Future Proof

Managing recordkeeping risk in the cloud:

Ensuring the proper creation, management and disposal of official records in cloud computing environments

Cloud computing is internet-based computing, whereby shared resources, software and information are provided to computers and other devices on-demand.[1] Service models for cloud computing can take a variety of forms, including software, platforms or infrastructure, or a combination of these delivered as a service via the internet. There are 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.

Official State records may be in the cloud

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. Where official government business is done using cloud computing these data stores will contain State records.

Manage risks to records in the cloud

In order to manage the recordkeeping risks associated with cloud computing, you 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
- monitor arrangements with cloud computing service providers.

Recordkeeping risks can include:

- the provider might fail to comply with NSW legislation or standards, including standards for recordkeeping
- the records may be subject to legislation and other requirements of the storage jurisdiction that are not compatible with your requirements
- there may be risks associated with unauthorised access to records
- there may be a risk of a loss of access to records
- there may be a risk of record destruction or loss
- the evidential value of records may be compromised or damaged.

Some records should be managed 'in house'

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. In some cases, you may decide that some records are simply too sensitive or important to trust to a cloud computing service provider.

Before you enter into cloud computing arrangements

Ask the service provider:

- how they propose 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 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 Australia's environment)

[1] Wikipedia contributors, 'Cloud computing,' *Wikipedia, the free encyclopedia,* http://en.wikipedia.org/w/index.php?title=Cloud_computing&oldid=368166834 (accessed 15 June, 2010).

- whether they will make a contractual commitment to comply with 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 provider after the termination of the contract
- whether you are able to regularly specify records to be destroyed and whether they are 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
- if they can give assurances 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)
- whether you will be consulted regarding any third party seeking to have access to your records
- 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, whether they can ensure that the structure of records (not just the content) and associated metadata is maintained
- whether they subcontract part of their service offering to third parties and, if so, what contractual agreements they operate under
- if there are any standards they are certified as meeting
- whether they will guarantee acceptable parameters for service provision in respect to possible disruptions, and what actions they will take in the event of service disruption (for example, do they offer any recompense?)

Records risk management checklist for cloud computing arrangements

Can you confirm that....?

1.	you have conducted a risk assessment of keeping official records under cloud computing arrangements and comply with the conditions listed in the *General authority for transferring records out of NSW for storage with or maintenance by service providers based outside of the State* (GA35)	
2.	the records to be made and kept in the cloud are not highly sensitive in nature	
3.	ownership of your records remains with your organisation	
4.	records are kept in accordance with the recordkeeping functionality and metadata requirements of the Standard on digital recordkeeping	
5.	the service provider has offsite back-up and disaster recovery measures in place	
6.	a full restoration of your information is possible within a reasonable timeframe in the event of an incident	
7.	the provider will return all required records and associated metadata in readable formats to your organisation when requested	

For more information see:

- *General authority for transferring records out of NSW for storage with or maintenance by service providers based outside of the State* (GA35)
- *Recordkeeping in brief Storage of State records with service providers outside of NSW* (RIB 54)
- *Standard on digital recordkeeping*