Records management and the cloud—a checklist

1. Records in the cloud are to be governed by the Archives Act 1983

□ Ensure your agency complies with Section 24 of the *Archives Act 1983*

Section 24 of the Archives Act provides that a person must not engage in conduct that results in the transfer of the custody or ownership of a Commonwealth record other than, relevantly under Section 24(2)(b) and (c), with the permission of the Archives or in accordance with a practice or procedure approved by the Archives, or in accordance with a normal administrative practice of which the Archives does not disapprove.

On this basis, the National Archives of Australia would not approve a decision to use a cloud service without appropriate controls and protections for Commonwealth records in place. Agencies should make a risk-based decision, taking into account all Commonwealth compliance interests, including risks to the records. Controls and protections should appropriately match the value of the records.

Section 24 requires agencies to consider carefully what records will reside in the cloud and to ensure that the terms of contracts with providers adequately address issues of control, ownership and management of records. Agencies should approach the National Archives if they have questions.

2. Records in the cloud should be authentic, accurate and trusted

□ Consider where your records are held

Cloud service providers may store records on multiple servers in multiple locations, including across different countries.

There may be risks to the authenticity, accuracy and reliability of the records if they are stored in jurisdictions that do not have the same protection for information, or where they may become subject to the laws of the country where they are stored. The consequences may be that your records are seized or accessed without your knowledge.

Because your records are likely to be stored on the same servers as other records, they may be caught up in discovery or other legal action affecting records sharing the same server.

Knowing the location of your records and assessing the risks that may be associated with the location helps ensure your records are appropriately secure. This is fundamental to an informed risk assessment.

□ Consider whether the cloud provider has sufficient audit management

Evidential value and authenticity of records can be diminished through unauthorised access. To maintain accurate and trusted records, it is important that the provider maintains adequate system logs and audits,

and can provide audit logs, or extract information from audit logs, specific to your information. The provider should be able to detect unauthorised access and prove that records are what they purport to be. Audit logs are also records. You should ensure that you have access to audit logs and consider what audit information needs to be kept and for how long.

□ **Evaluate the security**

Data and network security and, to an extent, physical security ensure that records remain authentic, accurate and trusted. The Australian Government Protective Policy Framework and the Australian Government Information Security Manual set out security requirements for records.

□ **Be aware of the use of third party subcontractors**

Cloud services may involve layers of subcontractors. They need to meet the same records management criteria as the primary provider.

3. Records in the cloud should be complete and unaltered

□ **Consider the impact of altered records**

Migration, conversion and refreshment are inevitable parts of managing digital records. If not done properly there is a risk that the records may become incomplete or damaged. This affects their value as evidence.

If certain conditions are met you can destroy a range of source records that are no longer needed once they have been copied, converted or migrated. The Archives authorises this destruction with the General Disposal Authority for Source Records that have been Copied, Converted or Migrated. Destruction of records that have been migrated, converted or refreshed should be undertaken in accordance with that authority.

Agencies need to assess the migration, conversion and refreshment techniques used by their cloud provider to ensure that records are not inadvertently altered or incomplete. Cloud providers should obtain the permission of the agency prior to conversion or migration of records.

Any alteration of records should be authorised by the agency, recorded and traceable.

□ **Consider the format in which records are transferred, created or stored in the cloud**

Agencies should be aware of, and authorise, any change in the format of records transferred to the cloud. Records created in the cloud may be either transferred to the agency or continue to be stored in the cloud. Consideration should be given to the format of these records. (For more information on format see Section 5.)

4. Records in the cloud should be secure from unauthorised access, alteration and deletion

□ Consider who has access to, and use of, your records

You should be able to specify who has the right to access records and when.

When records are accessed and used, further transactional records are created. This transactional information also belongs to the agency and provisions should be in place to ensure that the provider does not use this information for their own purposes. Access restrictions should be commensurate with the value of the record.

□ Assess the provider's viability

If a cloud provider ceases business, access to records may be lost either temporarily or permanently. The new provider may not honour previous arrangements and agencies may not know who has had access to their records. This may compromise your ability to ensure records are secure from unauthorised access, alteration or deletion.

□ Consider the risks of incomplete destruction of records

Because records in the cloud are often kept on many servers in many locations, it may be difficult to know whether they have been securely destroyed. Consider the risks to your agency if records are not destroyed when required.

Disposal of records is authorised by the Archives in agency-specific records authorities, the Administrative Functions Disposal Authority or other general records authorities. If cloud providers dispose of records on behalf of agencies, they must obtain approval from the agency and use the specified records authority.

Disposing of records in a timely manner makes business more efficient. There is a reduced risk to your agency and it is more likely that people will be able to find the right records when they need them. This limits the possibility of unauthorised access and reduces costs of unnecessary storage and maintenance of records.

5. Records in the cloud should be findable and readable

□ Consider the readability and usability of records stored or created in the cloud

Records have little value if they are not readable. Some providers require clients to use their own formats and software and the risks this poses to ongoing usability of the records should be considered when choosing a cloud service provider.

When records are returned to the agency, they must be in a format that the agency can use.
Contracts with cloud service providers should specify the format in which records are returned to the agency, formats used in storage, and processes to be followed when information is migrated. Preferably the provider should use open formats to support readability over time.

□ **Ensure records can be recovered**

To maintain access to records in the cloud, it is important that the provider undertakes regular backups and that business continuity plans are in place for recovery of records. Agencies should also be aware of safeguards for their records in the event of network breaks, service disruptions or network congestion.

□ **Evaluate the impact of corrupted records**

There is always a risk that digital records may become corrupted. If this happens it can be difficult or impossible to access and use records. It is important for your agency and the provider to address the need for restoring corrupted records.

□ **Consider the metadata required to identify and retrieve your records**

Metadata is the means by which records can be confirmed as complete and authentic. Metadata also ensures records are findable and useable.

Agencies also need to ensure that records have sufficient metadata to satisfy access and retention requirements.

Metadata in all records should comply with the Australian Government Recordkeeping Metadata Standard (AGRkMS).

Records stored in the cloud may benefit from further metadata schemes such as AS 5044 (AGLS).

Metadata is itself a record that needs to be managed and retrievable.

□ **Assess the likelihood of vendor lock-in**

A cloud service provider may require you to use proprietary software and hardware.

This may lock you into arrangements with that provider because of the difficulty in retrieving records in a format that can be migrated to another provider, or even to your own servers. The value of the record in those cases is severely reduced.

6. Records in the cloud should be related to other relevant records

□ **Consider metadata maintenance and management**

Mismanaged metadata may result in records that are difficult to find and understand and will decrease the integrity of the record. Mismanaged metadata may also weaken the ability to link a record with other records, and thus diminish its context.

Requirements for metadata should be developed before the records are transferred to the cloud. The contract between your agency and the provider should include minimum metadata requirements for process management of records.

□ **Consider how records in the cloud relate to records stored in-house**

Are records stored in the cloud related to records stored in-house? Are the connections between in-house records and records stored in the cloud clear? Systems for managing records in the cloud and in-house should be complementary. This may mean that additional metadata needs to be applied to records stored in the cloud to maintain their relationship links.

□ **Consider records classification**

Classification in records management means the systematic identification and arrangement of records into categories according to logically structured conventions and procedural rules. Proper classification of records not only helps identify and find records, it also assists in developing relationships between records. Records should be appropriately classified before they are stored in the cloud. This includes records created as a result of using the cloud.

With the exception of the Commonwealth Coat of Arms, *A Checklist for Records Management and the Cloud* by the National Archives of Australia is licenced under a Creative Commons Attribution 3.0 Australia licence (http://creativecommons.org/licenses/by/3.0/au/).

Enquiries regarding the licence and any use of this document should be sent to recordkeeping@naa.gov.au or the Publications Manager, National Archives of Australia, PO Box 7425, Canberra Business Centre ACT 2610, Australia.

This publication should be cited as: *A Checklist for Records Management and the Cloud*, National Archives of Australia, 2011.