DPC/G3.4

ACROSS GOVERNMENT POLICY

Cloud services planning guideline

Introduction

Cloud services present many opportunities, including the potential to reduce electronic storage and internal ICT capital investment requirements.

For any business transformation project, standard considerations and processes include elements such as project planning, technical specifications, budget and risk. For cloud services, there are additional considerations. This series of cloud services guidelines articulates those considerations.

Purpose

This guideline covers a broad range of subject areas. It is intended to assist in the planning process especially for those agencies who have less experience in leveraging cloud services. For others who are more experienced it may act as a useful check list. Importantly, the guideline encourages agencies to consider all these areas in the early stages of planning.

Guidance

Approach

When considering cloud services, it is important to correctly identify real concerns without creating barriers based on fear of new technology. You can do this effectively by learning from others' experiences, thoughtfully selecting the service and model for deployment that best fits your agency's risk tolerance, taking an agile approach to development and creating relationships with trusted vendors.

Identifying Opportunities

Cloud services need to align with an agency's business and ICT strategies. They also need to align with across government strategies and policies, for example, information security.

Legacy system replacement, technology refreshes and new service development provide good opportunities to consider cloud services.

For those experimenting with cloud services, an easy, low risk pilot is a good starting point. Using an agile delivery approach, agencies can quickly learn what works and what doesn't. Taking an iterative approach allows successful pilots to move through project stages without delay. Iterating also creates learning for other projects.

Your activity may be well suited for cloud services if any of the following are true:

- you need to reach your users anywhere they are via the Internet
- you are building a customer-facing service that requires wide scalability
- you need to build a highly available and highly distributed network
- you require the ability to quickly build servers
- you have no current physical footprint or data centre
- you don't have the time, core skills or resources to manage your own ICT infrastructure
- you have robust and reliable options to connect to cloud service providers.

Your activity may not be suited for cloud services if any of the following is true:

- your data classification requirements mean that your data is not allowed to leave a local network
- your data classification requirements exclude appropriate certified cloud providers (eg those that that have no on shore facilities)
- your applications are not cloud-ready as they have unsuitable hosting requirements or weren't designed with the cloud in mind
- the Total Cost of Opportunity for a particular cloud solution outweighs the benefits
- the timing is not right and cloud migration creates a conflict of priorities
- your organisation does not have the skills required for the cloud.

There is increasing opportunity for agencies to share information as cloud services mature. Even where business requirements vary, shared experiences can be valuable.

Choosing a Cloud Service and Deployment Model

There are three cloud service models:

Model	Potential Advantages	Potential Disadvantages
Software as a Service (SaaS) Providers' applications running on cloud infrastructure are accessed through thin-client (eg web browser) or program interfaces	• Easy technology setup • Rapid deployment • No upfront capital investment • Typically stable software • Most cost-effective model as only the software is leased	• Little control over deployment, upgrade and testing methodology • Likely limitations on amount of customisation and tailoring • Data privacy issues and difficulties in return of customer data • Integration can be difficult and unsupported (although this is becoming less common with the rise of open APIs)
Platform as a Service (PaaS) Customer-created or purchased applications are deployed onto a provider's cloud infrastructure	• No need for capital hardware investment • Rapid deployment • Support for integration	• More management effort due to responsibility for application updates and upgrades • Likely to be a shared platform, requiring security considerations • Data privacy issues • Not as cost effective as SaaS
Infrastructure as a Service (IaaS) Computer infrastructure (processing, storage, networks etc) are provided to the customer, to deploy their own software applications	• Removes the need to buy, house and maintain physical servers • Ability to respond quickly to changing demand • Greater level of control over Virtual Machine • Simplifies integration	• Most expensive • Responsibility for Virtual Machine Management • Need for new skills sets and regular training program to keep step with technology changes • Responsibility for backups

There are four common deployment models:

Model	Potential Advantages	Potential Disadvantages
Private cloud Cloud infrastructure is provisioned for exclusive use by a single organisation comprising many consumers	• More control • Good data security and compliance	• Typically more expensive • Lower economies of scale • Lower resilience
Community cloud Cloud infrastructure is provisioned for exclusive use by a community of consumers	• Economies of scale • Fair data security and compliance	• May require changes to existing processes/practices • Shared 'sovereignty'
Public cloud Cloud infrastructure is provisioned for open use by the general public	• Ease of access, service on demand • Economies of scale • Scalability/agility • Higher resilience	• Compliance and data security risks • Can be less reliable
Hybrid cloud Cloud infrastructure is a composition of two or more distinct cloud infrastructures	• Combination of above	• Combination of above

When choosing a model:

- identify the business and performance requirements using a user centred design approach such as the User Centred Design Toolkit
- understand the sensitivity of your data and classify it appropriately
- understand your agency's risk tolerance and develop scenarios to understand the benefits and risks of potential cloud models, especially to determine the requirements for security, privacy and controls
- consider your agency ICT strategy and its priorities
- consider how the cloud service will co-exist with your other ICT service delivery models
- consider the skills available to you and what skills will need to be brought in.

Technical Barriers and Interoperability/Integration

Consider the potential synergies with and impacts to existing technical architecture and infrastructure.

Cloud services may need to share data between applications/services. As cloud adoption progresses, there may be a need to exchange data between different cloud services and with legacy applications within an agency or across government. Architecture decisions may influence the choice of deployment options to reduce integration effort and costs.

Network Requirements

Guidance on the choices and considerations for utilising external and internal government networks is provided in the Cloud Computing Network Guideline.

Business Continuity and Needs

Business continuity and disaster recovery plans are required to manage sustained interruptions to service availability. You should confirm that a provider's business continuity and disaster recovery capabilities meet your needs.

For subscription-based services, you should ensure that subscription levels reflect requirements and are readily scalable up and down according to demand.

Data

Before selecting a model, you must understand the security, privacy, sensitivity, access and regulatory requirements of your data. The data that is to be processed, transmitted and stored by a business application should be classified in accordance with the Information Security Management Framework's classification requirements.

Only then can you accurately assess security and privacy risks and confirm the correct cloud deployment model to meet compliance requirements. This classification will also determine whether encryption is required to protect data in transit or at rest (in storage).

Where using the cloud means sharing infrastructure (in multi-tenant situations), you should consider whether your business information should be segregated from that of other customers.

Adequate controls will need to be in place to ensure the security and privacy of your information. Access should be managed and granted to individual users and periodically reviewed by the business owner or delegated authority. In most circumstances, user access and any potential security or privacy violations should be audited.

Other considerations for managing data in the cloud include appropriate backup and recovery processes. The service provider should maintain regular copies of all hosted data and be able to execute restore mechanisms at any point in time.

Further guidance for data and information can be found in:

- ISMF Guideline 8a: An approach to classification using the ISMF
- ISMF Ruling 2: Storage and processing of Australian Government information in outsourced or offshore ICT arrangements
- Off-site storage of SA Government data – executive guidance

Assurance

Conventional ICT service providers often have audits conducted on their systems, either by the customer or through the use of independent third-party auditors. Audits of cloud services may not be possible unless it is included as a term of the contract. It is important that any regulatory and assurance requirements are understood before entering into a contract.

Business Case

A business case for a cloud service should consider all of the elements required by a standard business case.

The business case should emphasise how the various deployment options contribute to achieving service delivery outcomes. It should outline all options, and provide an analysis of all costs (including the pricing model) and benefits for each option.

Common benefits that may be appropriate to include are:

- reduction of ICT infrastructure/reduced capital costs
- rationalisation or optimisation of infrastructure
- standardisation
- reduced implementation effort
- volume discounts.

Costs

Cloud services may be a low-cost option if they reduce the need for ICT infrastructure. However, an understanding of all operating costs will verify whether this is the case. Consider whether the application has a high data transfer requirement. Heavy reliance on networks and increased data transmission will add to an agency's costs.

The cost model needs to allow for unexpected peaks in demand and for scaling and changes to the service. Pricing needs to be transparent, especially for subscription-based licenses which, given the adoption and elasticity of cloud services, may vary considerably over time.

Consider the ongoing cost of data storage and data growth and costs relating to the decommissioning of exiting services.

A sound business case will ensure that the financial analysis identifies all costs when comparing proposed delivery options. It is most important to understand the Total Cost of Ownership (TCO), by identifying categories of spending and types of costs, including the obvious and the hidden costs, for example:

	Acquisition Costs	Operating Costs	Change Costs
Software	Obvious costs	Obvious costs	Hidden costs
Hardware	Obvious costs	Obvious costs	Hidden costs
Staff	Hidden costs	Hidden costs	Hidden costs
Communications	Hidden costs	Hidden costs	Hidden costs
Facilities	Hidden costs	Hidden costs	Hidden costs

For additional guidance on financial considerations refer to Cloud Financial Guideline.

Procurement

Normal requirements apply, including compliance with existing government procurement standards. However, applying an agile, minimum viable product approach may lessen the time and expense of an otherwise traditional large-scale procurement.

Contractual Terms

Consider your agency's contractual approach and needs before approaching the market.

Due to the (commodity) nature of their services, many cloud providers will have standard 'set' agreements. Being clear up front about your contractual requirements will provide a starting point for negotiating terms and conditions.

Careful evaluation of cloud provider contract terms is essential, including where the data is stored, provisions for reclaiming data from the provider, ownership and use of the data, and confirmation that the contract is agreed under Australian jurisdictional laws.

Exit Strategy

Ensure you have adequate contingency plans in case you, or other parties, need to terminate the service. Your plan will need to address likely business scenarios and should cover elements such as:

- business continuity
- the frequency of regular back ups
- migration of data to another solution
- exit costs
- damages.

For PaaS or IaaS models it should investigate the ability to move an application to another vendor or in-house.

Service Level Agreements

Depending on the cloud service model selected, the amount of control you have over your services may vary.

Expected levels of responsiveness, throughput, availability and reliability, and redundancy should all be part of the Service Level Agreement (SLA) with the cloud services vendor.

You should confirm that the SLA addresses adequate system availability, downtimes and scheduled outages, and that these are acceptable in terms of timing and duration to support business processes.

The SLA should also consider the availability and flexibility of support arrangements. For example, can the vendor increase the level of resources at short notice?

Business Process Impacts & Change Management

It is difficult to imagine a service transformation project that would not need a concerted change management program.

You will need to understand the business as well as the technological impact of cloud opportunities.

Some aspects that may change or cause concern to stakeholders, include:

- how enterprise information is managed and stored
- shifting staff roles and skills
- relationships with and dependence on vendors and other third parties
- reduction of control over services
- customer service/quality
- privacy and/or compliance concerns.

A good change management program based on keeping stakeholders actively informed and addressing their concerns will improve the likelihood of success of service transformation.

There are a range of tools that can assist you with engagement, including Better Together: Principles of Engagement and the User Centred Design Toolkit.

Skills Capability

Developing and implementing cloud services requires a greater focus on service skills. These include:

- project and program management
- business analysis
- architecture design and management
- procurement management
- contract management
- relationship management
- service design and service management.

Plan for sufficient resources to fill management roles that will oversee activities such as testing and ongoing operations. Other technical skills such as database management and configuration management may be provided by the vendor or may remain in-house.

If you do not have the required skills available in-house, consider training staff or contract the skills in, but make sure skills are transferred to staff. Include these costs in your business case calculations.

Governance

Consider existing governance frameworks and arrangements to ensure that the structure, responsibilities and controls for the project and ongoing services are adequate. It is likely that cloud services may need new roles and responsibilities that have not traditionally been in place.

It is critical to ensure management of ongoing costs as it is easy for these costs to escalate if controls are not in place.

Governance should consider six areas – accountability, transparency, integrity, stewardship, efficiency and leadership.

Management and Monitoring

Consider the extent to which you will be able to monitor the cloud services versus how much the vendor may monitor, administer or manage hardware, software and data.

Will you have the ability and capability to:

- use your/their tools for integrity and security checking and for network management?
- manage faults and fault response activity around incidents and service disruption?
- analyse, plan and implement configuration changes?
- coordinate planned upgrades or outages?
- adequately provide assurance in areas such as business continuity and disaster recovery?
- ensure that security and privacy breaches are reported and managed?

Where the vendor is selected to carry out these activities, is there adequate security and monitoring of computers that share or process data?

Reporting

When implementing cloud solutions, it is important that you establish the frequency and format of reporting. Regular reporting needs to support business objectives and measure business performance, especially to understand elements such as resource utilisation, throughput, availability and other measures of Quality of Service.

References, Links & Additional Information

Links to various guidelines and papers, including those relevant to planning can be found on the Cloud policy and guidelines page.

Document Control

ID	DPC/G3.4
Version	1.1
Classification/DLM	Public I1-A1
Compliance	Discretionary
Original authorisation date	December 2016
Last approval date	March 2018
Next review date	March 2020