Government of South Australia

State Records of South Australia

Cloud Computing and Records Management

Guideline

June 2015

Version **1**

Version control

Version:	1.0
Details:	New guideline
Issued:	5 June 2015
Primary contact:	Manager, Information Governance State Records of South Australia GPO Box 464 Adelaide SA 5001 Phone: 7322 7081

Classification: Public

Table of Contents

Introduction

Purpose

This Guideline sets out State Records' policy on the management of official records when created and/or stored using cloud computing technology, and clear direction on the recordkeeping risks that are to be considered and managed when planning use of 'the cloud'.

The Guideline should help South Australian (SA) Government agencies establish in-house policies and procedures for operation of cloud computing technology in order to meet business and accountability requirements and community expectations. It should also enable agencies to meet their legal obligations for the retention and disposal of official records under the *State Records Act 1997* (the Act).

Agencies are ultimately responsible and accountable for managing their records wherever they are held. Records of value need to:

- retain their integrity, authenticity and reliability
- be accessible and retrievable
- be securely destroyed when authorised, or retained if they have a permanent value.

At the present time, State Records does not have a Digital Archive with which to store, manage and provide access to digital materials of permanent value. The responsibility to securely store and manage these materials resides with agencies until such time as a Digital Archive has been established.

Scope

This Guideline addresses the recordkeeping risks associated with cloud computing that need to be considered in order that official records remain secure, retrievable, accurate and reliable.

It does not address operational concerns such as availability, reliability and quality of computing services; risks related to major service disruptions; risks related to agreements, warranties and indemnities, usage costs and quality of service; nor risks relating to general statutory and common law obligations.

For advice on other aspects to be considered in utilising cloud computing technology read *Overview and Considerations for Cloud Computing* issued by the South Australian Office for Digital Government (previously Office of the Chief Information Officer (OCIO)). Another useful resource is *A Guide to Implementing Cloud Services* issued by the Commonwealth Whole of Government Information and Communications Technology Office (previously AGIMO), as well as the accompanying suite of documents on cloud computing available from their website (http://www.finance.gov.au/policy-guides-procurement/cloud/).

The Privacy Committee of South Australia has also issued a guideline on *Privacy and Cloud Computing* available from the State Records website.

Legislative Context

The *State Records Act 1997* outlines the responsibilities of agencies to:

- ensure that the official records in their custody are maintained in good order and condition
- ensure that official records are managed and not destroyed without a determination made by State Records with the approval of the State Records Council - unless there is specific legislation requiring it.

The *State Records Act 1997* defines an official record as "a record made or received by an agency in the conduct of its business". Official records provide evidence of the functions and activities conducted by state government agencies and local government authorities. Agencies and authorities should be aware that both paper-based and electronic records created as part of an agency's business are considered to be official records for the purposes of the *State Records Act 1997*.

Agencies will need to consult their own legislation to determine if any obligations exist to maintain "custody", and whether that has ramifications for managing records in the cloud.

Agency obligations under the *Freedom of Information Act 1991* and *Information Privacy Principles* (IPPs) as laid out in Cabinet Administrative Instruction 1/89, as amended by Cabinet 18 May 2009, are also relevant to handling and managing South Australian Government records.

Acknowledgement

Acknowledgement is given to the Australasian Digital Recordkeeping Initiative (ADRI) for use of *Advice on managing the recordkeeping risks associated with cloud computing* ADRI-2010-1-v1.0, the Queensland State Archives *Managing the Recordkeeping Risks Associated with Cloud Computing* (2010) and the Public Record Office Victoria for *Recordkeeping Implications for Cloud Computing* (2013). This Guideline has also been informed by the work of the National Archives of Australia, Archives New Zealand and NSW State Records Authority.

Variation to this document

State Records may update or alter this Guideline from time to time as authorised by the Director of State Records, in consultation with the State Records Council.

Cloud Computing

The Commonwealth Whole of Government Information and Communications Technology Office (previously AGIMO) has adopted the US Government's National Institute of Standards and Technology (NIST) definition for cloud computing[1]. That is:

> *a model for enabling ubiquitous, 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.*

In other words, it is used to describe software and/or data housed in an off-site, geographically remote facility accessed over the Internet.

Regardless of the service model or method of deployment chosen (see Attachments B and C) when an agency proposes to use cloud services where official records will be created, stored, managed or accessed, the recordkeeping risks need to be identified, mitigated and managed. The final assessment should indicate the cloud service is an acceptable risk option.

South Australian Context

The SA Government issued the Digital by Default Declaration in November 2014, which recognised that "digital technology is critical to modernising and transforming our public services". The *South Australia Connected, ready for the future* (2013) strategy document outlines the intent of government to use ICT to connect citizens with government services, and the expectation that agencies use of ICT is strategic, purposeful, and best serves the people of the state.

The Office for Digital Government has issued *ICT Policy Statement 3: Cloud Services (April 2015)* with the intent of ensuring agencies "evaluate cloud services in every new or reformed ICT sourcing, procurement, or market approach. It also establishes an expectation that a cloud service should be chosen unless it will not deliver the best value for money outcome for government [...] given an equitable evaluation of business needs, resilience, and risk, as well as compliance with any relevant legislation, instructions, policies, standards, and rulings."

The *ISMF Ruling 2: storage and processing of Australian Government information in outsourced or offshore ICT arrangements – as applied to the South Australian Government* (OCIO/R4.2) issued by the Office for Digital Government states that SA Government information may be outsourced or offshored in ICT arrangements subject to a risk assessment being undertaken that consider the three dimensions of classification and protective (or dissemination limiting) markings that are described by the ISMF. The ultimate decision to accept or tolerate residual risks associated with outsourcing and offshoring arrangements remains with the agency Chief Executive".

[1] Australian Government Cloud Computing Policy v3.0 October 2014, p8
http://www.finance.gov.au/policy-guides-procurement/cloud/

Identify Recordkeeping Risks

Storage and maintenance of records with cloud computing service providers can have a variety of business and legal risks. Agencies should conduct a thorough risk assessment before entering into any arrangement with a 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 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. An agency should seek legal advice in regard to its own establishing and regulatory legislation.

The policy of the SA Government, as detailed in the *ISMF Ruling 2: storage and processing of Australian Government information in outsourced or offshore ICT arrangements – as applied to the South Australian Government* (OCIO/R4.2) is that information may be outsourced or offshored in ICT arrangements subject to a risk assessment being undertaken

Provider may fail to comply with legislation / standards of the record-creating jurisdiction

There is a risk that where cloud computing providers send records outside the geographic boundaries of the record-creating jurisdiction 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

Agencies 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 within 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

With the use of cloud computing services there is a risk 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 those of another organisation – therefore proper partitioning / security controls need to be put in place.

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

As cloud computing services are provided over the internet, it is more likely that there may be some periods of disruption to service where records are inaccessible. For business activities where continuous access is imperative, the impact of a loss of access may be severe. In addition, government agencies in Australia are subject to increasingly high expectations of access 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 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 (e.g. hacker, virus).

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

- loss of access to records because the 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
- an entity in another state or country accessing, claiming ownership or taking control of the records
- the records not being returned upon request or at the 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 provider
- providers may upgrade to hardware and / or software which is not compatible with that of the agency, meaning there is a risk of data loss or of records not being readable upon return
- the 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 manner, once authorised by the agency; 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 poses a serious risk where there is a specific requirement for information to be destroyed, such as records containing personal or sensitive information.

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.

Manage Recordkeeping Risks

To manage the recordkeeping risks associated with cloud computing, agencies should:

- identify and assess the risks associated with using a cloud computing service provider to store or process government records
- assess the capacity of the cloud application to perform recordkeeping functions
- perform 'due diligence' when selecting a service provider
- establish contractual arrangements to manage known risks
- routinely monitor arrangements with service providers.

Assess risks for different record types

The content or subject matter of records, and their level of sensitivity, will determine the level of risk attributed to a proposed cloud computing arrangement.

- What are the expectations of privacy, particularly where information about individuals may be sent interstate or offshore?
- Do the records have special secrecy or confidentiality requirements?
- How likely is it that the records might be required as evidence or proof of actions, transactions or decisions?

Perform due diligence when selecting a cloud computing provider

A cloud computing provider should be able to answer questions regarding functionality, reliability, availability, security, privacy, data ownership/stewardship, integration and customisation.

Questions relating to recordkeeping have been provided by the Australasian Digital Recordkeeping Initiative (ADRI) (see Attachment A).

Establish contractual arrangements to manage known risks

Agencies should ensure contractual arrangements with any service provider recognise that:

- ownership of the records remains with the agency
- the agency has a continuing responsibility for the proper management of those records, including disposal of records in accordance with an approved disposal schedule
- records and associated metadata will be returned to the agency when requested.

Agencies should consider and plan for how records and associated metadata will be managed when contracts are terminated. In particular, the data should be returned in a useable form, and removed permanently from the service provider's systems.

Where possible, service level agreements should include requirements for regular reporting against recordkeeping measures. This may include the need for regular independent auditing relating to security and recoverability. Arrangements should also specify that the agency will be advised of any changes to data storage arrangements, back up and recovery procedures or security controls.

Monitor arrangements with cloud computing service providers

As circumstances change, it is important to monitor arrangements with service providers to ensure the agency's recordkeeping objectives continue to be met, and to check for any unacceptable risks that might emerge or escalate.

Attachment A - Checklist

The following 'Recordkeeping checklist for government agencies considering using cloud computing service providers' is taken from *Advice on managing the recordkeeping risks associated with cloud computing* (ADRI-2010-1-v1.0) issued by the Australasian Digital Recordkeeping Initiative (ADRI). The document in full can be found on http://adri.gov.au.

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?		

Attachment B – Cloud Service Models

Various types of cloud environments may be available from a service provider. In most cases cloud services fall under one or more of the following three categories.

Software-as-a-Service (SaaS) – provides complete business applications delivered over the web. The business applications are hosted by a provider and delivered as a service term (such as email or financial applications). Applications are accessed from various devices through a client interface such as a web browser or through a program interface. The cloud infrastructure, including applications, servers, operating systems and storage, is managed by the provider.

Platform-as-a-Service (PaaS) – is the online delivery of a custom application development or deployment environments in which applications can be built and run on service provider systems. Developers can build custom web applications without installing any tools on agency computers and then deploy those applications without requiring specialised system administration skills. The infrastructure required is supplied by the cloud service provider. The agency has control over the deployed applications and possibly the configuration settings for the environment.

Infrastructure-as-a-Service (IaaS) - is the online delivery of virtual infrastructure components (such as servers, storage and network access). It provides generic computing resources, such as the infrastructure needed to deploy and run an agency's own software applications.

Attachment C – Cloud Deployment Models

Private cloud - the cloud infrastructure is provided for exclusive use by a single organisation comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organisation, a third party, or some combination of them, and it may exist on or off premises.

Community cloud - the cloud infrastructure is provided for exclusive use by a specific community of consumers from organisations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organisations in the community, a third party, or some combination of them, and it may exist on or off premises.

Public cloud - the cloud infrastructure is provided for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organisation, or some combination of them. It exists on the premises of the cloud provider.

Hybrid cloud - the cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardised or proprietary technology that enables data and application portability.

Attachment D – Benefits

The Office of Digital Government suggests that adopting a cloud service may provide the following business benefits:

Scalability – enabling the system to handle a growing amount of work and the capability to accommodate that growth, making the agency flexible and responsive to change. Faster responsiveness can reduce the time to implement new services and thereby benefit service delivery. There is no financial commitment for infrastructure purchase and maintenance.

Efficiency - reallocation of IT operational activities (from support of onsite applications) offers opportunity to focus on other business needs. Use of cloud services may provide opportunity to create new solutions that were previously not technically or economically feasible. Use of cloud may provide the ability to de-couple applications from existing infrastructure.

Cost Containment - services and storage become available on demand without the serious financial commitments required for infrastructure purchase and maintenance and they are priced as a pay-as-you-go service. Reduction of operating costs: less energy consumption; less cost and complexity in doing both routine computing tasks and computationally-intensive problems; potential to reduce support and maintenance costs through transitioning legacy systems to new systems; reduced wasted resources, e.g. unused server space.

Flexibility - agencies can save time at set-up, as cloud computing becomes functional faster than other systems. To transition to the cloud, agencies are not required to install additional hardware or software and implementation can be undertaken remotely. There is potential to access latest technology through software applications being automatically updated at the network level.

Availability - cloud software architectures are designed from the bottom up for maximum network performance – potentially delivering improved application level availability than conventional IT solutions.

Resiliency - there is no single point of failure enabling a highly resilient computing environment. The failure of one node of a system in a cloud environment will have no impact on overall information availability and reducing the risk of perceivable downtime.

While Cloud Computing has many benefits there are also risks. This Guideline addresses the risks associated with recordkeeping, however a wider perspective can be gained from consulting the Office of Digital Government and its publications