Situational Analysis to Inform Cloud Transition

Cloud Policy Fact Sheet 3.1

When planning transition to the cloud, it is essential you understand your agency's current situation. Identifying how information is stored and used and the maturity of internal policies will assist your planning process. Performing this analysis will align the transition to cloud with your business strategy and ensure cloud products and services are a fit for your agency's purposes.

Objective

Assess your agency's workloads and maturity of existing policies and systems.

Process

To plan for your agency's cloud transformation, you will need to gain an understanding of where you are starting from to inform the planning process, address any gaps and determine your agency's needs. Your assessment should consider the following issues.

How does the transition align with your agency's purpose and objectives?

To successfully transition to cloud, business managers need to drive and support the transition by developing policies that inform and allow ICT to enable cloud transformation.

- What are the business priorities for your agency? Define the desired business outcomes and align the transition to the cloud workload with your business strategy.
- Are there existing internal policies which address ICT procurement? Are current policies adaptive and flexible to allow for the agency's needs when procuring cloud services.
- Capability of internal systems and polices to guide migration– which supporting functions within your agency need to lift their maturity to support adopting public cloud services, in particular data classification, disaster recovery and digital security.
- Is cloud transition reflected in your ICT budget and is it flexible to allow for unexpected costs? If not, how can this be accommodated?
- Are there potential savings for your agency that will result from moving to the cloud? Capturing the current costs and estimating future savings is important for your business planning and ongoing reporting.

Where is your data stored and how is it managed?

- What internal policies determine how your data is managed, is there a data management policy?
- What is the current level of storage you are using and what types of storage do you use?
- What are the costs associated with your data centres and servers?
- How much data do you create and store on a daily, monthly, and yearly basis, and how fast is that growing?
- What kind of databases do you currently employ?

What processes are used for classification of your data?

Understanding the classification of your data is vital as the suitability of certain cloud providers is dependent on how the data is classified. Sensitive and classified data may be subject to privacy and data sovereignty laws which will determine how and where the data can be stored. See the "WA Government Data Offshoring position and guidance" fact sheet for further information.

Disaster Recovery

Citizens expect Government to continue delivering services and products despite disruptive events. Meeting this expectation is an essential capability of Government which does not diminish through the transition to the cloud.

Disaster recovery planning provides a platform to ensure your agency's critical business functions and services are maintained with minimal interruption.

Disaster recovery is an important consideration in planning your agency's transition to the cloud. You should assess the maturity of your current policies and processes, and ensure you have identified and prioritised critical business ICT services, assets and information exchanges provided by, or to other agencies or external parties.

The ICT Disaster Recovery for Business Continuity Policy and supplementary guide will assist your agency to assess or develop your disaster recovery plan.

Digital Security

Agencies are custodians of important information about the State, businesses and citizens, and have a moral and legislative obligation to safeguard these assets. For the community to fully utilise digital services, agencies must be trustworthy custodians of information.

Digital security is an important consideration during your transition to the cloud. In gauging the current situation, you should consider your information security management systems, risk registers and the governance processes currently in place to compare with the security provided through maintained infrastructure.

Determine the current cost of operation

A Total Cost of Ownership (TCO) is a tool designed to determine the direct and indirect costs of a product or system against their current operating model. A TCO not only considers the costs of software acquisition, staff and maintenance but other hidden costs which are not normally considered, for example electricity, cooling, staff training and IT footprint.

In assessing your agency's current costs, using TCO will produce a financially accurate starting point to compare with the estimated costs of cloud services. This will help your agency's business planning and ongoing reporting.

The Factsheet "Undertake a total cost of ownership for transition to the cloud" provides further information on conducting a TCO.

Consider learnings from previous cloud deployments.

Where other agencies have successfully transitioned to cloud, there are opportunities for you to learn from their experiences. The Factsheet "Western Australian government case studies in cloud transition", documents the experiences of other WA government agencies in transitioning to the cloud. The case studies discuss their drivers for adopting cloud, the benefits and pitfalls and key learnings.

Useful tools

Office of Digital Government, April 2017. Whole of Government ICT Disaster Recovery for Business Continuity Policy

Office of Digital Government, April 2017. Whole of Government ICT Disaster Recovery for Business Continuity Policy: A supplementary guide.

Insurance Commission of Western Australia (ICWA). Risk Management Guidelines and Business Continuity Guidelines.

Office of Digital Government, June 2017. The Western Australian Whole of Government Digital Security Policy. Government of Western Australia, Perth.

Office of Digital Government, June 2017. Whole-of-Government Digital Security Policy - A supplementary guide. Government of Western Australia, Perth.

Related Cloud Policy Fact Sheets

1.2 WA Government Data Offshoring position and guidance

5.2 Undertake a total cost of ownership for transition to the cloud

8.2 Western Australian government case studies in cloud transition