Australian Government

Department of Finance and Deregulation

CLOUD COMPUTING STRATEGIC DIRECTION PAPER

Opportunities and applicability for use by the Australian Government

April 2011

Version 1.0

The Department of Finance and Deregulation acknowledges the assistance and the valuable resource material provided by the various ICT industry organisations in reviewing this document.

Disclaimer

Reference to any specific commercial product, process or service by trade name, trademark, manufacturer, or otherwise, within this document does not constitute or imply its endorsement, recommendation or favouring by the Department of Finance and Deregulation.

Contact us
Inquiries regarding the licence and any use of this document are welcome at:
Assistant Secretary
Governance and Policy Branch
Australian Government Information Management Office
Department of Finance and Deregulation
John Gorton Building
King Edward Terrace Parkes ACT 2600
Email: AGA@finance.gov.au

Table of Contents

FIGURES

INTENTIONALLY BLANK

Executive Summary

The rapid growth in the availability of cloud services and high speed broadband connectivity, such as provided by the National Broadband Network (NBN), present opportunities and challenges to all levels of government in Australia in delivering services to individuals and industry.

"Cloud computing is a new way of delivering computing resources, not a new technology."[1]

The Australian Government Cloud Computing Strategic Direction paper describes the whole-of-government policy position on cloud computing. In summary, this policy states that:

> agencies may choose cloud-based services where they demonstrate value for money and adequate security[2].

This paper provides guidance for agencies about what cloud computing is and some of the issues and benefits that agencies need to understand.

The paper recognises that the public cloud is still evolving, particularly in areas such as security and privacy. These issues need to be adequately resolved before critical government services can be transitioned to the cloud. As a result, the paper outlines three concurrent streams of work:

- Stream One – provides agencies with guidance and documentation.
- Stream Two – encourages agencies to adopt public cloud services for public facing "unclassified" government services and to undertake proof of concept studies to fully understand the risks of the cloud environment.
- Stream Three – encourages a strategic approach to cloud. This work is dependent upon greater clarity around projects commissioned under the Data Centre Strategy.

[1] ENISA: *Cloud computing: benefits, risks and recommendations for information security*, European Network and Information Security Agency.
[2] adequate security requires meeting the mandatory requirements outlined in the PSPF.

INTENTIONALLY BLANK

1. Introduction

Cloud computing advocates are claiming that cloud computing will "transform the way IT is consumed and managed, promising improved cost efficiencies, accelerated innovation, faster time-to-market, and the ability to scale applications on demand"[3].

According to Gartner[4] while the hype grew exponentially during 2008 and has continued through 2009 into 2010, it is clear that there is a major shift towards the cloud model and that the benefits may be substantial.

The shape of the cloud is emerging, and it is developing rapidly both conceptually and in reality. However, the legal/contractual, economic and security aspects of cloud computing are still relatively immature.

International governments such as the United States, the United Kingdom, Canada, and New Zealand, like Australian governments, see cloud services as an opportunity to improve business outcomes through eliminating redundancy, increasing agility and providing information and communication technology (ICT) services at a potentially cheaper cost.

In Australia, the financial sector and some government agencies have commenced investment in, and adoption of, cloud services. The roll-out of the NBN will likely accelerate the usage of cloud computing, particularly for small and medium enterprises.

1.1 Why is an Australian Government Cloud Computing Strategy required?

The Australian Government's business operations are highly dependent upon ICT, with Australian Government agencies, operating under the Financial Management and Accountability Act 1997 (FMA), spending an estimated $4.3 billion per annum on ICT.

Traditionally, computing services have been delivered through desktops, laptops or mobile devices operated by proprietary software, with each being treated differently. There are differing requirements by the executive, legislative, and judicial branches of government, as well as varying levels of privacy and security required for government transactions and the applications they use.

The Review of the Australian Government's use of ICT (the ICT Review), undertaken by Sir Peter Gershon, recommended that the government tighten the management of ICT business as usual funding through quantifying both back office service levels and associated costs of agency's current provision arrangements to determine what improvements can be realised through their own efforts.

From the perspective of improving the provision of ICT infrastructure capabilities, the review also recommended the development of a whole-of-government approach for future data

[3] Leighton, Tom: *Akamai and Cloud Computing: A Perspective fro m the Edge of the Cloud* (white paper), Akamai Technologies

[4] *Gartner Hype Cycle for Cloud Computing, 2009*

centre requirements over the next 10 to 15 years in order to avoid a series of ad hoc investments which will, in total, cost significantly more than a coordinated approach.

Sir Peter estimated that costs of $1 billion could be avoided by developing a data centre strategy for the next 15 years. The work on how best to provision ICT infrastructure capabilities (irrespective of ICT ownership) is being handled independently through the Australian Government Data Centre Strategy[5].

It is envisaged the development of cloud hosted end-to end services, targeted to the public sector, is very likely to reduce the demand for data centre capacity for agencies.

The benefits, risks, and issues associated with cloud computing have become a topic of interest as Australian Government agencies seek innovative ways to deliver government services. This is due to an increasing demand from agencies (as ICT users) for highly available, more responsive and flexible ICT service delivery that is cost effective.

Many agencies have already started using software services delivered from cloud, or cloud-like, providers (i.e. online surveys and employment forms). The increase in autonomy for agency line of business[6] areas to deploy cloud computing services threatens the established agency ICT and security governance controls.

Some agencies have already commenced small pilots and proofs of concept to evaluate the potential of application, platform and infrastructure cloud computing.

Examples of these include:

Agency	Pilot / Proof of Concept / Implementation
Australian Taxation Office (ATO)	eTax, Electronic Lodgement System (ELS) and Tax Agent Board administrative support systems are all IT capabilities employing cloud service types.
Australian Bureau of Statistics (ABS)	Implemented virtualisation software to transition to a private cloud environment.
Treasury / ATO	Standard Business Reporting (SBR) and Business Names projects have implemented private/community cloud capabilities.
Department of Immigration and Citizenship (IMMI)	Cloud Computing Proof of Concept to investigate the provision of an end-to-end online client lodgement process on a cloud platform.

[5] In 2009, the Government endorsed the Australian Government Data Centre Strategy. The principle recommendation of this strategy is that data centre requirements should be planned, procured and managed on a whole-of-government basis and that data centre facilities and services will be available via a whole-of-government panel. Portfolios, groups of agencies and large agencies which have aggregated demand above a level of 500 square metres will be able to use the panel arrangements to acquire government data centre sites, facilities and services. Smaller agencies will participate in aggregated arrangements, coordinated by Finance, to enable them to achieve the required efficiency.

[6] Line of Business is defined in the Australian Government Architecture Reference Models

New advances in cloud computing make it possible for agencies to share the same ICT infrastructure and to access software, services, and data storage through remote infrastructure. This makes it possible for ICT to become a new "utility" model.

1.2 Objective

The primary objective of the Australian Government Cloud Computing Strategic Direction paper is to develop a principles and risk based pathway for agencies to rationalise their ICT asset base and to adopt cloud computing where appropriate. Cloud computing is just one of many sourcing models agencies should consider and is not necessarily a suitable replacement for all of their current sourcing models.

Migrating some or most of an agency's service delivery to the cloud will involve a major change to the procurement, supply, and security of ICT. Modification to the skill set required of agency ICT personnel to accommodate these changes will be required.

The understanding and mitigation of a new set of risks will be necessary to accommodate this new sourcing model.

Issues such as these may increase the risk at this time for agencies wanting to rapidly implement cloud computing arrangements.

The paper includes:

- An overview of cloud computing;
- Identification of cloud-enabling policy requirements including governance, procurement;
- Identification of cloud-enabling operational requirements including virtualisation, security, privacy and transition;
- Outline of potential risks, issues and benefits associated with cloud computing;
- Identification of opportunities for government to adopt cloud computing; and
- An overview of current whole-of-government initiatives that relate to the cloud strategy.

1.3 Audience

The target audience includes:

- APS Senior Executive;
- Australian Government Chief Information Officers;
- Other Australian governments; and
- ICT industry.

2. What is Cloud Computing?

Australian Government Definition

The Australian Government has adopted the US Government's National Institute of Standards and Technology (NIST) definition for cloud computing[7].

Cloud computing is an *ICT sourcing and delivery* model for enabling 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 promotes availability and is composed of five 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's 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, laptops, and PDAs).
- ***Resource pooling*** – the provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g. country, state, or data centre). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.
- ***Rapid elasticity*** – capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale and be rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.
- ***Measured Service*** – cloud systems automatically control and optimise resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (for example, 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 utilised service.

Cloud computing is the result of several technology advances including:

[7] The complete NIST definition can be found at Attachment 4 and at http://csrc.nist.gov/groups/SNS/cloud-computing/. Also included in Attachment 4 is the Gartner definition of cloud computing.

- reliable, high-speed networks, such as the NBN;
- very large, global-class infrastructures deployed by vendors like Google and Amazon;
- virtualisation capabilities;
- commodity server hardware;
- open source software (e.g. Linux, Apache, and Hadoop), which has slashed the cost of software for data centres; and
- adoption of open Web 2.0 standards, which has made development of applications in the Cloud much easier and faster.

Figure 1: Gartner Hype Cycle for Cloud Computing, 2010[8], identifies which aspects of cloud computing are in the hype stage, applications/technologies approaching significant adoption, and those that are reasonably mature. While "security as a service" is closer to the plateau of productivity than "virtualisation" for example, the former still has 2 to 5 years to mainstream adoption, while the latter less than 2 years. This essentially means that market penetration is higher for virtualisation, while maturity of the technology and business models is more advanced for security as a service.

Due to cloud computing being at the peak of the hype cycle, agencies that seek to transition to a cloud computing arrangement may have to consider increased risks at this time.

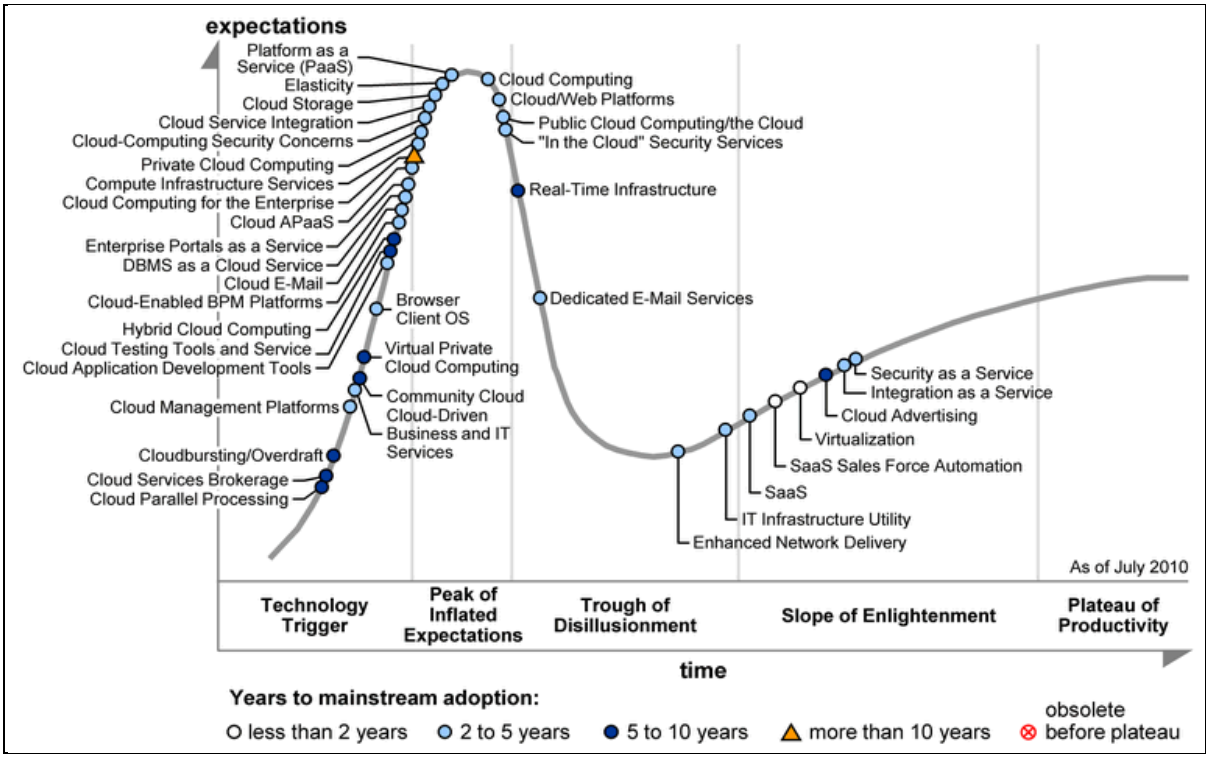

Figure 1: Gartner Hype Cycle for Cloud Computing, 2010

Note: The above Hype Cycle Graphic was published by Gartner, Inc. as part of a larger research note and should be evaluated in the context of the entire report.

[8] Gartner, Hype Cycle for Cloud Computing, 2010 (ID Number: G00201557). Disclaimer: The Hype Cycle is copyrighted 2010 by Gartner, Inc. and its affiliates/ and is reused with permission. Hype Cycles are graphical representations of the relative maturity of technologies, IT methodologies and management disciplines. They are intended solely as a research tool, and not as a specific guide to action. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

2.1 Types of Cloud Computing

There are four basic cloud delivery models, as outlined by NIST, which relate to who provides the cloud services. Agencies may employ one model or a combination of different models in delivery of applications and business services.

Type	Description
Private or internal cloud	Cloud services are provided solely for an organisation and are managed by the organisation or a third party. These services may exist off site.
Community cloud	Cloud services are shared by several organisations and support a specific community that has shared concerns (e.g. mission, security requirements, policy, and compliance considerations). These services may be managed by the organisations or a third party and may exist off site. A special case of Community Cloud is the Government or G-Cloud. This type of cloud is provided by one or more agencies (service provider role), for use by all, or most, government agencies (user role).
Public cloud	Cloud services are available to the public and owned by an organisation selling cloud services, for example, Amazon.
Hybrid cloud	An integrated cloud services arrangement that includes a cloud model and something else (another cloud model, agency back end systems, etc.), e.g. data stored in private cloud or agency database is manipulated by a program running in the public cloud.

2.1.1 Advanced Virtualisation

Advanced virtualisation is a technology rather than a cloud delivery model. It can be defined as a virtual ICT infrastructure that has automated management.

The cloud characteristics that are not intrinsic in virtualisation are:

- Capability to undertake usage based billing and invoicing;
- On-demand self-service, at least for end-users (to some extent);
- Broad network access; and
- Rapid elasticity (to some extent).

Advanced virtualisation has been included to provide a complete set of information for agencies.

2.2 Cloud Service Capability

The Australian Government has adopted the three basic types of cloud service offerings, defined by NIST, and generally accepted by industry.

Cloud Services	Description
Software as a Service (SaaS)	Offers renting application functionality from a service provider rather than buying, installing and running software yourself. Examples include Salesforce.com and Gmail.
Platform as a Service (PaaS)	Provides a platform in the cloud, upon which applications can be developed and executed. Examples include Salesforce.com, through Force.com, and Microsoft (Azure).
Infrastructure as a Service (IaaS)	Vendors offer computing power and storage space on demand. Examples include, Rackspace and Amazon S3.

The environmental scan at Attachment 2 provides a sample of information on the adoption of cloud computing by industry and international governments.

A summary of major cloud vendors is also included in Attachment 3: Prominent Global / Public Cloud Vendors.

3. Potential Risks and Issues of Cloud Computing

As cloud computing is a new ICT sourcing and delivery model NOT a new technology, many of the risks and issues associated with cloud are also not new.

However, as most agency systems were designed to operate in a secure environment, agencies need to fully understand the risks associated with cloud computing both from an end-user and agency perspective and, based on this, adopt principle and risk-based approaches to their strategic planning.

Depending upon the cloud model adopted, an understanding and mitigation of the following issues will be required:

Issue	Explanation
Application design	• There may be less opportunity for customisation of applications and services. This may increase complexity when integrating cloud services with existing legacy environments; • Applications (could be either SaaS or Line of Business applications, etc) will need to be treated at arms length from the infrastructure layer (IaaS); • Applications will need to be designed to accommodate latency; and • Existing software licensing models may not facilitate a cloud deployment.
Architecture	• Moving to a cloud environment will require more emphasis on business design where cloud services will interface/impact business systems; • Prior to making a decision to move to a cloud computing environment, agencies must address the impact on business processes and eliminate any technical barriers; and • Finance recommends agencies use an architectural framework, such as the Australian Government Architectural framework (AGA) to assist in identifying potential opportunities to deliver common and shared cloud services across agencies.
Business continuity	• Because the cloud is dependent on internet technologies, any internet service loss may interrupt cloud services; • Due to the dynamic nature of the cloud, information may not be immediately located in the event of a disaster; and • Business continuity and disaster recovery plans must be well documented and tested.
Data location and retrieval	• The dynamic nature of the cloud may result in confusion as to where information actually resides (or is transitioning through) at a given point in time; • When information retrieval is required, there may be delays impacting agencies that frequently submit to audits and inspections; and • Due to the high availability nature of the cloud, there is potential for co-location of information assets with other cloud customers.
Funding model	• Due to the cloud's pay-per-use model, some part of ICT capital budgeting

Issue	Explanation
	will need to be translated into operating expenses (OPEX), as opposed to capital expenditure (CAPEX), which may have different levels of authorisations to commit expenses and procure services.
Legal & regulatory	• Need to have the ability to discover information under common law; • Need to be aware of Australian legislative and regulatory requirements including Archives Act, FOI Act and Privacy Act; • Need to be aware of data sovereignty requirements; • Need to be aware of legislative and regulatory requirements in other geographic regions, as compliance may be a challenge for agencies, for example, the US Government's Patriot Act; and • Little legal precedent exists regarding liability in the cloud and because of this, service agreements need to specify those areas the cloud provider is responsible for.
Performance and conformance	• Need to ensure that guaranteed service levels are achieved. This includes environments where multiple service providers are employed (e.g. combined agency and cloud environments). Examples include: o Instances of slower performance when delivered via internet technologies; o Applications may require modification; o Monitoring and reporting are adequately delivered for the period between service introduction and exit; and o Failure of service provider to perform to agreed-upon service levels.
Privacy	• Risk of compromise to confidential information through third party access to sensitive information. This can pose a significant threat to ensuring the protection of intellectual property (IP), and personal information.
Reputation	• Damage to an agency's reputation resulting from a privacy or security breach, or a failure to deliver an essential service because risk was inadequately addressed must be considered for cloud computing applications.
Skills requirements	• A direct result of transitioning to a cloud environment means: o Less demand for hardware and system management software product-specific skills; and o More demand for business analysts, architects, portfolio and program and change managers, and vendor/contract managers.
Security	• Must ensure cloud service providers and their service offerings meet the requirements of the Protective Security Policy Framework (PSPF), the Australian Government Information Security Manual (ISM) and the Privacy Act 1988; and • With cloud computing, an agency may have limited ability to prescribe the protective security of the cloud environment. Yet agencies will remain ultimately responsible for the information that is stored and/or processed in the cloud. Management must maintain assurance that the security of the cloud service provider is in accordance with the PSPF.

Issue	Explanation
Service provision	• Reputation, history and sustainability should all be factors to consider when choosing a service provider; • Agencies should take into consideration the volatility of the growing cloud computingmarket; and • Agencies should ensure they address portability of data in the case of service provider failure.
Standards	Strategies for open standards, interoperability, data portability, and use of commercial off the shelf (COTS) products are required for reducing the risk of vendor lock-in and inadequate data portability. Examples include: • Potential for inadvertent use of cloud services creating "islands" of cloud technologies that will reduce interoperability across cloud types and associated implementations; • A cloud provider decides to no longer stay in business, an agency's data/application/processes must be able to be moved to another provider; and • Certification of projects by vendors for prescribed platforms and versions.

4. Potential Business Benefits of Cloud Computing for Australian Government Agencies

Transitioning to cloud services may offer the following business benefits for Australian Government agencies – the level of benefit will depend on the cloud model adopted.

Benefit	Detail
Scalability	Unconstrained capacity allows for more agile enterprises that are scalable, flexible and responsive to change. For example: • Faster responsiveness can benefit government service delivery, and meet the needs of citizens, businesses, employees, suppliers and corporate relations. For example, ability to provision and utilise a service in a single day; • Option of scalability is provided without the serious financial commitments required for infrastructure purchase and maintenance; and • Provisioning and implementation are undertaken on demand, allowing for traffic spikes and reducing the time to implement new services. *Agencies, however, need to be aware that when transitioning from legacy systems, data migration and change management can slow down the "on demand" adoption of cloud computing.*
Efficiency	Reallocation of IT operational activities offers opportunity for agencies to focus on: • Research and development including new and innovative applications allowing for business and product growth (improved service delivery); • Creating new solutions that were not technically and/or economically feasible without the use of cloud services; • Enabling prototyping and market validation of new approaches much faster and less expensively; • Providing the ability to de-couple applications from existing infrastructure; and • Rationalising legacy systems.

Cost Containment	Changes to an agencies cost model can be modified by the following:
	• Services and storage become available on demand without the serious financial commitments required for infrastructure purchase and maintenance. Additionally, they are priced as a pay-as-you-go service;
	• Transfer of costs
	  ○ From CAPEX to OPEX
	  ▪ no need to invest in high-cost IT equipment; for example, able to test software solutions without capital investment;
	  ○ Reduction of operating costs
	  ▪ reduced energy consumption;
	  ▪ less expense in managing IT systems;

Benefit	Detail
	▪ less cost and complexity in doing both routine computing tasks and computationally-intensive problems; ▪ reduced associated with time delays; ▪ potential to reduce support and maintenance costs through transitioning legacy systems to new systems; ▪ potential to reduce the demand for data centre resources; and ▪ potential to reduce the Government's carbon footprint. *Note: agencies will need to compare current costs against potential cloud expenses and consider models for lowering total cost of ownership (TCO) to understand whether cloud services will offer any potential savings.*
Flexibility	• Agencies can save time at set-up, as cloud computing becomes functional faster than other systems; • To transition to the cloud, agencies are not required to install additional hardware or software; • Implementation can be undertaken remotely; and • Potential to access latest technology through software applications being automatically updated by cloud providers.
Availability	• Cloud software architectures are designed from the bottom up for maximum network performance – potentially delivering improved application level availability than conventional IT solutions; and • Greater flexibility and availability of 'shared' information enables collaboration from anywhere in the world – all that is required is an internet connection.
Resiliency	• The potential for failure in a highly resilient computing environment is reduced. The failure of one node of a system in a cloud environment will have no impact on overall information availability and reducing the risk of perceivable downtime.

5. Potential Opportunities of Cloud Computing for Australian Government Agencies

In 2010-2011, there are a number of tactical opportunities where cloud services can be utilised by Australian Government agencies.

Table 1: Tactical Application and Use of Cloud by Government at the Information and Technology Layers sets out these opportunities. The table shows, for example, that it is possible now to move government data that is intended for public consumption or use to the public cloud.

Transitioning citizen (personal) information to the public cloud is not expected to be a viable option within the next several years until the security and privacy concerns highlighted in this document are adequately addressed. This is in contrast to the use of private and hybrid clouds, which represent more immediate or short term opportunities.

Table 1: Tactical Application and Use of Cloud by Government at the Information and technology layers

Decisions to transition at the information and services layers should be made based on a risk-managed approach taking into account information assurance requirements. The content of the Data Centre with Advanced Virtualisation column represents a service provider view, while the content of the Private Cloud, Hybrid cloud, Community Cloud (Incl. G-Cloud) and Public Cloud columns represents a user view.

Layer	Example	Data Centre with Adv. Virtualisation	Private[9] Cloud	Hybrid cloud	Community Cloud (Incl. G-Cloud)	Public Cloud
Information and Services layers						
Citizen-facing services	Citizen-driven (joined-up) service delivery (lines of business)	Now-5 years				3-5 years
Business Processes	Consolidated or shared business processes, for example, Financial, HR, Budgeting, Procurement, content management, case management	Now-5 years				3-5 years
Applications	Custom applications/Packaged applications/external services	Now-5 years				3-5 years
Citizen Information	Concerns individual citizens, covered by privacy and data protection (security)	1-2 years		3-5 years		6-10 years
Public Information	Open government data / mashups Collaborative tools, e.g. blogs, wikis, data.gov.au					Now
Technology layer						
Channels (online)	Government websites and portals Web2.0 technologies (e.g. gmail) Discovery tools, for example Google Search			Now		Now
Technology (Infrastructure)	IT and telecommunication infrastructure – utility model	Now				
Technology (process / storage capability)	Process and analyse large datasets Use as a storage platform	Now				

[9] Private Cloud is an Enterprise Cloud as defined by Gartner

6. Australian Government Cloud Computing Policy

6.1 Policy Statement

The Australian Government and its agencies may choose cloud based services if they demonstrate value for money and adequate security[10].

6.2 Vision

The vision for a whole-of-government principles and risk-based approach to cloud computing is to enable the government's ICT ecosystem to meet the wide range of agency business requirements in an optimal manner with regard to cost, security, flexibility, and operational reliability/ robustness.

6.3 Key Drivers for Adoption

The key drivers for agencies to adopt the cloud strategy are:

Driver	Outcome
Value for Money	• To reduce duplication and cost; • Leveraging economies of scale; • Increased savings through virtualisation; • Allow for "measured" payment (pay as you use); • Reduced energy use; • Enable agencies to reinvest in, and concentrate on, core objectives; • Adopt, where fit for purpose, modern technologies and practices that improve ICT effectiveness and efficiency.
Flexibility	• Create a flexible services-oriented environment for agencies; • Rapid provisioning and deployment of services and on demand scalability and elasticity for services and capabilities.
Operational reliability / robustness	• High resiliency and availability; • Standard offering.

6.4 Strategy Overview

- The strategy is based on a principle and risk-based approach. It is both tactical and strategic; it is phased to prepare agencies to utilise cloud offerings as they mature noting that public cloud services are still evolving.
- From early 2011 onwards, agencies will investigate opportunities and implement cloud solutions through a risk-managed approach taking into consideration value for money, benefits, security requirements and service level requirements. The value for money assessment will incorporate tangible and intangible, real and imputed, capital and recurrent costs and benefits.
- Agencies will be required to notify Finance when considering cloud-based services to inform possible whole-of-government approaches.

[10] adequate security requires meeting the mandatory requirements outlined in the PSPF.

- Finance, in consultation with the Cloud Information Community (CLIC) , will develop guidance to support agencies in the facilitation of effective outcomes for government.

	Stream 1 (enabling)	**Stream 2 (Public Cloud)** ***{in parallel with stream 1}***	**Stream 3 (Private, Public and Community Clouds)**
Timing	2011	2011 onwards	Mid 2011onwards
Direction	***Preparing to Adopt Cloud****: Policy, Principles, Contract Guidance and Knowledge Sharing*	***Tactical:*** *Public Cloud adoption as offerings mature*	***Strategic:*** *Whole-of-government Approach integrated with Data Centre Strategy for Private and Community Clouds.*
Cloud Delivery Models	Not applicable	Commercially Available Public Clouds Hybrid Clouds	Advanced Virtualisation and /or Private / Community Clouds <u>Enabling projects</u> 1. Data Centre As A Service (DCaaS) 2. Optimising Data Centre Use project
Procurement	Guidance prepared for agencies	Commonwealth Procurement Guidelines (CPGs) review	Investigate requirement for Whole-of-government Service Provider Panel for public cloud services
Risk-based Approach	Risk management guidance prepared for agencies	Public Clouds – Low risk information dissemination / services	Public Clouds – Low risk services Outsourced Private Clouds – Medium risk services Community Clouds for Government – Low, Medium and High risk services
Examples	Information sharing	*Public Information* – open government data; mashups *Channels* – Government websites and portals, Web2.0, discovery tools, Applications - collaboration tools, developer/testing tools	*Applications* - agency-specific (custom) applications *Business processes* – consolidated / shared business processes *Citizen facing services* - citizen-driven service delivery *Citizen information* (note: privacy and security issues) *Technology* – IT and telecommunication infrastructure (tied with Data Centre Strategy)

6.5 Deliverables

Stream	Output	Target Completion
1. Enabling Preparing to adopt cloud: policy, principles, contract guidance and knowledge guidance	a) Establishment of Cloud Information Community (CLIC)	January 2011 (completed)
	b) Development of a Cloud Framework, including: • "Use of Cloud" Principles • Governance Framework • Cloud Best Practice Guidance • Risk-based Service Provider Certification Program.	December 2011
2. Public Clouds A tactical (or opportunistic) approach to cloud services with agencies adopting public cloud as offerings mature	a) AGIMO public-facing websites transitioned to private cloud (e.g. www.data.gov.au and www.govspace.gov.au) with data.gov.au data sets hosted in a public cloud.	March 2011 (completed)
	b) Investigate sourcing model, e.g. Whole-of-government (WofG) Public Cloud Service Provider Panel	December 2011
	c) Proof of Concepts / Pilots undertaken by agencies.	Agency defined
3. Private and Community Clouds A strategic approach to cloud services with the integration of a whole-of-government approach to cloud with the Data Centre Strategy	a) Integration with Data Centre Strategy (projects that support future cloud capability) i) The ***Optimising Data Centre Use*** project will provide guidance to assist in pre-positioning agencies to use advanced virtualisation and cloud-type technologies ii) The ***DCaaS*** project will assess cloud technologies in providing common data centre facilities and ICT solutions for the 50 smaller Australian Government agencies.	May 2011 (item i) / February 2012 (item ii)
	b) Investigation and adoption of Private and/or community clouds.	Agency defined
	c) Investigation and establishment of a Government "Storefront" or Government Community Cloud	December 2012
	d) Expansion of the Cloud Information Community to undertake governance role for the Government "Storefront" or the Community Cloud/Government "Storefront" (tbc).	December 2012

6.5.1 Stream 1: Enabling (2011)

Preparing to Adopt Cloud: Policy, Principles, Contract Guidance and Knowledge Sharing.

6.5.1.1 Establishment of a Cloud Information Community

a) *Facilitate the sharing of knowledge in the adoption and management of cloud services through the establishment of a Cloud Information Community.*
The knowledge gained by monitoring international cloud activity and adoption of cloud services by agencies will be shared through the establishment of a Community of Interest (the Cloud Information Community). This will include lessons learned from agency adoption of cloud services and information gained through research.

b) *Finance will monitor local and international adoption of cloud services and service provider offerings.*
Cloud computing has drawn significant attention at the broad political and national levels. Governments of the US, UK, and some European Union countries are working on implementing cloud frameworks. The Australian Government will continue to monitor local and international trends on cloud services and integrate/leverage any learnings.

6.5.1.2 Whole-of-government Cloud Framework

AGIMO will develop a Cloud Framework incorporating principles; governance; best practice guidance including security, privacy, portability; and service provider certification requirements.

A Cloud Framework is required to cater for issues such as security, privacy, portability and service provider certification. This work is to be undertaken in collaboration with the Cyber Security Policy Coordination Committee, Protective Security Policy Committee, the Australian Information Commissioner, the Office of the Australian Information Commissioner (OAIC) and other authoritative agencies.

Components of the Government Cloud Framework may include:

a) Part A: Australian Government Cloud Principles.
There are significant risks and issues associated with cloud computing. Guiding principles are necessary to ensure that agencies consider (and address) these risks and issues. The Principles will draw from the Cross Agency Services Architecture Principles and the Protective Security Policy Framework (PSPF).
(http://www.finance.gov.au/publications/cross-agency-services-architecture-principles/index.html, http://www.ag.gov.au/pspf)
Examples may include:
- Must be risk-based;
- Must be cost effective;
- Must be flexible and responsive;
- Must avoid technology lock-in; and
- Must have sound contract arrangements that are effectively managed.

The Australian Government Cloud Principles will form part of the Australian Government Cloud Framework.

b) Part B: Governance and compliance framework for community clouds.

A governance framework is required for shared arrangements such as community clouds. This governance framework will need to cater for contract/agreement negotiation, change management, and transition of agencies to or from a community. A lead agency model is likely to be applied to any governance model.

The Governance framework will form part of the Australian Government Cloud Framework.

Finance will work in collaboration with the Attorney-General's Department (AGD) and the Defence Signals Directorate (DSD) to ensure consistency with the PSPF.

c) Part C: Development of guidance to inform agencies on issues associated with cloud computing.

Good practice guidance on privacy and security will form part of the Australian Government Cloud Framework. The Cloud Framework will also draw upon policy, good practice guidance and advice on protective security (includes information security – confidentiality, integrity, and availability) from the PSPF.

d) Part D: Service Provider Certification Program.

It is envisaged that a risk-based Service Provider Certification Program[11] will be one of the outputs.

Initial investigation work will involve:

- evaluating agency risk assessments already undertaken for proof of concept work, for example, Department of Immigration and Citizenship's (DIAC) online client lodgement integrated with DIAC systems for a limited set of temporary visa classes
    - determine whether any of the agency risk assessments are adequate for whole-of-government use
    - undertake a gap analysis to determine additional risk assessment requirements;
- review the US Government's Federal Risk and Authorization Management Program (FedRAMP) and Standards Acceleration Jumpstarting Adoption of Cloud Computing (SAJACC) programs; and
- Consideration of a cloud computing specific service provider certification program will be done in collaboration with the PSPF information security review, which is currently underway.

[11] The US Government are handling evaluation and certification of Cloud Service Providers through the Federal Information Security Management Act of 2002, or "FISMA". FISMA is a United States federal law pertaining to the information security of federal agencies' information systems. It applies to all information systems used or operated by U.S. federal agencies -- or by contractors or other organizations on behalf of the government. (http://en.wikipedia.org/wiki/FISMA)

6.5.2 Stream 2: Public Cloud (2011 onwards)

Tactical: Public Cloud adoption as offerings mature.

6.5.2.1Finance transitions AGIMO public-facing websites to public cloud.

Finance will transition public-facing websites to the public cloud.

Finance will transition AGIMO public-facing websites to the public cloud (for example, initial implementations may be: www.data.australia.gov.au (beta version), www.data.gov.au, and www.govspace.gov.au). This work will be used to assess viability of establishing a whole-of-government Public Cloud Service Provider Panel.

6.5.2.2 Sourcing Model.

Finance will investigate the viability of a whole-of-government service provider panel for public cloud services (based on outcome of evaluation of the Data Centre Strategy Integration).

There are a number of service level issues related to cloud services which will require careful consideration, for example, portability of data; business continuity; data security; vendor continuity; reporting; and disaster recovery and business continuity. A review of the whole-of-government ICT contract (GITC) should be undertaken to mitigate these service level issues.

The transition of AGIMO public-facing websites to the public cloud will be evaluated to assess the viability of establishing a whole-of-government public cloud service provider panel.

6.5.2.3 Proof of Concepts / Pilots undertaken by agencies.

a) Investigate.

Agencies are encouraged to investigate opportunities to utilise Public and Hybrid Clouds with agencies to notify Finance when they are considering cloud-based services.

There are tactical opportunities for government agencies to consider cloud-computing services. These opportunities are primarily dependant on the sensitivity (security classification) of the data. For example, publicly available data would be suitable for the public cloud, whereas personal information would likely be restricted to private or hybrid clouds. Agencies may choose to evaluate whether the use of improved business processes, security technologies (e.g. encryption) or other mitigation strategies can realise further opportunities.

Agencies will conduct Proof of Concept activities utilising public/hybrid cloud services, or may elect to pilot the use of public/hybrid cloud services.

Agencies must notify Finance when they are considering cloud-based services to inform possible whole-of-government approaches.

b) Adopt.

Agencies are encouraged to consider the use of Public and Hybrid Clouds (subject to cost/benefit and risk considerations).

The decision to utilise public cloud services is to be based on favourable cost/benefit and risk assessments.

6.5.3 Stream 3: Private and Government / Community Clouds (Mid 2011 onwards).

Strategic: Whole-of-government Approach integrated with the Data Centre Strategy.

6.5.3.1 Data Centre Strategy Integration.

The Data Centre Strategy program of work will undertake projects that will provide future cloud capability:

a) The **Data Centre as a Service** (DCaaS) project will assess cloud technologies in providing common data centre facilities and ICT solutions for the 50 smaller Australian Government agencies.

b) The **Optimising Data Centre Use** project will provide guidance to assist in pre-positioning agencies to use cloud-type technologies.

At this time, it is not known whether the Data Centre as a Service will utilise cloud services (indicative timeframe 2012-2013).

6.5.3.2 Government "storefront".

Finance will investigate a whole-of-government service / vendor catalogue or Government Cloud.

An investigation will be undertaken to ascertain the requirements for a Government "storefront" that is, a service / vendor catalogue for agencies to choose from or whether the provision of cloud services should be centralised (that is a Government Cloud environment). This investigation will be undertaken pending the outcomes of the Data Centre Strategy projects indicated in Data Centre Strategy Integration.

6.5.3.3 Investigation and adoption of private and/or community clouds.

a) Investigation of Community Clouds.

Portfolios/ Agencies should investigate opportunities to utilise Community Clouds.

There are opportunities for government agencies to consider shared cloud-computing arrangements. These opportunities may exist within and/or across portfolios.

b) Adoption of Private Clouds.

Agencies should consider Private Clouds and/or Advanced Virtualisation.

The decision to move an agency's IT environment to either a private cloud or to use advanced virtualisation must be based on favourable cost/benefit and risk assessments.

c) Adoption of Community Clouds.

I. Agencies should consider the use of Community Clouds.

Agencies/portfolios may conduct proof of concept activities utilising community cloud services, or may elect to pilot the use of a community cloud. The decision to utilise community cloud services must be based on favourable cost/benefit and risk assessments.

II. Expand role of the Cloud Information Community (established in Stream 1) .

Dependent upon the completion of the Data Centre projects indicated in Data Centre Strategy Integration, Finance will investigate and establish a new Terms of Reference for the Cloud Information Community which may include:

- Overseeing the operation of the vendor / service catalogue.
- Overseeing the chargeback models for a community cloud.

It is envisaged that membership for this group would include both IT and business people, for example, finance, procurement and program executives.

Attachment 1: Related Documents.

Agencies should not consider cloud services in isolation. Other related Australian Government agendas, policies, strategies, frameworks and standards will affect an agency's decision to move to a cloud environment. Agencies should pay particular attention to the requirements laid out in the Protective Security Policy Framework (PSPF) and the Australian Government Information Security Manual (ISM).

Whole-of-Government Agenda

- APS Reform Agenda: The Blueprint, Ahead of the Game outlines a comprehensive reform agenda.
- Service Delivery Reform: Agenda of the secretaries committee on Service Delivery with work lead by the Department of Human Services.
- Gov 2.0: Government 2.0 is about the use of Web 2.0 technology to encourage a more open and transparent form of government, where the public has a greater role in forming policy and has improved access to government information.

Strategies

- Whole-of-government Vision and Strategy for government wide ICT: Under development.
- Data Centre Strategy: Cloud computing at the infrastructure layer (Infrastructure as a Service – IaaS) is an integral component of the Australian Government Data Centre Strategy 2010-2025 released in March 2010. Data Centre rationalisation will bring substantial savings in cost and energy consumption; at the same time, it will improve service standards and increase the ability to cope with disruption.
- Cyber Security Strategy: The Strategy was launched on 23 November 2009 and articulates the overall aim and objectives of the Australian Government's cyber security policy and sets out the strategic priorities that the Australian Government will pursue to achieve these objectives. The Strategy also describes the key actions and measures that will be undertaken through a comprehensive body of work across the Australian Government to achieve these strategic priorities.

Policies, Frameworks and Standards.

- Australian Government Architecture (AGA) framework.
- ICT Customisation and Bespoke Development Policy.
- Green ICT – see Principle for Sustainable Design.
- Guide to Open Source Software.
- Protective Security Policy Framework.
- Various procurement policies including Telecoms Co-ordinated Procurement; Desktop Co-ordinated Procurement and Common Operating Environment (COE).

Other Government initiatives

- Australian Government Internet Gateway Reduction Initiative: Reduces the number of Australian Government internet gateways to the minimum required for improved security, reliability, and operational efficiency. This will see a reduction from about 124 gateways to between four and eight over the next four years.

- National Broadband Network (NBN): The Australian Government has established a Government business enterprise, NBN Co Limited, to design, build and operate an open access, high-speed network to 93% of all Australian premises with fibre-based services and 7% with next generation wireless and satellite technologies, subject to final design.

Attachment 2: Environmental Scan

Economy	Programs/Policies	Implemented Clouds/Pilot Tests
Australia	In development	**Government** **West Australian Department of Treasury and Finance (DTF):** Private Cloud (IaaS). Announced August 2010. **West Australian Health (WA Health):** Private Cloud (IaaS). Announced August 2010. Anticipated completion for WA Health data centres are April 2011 and June 2011. **Department of Immigration and Citizenship (DIAC):** Hybrid Cloud (IaaS). Completed Proof of Concept as of June 2010. Some issues include physical proximity to service and centrality versus distributed centres. **Department of Human Services (DHS):** Public Cloud (SaaS). Proof of Concept stage. **Australian Maritime Safety Authority (AMSA):** Public Cloud (SaaS/PaaS). Development of a pilot cloud-based application on a vendor platform (Force.com). It was found that the majority of problems encountered in the cloud-based environment are encountered with traditional software (i.e. platform lock-in, vendor management maturity, etc) and that it is important to assess whole-of-life costs. It is possible that choosing a low-risk, low-transaction-volume application can expose potential problems. Although business users found the end result a success, there was some doubt about whether the vendor was ready to support government clients in the region. Australian Government Information Management Office (AGIMO): (Iaas/Paas) The data sets on data.gov.au were migrated onto the public Amazon cloud. The data.gov.au and govspace.gov.au websites were migrated onto a private cloud. **Industry** **Westpac:** Private Cloud (IaaS). Announced March 2010. Completed Proof of Concept trial of an internal 'private cloud', which was of a sufficient scale to warrant its own infrastructure. **Visy:** Private Cloud (IaaS). Announced in July 2010 that it had awarded Telstra a $50 million contract to support their business applications in the cloud. **MYOB:** SaaS. Announced a roadmap for a move to the cloud in May 2010. **Commonwealth Bank:** Private Cloud (IaaS/PaaS/SaaS). Announced Proof of Concept trials in July 2010 of a hypervisor-agnostic cloud computing platform. They are aiming for a standard, virtualised infrastructure stack and applications housed in an enterprise 'app

Economy	Programs/Policies	Implemented Clouds/Pilot Tests
		store'. **SAP:** Private Cloud (IaaS/SaaS). Announced June 2010. Will be segmenting its emerging cloud-computing strategy across multiple development platforms. **General Interest**: Australian and New Zealand Banking Group (ANZ) announced their interest in May 2010.
United States	**Overall**: On 9 December 2010, the US Government released the 25 Point Implementation Plan to Reform Federal Information Technology Management. This plan announced a Cloud First policy where each agency will identify three "must move" services within three months, and move one of those services to the cloud within 12 months and the remaining two within 18 months. The US released a Federal Cloud Computing Strategy in February 2011. The strategy entifies what cloud computing is, its benefits and provides a decision framework for migrating to cloud. The strategy aims to move approximately $20bn of an $80bn IT spend to the cloud. The high-value and ready services would be the first to move to the cloud. Every agency is required to think through the cloud strategy and then evaluate its technology sourcing strategy. Generally, the US Administration sees in cloud computing an opportunity to eliminate redundancy and drive down computing costs significantly. However, it is seen as a long-term project of at least a decade with significant governance, security, and privacy issues that need to be addressed. Some US agencies have already successfully adopted cloud technologies and further pilots are anticipated for 2011. **Risk Management**: Federal Risk and Authorization Management Program (FedRAMP), which has an initial focus on cloud computing. **Monitoring**: Dashboard is a website enabling federal agencies, industry, the general public and other stakeholders to view details of federal information technology investments **Standards development**: National Institute of Standards and Technology (NIST), which promotes the effective and secure use of the technology within government and industry by providing technical guidance and promoting standards.	**Apps.gov:** SaaS. Aims to find a balance between 'late adoption' and 'cutting edge'. Launched September 2009. RFQ for the "Infrastructure as a Service" stage has been released and will be awarded in December. Pre-procurement activities for "Platform as a Service" have begun. **Defense Information Systems Agency (DISA):** Private Cloud (IaaS). Examples: Forge.mil, GCDS and RACE. **Magellan (managed by the US Department of Energy [DOE]):** Private Cloud (IaaS). This has been established to determine the viability of cloud computing in terms of cost-effectiveness and energy-efficiency for scientists to accelerate discoveries in a variety of disciplines. **National Business Center (NBC) Cloud Computing** (managed by the Department of the Interior: Private Cloud (IaaS/PaaS/SaaS). Offering six cloud computing products for its clients: NBCGrid (IaaS), NBCFiles (cloud storage), NBCStage (PaaS), NBC Hybrid Cloud (allows clients to combine NBCGrid, NBCFiles with existing infrastructure), NBCApps (application marketplace), & NBCAuth (SaaS directory service, authentication and SSO product). **NASA Nebula and OpenStack:** Public Cloud (IaaS). Nebula is a Cloud Computing pilot by the NASA Ames Research Center. It integrates a set of cloud capabilities to achieve cost and energy efficiencies. The Nebula technology has recently been chosen as the cornerstone of OpenStack. The goal of OpenStack is to allow any organisation to create and offer cloud computing capabilities using open source software running on standard hardware.

Economy	Programs/Policies	Implemented Clouds/Pilot Tests
United Kingdom	**Policy**: The UK's CIO Council has endorsed an IT strategy that shifts to provision of infrastructure as a service. The UK approach to cloud computing comprises three strategic elements: a Government Apps Store, a secure Government Cloud and consolidation of data centres. The UK is primarily using a private government cloud, but one which has different security risk factors for different types of information. UK agencies will be able to get private cloud services from their Government Cloud body. In March 2011, the UK Government moved from the consideration and development of the concept of cloud computing to the next stage of their strategy, which is around building capability. This phase will occur over the next ten years and will begin the transition of digital services to the G-Cloud, including implementation of an Applications Store for Government and Data Centre Consolidation. Individual public sector organisations are expected to transition in a phased manner. A high-level implementation roadmap for 2010-2014 has been developed. From 2011 to 2014, it is expected that there will be increasing data centre consolidation. The G-Cloud Authority will be designed and set up in 2011. The Application Store for Government will be set up in 2011. Some public sector usage of G-Cloud Services and the public cloud will begin in 2011. G-Cloud standards will also be developed in 2011. New public sector organisations would begin to use the G-Cloud in 2012-2014, including other central departments, local and regional governments and the wider public sector.	**G-Cloud:** Private Cloud (IaaS/SaaS). The UK is of the opinion that a public cloud would be most useful for applications such as public websites and other public domains.
European Union	**Policy**: Seventh Framework Programme (FP7). The EU has recently released a report titled "*The Future of Cloud Computing: Opportunities for European Cloud Computing Beyond 2010*". Recommendations: EC to stimulate research and technological development in cloud computing and set up right regulatory framework to facilitate uptake of cloud computing.	

Economy	Programs/Policies	Implemented Clouds/Pilot Tests
Canada	**Policy**: Canada Cloud Computing. Canada's business case for cloud computing is based on optimisation, efficiency, and the reduced use of space, power, and other resources. Canada's Cloud Architecture is tiered with security concerns. A major concern is whether a particular application has different security levels, and if so whether they can all still reside in the same cloud.	
Japan	**Policy**: Japan's Ministry of Internal Affairs and Communications (MIC) released a report outlining the Digital Japan Creation Project (ICT Hatoyama Plan) which seeks to create new Information and Communications Technology (ICT) markets to help boost Japan's economy.	**The Digital Japan Creation Project (ICT Hatoyama Plan):** Community Cloud (IaaS). Outline to create a nation-wide Cloud Computing infrastructure tentatively called the Kasumigaseki Cloud.
Singapore		In May 2010, as part of its efforts to promote the adoption of Cloud Computing, the Infocomm Development Authority of Singapore (IDA) launched the first Open Call for Cloud Computing Proposals. After evaluation, some of the proposals awarded with cloud resources included: • video hosting and streaming platforms • social media monitoring and analysis solution • document sharing platform • marketplace for cloud services • asset traceability and management Software-as-a-Service, with Radio Frequency Identification (RFI) technology • commodity trading and investment risk assessment solutions • Smart traffic application • mobile phone data screening solution

Attachment 3: Prominent Global / Public Cloud Vendors

(The following list is provided as an example only. It is not an exhaustive list of all vendors providing public cloud based services)

Vendor	Model	Description
Amazon Web Services	IaaS	Amazon offers several different in-the-cloud services. The best known is Amazon Elastic Compute Cloud (EC2) which is a web service that offers resizable compute capacity in the cloud. Key features include: elasticity, control, and flexibility. Other Amazon services include Amazon Simple Storage Service (S3), Simple DB, Cloudfront, Simple Queue Service (SQS), and Elastic MapReduce.
Microsoft Azure Services Platform	IaaS / PaaS	Microsoft Azure Services Platform is a Windows-like cloud computing architecture that offers remote computing power, storage and management services. It has four major parts: • **Windows Azure:** Windows-based environment for running applications and storing data on servers in Microsoft data centers • **Microsoft .Net Services:** Distributed infrastructure services • **Microsoft SQL Services:** Data services in the cloud based on SQL Server • **Live Services:** Access data from Microsoft's Live applications and others and allow synchronising this data through Live Mesh.
Savvis	IaaS	Savvis offers two features: a web portal that allows customers to provision their own virtual computing and storage capabilities on either private or shared resources. Savvis offers scalability, flexibility and virtualised utility hosting on demand.
Google Apps Engine	SaaS	Google offers some of the best known cloud computing services available, including Gmail, Google Docs, Google Calendar, and Picasa. They also offer some lesser known cloud services targeted primarily at enterprises, such as Google Sites, Google Gadgets, Google Video, and most notable, the Google Apps Engine. Google Apps Engine is a free setup that allows the users to write and run their web applications on Google infrastructure. While it has been criticised for limited programming language support, the Apps Engine debuted Java and Ajax support in April 2010. A key advantage is scalability of the applications. GoogleApp Engine for business provides centralised administration, reliability, support and enterprise features.
VMware vCloud	IaaS	VMware offers private as well as public cloud computing. The Private cloud computing has been designed to ensure security and compliance by deploying a private cloud infrastructure inside a business's firewall. The public cloud offers customers the freedom of open standards and interoperability of applications. It includes a common management and infrastructure platform.
Rackspace	IaaS	Similar to Google apps: i.e. provisioning of infrastructure for development of web applications.
Verizon	Security	Verizon has teamed up with Novell to provide cloud-based identity and access management services to help companies in outsourcing their applications to the cloud. They claim that the move will expedite cloud computing without compromising security.
GoGrid	IaaS	GoGrid offers "**point-and-click infrastructure**". It provides a multi-tier, cloud computing platform that allows users to manage the cloud hosting infrastructure completely on demand through an intuitive, web interface.
AppNexus	IaaS	With AppNexus, a user can launch several operating systems, run a variety of applications, load balance these applications and store secure data.

Salesforce	PaaS/SaaS	Salesforce.com are known primarily for • The Sales Cloud and the Service Cloud, applications for sales and customer service (also known as customer relationship management or CRM) • Force.com, a cloud platform for building and running business applications • Chatter, an enterprise collaboration application
Telstra	SaaS/IaaS	Telstra have partnered with a number of providers to offer on-demand ICT services including software, platform, infrastructure and network.
OpenNebula	IaaS	OpenNebula is a widely used open-source tool for the efficient, dynamic and scalable management of VMs within datacenters (private clouds) involving a large amount of virtual and physical servers. It supports Xen, KVM and on-demand access to Amazon EC2.
Joyent	SaaS	The Joyent platform, which "enables teams to effectively communicate and collaborate with email, calendaring, contacts, file sharing, and other shared applications," already serves billions of Web pages every month and helped LinkedIn scale to 1 billion page views per month. Self-described as an "On-Demand Computing" provider, Joyent has developed, built and scaled some of the earliest Ruby on Rails applications – and as a result, developed a world-class infrastructure, a methodology around how to deploy and scale (both up and down) Rails applications.

Attachment 4: Definitions of Cloud Computing

1. National Institute for Standards and Technology (NIST)

An agency of the US Department of Commerce

Cloud computing is a model for enabling 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 promotes availability and is composed of five essential **characteristics,** three **service models**, and four **deployment models**.

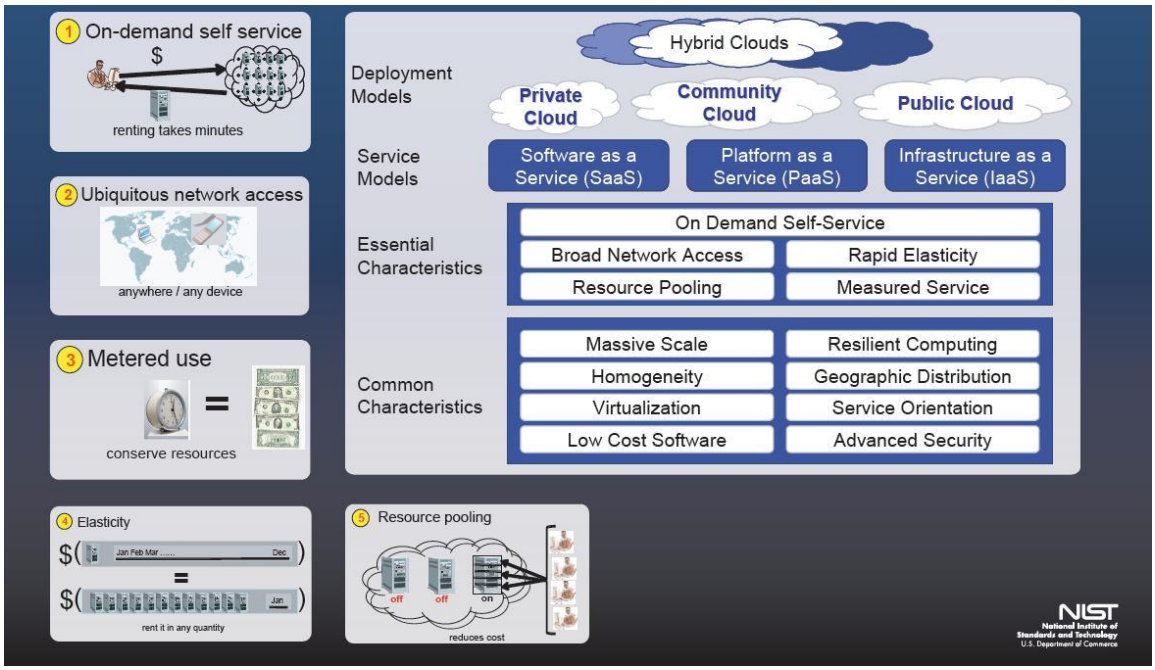

Figure 2: Visual Model of NIST Working Definition of Cloud Computing

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's 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, laptops, and PDAs).

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, network bandwidth, and virtual machines.
Rapid elasticity	Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.
Measured Service	Cloud systems automatically control and optimise resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported providing transparency for both the provider and consumer of the utilised service.

Service Models

Cloud Software as a Service (SaaS)	The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). 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.
Cloud 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 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 application hosting environment configurations.

Cloud 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, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

Deployment Models

Private cloud	The cloud infrastructure is operated solely for an organisation. It may be managed by the organisation or a third party and may exist on premise or off premise.
Community cloud	The cloud infrastructure is shared by several organisations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organisations or a third party and may exist on premise or off premise.
Public cloud	The cloud infrastructure is made available to the general public or a large industry group and is owned by an organisation selling cloud services.
Hybrid cloud	The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardised or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).

Note: Cloud software takes full advantage of the cloud paradigm by being service oriented with a focus on statelessness, low coupling, modularity, and semantic interoperability.

2. Gartner

Gartner defines cloud computing as "a style of computing where scalable and elastic IT-enabled capabilities are provided "as a service" to external customers using Internet technologies."[12] Five attributes support outcomes:

Attribute	**Description**
Service-based	Consumer concerns are abstracted from provider concerns through service interfaces

[12] Gartner: *Gartner Highlights Five Attributes of Cloud Computing*, 2009.

Scalable and Elastic	Services scale on-demand to add or remove resources as needed
Shared	Services share a generalised pool of resources to build economies of scale
Metered by Use	Services are tracked with usage metrics to enable multiple payment models
Internet Technologies	Services are delivered through use of Internet identifiers, formats and protocols

Attachment 5: Terminology

These terms have been sourced from:

- Meghan-Kiffer Press

  http://www.mkpress.com/CloudReading/

  - National Institute of Standards and Technology (NIST)
  - Commonly used Cloud Computing terms
  - Dot.Cloud
  - TechTarget.com
- TechRepublic: A ZDNET tech community

  http://blogs.techrepublic.com.com/datacenter/?p=2308

Term	Definition
Adequate Security	Adequate security requires meeting the mandatory requirements outlined in the Australian Government Protective Security Policy Framework (PSPF).
Advanced Virtualisation	Advanced virtualisation is when the virtual ICT infrastructure includes servers, storage and networks, and has automated management of the virtual environment. For example, authorised users, such as developers, can create and take down virtual environments through a self-service arrangement.
Agility	In business, agility means the capability of rapidly and cost efficiently adapting to changes. See agile enterprise.
Agile enterprise	A fast moving, flexible and robust firm capable of rapid and cost efficient response to unexpected challenges, events, and opportunities. Built on policies and *business processes* that facilitate speed and change, it aims to achieve continuous competitive advantage in serving its customers. Agile enterprises use diffused authority and flat organisational structure to speed up information flows among different departments, and develop close, trust-based relationships with their customers and suppliers: the agile enterprise is the process-managed enterprise with a self-organising workforce that requires employees to assume multiple roles, improvise, spontaneously collaborate, and rapidly redeploy from one work team to another and another, while simultaneously learning from and teaching their peers.
Amazon EC2	Amazon's Elastic Compute Cloud Web service, which provides resizable computing capacity in the cloud so developers can enjoy great scalability for building applications.
Amazon S3	Amazon Simple Storage Services — Amazon's cloud storage service.
Application as a Service (AaaS)	see *SaaS.*
Cloud	A metaphor for a global network, first used in reference to the telephone network and now commonly used to represent the Internet.
Cloud broker	An entity that creates and maintains relationships with multiple cloud service providers. It acts as a liaison between cloud services customers and cloud service providers, selecting the best provider for each customer and monitoring the services. A cloud broker has no cloud resources of its own.

Cloud bursting	Cloud bursting is a technique used by hybrid clouds to provide additional resources to private clouds on an as-needed basis. If the private cloud has the processing power to handle its workloads, the hybrid cloud is not used. When workloads exceed the private cloud's capacity, the hybrid cloud automatically allocates additional resources to the private cloud.
Cloud computing	Refers to style of computing in which various resources—servers, applications, data, and other often virtualised resources—are integrated and provided as a service over the Internet. Cloud computing isn't a new technology nor a new architecture... it's a new delivery model.
Cloud Computing Services	Cloud providers fall into three categories: software-as-a-service providers that offer web-based applications; infrastructure-as-a-service vendors that offer Web-based access to storage and computing power; and platform-as-a-service vendors that give developers the tools to build and host Web applications.
Cloud operating system	A computer operating system that is specially designed to run in a provider's datacenter and be delivered to the user over the Internet or another network. Windows Azure is an example of a cloud operating system or "cloud layer" that runs on Windows Server 2008. The term is also sometimes used to refer to cloud-based client operating systems such as Google's Chrome OS.
Cloud Oriented Architecture	IT architecture that lends itself well to incorporating cloud computing components
Cloud portability	The ability to move applications and data from one cloud provider to another. See also *Vendor lock-in.*
Cloud provider	A company that provides cloud-based platform, infrastructure, application, or storage services to other organisations and/or individuals, usually for a fee.
Cloud Services	A delivery model for information services for businesses and individuals that build on a cloud platform to create dynamic processes and applications.
Cloud Service Architecture (CSA)	Architecture in which applications and application components act as services on the Internet.
Cloud storage	A service that allows customers to save data by transferring it over the Internet or another network to an offsite storage system maintained by a third party
Cloudsourcing	Replacing traditional IT services with cloud services, for example, outsourcing storage or taking advantage of some other type of cloud service.
Cloudstorming	Connecting multiple cloud computing environments. Also called cloud networking.
Cloudware	Software that enables creating, deploying, running, or managing applications in the cloud.
Cloudwashing	slapping the word "cloud" on products and services you already have.
Cluster	A group of linked computers that work together as if they were a single computer, for high availability and/or load balancing.
Community Cloud	The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (eg, mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.
Consumption-based pricing model	A pricing model whereby the service provider charges its customers based on the amount of the service the customer consumes, rather than a time-based fee. For example, a cloud storage provider might charge per gigabyte of information stored. See also *Subscription-based pricing model.*
Customer self-service	A feature that allows customers to provision, manage, and terminate services themselves, without involving the service provider, via a Web interface or programmatic calls to service APIs.

Elastic computing	The ability to dynamically provision and de-provision processing, memory, and storage resources to meet demands of peak usage without worrying about capacity planning and engineering for peak usage.
External cloud	Public or private cloud services that are provided by a third party outside the organisation.
Federation	Act of combining data or identities across multiple systems. Federation can be done by a cloud provider or by a cloud broker.
Google App Engine	A service that enables developers to create and run Web applications on Google's infrastructure and share their applications via a pay-as-you-go, consumption-based plan with no setup costs or recurring fees.
Google Apps	Google's SaaS offering that includes an office productivity suite, email, and document sharing, as well as Gmail, Google Talk for instant messaging, Google Calendar and Google Docs, spreadsheets, and presentations.
Governance	Governance refers to the controls and processes that make sure policies are enforced.
Grid Computing	(or the use of a computational grid) is applying the resources of many computers in a network to a single problem at the same time - usually to a scientific or technical problem that requires a great number of computer processing cycles or access to large amounts of data.
Hardware as a Service (HaaS)	see *IaaS.*
Hosted application	An Internet-based or Web-based application software program that runs on a remote server and can be accessed via an Internet-connected PC or thin client. See also *SaaS.*
Hybrid cloud	**The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (for example, cloud bursting for load-balancing between clouds).**
Infrastructure as a Service (IaaS)	Cloud infrastructure services, whereby a virtualised environment is delivered as a service over the Internet by the provider. The infrastructure can include servers, network equipment, and software.
Integration	Integration is the process of combining components or systems into an overall system. Integration among cloud-based components and systems can be complicated by issues such as multi-tenancy, federation and government regulations.
Intercloud	The Intercloud is similarly a "cloud of clouds." Both public and private versions (intraclouds) not only co-exist, but interrelate. Intraclouds (private clouds) will exist for the same reasons that intranets do: for security and predictability.
Internal cloud	A type of private cloud whose services are provided by an IT department to those in its own organisation.
Interoperability	Interoperability is concerned with the ability of systems to communicate. It requires that the communicated information is understood by the receiving system. Interoperability is not concerned with whether the communicating systems do anything sensible as a whole. (The definitions of interoperability, integration and portability are based on the work at http://www.testingstandards.co.uk/interop_et_al.htm.) (NIST)
Location-Independent Resource Pooling	Resource pooling allows a cloud provider to serve its consumers via a multi-tenant model. Physical and virtual resources are assigned and reassigned (NIST)
Mashup	A Web-based application that combines data and/or functionality from multiple sources.

Measured Service	In a measured service, aspects of the cloud service are controlled and monitored by the cloud provider. This is crucial for billing, access control, resource optimisation, capacity planning and other tasks.
Microsoft Azure	Microsoft cloud services that provide the platform as a service (see PaaS), allowing developers to create cloud applications and services.
Middleware	Software that sits between applications and operating systems, consisting of a set of services that enable interoperability in support of distributed architectures by passing data between applications. So, for example, the data in one database can be accessed through another database.
Multi-tenancy	Property of multiple systems, applications or data from different enterprises hosted on the same physical hardware. Multi-tenancy is common to most cloud-based systems.
On-demand service	A model by which a customer can purchase cloud services as needed; for instance, if customers need to utilise additional servers for the duration of a project, they can do so and then drop back to the previous level after the project is completed.
Platform as a Service (PaaS)	Cloud platform services, whereby the computing platform (operating system and associated services) is delivered as a service over the Internet by the provider. For example, an application development environment that can be subscribed to and used immediately.
Pay as you go	A cost model for cloud services that encompasses both subscription-based and consumption-based models, in contrast to traditional IT cost model that requires up-front capital expenditures for hardware and software.
Policy	A policy is a general term for an operating procedure. For example, a security policy might specify that all requests to a particular cloud service must be encrypted.
Private cloud	A private cloud attempts to mimic the delivery models of public cloud vendors but does so entirely within the firewall for the benefit of an enterprise's users. A private cloud would be highly virtualised, stringing together mass quantities of IT infrastructure into one or a few easily managed logical resource pools.
Public cloud	Services offered over the public Internet and available to anyone who wants to purchase the service.
Rapid Elasticity	Elasticity is defined as the ability to scale resources both up and down as needed. To the consumer, the cloud appears to be infinite, and the consumer can purchase as much or as little computing power as they need.
Reuse	Reuse of pre-existing software has been the Holy Grail of software engineering for years (e.g., subroutines, code libraries, patterns, object inheritance, components and frameworks). In the world of service-oriented architecture, reuse goals take a major step forward through designing services that are abstract, stateless, autonomous loosely coupled. And the key is that the abstractions of services represent reusable business process segments, not just reusable software. Those process segments can be reused as companies design innovative business processes as "situational" business processes "situational business processes" across for multiple business channels. That is, they can be adapted to completely new business situations. So it is that software flexibility and reuse enables business process flexibility and reuse "reuse." That's the stuff of business agility in hyper-competitive markets.
Software as a Service (SaaS)	Cloud application services, whereby applications are delivered over the Internet by the provider, so that the applications don't have to be purchased, installed, and run on the customer's computers. SaaS providers were previously referred to as ASP (application service providers). SaaS removes the need for organisations to handle the installation, set-up and often daily upkeep and maintenance.
Salesforce.com	An online SaaS company that is best known for delivering customer relationship management (CRM) software to companies over the Internet.

Service migration	The act of moving from one cloud service or vendor to another.
Service provider	The company or organisation that provides a public or private cloud service.
Service Level Agreement (SLA)	A contractual agreement between a service provider and a consumer where the consumer's requirements are specified and a service provider defines the level of service, responsibilities, priorities, private and security and guarantees regarding availability, performance, and other aspects of the service.
Subscription-based pricing model	A pricing model that lets customers pay a fee to use the service for a particular time period, often used for SaaS services. See also *Consumption-based pricing model.*
Ubiquitous Network Access	Ubiquitous network access means that the cloud provider's capabilities are available over the network and can be accessed through standard mechanisms by both thick and thin clients. This does not necessarily mean Internet access. By definition, a private cloud is accessible only behind a firewall. Regardless of the type of network, access to the cloud is typically not limited to a particular type of client). (NIST)
Utility computing	Online computing or storage sold as a metered commercial service in a way similar to a public utility.
Web 2.0	The term "Web 2.0" describes the changing trends in the *usage* of World Wide Web technology and Web design that aim to enhance creativity, communications, secure information sharing, collaboration and functionality of the Web.
Web 3.0	A supposed third generation of Internet-based services. Web 1.0 was read-only, Web 2.0 is read-write, and Web 3.0 "Web 3.0" will be read-write-execute. Web 3.0 (the intelligent Web "the intelligent Web") will involve yet another step-change in how we use the Internet and tame the "infoglut". For example, "ontologies" will provide the semantics behind the "Semantic Web" opening up new possibilities for "intelligent agents" to do our bidding, and open "information extraction (IE)" will power new forms of search in a way that avoids the tedious and error-prone tasks of sifting through documents returned by a search engine.
Vendor lock-in	Dependency on the particular cloud vendor and difficulty moving from one cloud vendor to another due to lack of standardised protocols, APIs, data structures (schema), and service models.
Vertical cloud	A cloud computing environment that is optimised for use in a particular industry, such as health care or financial services.
Virtual private data centre	Resources grouped according to specific business objectives.
Virtual Machine (VM)	A file (typically called an image) that, when executed, looks to the user like an actual machine. Infrastructure as a Service is often provided as a VM image that can be started or stopped as needed. Changes made to the VM while it is running can be stored to disk to make them persistent. (NIST)
Virtualisation	The simulation of the software and/or hardware upon which other software runs
Virtual Private Cloud (VPC)	A private cloud that exists within a shared or public cloud, e.g., the Amazon VPC that allows Amazon EC2 to connect to legacy infrastructure on an IPsec VPN.
Windows Live Services	Microsoft's cloud-based consumer applications, which include Windows Live Mail, Windows Live Photo Gallery, Windows Live Calendar, Windows Live Events, Windows Live Skydrive, Windows Live Spaces, Windows Live Messenger, Windows Live Writer, and Windows Live for Mobile.