Public Record Office Victoria

Cloud Computing Policy

Guideline 1

Cloud Computing Decision Making

Version Number: 1.0

Issue Date: 26/06/2013

Expiry Date: 26/06/2018

Table of Contents

Copyright Statement

Disclaimer

The State of Victoria gives no warranty that the information in this version is correct or complete, error free or contains no omissions. The State of Victoria shall not be liable for any loss howsoever caused whether due to negligence or otherwise arising from the use of this Guideline. This Guideline does not constitute, and should not be read as, a competent legal opinion. Agencies are advised to seek independent legal advice if appropriate.

1. Introduction

Victorian Government agencies are increasingly using cloud computing solutions of various kinds for the storage and management of data. This trend is likely to accelerate as cloud computing becomes more cost effective, flexible and responsive over time.

The National Institute of Standards and Technology (NIST), a United States Department of Commerce agency, defines cloud computing as:

"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[1]*".*

This Guideline intends to support agencies' moves to using cloud computing solutions. It provides a recommended series of steps or processes that can help agencies in their decision making processes when looking at cloud service providers from a data management and retention perspective.

1.1. Public Record Office Victoria Standards

Under section 12 of the *Public Records Act 1973*, the Keeper of Public Records ('the Keeper') is responsible for the establishment of Standards for the efficient management of public records and for assisting Victorian government agencies to apply those Standards to records under their control.

Recordkeeping Standards issued by PROV reflect best practice methodology. This includes International Standards issued by the International Organisation for Standardisation (ISO) and Australian Standards (AS) issued by Standards Australia in addition to PROV research into current and future trends.

Heads of government agencies are responsible under section 13b of the *Public Records Act 1973* for carrying out, with the advice and assistance of the Keeper, a programme of efficient management of public records that is in accordance with all Standards issued by the Keeper.

In Victoria, a programme of records management is identified as consisting of the following components:

- A recordkeeping framework
- Recordkeeping procedures, processes and practices
- Records management systems and structures
- Personnel and organisational structure
- Resources, including sufficient budget and facilities.

[1] P Mell & T Grance 2010, *The NIST Definition of Cloud Computing, National Institute of Standards and Technology, Gaithersburg, viewed 18 December 2012,* < *http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf*>p. 2.

A programme of records management will cover all an agency's records in all formats, media, and systems, including business systems.

As well as its integrated suite of standards, specifications and guidelines, PROV from time to time issues thematic representations of requirements as Policies. These Policies draw together requirements from several standards as they relate to a particular subject area (eg. Social Media; Cloud Computing). As they derive their authority from the standards, which are mandated instruments of the Public Records Act, Policies are binding on agencies.

Guidelines that link to Policies are created to assist agencies in the practical implementation of the policy requirements, and provide explanation, tools and options for complying with the Policy to which they relate.

1.2. Purpose

The purpose of this Guideline is to facilitate implementation of requirements contained in the *PROV Cloud Computing Policy*.

1.3. Scope

This Guideline applies to the decision-making process for agencies considering or engaging in cloud computing solutions involving the storage and management of data. It covers the relevant questions that agencies will ask to ensure that any cloud computing solution fulfils their data management and storage needs.

It does not cover the due diligence, cost modelling or service efficiency aspects of the decision making process except insofar as they apply to the management of data.

1.4. Related Documents

This Guideline must be read and implemented in conjunction with *Cloud Computing Policy* and with *Cloud Computing Guideline 2: Cloud Computing Tools*, other Public Record Office Victoria (PROV) Standards and associated documentation, including appropriate Retention and Disposal Authorities (RDAs). The Policy and other Guidelines associated with this Guideline are detailed below:

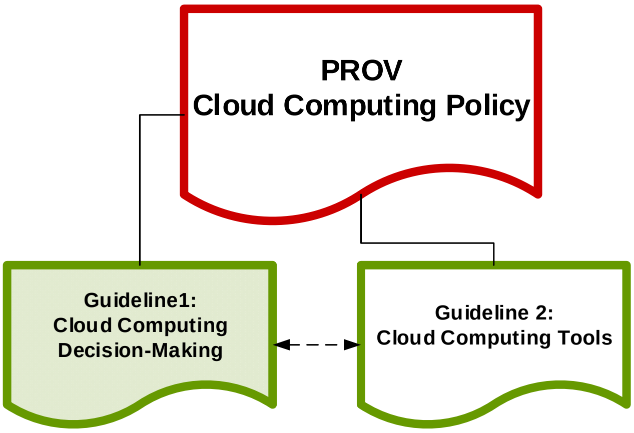

Figure 1: Relationship Diagram

2. Decision-Making for Cloud Computing

As agencies move services and / or storage of data into cloud environments, there are a number of factors that will need to be considered in helping to select a provider or service that meets all the needs of the agency.

Most organisations will have, and use, procurement processes that involve assessment of many aspects of the proposed service. Agencies will look at factors such as cost, value, efficiency, scalability, and range of services in their assessments. These factors are not considered explicitly by the *PROV Cloud Computing Policy* or this Guideline.

The ways in which the environment will support the appropriate treatment of agency data is an important area to consider. This includes, but is not limited to, considerations around:

- Data security and protection
- Data privacy
- Where relevant, data confidentiality
- Ability to execute authorised and complete destruction of data, and prevent unauthorised disposal
- The longevity of the systems within the cloud
- Data integrity and completeness, including maintenance of metadata
- Data authenticity, and the ability to audit / demonstrate it
- Protection of copyright and proprietary interests in data
- Data retrievability (while within the cloud) and extractability (if the service is discontinued).

All of these factors will need to be incorporated into the decision making process for choosing a cloud environment. Addressing the needs for appropriate treatment of data may shape decisions about:

- The level of service required
- The contract conditions imposed
- The audit regime adopted
- Restrictions on the physical location of the cloud servers
- Restrictions on the selection of providers by country of registration
- Restrictions on the kind of cloud environment selected (ie. public, private or community).

Agencies should be mindful of their obligations with respect to public sector data in choosing cloud solutions, and focus on selecting providers and services that can deliver quality outcomes in their treatment of agency data.

3. Compliance with legislation, standards and policies

Agency data is subject to a raft of regulatory and policy requirements in terms of how it is to be created, managed, preserved, and disposed of. These requirements are not waived or modified when an agency decides to use a cloud service for delivering storage or data management needs.

3.1. Understand the relevant requirements

It is important to get an idea of what requirements operate on the agency's management of data. Some of these will be state or Commonwealth level, while others may be derived from industry or agency specific legislation or derived from internal decisions of the agency. Areas to consider are:

- Public records requirements
- Privacy requirements
- FOI and legal disclosure requirements
- Transparency and accountability requirements
- Security requirements
- Evidence and evidentiary integrity requirements
- Document disposal and prevention of unlawful destruction or disposal
- Copyright protection.

The Requirements Checklist and Document Map which form part of *Cloud Computing Guideline 2: Cloud Computing Tools* can help with the identification of all-of-government requirements. This list is a guide only and agencies are encouraged to conduct their own research to ensure that specific and unique requirements and policies are captured.

3.2. Identify key questions to support compliance

It might be helpful to phrase requirements as succinct questions, rather than in detailed, dense blocks of text, in discussions with potential providers.

For example, instead of presenting potential providers with the entire set of Information Privacy Principles and seek their compliance, it is advisable to ask, "How do you protect my data from being seen, altered, or deleted by people that I have not authorised to do so?" This approach encourages compliance that is based on active understanding.

4. Risk assessment

Assessing the risks involved in any new enterprise or activity is part of good business practice. Please note that the Department of Treasury and Finance have a *Risk Management Framework* for Victorian government[2]. This framework is in line with the *Australian and New Zealand Standard on Risk Management Principles, Framework and Process (AS/NZS 31000:2009)*.

Before conducting any risk assessments, it is recommended to make use of or factor in any existing in-house methodologies, tools and guidelines.

4.1. Identify and list risks

An important part of assessing risks is to ensure they are identified. As part of this exercise, it is crucial to capture all associated risks through stakeholder consultation, risk analysis and some scenario planning. (Guideline 2 provides an editable risk assessment template which builds in the main known risks to data of using a cloud environment).

4.2. Establish how significant they are via a risk matrix

Using a risk matrix, identified risks could be plotted in accordance to their Likelihood and Consequence. This technique is beneficial to allow the assessor to visually see the relationship between risks and their priorities.

Factors to consider in assigning Likelihood are:

- Has the outcome identified in the risk actually transpired for the organisation in the past?
- Has the outcome identified in the risk occurred to other organisations?
- Has the service provider been involved in any outcomes similar to those identified in the risk?
- Identify any “near misses” in which this risk was just avoided?

Factors to consider in assigning Consequence are:

- If the outcome identified in the risk transpired, would it cost a lot of money to repair it?
- If the outcome identified in the risk transpired, would it cause damage to the rights, entitlements or security of Victorian citizens?
- If the outcome identified in the risk transpired, would it cause “front page of the newspaper” political embarrassment or censure for the government?
- If the outcome identified in the risk transpired, would it give rise to legal sanctions or regulatory breaches?

[2] The Department of Treasury and Finance ‘*Risk Management Framework*’ is available from the Department of Treasury and Finance website: <http://dtf.vic.gov.au/CA25713E0002EF43/pages/economic-and-financial-policy-victorian-risk-management-framework>.

It is useful to engage both internal and external stakeholders and take lessons learnt from past cases when assigning Likelihood and Consequence rankings to risks.

Guideline 2 provides sample risk matrix that might be helpful in this step.

4.3. Plan for how risks can be effectively remediated

When selecting remediation strategies, one should be looking for actions, limitations or requirements that will:

- Nullify the risk altogether; or
- Reduce the risk to an acceptable/manageable level

Examples of remediation strategies include:

- Changing the audit protocols to reduce the risk of loss of authenticity
- Adding new contract clauses about privacy protection to reduce the risk of privacy breaches
- Adding a requirement for an off-cloud back up of vital data to reducing risks of inadvertent data loss
- Deciding to not store data with a security classification above a certain level in the cloud to nullify the risk of serious security breaches

5. Coverage of data needs in contracts

Like any business service, cloud computing will involve one or more service agreements or contracts. The nature of these contracts will vary according to the service provided.

5.1. Make sure that agreements and contracts cover all required areas

Guideline 2 includes a contract checklist, which agencies can use to make sure that all the essential restrictions and requirements are included. Contracts should identify:

- Who owns the data
- Access requirements (Who can access the data, when, how, and why)
- Security and privacy
- Jurisdiction and location

The agreement should identify the physical and legal location of the service provider, and any restrictions on where agency data will physically be stored. For example, if choosing a provider with servers in multiple countries, the agreement should express any limitation on where agency data will go – which might include limiting it to Australia, or excluding certain countries from the list for legal requirements reasons.

Preferably, the agreement should specify the jurisdiction in which the agreement is enforced and how dispute settlement will be resolved. Selecting providers that are either Australian companies or have a subsidiary in Australia may offer greater protection in this regard.

6. References

Legislation

Crimes (Document Destruction) Act 2005
Electronic Transactions Act 1999
Evidence (Document Unavailability) Act 2006
Health Records Act 2001
Information Privacy Act 2000
Public Records Act 1973

All current Victorian legislation is available at http://www.legislation.vic.gov.au

Policies and Guidelines

Australian Government Information Management Office (AGIMO) 2012, *Community Cloud Governance: Better Practice Guideline*, AGIMO Canberra, accessed January 2013 <http://agimo.gov.au/policy-guides-procurement/cloud/>.

Australian Government Information Management Office (AGIMO) 2012, *Financial Considerations for Government Use of Cloud Computing*, AGIMO Canberra, accessed January 2013 <http://agimo.gov.au/policy-guides-procurement/cloud/>.

Australian Government Information Management Office (AGIMO) 2012, *Negotiating the Cloud: Legal Issues in Cloud Computing*, AGIMO Canberra, accessed January 2013 <http://agimo.gov.au/policy-guides-procurement/cloud/>.

Australian Government Information Management Office (AGIMO) 2012, *Privacy and Cloud Computing for Australian Government Agencies*, AGIMO Canberra, accessed January 2013 <http://agimo.gov.au/policy-guides-procurement/cloud/>.

Department of Treasury and Finance Government Services Division (DTF GSD) 2012, *Victorian Government Information Security Policy and Guidelines*, DTF GSD Melbourne, accessed January 2013 <http://www.egov.vic.gov.au/policies-and-standards/security-policies-and-standards/victorian-government-information-security-policy-standards-and-guidelines.html>.

Department of Treasury and Finance (DTF) 2011 Risk Management Framework, DTF Melbourne, accessed June 2013, <http://dtf.vic.gov.au/CA25713E0002EF43/pages/economic-and-financial-policy-victorian-risk-management-framework>.

National Archives of Australia (NAA) 2012 *Records Management and the Cloud*, NAA Canberra, accessed January 2013 <http://www.naa.gov.au/records-management/agency/secure-and-store/rm-and-the-cloud/index.aspx>.

Public Record Office Victoria (PROV) 2013, *PROV Cloud Computing Guideline 2: Cloud Computing Tools*, PROV North Melbourne, accessed January 2013 <http://prov.vic.gov.au/government/standards-and-policy/policies/cloud-computing>.

Public Record Office Victoria (PROV) 2013, *PROV Cloud Computing Policy,* PROV North Melbourne, accessed January 2013 <http://prov.vic.gov.au/government/standards-and-policy/policies/cloud-computing>

Standards

Public Record Office Victoria (PROV) 2010, *PROS 10/10 Strategic Management Standard*, PROV North Melbourne, accessed January 2013, <http://prov.vic.gov.au/government/standards-and-policy/strategic-management>.

Public Record Office Victoria (PROV) 2010, *PROS 10/13 Disposal Standard*, PROV North Melbourne, accessed January 2013, <http://prov.vic.gov.au/government/standards-and-policy/disposal>.

Public Record Office Victoria (PROV) 2010, *PROS 10/17 Operations Management Standard*, PROV North Melbourne, accessed January 2013, <http://prov.vic.gov.au/government/standards-and-policy/operations-management>.

Public Record Office Victoria (PROV) 2011, *PROS 11/01 Storage Standard*, PROV North Melbourne, accessed January 2013, <http://prov.vic.gov.au/government/standards-and-policy/storage>.

Public Record Office Victoria (PROV) 2011, *PROS 11/07 Capture Standard*, PROV North Melbourne, accessed January 2013, <http://prov.vic.gov.au/government/standards-and-policy/capture>.

Public Record Office Victoria (PROV) 2011, *PROS 11/09 Control Standard*, PROV North Melbourne, accessed January 2013, <http://prov.vic.gov.au/government/standards-and-policy/control>.

Public Record Office Victoria (PROV) 2011, *PROS 11/10 Access Standard*, PROV North Melbourne, accessed January 2013, <http://prov.vic.gov.au/government/standards-and-policy/access>.

Standards Australia / Standards New Zealand 2009, *AS/NZS 31000: 2009: Risk Management Principles, Framework and Process*, Standards Australia/Standards New Zealand, Sydney.

Other Resources

P Mell & T Grance 2010, *The NIST Definition of Cloud Computing,* National Institute of Standards and Technology, Gaithersburg, Accessed December 2012, <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>.

For more information about Cloud Computing and public sector data, please contact:

Standards & Policy Team
Public Record Office Victoria
Ph: (03) 9348 5600
Fax: (03) 9348 5656
Email: agency.queries@prov.vic.gov.au
Web: www.prov.vic.gov.au