Risk Assessment for Cloud Transition

Cloud Policy Fact Sheet 4.1

A risk assessment enables an agency to identify the risks and vulnerabilities within your ICT program that could affect adoption of the cloud. A risk assessment allows you to plan and initiate actions (controls) and treatments to address these risks.

Objective

Conduct a risk assessment.

Process

Risk assessment involves evaluating which risks need to be treated, and the selection of the most appropriate risk treatment strategy and controls. This Fact Sheet provides a guide for what to consider during your agency's risk assessment of the transition to the cloud.

Conducting a risk assessment is essential to identify existing and new risk factors which can emerge during the transition to the cloud or due to the adoption of cloud services.

Initialise risk assessment

Understand your current situation in terms of how information is stored and used and the maturity of internal policies which will assist the migration to cloud and determine your agency's needs. Refer to the Fact Sheet "Situational analysis to inform Cloud transition".

Plan the risk assessment

Planning the risk assessment requires determining the scope, schedule and resources, risk treatment and monitoring strategy based on your current situation and anticipated needs. Risk assessment for the cloud requires reviewing complex migration decisions such as the potential impacts on cost, schedule, business continuity, and identifying key controls.

The risk assessment and management process for migration to the cloud can be undertaken using the agency's existing risk management framework and processes.

Identify and categorise risks

Identifying the risks involves determining as many potential risk factors as possible so that the agency is aware of the possible issues that may arise during or as a result of the migration.

Different risk identification techniques may be useful to use in the different sections of your agency. The ISO/IEC 31010:2009 Risk management – Risk assessment techniques, is a supporting standard that provides useful descriptions of a variety of systematic risk identification techniques.

Risks should be categorised in accordance with their potential impact on the agency's overall business continuity and ability to fulfil its functions.

Categorising risks by the domain or section of the agency that is affected can be useful to identify responsibility for risk control areas or mechanisms. An example of this approach is shown in the

'Table of suggested risks for cloud sourcing' in section 3.2 of Risk Identification in the *ICT-as-a-service risk assessment - guideline* (Queensland Government, 2014).

Assess and control risks through mitigating strategies

This activity identifies the potential actions (controls) for mitigating the risks.

Develop the mitigating strategies and actions to address the risks. This may involve looking at external case studies and relevant policies and legislation as well as your agency's current practices.

Rank the risks and prioritise actions (controls)

Assess the risk and consequence of each risk occurring, taking into account existing controls. The highest priority for action should be given to risks that are evaluated as being unacceptable, these should be treated through improving controls or developing new controls.

Migration decision and risk monitoring

Migrating to the cloud should be based on the agency's understanding of the potential risks and with fully developed control measures for risk mitigation in place. See Table 1 for an example of a risk management matrix populated with some common risks which agencies will need to address.

Your agency's business management frameworks will need to be updated to require ongoing monitoring of the risks and mitigating strategies in place for the transition and the adoption of cloud services.

Offshoring and data classification

Western Australian public sector agencies must give strong care and consideration to the nature and sensitivity of their data, and where it will be stored. Cloud Policy Fact Sheet 1.2 outlines the WA Government's data offshoring position and provides guidance for the public sector.

Protect Intellectual Property

Offshored intellectual property is vulnerable to law enforcement intrusions, theft or misappropriation. These may result in an accidental or wilful disclosure of confidential information and trade secrets. Ensure the mechanisms to protect your agency's information are in the contract and are monitored continuously.

Retrieval of Data

Entrusting data management responsibilities to providers located offshore may render data controls inadequate. Proximity and geopolitical risks may affect the provider's ability to enable rapid retrieval of data (e.g. for administrative purposes or litigation). Ensure the provider stores data in accordance with your agency's accountability requirements and applicable Australian and Western Australian legislation and guidelines.

Know the Provider

Maintain your relationship with the provider and be aware of any changes to ownership or subcontractors or to their risk profile. These may result in inadequate data management controls and compromise the security of the data. Ensure the contract provides contingencies for such changes.

Useful tools

European Commission. Adequacy of the protection of personal data in non-EU countries.

Government of Western Australia:

- Department of Finance. Western Australian Government risk management guidelines for using offshore ICT arrangements to store and process information. November 2014.

- Office of Digital Government. Cloud Policy – Factsheet 3.1 'Understand your current situation'. November 2017.

International Organisation for Standardisation (ISO):

- ISO/IEC 27000 family - Information security management systems
- ISO/IEC 31010:2009 Risk management – Risk assessment techniques - supporting standard for ISO 31000:2009 Risk management – Principles and guidelines.

Queensland Government:

- Queensland Government Chief Information Office. ICT-as-a-service risk assessment guide. February 2014.
- Queensland Government Chief Information Office. ICT Risk Management Table.
- Queensland Government Chief Information Office. ICT Risk management tools and techniques.
- Queensland Treasury. ICT Risk Management Matrix. July 2011.

Tasmanian Department of Premier and Cabinet Office of eGovernment. Tasmanian Cloud Policy. October 2015. 'Appendix 1 - Cloud Risk Assessment'

Related Cloud Policy Fact Sheets

1.2 WA Government Data Offshoring position and guidance

Table 1. Example of a Risk management matrix.

	Risk assumption	Risk category	Mitigating Strategy	Project Actions
1	Time constraints set on implementing cloud migration.		• Develop a prioritised plan	• Use a risk management process to prioritise mandatory principles associated with cloud migration
2	Latency		• Review business continuity and service capacity	• Ensure the project contains elements in its scope to investigate and address any perceived incapacity
3	Portability of the data		• Develop a cloud data approach	• Choose cloud services with multi-vendor adoption • Favour vendors that offer portability and interoperability • Use an abstraction layer in front of proprietary cloud services
4	Data privacy		• Understand the value or sensitivity of the data that will be stored or processed by the agency • Develop data security protocols	• Classify data • Implement an Information Security management system • Review governance and accountability • Assess and treat security
5	Data sovereignty		• Review the requirements of the State Records Act 2000	• Ensure the terms and conditions of contracts meet your obligations under the Act.
6	Data security		• Understand data classification and related security requirements	• Ensure security standards meet ISO27001 – Information Security Standard
7	Service performance		• Ensure the project contains elements in its scope to produce and measure service performance and align penalties to organisational risk	• Ensure service broker agreements address service performance criteria for the agency
8	Service downtime		• Plan appropriate measures for acceptable downtime and penalties	• Build a Disaster Recovery Plan for business continuity
9	Cost of the service		• Review current expenditure vs cloud	• Conduct a TCO – see Factsheet 'Conduct a total cost of operation comparison'
10	Legislative environment		• Review legislative requirements including polices and Premiers Circulars	• Ensure internal policies are up to date and reflect the legislative requirements
11	Lack support from the business unit		• Senior Management to provide visible commitment to the approach.	• Ensure adequate education, awareness and understanding of cloud migration risk management and its application to the agency's business environment. • Seek senior management intervention

Table 2. Examples of other risks associated with offshoring.

Protection of Information

- Privacy
- Security
- Confidentiality
- Records management requirements
- Ownership of records
- Custody of records
- Retrieval of records
- Disposal of records
- Auditing
- Compensation for data loss/misuse
- Appropriate approvals

Liability

- Limitations on liability
- Indemnity

Performance Management

- Service levels
- Response times
- Flexibility of service
- Business continuity and disaster recovery

Ending the contract/exit strategy

- Early termination fees
- Termination for default
- Provider's right to terminate
- Legal advice on termination
- Disengagement/transition of services

Other risks

- Change of contract party
- Application of foreign laws
- Intellectual property ownership

Managing the contract

- Understanding the contract terms
- Enforcing the terms of the contract
- Auditing the provider
- Maintaining a relationship with the provider
- Awareness of contractual rights and obligations
- Seeking legal advice if necessary