TAHO
Tasmanian Archive + Heritage Office

Information Management Advice 44 Cloud Computing Information Security Considerations

Introduction

Cloud computing offers potential benefits including cost savings, agility and improved business outcomes for Tasmanian government agencies, however there are a variety of information security risks that need to be carefully considered.

The Tasmanian Government requires that each agency implement Information Security Policy, Plans and Procedures and assess and manage the exposure risk of confidential information under its control.

This Advice identifies specific resources and illustrates an example approach that can assist agencies to perform the required risk assessment, and make an informed decision as to whether cloud computing is suitable to meet their business requirements with an acceptable level of risk. This Advice also provides a brief overview of how the Personal Information Protection Act 2004 applies to cloud computing technologies. A Checklist of the questions to consider, as outlined in this advice, is attached.

See Guideline 17 Managing Recordkeeping Risk Associated with Cloud Computing for more information on cloud computing, including mandatory compliance statements.

Context

The Tasmanian Government Information Security Policy Manual applies to the management of all aspects of the security of government information including ICT systems. The Tasmanian Government Information Security Classification standard applies to the management of all information. This advice supports these standards in relation to security considerations for Cloud Computing.

Cloud Computing and Personal Information Protection Act

"Cloud computing" is the term used for information technology infrastructure that hosts data or applications in the "cloud" – that is, it refers to offsite, geographically remote software or data storage accessed via the Internet. Data or applications are usually accessed on demand through a web browser instead of being stored on individual computers. Cloud computing technology is being used increasingly by Tasmanian government agencies to reduce capital and operational costs, as the cost of storing data or accessing applications via offsite methods greatly reduces the need for technology infrastructure, IT support and staffing. Cloud computing also allows departments to pool resources efficiently and quickly.

The *Personal Information Protection Act 2004* will only apply where the data stored includes personal information about an identifiable individual. If the information is de-identified or is not personal information, the Act will not apply.

However, given the increasing sophistication of data mashing, data-matching and the risk of subsequent re-identification, de-identification of government data requires substantial work and resources on the part of an organisation. Accordingly, any cost savings in using cloud computing may be diminished if an organisation attempts to effectively de-identify the personal information it holds in order to use cloud services.

Where the data contains personal information, there are important privacy considerations – particularly in relation to data security – that need to be addressed if an organisation plans to use cloud computing technology for hosting and accessing its data or applications. Despite the potential cost benefits of cloud computing, the cost in addressing the privacy issues might outweigh capital and operational savings to an organisation. Furthermore, implementing cloud technology requires a different "mindset" than traditional IT services – using the cloud may swiftly reveal failures in security and procedural processes that have not been properly thought out. The desire to reduce costs will need to be balanced with other factors, including ensuring privacy protections, when deciding whether or not to use cloud computing technologies.

There are three distinct ways in which a Tasmanian government agencies can conceivably use cloud computing. These differ as to where the cloud server is located or hosted:

- **private cloud:** within the organisation only – the agency hosts the cloud in Tasmania or uses cloud technology within its organisation;
- **community cloud:** within the Tasmanian government – a centrally hosted cloud in Tasmania that is used by various government Departments and organisations;
- **public cloud:** either within Australia but outside of Tasmania (with the data hosted in Australia), or offshore (hosted by a cloud computing service provider whose data servers are located overseas).

Private Clouds and Tasmania Community Cloud Services

Data Security

Where a Tasmanian government agency wishes to use cloud technology to host its data, and that cloud service provider is located within Tasmania, the organisation will need to ensure it complies with Personal Information Protection Principle (PIPP) 4 which deals with data security.

Principal 4 states that an organisation must take reasonable steps to protect personal information it holds from misuse, loss, unauthorised access, modification and disclosure. This places an obligation on the organisation to ensure that the cloud service provider has adequate security measures to protect the data. This could range from encrypting all data, to restricting access to servers. Traditionally, an organisation could secure the data it holds by physical means (restricting access to the server room) or technological means (password protection, encryption, restricted access). In contrast, when data is housed in the cloud, the organisation relinquishes the physical aspect of control. Given the offsite nature of the data storage, security measures in the cloud require a different security focus than traditional IT services. What reasonable steps an organisation can therefore take to ensure data security will differ depending on the circumstances and the data stored.

Where a single cloud is being shared by multiple government departments (a "community cloud"), it is important that there is adequate separation and segregation between the various datasets to prevent any inadvertent disclosure. Data segregation must occur where a government department is sharing a cloud server with, for example, private sector organisations. This is also relevant where a government department has multiple business units which may require data segregation – for example, some larger departments have distinct, separate business units which hold data that other units should not need to access. Processes or arrangements for data segregation and security will need to be agreed with the cloud service provider. This may

include a data classification system whereby only some information – such as non-personal or de-identified information – is stored in the cloud.

Under Principle 4, an organisation must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose. As this will also apply to any data hosted in the cloud, the agency will need to have methods to ensure that the cloud service provider is compliant with Principle 4. Note that obligations relating to the preservation of state records, including compliance with the *Archives Act 1983*, will still apply.

It is important that the contract and the cloud services be reviewed at least annually to ensure that data security measures are kept up-to-date.

Contract with the Cloud Service Provider

Agencies must only use a cloud service provider that agrees that privacy protection is essential. The contract between the service provider and the state government agency must:

- ensure that the service provider complies with the Personal Information Protection Principles in the *Personal Information Protection Act 2004*;
- set out the procedures that need to be followed in the case of any potential security breach, including notification to the state government agency of any breaches; and
- contain the right for the agency to audit the service provider to ensure it is complying with the *Personal Information Protection Act 2004*.

Note that even if the data centre is located inside Tasmania, it may be that the private sector organisation is owned or operated by a foreign company. This could mean that a foreign government could access the data as the subsidiary's server may be within the possession or control of the parent foreign company. Agencies must conduct adequate due diligence on the prospective cloud service provider, their business practices and their security regimes.

Questions to Consider

- When the additional steps required to ensure privacy protection are considered, is there an actual cost savings benefit to the agency?
- Does the agency know exactly, geographically, where the data will be stored, keeping in mind the possibility it may be across different countries or continents?
- Is the agency data segregated from other customers or government departments?
- Who will have access to the data? How will system administrators or staff of the cloud service provider be prevented from unauthorised access to the data?
- Does the service provider have methods of notification of, and responding to, data security breaches?
- Does the contract permit the agency to audit the provider to ensure compliance with the Personal Information Protection Act?
- Is the service provider owned or controlled by a foreign company? What control does the foreign company have over the service provider?

How will personal information be destroyed or retrieved when it is no longer needed, bearing in mind any requirements under the *Archives Act*?

Public Clouds Outside of Tasmania

Data Security

Where the provider is located outside of Tasmania, taking reasonable steps to protect personal information from misuse, loss, unauthorised access, modification or disclosure under PIPP 4 may be difficult or even impossible. By using a cloud service, the agency is relinquishing some – if not all – control over their data. This includes being able to control security measures.

As noted above, it is likely that a cloud service provider will be an agent for the agency. This means that if there is a data security breach, the agency will remain responsible for any breach that occurs. The risks for the agency are compounded when information is stored offshore, as the organisation cannot control who can access the data or any security or encryption methods. There is also a real problem of enforceability or remedying a breach if it occurs in relation to data stored in an offshore server.

Given that many cloud computing service providers are in jurisdictions which do not have similar privacy or data protection laws, if a security breach occurs, an individual in Tasmania will be powerless to take action against the cloud service provider and will only be able to complain to the government agency, which may similarly be unable to assist due to its lack of control over the data.

Where the cloud server is located offshore, it may also be possible for foreign governments to access the information, if that government requires it. For example, the *Patriot Act 2001* and associated anti-terrorism legislation in the United States contain provisions allowing the US Government to access data in specified circumstances, but prohibiting the data custodian notifying anyone. Allowing access to foreign governments could be a breach of the unauthorised access restriction in PIPP 4. Depending on the type of information held, foreign governments may also put pressure on the cloud service provider to remove information or stop providing the cloud service in breach of the *Personal Information Protection Act*. This could have other serious implications, including under the *Archives Act*.

Some cloud service providers may host Tasmanian government data across servers located in several different jurisdictions (some of which may have privacy laws and some which may not), making data security compliance impracticable. Data might also not reside in one particular place, resulting in confusion if a breach occurs.

Contracted Service Providers

If the cloud service provider is providing additional services or manipulating the data in some way which goes beyond a mere agency arrangement (that is, the cloud provider is doing something more than storing data or providing access to it), the cloud provider might then be seen as being a contracted service provider rather than an agent. This means that the organisation will have to comply with the PIP Principals. The cloud provider would usually need to agree to be contractually bound by the *Personal Information Protection Act 2004*, or fulfil the requirement that a similar privacy scheme to the *Personal Information Protection Act 2004* operates in that state or country.

If a cloud provider has to comply with the *Personal Information Protection Act 2004*, it will have to understand its obligations both in its own jurisdiction and in Tasmania. Note that there are some significant international jurisdictions that do not have similar privacy laws.

Other Potential Concerns

Other potential problems with offshore cloud service providers might include:

- sale of business to another entity – a change of control may impact on contracts or obligations of the cloud service provider;
- risk of insolvency or bankruptcy to the service provider;
- changes to business units or practices that are made without the knowledge of their IT units;
- machinery of government of changes; and/or
- retrieval or destruction of information once, or if, the contract with the cloud service provider terminates.

The risk with all of the above is that, when data is stored in an offshore cloud, the agency loses control of the data, particularly if something goes "wrong". Accordingly, the focus should be the issue of control if a breach occurs, and what happens when the relationship with the cloud service provider ends. The agency should therefore ensure that transition out provisions are clearly drafted and worded. Finally, even if an agency is only using a cloud service provider as a backup service (i.e. "at rest" data), these principles and the requirement to comply with the *Personal Information Protection Act 2004* will still apply.

Questions to Consider

- When the additional steps required to ensure privacy protection are considered, is there an actual cost savings benefit to the agency?
- Is there data protection or privacy legislation in place in the foreign jurisdiction that at minimum meets the requirements in the *Personal Information Protection Act 2004*? Is the relevant law enforceable?
- Does the service provider have methods of notification or responding to data security breaches?
- Can the service provider guarantee that access will not be given to foreign governments or law enforcement? Is there a legislative requirement in that jurisdiction that prevents the agency from being notified of any potential access?
- What happens at the conclusion of the contract with the cloud service provider? Will information be able to be retrieved or destroyed in compliance with the *Personal Information Protection Act 2004* and the *Archives Act 1983*?

Approach

Agencies must perform a risk assessment against the information that they are proposing to manage in the cloud, and must document this assessment in a risk management plan.

An approach to managing risk is outlined in the Australian/New Zealand Risk Management Standard: *AS/NZS ISO 31000:2009* A copy of this standard is available via the DPAC website.

Refer *State Records Guideline 25 Managing Information Risk*, and *Advice 60 Risk Management* located on our website, for additional information.

Key Elements of the Risk Management Process

The key elements of the risk management process are as follows:

Communication and consultation – communication and consultation with external and internal stakeholders should take place during all stages of the risk management process. This ensures that those accountable for implementing the risk management process and stakeholders understand the basis on which decisions are made, and the reasons why particular actions are required.

Establishing the context – establish the external, internal, and risk management context in which the rest of the risk management process will take place. By establishing the context, the organisation articulates its objectives, defines the external and internal parameters to be taken into account when managing risk, and sets the scope and risk criteria for the remaining process.

Risk assessment – risk assessment is the overall process of risk identification, risk analysis and risk evaluation. *IEC/ISO 31010:2009 Risk Management – Risk Assessment Technique* provides further guidance on risk assessment techniques.

Risk identification – the aim is to generate a comprehensive list of risks based on those events that might create, enhance, prevent, degrade, accelerate or delay the achievement of objectives.

Risk analysis – risk is analysed by determining consequences and their likelihood, and other attributes of the risk. It provides an input to risk evaluation, decisions on whether risks need to be treated, and on the most appropriate risk treatment strategies and methods.

Risk evaluation – involves comparing the level of risk with risk criteria and making decisions about which risks need treatment and the priority for treatment implementation.

Risk treatment – risk treatment involves selecting one or more options for modifying risks, and implementing those options. When implemented, treatments provide or modify the controls.

Monitoring and review – risks and the effectiveness of controls and risk treatments need to be monitored, reviewed and reported to ensure changing context and circumstances do not alter priorities.

Recommended Reading

Australian Government Department of Defence (Defence Signals Directorate), *Cloud Computing Security Considerations,* published 12 April 2011.[1]

Australian Government Department of Defence (Defence Signals Directorate), *Information Security Manual (ISM)*, published November 2010.[2]

[1] http://www.asd.gov.au/infosec/cloudsecurity.htm
[2] http://www.asd.gov.au/infosec/ism/index.htm

Further Advice

For more detailed advice, please contact:

Government Information Strategy Unit
Tasmanian Archive and Heritage Office
91 Murray Street
HOBART TASMANIA 7000
Telephone: 03 6165 5581
Email: gisu@education.tas.gov.au

Information Security Classification

This document has been security classified using the Tasmanian Government Information Security classification standard as PUBLIC and will be managed according to the requirements of the Tasmanian Government Information Security Policy.

Document Development History
Build Status

Version	Date	Author	Reason	Sections
2.0	April 2015	Christine Woods	Template	All
1.0	January 2014	Allegra Huxtable	Initial Release	All

Amendments in this Release

Section Title	Section Number	Amendment Summary
All	All	Document imported into new template

Issued: January 2014

Ross Latham
State Archivist

Attachment A: Checklist of Contract Provisions

Contract Provisions	
Agency has confirmed that the service provider complies with the Personal Information Protection Principles in the *Personal Information Protection Act 2004*;	
The Contract includes procedures that need to be followed in the case of any potential security breach, including notification to the state government agency of any breaches	
The Contract includes provisions for the agency to audit the service provider to ensure it is complying with the *Personal Information Protection Act 2004*.	
When the additional steps required to ensure privacy protection are considered, is there an actual cost savings benefit to the agency?	
Does the agency know exactly, geographically, where the data will be stored, keeping in mind the possibility it may be across different countries or continents?	
Is the agency data segregated from other customers or government departments?	
Who will have access to the data? How will system administrators or staff of the cloud service provider be prevented from unauthorised access to the data?	
Is the service provider owned or controlled by a foreign company? What control does the foreign company have over the service provider?	
How will personal information be destroyed or retrieved when it is no longer needed, bearing in mind any requirements under the *Archives Act 1983*?	
The Contract includes provisions that state what happens to the agency data in the event of a sale of business to another entity – a change of control may impact on contracts or obligations of the cloud service provider	
Provision in the Contract that identifies what happens to the agency data if the service provider becomes insolvent or bankrupt	
Contract includes provisions for the retrieval or destruction of information once, or if, the contract with the cloud service provider terminates	
Is there data protection or privacy legislation in place in the foreign jurisdiction that at minimum meets the requirements in the *Personal Information Protection Act 2004*? Is the relevant law enforceable?	
Does the service provider have methods of notification or responding to data security breaches?	
Can the service provider guarantee that access will not be given to foreign governments or law enforcement? Is there a legislative requirement in that jurisdiction that prevents the agency from being notified of any potential access?	
What happens at the conclusion of the contract with the cloud service provider? Will information be able to be retrieved or destroyed in compliance with the *Personal Information Protection Act 2004* and the *Archives Act 1983*?	