Government of Western Australia
Department of the Premier and Cabinet
Office of Digital Government

Risk ssessment for loud ransition

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 contneui2.437 (s)83 (t)- ion oo 0 Tdβatappruulⁱ(ul)2.618ratm29-

‘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.

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 –

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		•	

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

-