Stock Take*[18] provides an overview of existing regulation that applies to cloud services in Australia. The Stock Take covers a range of topics including deregulation, competition and copyright, contractual arrangements and consumer protection, data protection and privacy, cybersecurity, government use of cloud computing and government access to data in the cloud.

---

[14] http://www.dsd.gov.au/infosec/ism/

[15] http://www.finance.gov.au/procurement/procurement-policy-and-guidance/commonwealth-procurement-rules/

[16] *Public Governance, Performance and Accountability Act 2013*

[17] http://agimo.gov.au/files/2012/04/ICT_Customisation_and_Bespoke_Development_Policy.pdf

[18] http://www.communications.gov.au/digital_economy/cloud_computing

Cloud Security Considerations

The Australian Signals Directorate's *Cloud Security Considerations[19]* paper provides entities with a risk-based approach to the assessment of the viability of using cloud services by detailing a comprehensive list of issues to consider.

The paper assists entities to conduct a risk assessment and make an informed decision regarding whether an entity's proposed use of cloud services has an acceptable level of risk relevant to the security requirements of the information.

A Guide to Implementing Cloud Services

The *A Guide to Implementing Cloud Services[20]* provides an overarching risk-managed approach for entities to develop an organisational cloud strategy and implement cloud-based services.

The guide is aimed at experienced business strategists, architects, project managers, business analysts and IT staff to realise the benefits of cloud computing technology, focuses on activities to identify and implement cloud opportunities and advocates for a coordinated approach to the implementation of cloud services between business and ICT managers.

Privacy and Cloud Computing for Australian Government Agencies

The *Privacy and Cloud Computing for Australian Government Agencies[21]* guide provides entities with an understanding of how to comply with privacy laws and regulations when choosing cloud services.

The guide aims to give entities an awareness of their privacy and security obligations, advises on a risk-based analysis of their information and to ensure that the contractual arrangements they enter into with ICT providers adequately address their privacy obligations to citizens information.

Negotiating the Cloud – Legal Issues in Cloud Computing Agreements

The *Negotiating the Cloud – Legal Issues in Cloud Computing Agreements[22] guide* provides entities with an understanding of the typical legal issues involved when entering into cloud services agreements. The guide highlights the core set of legal issues that entities should consider with any cloud services agreement.

Entities are reminded to use contractual instruments to ensure cloud services providers address the legislative and regulatory requirements on behalf of an entity.

Financial Considerations for Government use of Cloud Computing

The *Financial Considerations for Government use of Cloud Computing[23]* guide provides entities with an understanding of the often complex financial considerations entities should address when procuring cloud services.

---

[19] http://www.dsd.gov.au/infosec/cloudsecurity.htm

[20] http://agimo.gov.au/files/2012/09/a-guide-to-implementing-cloud-services.pdf

[21] http://agimo.gov.au/files/2013/02/privacy-and-cloud-computing-for-australian-government-agencies-v1.1.pdf

[22] http://agimo.gov.au/files/2013/02/negotiating-the-cloud-legal-issues-in-cloud-computing-agreements-v1.1.pdf

[23] http://agimo.gov.au/files/2012/04/financial_considerations_for_government_use_of_cloud_computing.pdf

Records Management in the Cloud

The *Records Management in the Cloud[24]* guide provides entities with a risk-based approach to the management of information in cloud services. The guide provides a checklist to assist entities determine if a proposed cloud service complies with the requirements of the *Archives Act 1983*.

Community Cloud Governance – Better Practice Guide

The *Community Cloud Governance – Better Practice Guide[25]* provides entities with an appropriate governance framework to manage the roles and responsibilities of entities that may wish to develop or enter into a community cloud.

Australian Public Service Mobile Roadmap

The *Australian Public Service Mobile Roadmap[26]* will assist entities build a consistent, whole-of-government approach to the adoption of mobile technology that will extend services to citizens, improve entity and staff productivity, and engage more effectively.

Australian Public Service Better Practice Guide for Big Data

The *APS Better Practice Guide for Big Data[27]* aims to support the adoption of big data analytics by non-corporate commonwealth entities. The guide provides advice to entities on key considerations for adopting and using big data. It also aims to assist entities make better use of their data assets whilst ensuring that the Government continues to protect the privacy rights of individuals and security of information.

Australian Government Architecture Framework

The AGA aims to assist in the delivery of more consistent and cohesive service to citizens and support the more cost-effective delivery of ICT services by government, by providing a framework that:

- provides a common language for entities involved in the delivery of cross-entity services;
- supports the identification of duplicate, re-usable and sharable services;
- provides a basis for the objective review of ICT investment by government; and
- enables more cost-effective and timely delivery of ICT services through GovShare, a repository of standards, principles and templates that assist in the design and delivery of ICT capability and, in turn, business services to citizens.

Standards

The Australian Government is committed to and will continue contributing to the development of international cloud standards via its work with Standards Australia on the Joint Technical Committee 1 SC27 and SC38 programs of work.

---

[24] http://www.naa.gov.au/records-management/agency/secure-and-store/rm-and-the-cloud/

[25] http://www.finance.gov.au/sites/default/files/community_cloud_governance_better_practice_guide.pdf

[26] http://www.finance.gov.au/blog/2013/06/12/aps-mobile-roadmap/

[27] http://www.finance.gov.au/big-data/