Cloud Computing in a Government Context

Introduction

There has been a lot of hype around cloud computing to the point where, according to Gartner,¹ it has become 'deafening'. However, it is important to see through the hype when considering whether or not to jump aboard a cloud. As the word 'cloud' suggests, cloud computing delivers IT services via the internet from a service provider that is geographically remote from the consumer. It has the potential to offer a faster and more efficient service at significantly less cost by providing shared resources and computing services to multiple users and devices with minimal management and service provider interaction. Such efficiencies make cloud computing extremely attractive and 'clouds' are increasingly being used by government and industry in Australia.² However, cloud computing also poses risks and any decision to utilise the service of a cloud provider needs be based on a thorough analysis of the benefits and risks of the various 'cloud' options available.

Characteristics of Cloud Computing

Cloud computing may be distinguished from more traditional computing services in several ways. Cloud services can be delivered on demand as a self-service to be purchased as needed. The broadband capability of cloud services enables consumers to access computing resources from a range of computing devices such as desktops, laptops and mobile phones. Cloud computing services can be shared by multiple customers leading to greater efficiencies in cost and delivery. The provider has the ability to scale resources up and down to meet consumer demand and the consumer can purchase as much or as little as needed. Finally, cloud systems automatically control and optimise the resource use, metering such things as storage, processing, bandwidth and active user accounts. This means that resource usage can be monitored, controlled and reported to provide transparency to the service provider and consumer.³

The services provided via a cloud will vary depending upon the type of deployment model, the degree of shared access or public availability of the service, and the level of service purchased. Such factors influence the degree of benefit and risk involved.

² For instance, the West Australian Department of Treasury and Finance and West Australian Health announced private cloud computing developments in August 2010; the Commonwealth Department of Human Services and Australian Maritime Safety Authority have public clouds under development; Westpac, the Commonwealth Bank and Visy are developing private clouds.
Cloud Deployment Models

Cloud services may be delivered using one or more of four cloud deployment models or modes of delivery, each of which carries inherent benefits and risks. These are:

1. **Public Cloud** which involves an organisation using a service provider's cloud infrastructure that is shared via the internet with many other organisations and individuals. This generates competitive economies of scale but carries inherent security risks associated with its wide availability.

2. **Private Cloud** attempts to mimic the delivery model of public cloud service provider but it does so entirely within the firewall and for the benefit of the consumer, which is usually a large organisation. A private cloud connects together large amounts of IT infrastructure into one or two local resource pools. This provides many of the advantages of a public cloud but with greater control and security. For instance, a private cloud may enable the organisation to negotiate suitable contracts with the service provider instead of being forced to accept the generic contracts offered by some public cloud vendors.

3. **Community Cloud** is a private cloud that is shared by several organisations or government agencies that have similar needs in terms of data sensitivity and security. This model provides most of the benefits of a private cloud with additional economies of scale that make it more cost effective. For example, the UK Labour Government proposed the development of a community cloud or G-Cloud (discussed below).

4. **Hybrid Cloud** as the name suggests involves a combination of cloud models. For example, the organisation could use IT resources from a public cloud to manage non-sensitive data which could be set up to interact with sensitive data stored and processed on a private cloud.

In addition to the choice of deployment model the consumer makes a choice about what level of service they require. This will depend upon the needs of the organisation and may range from basic infrastructure to a full-suit of services including software specifically designed for the organisation. As the service provided becomes more comprehensive greater efficiencies may be achieved but in addition, control shifts away from organisation to the service provider. This, as we shall see, has significant implications for the risks an organisation is prepared to tolerate and will influence the choice of service provider, mode of delivery and computing services purchased.

Cloud Computing Service Models

Generally there are three cloud computing service models available:

1. **Infrastructure as a Service** (IaaS) involves the provision of a virtualised environment of servers, computer processing and memory, data storage, network connectivity and software. The environment may be shared by multiple users. IaaS enables the consumer to run operating systems and software applications of their choice. The service provider normally maintains the physical hardware and the consumer controls and maintains the operating systems and software.

---

4 Ibid.
2. **Platform as a Service** (PaaS) involves the provision of operating systems and associated web servers. The consumer uses the service provider’s cloud infrastructure to deploy web applications and other software developed by the consumer with the support of the service provider. The provider controls and maintains the physical computer hardware, operating systems, and server applications. The consumer controls the software applications they develop.

3. **Software as a Service** (SaaS) involves the provision of software applications such as email and an environment in which users can collaboratively develop share files such as documents and spreadsheets. Typically the service provider controls and maintains the physical hardware, operating systems, and software applications. The consumer typically has limited control over application and configuration settings specific to the applications they are using.\(^5\)

As is evident from the description of cloud deployment and service models, there is a variety of communication and information technology platforms and services on offer. There is no ‘one size fits all’. Services can be tailored to the needs of the consumer according to region, size of the organisation or business, sector characteristics, workload, demand and security concerns. Before considering cloud computing as an option, the organisation must assess the benefits and risks of the various cloud computing options to determine which service is appropriate for their needs.

**Risks associated with cloud computing for government organisations**

Government organisations are likely to have specific needs for data security, privacy and access that constrain the way they use of cloud computing or limit its provision to particular providers, service and deployment models. If government organisations choose to use a private cloud they will have greater control than if they choose to use a community or public cloud. The degree of control required will depend upon the sensitivity of the data being managed. Data already in the public domain that is non-sensitive will require less protection than sensitive data subject to privacy concerns. The management of private data will be of particular concern for government agencies and organisations. The risks are particularly acute when the service provider operates from a foreign country where the security of data may be subject to foreign laws. It is important, therefore, to evaluate the choice of deployment model according to the sensitivity of the data being stored and managed and the legislative framework that governs that information.

**Privacy of Personal Information**

In Victoria, the use of cloud computing by government agencies, statutory bodies and local councils to manage personal information will need to comply with the Information Privacy Act 2000 (Vic) and Information Privacy Principles (IPPs).\(^6\) IPP4 and IPP9 are particularly relevant to the cloud computing context:

---

\(^5\) Ibid.

**Principle 4 Data Security**

4.1 An organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.

4.2 An organisation must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose.

This Principle places an obligation on the government organisation to ensure that the provider of cloud computing services has adequate security measures in place to protect data from misuse, loss, unauthorised access, modification or disclosure and that when that data is no longer needed it is destroyed or de-identified in accordance with 4.2.

**Principle 9 Transborder Data Flows**

9.1 An organisation may transfer personal information about an individual to someone (other than the organisation or the individual) who is outside Victoria only if –

(a) the organisation reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of the information that are substantially similar to the Information Privacy Principles; or

(b) the individual consents to the transfer; or

(c) the transfer is necessary for the performance of a contract between the individual and the organisation, or for the implementation of pre-contractual measures taken in response to the individual’s request; or

(d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the organisation and a third party; or

(e) all of the following apply –

   (i) the transfer is for the benefit of the individual;

   (ii) it is impracticable to obtain the consent of the individual to that transfer;

   (iii) if it were practicable to obtain that consent, the individual would be likely to give it; or

(f) the organisation has taken reasonable steps to ensure that the information which it has transferred will not be held, used or disclosed by the recipient of the information inconsistently with the Information Privacy Principles.

Traditionally, information may only be transferred outside Victoria if the recipient is capable of protecting its privacy to standards similar to those in the IPPs. Under cloud computing agreements ensuring compliance under clauses (a) and (f) of IPP 9 may be particularly problematic. It may be possible to include such clauses in the contract with the service provider, in accordance with section 17(2) of the Information Privacy Act. Specially tailored contracts may be possible for private or community cloud computing services. Public contracts that are generic will be more difficult if not impossible to amend. Even when privacy principles are written into a contract there may be difficulties associated with enforcement and remedial action.
If the data is transferred interstate or overseas it is likely that the privacy law, if any, of the storage jurisdiction will apply and if so, the consumer will need to evaluate the extent to which those laws offer analogous protections to the Victorian Act and its principles. Western Australia and South Australia do not currently have privacy laws in place and some significant international jurisdictions, the United States and Singapore for instance, do not have privacy laws analogous to those in Victoria.\(^7\)

**Record keeping, access and auditing**

The Public Records Act 1973 (Vic) requires government records to be managed securely so as to ensure their integrity and reliability should they be required in legal proceedings under the Evidence Act 2008 (Vic) or for another purpose.\(^8\) Reliable and secure storage of public documents is also essential for government compliance with the Freedom of Information Act 1982 (Vic). In addition, records need to be readily available for the purposes of financial and performance audits that government organisations may be subject to under the Audit Act 1994 (Vic).

As the discussion thus far suggests, when records are stored on cloud servers the integrity of records and their availability may be at higher risk of being compromised. The level of risk will depend upon the type of cloud service and deployment model, the content and sensitivity of the records and their importance to the government organisation. In some cases, an organisation may decide that some records are simply too sensitive or important to trust to a cloud computing service.\(^9\)

**Additional Risks**

While data security and privacy issues will be a major concern for government, there are in addition risks associated with the fact that the service provider operates as a separate business entity. In particular, there is the risk that the business might fail and contracts entered into with service providers will need to include contingency provisions that protect and provide for data retrieval if business continuity is interrupted.

The use of the internet to access IT services also poses the usual access and interruption of access risks. The greater dependency on the services of a cloud provider the greater will be the potential for disruption to an organisation's operations should internet connection fail.

When a privacy or security breach occurs or there is a loss of business continuity that results in a failure to deliver an essential service the damage to the organisation's reputation could be significant.\(^10\)

---


\(^8\) *Public Records Act 1973* (Vic) s 7 provides that the Keeper of Public Records is responsible for the authentication of public records required in legal proceedings. Section 156 of the *Evidence Act 2008* (Vic) makes provision for public documents authenticated by 'an officer entrusted with the custody of a public document' to be admitted as evidence before a court.


\(^10\) Australian Government, Department of Finance and Deregulation, above n 3, 15.
Assessing the risks

Prospective cloud users will need to assess security risks associated with transferring, storing and accessing data stored in a geographically remote virtual location. As discussed above, these concerns will be greater for data stored in a public cloud than those stored in a private cloud. However, the security risks will also need to be traded off against the relative cost efficiencies associated with more cost effective public versus cost intensive private clouds. The choice of cloud service provider and level of service will depend upon at least three intersecting considerations: the record storage and retrieval needs of the organisation, the sensitivity of the records being stored, and the type and reliability of the cloud service and service provider.

The government organisation should use 'due diligence' when making a choice whether or not to use a cloud service and if so, which service provider and level of service to use. When purchasing SaaS for instance, greater control is passed to the service provider and there is therefore potentially greater risk of data security being breached. This may not always be the case, however, in some instances there could be greater security in having data stored off-site. For instance, there are commercial services that offer data storage for highly sensitive data to guard against its loss in the case of disaster or magnetic destruction.

Managing the risks

Security of highly sensitive data is especially vulnerable in a public or community cloud. SaaS poses the greatest risk because it places the most responsibility on the service provider. Paas and IaaS offer progressively greater security simply because the organisation maintains greater control.

Data is at risk while in transit (data at rest) and while it is stored (data in motion). One means of managing the risk is to encrypt the data transferred to and stored by a cloud provider. Encryption is a key component of cloud security but will be ineffective if keys are exposed or encryption endpoints are insecure. Phishing for instance is a risk for data in motion and while encryption offers good protection there remains the risk that someone may trick an end user into providing their credentials for access to clouds.

It is imperative, therefore, that the contract entered into between a government agency or organisation and a cloud provider be drafted, where possible, to include provisions that comply with the Privacy Principles in the Victorian Information Privacy Act, and contain procedures that will need to be followed should there be a breach of security. Audit provisions should also be included that allow the organisation to monitor the security of the data being stored by a cloud provider, even when the service provider is located within Victoria.

Government agencies and organisations may need to be able to discover information under common law or comply with legislative requirements of FOI, Public Records and Privacy legislation. Little precedent exists regarding the liability of cloud providers, which is why contracts for services should, where possible, clearly specify what the cloud provider is responsible for.

---

11 Phishing is a way of attempting to acquire sensitive information by masquerading as a trustworthy entity in an electronic communication.
Key questions to consider:  
- What are the relative cost, efficiency and data security benefits and risks of using a cloud service provider?  
- Where will the data be stored geographically?  
- If data is stored outside Victoria, what is the privacy legislation in that jurisdiction and does it meet the requirements of the Information Privacy Act 2000 (Vic)?  
- Is the cloud provider owned or controlled by a foreign company?  
- Can the organisation’s data be segregated from data stored by other customers of the cloud?  
- Who will have access to the data?  
- What notification processes are in place should security breaches occur?  
- What business continuity and disaster recovery plans are in place?  
- Does the contract provide for the auditing of the service provided?  
- How will data be destroyed or retrieved when it is no longer needed? Does this comply with the Public Records Act 1973 (Vic)?

With cloud computing a government agency or organisation may have limited ability to control or prescribe controls over the cloud environment. Yet they remain ultimately responsible for the data and information that is stored and processed in a cloud.

The Commonwealth Department of Finance and Deregulation has reviewed the risks and benefits of cloud computing for a 'whole of government' approach at the Federal level. They acknowledge the need to cater for issues such as security, privacy, portability and service provider certification. They recommend the establishment of a Cloud Information Community that facilitates the sharing of information and knowledge about the adoption and management of cloud services. Other risk management strategies include the drafting of 'Government Cloud Principles' to assist agencies in their use of cloud services; a government compliance framework for shared arrangements such as community clouds that sets standards for contractual arrangements, change management, transition arrangements; good practice guidelines on privacy and security; and a cloud service provider certification program.  

G-Cloud Case-Study

In 2009, the Labour government in the United Kingdom proposed the introduction of a G-Cloud (Government Cloud), which would consist of a range of cloud services offered to public sector organisations. Whether or not the new UK government will continue with the G-Cloud is uncertain. However, what the G-Cloud proposed was a wholesale shift to shared ICT services. These were to include both 'public cloud' services and common and custom 'private cloud' services purchased by public sector organisations. Cost savings were envisaged and made possible through the 'rationalising, sharing and re-using of software and infrastructure across organisational boundaries'.

---

15 Australian Government Department of Finance and Deregulation, above n 3.  
17 There is uncertainty surrounding its future in the wake of the new government’s spending and IT review, undertaken in February 2011.
G-Cloud services would be selected and purchased from the Government Applications Store (Apps Store) and automatically provided by either 'public cloud providers or from a private cloud platform hosted in one of a much reduced number of List X compliant government data centres'.

The Apps Store was proposed as the 'marketplace in which trusted services could be trialled and then purchased from a variety of sources'. It was to be designed to encourage existing and new suppliers to the Public Sector to 'promote and trial their services as 'free' prototypes in order to gauge market interest. Services available through the Apps Store were to be 'certified to demonstrate their compliance with Public Sector requirements'. Purchasers would 'buy certified services from an on-line catalogue under a cross-public sector framework contract'. Payment for services was to be on a per use or subscription basis. In order to avoid becoming 'locked-in' to a particular infrastructure provider there was to be a choice of at least two providers for each application.

G-cloud was intended as an 'internal brand offering secure, trusted and shared public sector ICT services'. All G-Cloud services were to have common characteristics including pre-certified standards compliance covering areas such as service delivery, technical and information assurance, provided from an efficient and sustainable data centre through the Apps Store.

The G-Cloud was to include dedicated private services for public sector organisations as well as trusted public cloud services across all three delivery modes: Saas, Paas and IaaS.

**Conclusion**

Government organisations and agencies will need to adopt a principled and risk-based approach to cloud computing that is both tactical and strategic. A risk-managed approach that takes into consideration value for money, benefits, security requirements and service level requirements has the potential to deliver tangible benefits. As the technology improves, government agencies and organisations will want to maintain sufficient control and flexibility in contracts with cloud services providers to enable them to take advantage of new innovations, particularly those that offer greater security and reliability.