ADRI

Advice on managing the recordkeeping risks associated with cloud computing

ADRI-2010-1-v1.0

CAARA

Council of Australasian Archives
and Records Authorities

Version 1.0
29 July 2010

Further copies of this document can be obtained from the ADRI Web site
http://www.adri.gov.au/ or http://www.adri.govt.nz/

The Australasian Digital Recordkeeping Initiative gives no warranty that the information in this version is correct or complete, error free or contains no omissions. The Australasian Digital Recordkeeping Initiative shall not be liable for any loss howsoever caused whether due to negligence or otherwise arising from the use of this document type.

Document Control

Version	Date	Author	Comment
0.1	11/03/2010	Cassie Findlay	First draft
0.2	1/04/2010	Cassie Findlay	Second draft
0.3	17/05/2010	Cassie Findlay	Third draft
0.4	25/06/2010	Cassie Findlay	Fourth draft
1.0	29/07/2010	Cassie Findlay	CAARA endorsed version

Endorsement

This document has been endorsed by the Australasian Digital Recordkeeping Initiative as an advice document on 25 June 2010date.

This document has been approved by the Council of Australasian Archives and Records Authorities on 29 July 2010.

Acknowledgements

This advice was based initially on the State Records NSW publication *Recordkeeping in brief: Storage of State records with service providers outside of NSW* (RIB 54)[1].

The ADRI working group that developed this advice comprised members from State Records NSW, Public Record Office Victoria and Archives New Zealand.

We would like to acknowledge the help given by those people and organisations who commented on drafts of this document.

Australasian Digital Recordkeeping Initiative (ADRI)

The Australasian Digital Recordkeeping Initiative (ADRI) is composed of representatives from all state and national archival authorities in Australia and New Zealand. The members of ADRI are:

[1] State Records Authority of New South Wales, *Recordkeeping in brief: Storage of State records with service providers outside NSW* (RIB 54), 2009. Available online at: <http://www.records.nsw.gov.au/recordkeeping/government-recordkeeping-manual/guidance/recordkeeping-in-brief/storage-of-state-records-with-service-providers>

- National Archives of Australia
- Archives New Zealand
- Public Record Office Victoria
- State Records NSW
- ACT Territory Records
- Archives Office of Tasmania
- Northern Territory Archives Service
- Queensland State Archives
- State Records South Australia
- State Records Office Western Australia

The aim of the Initiative is to develop and harmonise a uniform set of standards, guidelines, and practices for digital recordkeeping. A related aim is to improve the organisational capability, capacity, and expertise within the collaborating institutions in relation to digital recordkeeping.

ADRI is a working group of the Council of Australasian Archives and Records Authorities (CAARA). CAARA is the peak body of government archives and records institutions in Australia and New Zealand.

Contents

1 Purpose

The primary audience for this advice is member institutions of the Council of Australasian Archives and Records Authorities (CAARA). It is envisaged that CAARA member institutions will adapt the advice for dissemination to public offices in their jurisdictions.

Secondary audiences for this advice are public offices and cloud computing service providers seeking advice on the recordkeeping issues associated with cloud computing.

2 Background

According to the US National Institute of Standards and Technology (NIST), 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.”[2]

Service models for cloud computing can take a variety of forms[3], including software, platforms or infrastructure or a combination of these delivered as a service via the internet. Cloud computing usually involves the transfer to or creation of content in data stores which are maintained by the service provider and geographically remote from the customer. There are also a range of applications that can be delivered to users via cloud computing models, from email or content management to specialist applications for activities such as project management or human resources management.

Cloud computing is now being used by many government organisations in Australasia. This means that potentially large volumes of official records of government are being stored or processed in physical locations often outside Australian / New Zealand territorial boundaries.

This raises a number of risks both for government organisations and for members of the public who rely on the proper management of government information to provide evidence of their rights and entitlements, and to demonstrate the workings of government for accountability purposes.

While there are risks that need to be managed as part of the implementation of cloud computing services, it is important to recognise that they can also present opportunities not only for better service delivery but also for improved recordkeeping and information management. Some of the benefits include:

- cost savings
- reduced pressure on ICT departments to provide ever increasing storage capacity
- access to services outside normal office environments
- better opportunities for collaboration with geographically dispersed users
- potential opportunities for greater automation of recordkeeping as part of business processes, and
- more time for ICT personnel to devote to other issues where server maintenance and related tasks are lessened.

Records and archives authorities have a role to play in advising government organisations appropriately on the use of cloud computing for the storage and processing of government information. Government organisations need to ensure

[2] The NIST Definition of Cloud Computing, Authors: Peter Mell and Tim Grance, Version 15, 10-7-09. Available online: http://csrc.nist.gov/groups/SNS/cloud-computing/

[3] There are two basic models. One is where data storage is fully virtualised, with the internet itself serving as the storage space. This means no-one knows where the data resides and effective controls are difficult if not impossible to place on it. The other more common model is where the data is physically located on a server somewhere (possibly in multiple locations).

this advice is followed when entering into cloud computing arrangements so that recordkeeping risks can be properly managed.

3 Scope

This guidance is suitable for adoption by CAARA members for dissemination to all ‘agencies’ as defined by local archival legislation or other standards and instruments.

4 Managing the recordkeeping risks associated with cloud computing

In order to manage the recordkeeping risks associated with cloud computing, government organisations should:

- identify and assess the risks involved in using cloud computing service providers to store or process government information including records
- perform ‘due diligence’ when selecting a cloud computing service provider
- establish contractual arrangements to manage known risks, and
- monitor arrangements with cloud computing service providers.

4.1 Identify risks

Storage and maintenance of records with cloud computing service providers can have a variety of business and legal risks. Organisations should conduct a thorough risk assessment before entering into any arrangement with a cloud computing service provider. This is particularly important because of the practical difficulties in establishing relationships with global providers and making site inspections of remote facilities.

The act of sending or storing of records outside a State, Territory or Country might be, in itself, a breach of local laws

Before entering into arrangements with cloud computing providers, agencies should investigate any legislative impediments to the transfer or storage of records outside the physical boundaries of the State, Territory or Country which may be contained in, for example, archives / records or privacy legislation.

Provider might fail to comply with legislation or standards of the record-creating jurisdiction

There is a risk that where service providers send records outside the geographic boundaries of the record-creating jurisdiction that they might fail to comply with the legislative or regulatory requirements of the creating jurisdiction. For example, not all jurisdictions internationally have legislation governing the protection and management of private or personal information that are of equivalent strength to Australia’s and New Zealand’s laws.

Records may be subject to legislation and other requirements of the storage jurisdiction

Organisations should also seek advice as to whether there is any legislation in the relevant interstate or overseas jurisdiction that will apply to the storage and maintenance of their records. For example, it is likely that the privacy laws of an overseas jurisdiction will apply to any information stored within the jurisdiction, even if the information did not originate in that jurisdiction. Other laws may permit access to your information by investigative or watchdog bodies in the jurisdiction in which the information is stored.

There is a possibility that, if an overseas law enforcement agency subpoenas a cloud computing service provider for access to your organisation's records, you may not be consulted or even notified of this.

There may be risks associated with unauthorised access to records

There is a risk with the use of cloud computing services of unauthorised access to records which may result in breaches to privacy or other laws. This risk can be increased where service providers subcontract parts of their operations to other companies. It is also likely that the provider will co-locate your records with another organisation's – so proper partitioning / security controls need to be put in place.

There may be a risk of a loss of access to records

Due to the provision of cloud computing services over the internet, it is potentially more likely that there may be some periods of disruption to service where records are inaccessible. For business activities in which continuous access to information is imperative, the impact of a loss of access may be severe. In addition, government organisations in Australia are subject to increasingly high expectations of access to government information under current and emerging freedom of information laws. The use of cloud computing services poses a risk that access may not be provided in a timely way.

There may be a risk of record destruction or loss

Digital records stored as part of cloud computing arrangements are subject to all the same threats and risks as records stored anywhere, for example:

- records being destroyed as a result of a disaster such as a fire or flood, or
- records being compromised or destroyed as a result of cyber attack (eg hacker, virus).

In cloud computing situations, however, there are additional risks including:

- loss of access to records because the service provider has gone out of business or has been taken over by another company, which may not choose to honour your contract or to provide the agreed level of service
- a person in another State or country accessing, claiming ownership or taking control of the records
- the records not being returned upon request or at conclusion of the contract, or returned only on payment of a large fee
- inadequate backup and restoration arrangements as a result of cost cutting by the service provider
- that storage providers may upgrade to hardware and / or software which is not compatible with the organisation's, meaning there is a risk of data loss or of records not being readable upon return
- that the service provider disposes of digital records without the approval of the client organisation.

There can also be a risk of records not being disposed of in a timely way, once authorised by the agency, because it is common for service providers to replicate records for multiple backup, sending copies to sites in different locations or even different jurisdictions. This can mean that time-expired records are not properly deleted from every server held in every site. This can be a serious risk where there is a specific requirement for information to be destroyed, such as personal or sensitive information in records.

The evidential value of records may be damaged

Government records need to be managed in such a way that they can be shown to be authentic and reliable. If an organisation is not able to prove that records could not or have not been altered or tampered with in any way, this will reduce or negate their value as evidence. In addition, the evidential value of records may be affected if appropriate audit trails and descriptions of management processes performed on records while they are kept in cloud computing systems are not maintained.

4.2 Assessing risks for different records

The level of risk that an organisation attributes to a proposed cloud computing arrangement will vary according to the content or subject matter of the records and their level of sensitivity and importance to the business of the organisation or the government. In some cases, an organisation may decide that some records are simply too sensitive or important to trust to a cloud computing service provider.

- If records are likely to be required for legal proceedings, for example, what would the impact be if the evidential value of the records was lessened or negated because it could not be proved that they could not have been altered?
- Are there particular types of records with special secrecy or confidentiality requirements? For example, records documenting discussions and arrangements between corrections staff, lawyers and prisoners?
- Are there particular types of records which are too commercially valuable to entrust to a cloud computing provider? For example, records of original research?
- If records contain information about individuals, public expectations and concerns need to be taken into account. What would the community reaction be to knowing that particular types of information had been sent offshore?

For example:

One organisation was considering the acquisition of an application to help with the management of its occupational health and safety and workers compensation records. One of the products tendering was a cloud computing application which stored all client data in a country with a less stringent privacy regime than Australia’s. After conducting a risk assessment the organisation decided that given the sensitive and personal nature of many of the records that the system would be managing, the best option would be to acquire an application that could store the information in-house.

4.3 Perform ‘due diligence’ when selecting a cloud computing provider

Organisations should exercise due diligence when entering into arrangements with cloud computing service providers, including checking reference sites or referees where appropriate.

Ask service providers:

- how easy / difficult / costly it will be for them to meet any recordkeeping requirements specified by your organisation, for example additional metadata fields, to meet local regulatory or business recordkeeping requirements
- whether any additional charges would be levied by the service provider in the event of the organisation seeking to remove information from 'the cloud'
- if they will commit to storing and processing your information in specific jurisdictions that are acceptable to your organisation (that have, for example, legal frameworks more compatible with Australasia's)
- whether they will make a contractual commitment to obey privacy requirements on behalf of their customers – both local to the organisation and in the location or locations(s) where the information is stored
- for an assurance that no copy of the records or information is retained by the service provider after the termination of the contract.
- whether you are able to regularly specify records to be destroyed
- whether they prepared to provide you with certificates of destruction
- whether they are regularly subjected to external security audit or certification processes
- how many administrators will have access to your records and details of controls over their access
- how third party access to your records would be managed, for example if required by a government watchdog organisation in the jurisdiction in which the records are stored
- if they have measures such as multiple geographically separated back-up sites in place, so that they can do a complete restoration of your records if needed, and how long this would take
- as well as complete restoration of data, how will they go about finding and restoring particular specified records or sets of records and what timeframes will they guarantee for this. For example, if someone accidentally deletes some records or if some data becomes corrupted
- when restoring records, can they ensure that the structure of records (not just the content) and associated metadata is maintained
- what are the guaranteed service provision parameters offered by the provider (given the greater likelihood of service disruption due to provision over the internet) – what action will they take in the event of service disruption, do they offer any recompense
- whether service providers subcontract part of their service offering to third parties and, if so, what contractual agreements they operate under
- whether there are any relevant standards they are certified as meeting

4.4 Establish contractual arrangements to manage known risks

Organisations should ensure that all contractual arrangements with any service provider recognise that:

- ownership of the records remains with the State / Commonwealth / New Zealand government, and

- the organisation has a continuing responsibility for the proper management of those records
- records and associated metadata will be returned to the organisation when requested (with any associated fee structure specified).

Other contractual inclusions might include:

- recordkeeping functionality and metadata specifications serving to meet (the organisation)'s regulatory and business recordkeeping requirements
- (the organisation)'s records cannot be used for applications not specified in the contract (for example, to data match with databases owned by other clients of the contractor)
- personal information is to only be used for the purpose for which it was gathered, in accordance with relevant privacy laws, as amended from time to time
- (the organisation)'s records are not to be shown to a third party without the written agreement of (the responsible organisation)
- (the organisation)'s records are not to be disposed of without the written agreement of (the responsible organisation)
- (service provider) is not permitted to transfer (the organisation)'s records to a third party for any purpose unless authorised to do so by (the organisation)
- at the conclusion of (the organisation)'s use of the services of (service provider) all specified records and associated metadata are to be returned to (the responsible public office) in an accessible format / nominated format/s: (X, Y, Z)
- at the conclusion of the (the organisation)'s use of the services of (service provider) all specified records and associated metadata are removed permanently from (service provider)'s systems.

A particular issue that organisations should consider with contractual arrangements for cloud computing is the need to make provision for the return of the records to the public office if and when contracts are terminated. It is important that any associated fees or service restrictions are fully documented, to prevent organisations becoming locked in to continuing to use an underperforming service provider.

In addition, specific provisions may be required to ensure that the records are returned in a useable form.

For example:

One organisation used a 'cloud' project management software application for the management of a key project. At the conclusion of the project, the organisation had no further need to use the particular software application. With the conclusion of the contract with the cloud service provider, they wished to remove the information relating to their project from the cloud and store it in their own recordkeeping system for future reference. However, the information was in proprietary formats and were structured in a way that would make it extremely difficult to migrate the records into the organisation's recordkeeping systems. The organisation had an ongoing business need for access to the record and had to either continue to pay the service provider for ongoing access to the application, or recreate the information in another form, both costly options.

4.5 Monitor arrangements with cloud computing service providers

As circumstances change, it is important to continue to monitor how well your organisation’s recordkeeping and information management objectives are being met by any cloud computing services used, and to check for any unacceptable risks that might emerge.

Where possible, organisations should include a service level agreement as part of any contractual arrangements with service providers. This should specify detailed performance metrics against which the service provider can be measured to ensure that all relevant requirements are being met.

Arrangements with service providers should specify that your organisation should be advised of any changes to its data storage arrangements, such as changes of location, back up and recovery procedure or security controls.

5 Bibliography

John Brodkin, ‘Gartner: Seven cloud-computing security risks’, *InfoWorld*, July 2 2008. Available online at: http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853

Jarina D’Aruria and Kim S Nash, ‘Cloud computing special part 2: Cloud control’, CIO, 6 July 2009. Available online: http://www.cio.com.au/article/309978/cloud_computing_special_part_2_cloud_control?fp=4&fpid=51235

Robert Gellman, *Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing*, World Privacy Forum, February 23, 2009. Available online at: http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf

Brad Howarth, ‘Cloud computing special part 1: Looking for the silver lining’ *CIO*, 6 July 2009. Available online at: http://www.cio.com.au/article/309984/cloud_computing_special_part_1_looking_silver_lining?fp=4&fpid=51235

Peter Mell and Tim Grance, *The NIST Definition of Cloud Computing*, Version 15, 10-7-09. Available online: http://csrc.nist.gov/groups/SNS/cloud-computing/

National Archives and Records Administration, *Frequently Asked Questions About Managing Federal Records In Cloud Computing Environments*, 2010. Available online at: http://www.archives.gov/records-mgmt/faqs/cloud.html

David C. Wyld, *Moving to the Cloud: An Introduction to Cloud Computing in Government*, IBM Center for the Business of Government, 2009. Available online at: http://www.businessofgovernment.org/pdfs/WyldCloudReport.pdf

Appendix A: Recordkeeping checklist for government organisations considering using cloud computing service providers

1. Should a cloud computing application be considered?

- Is the transfer or storage of official records outside of State / Country boundaries permitted under local regulatory frameworks?
  → If no, do not proceed.

- Is the information to be maintained under cloud computing arrangements of a highly sensitive or personal nature?
  → If yes, any arrangement with a service provider must involve storage of the records in a jurisdiction with an privacy regime equivalent to Australasia's and with adequate security measures in place (see questions below for more detail).

2. Where a cloud computing application is being considered, use the checklist below to guide your assessment of the risks associated with the use of the application.

	Requirement	**Yes**	**No**
1.	Can you confirm that ownership of the records will remain with your organisation?		
2.	Can you specify recordkeeping functionality and metadata requirements for the records to the service provider in order to meet your regulatory and business recordkeeping requirements?		
3.	Will the information be physically stored in a jurisdiction that is acceptable to your organisation (that have, for example, legal frameworks more compatible with Australasia's)		
4.	Will the service provider make a commitment to obey local privacy requirements on your organisation's behalf?		
5.	Can you obtain an assurance that no copy of your organisation's records or information is retained by the service provider after the termination of the contract?		
6.	Is the service provider regularly subjected to external security audit or certification processes?		
7.	Does the service provider have offsite back-up and disaster recovery measures in place?		
8.	Is a full restoration of your information possible within a reasonable timeframe in the event of an incident?		
9.	Is a partial restoration of your information possible within a reasonable timeframe in the event of an incident?		
10.	Will you be consulted regarding any third party seeking to have access to your records?		
11.	Can you obtain assurance that your records cannot be used for applications not specified in the contract (for example, to data match with databases owned by other clients of the		

	contractor)		
12.	Will the service provider undertake, at the conclusion of (the organisation)’s use of the services of (service provider), to return all specified records and associated metadata to (the responsible organisation) in an accessible / nominated format/s?		
13.	Will the service provider guarantee acceptable parameters for service provision in respect to possible disruptions?		