New Zealand Government

GEA-NZ Guide: Managing Shadow Cloud Services

Version 1.0 (May 2018)

Document Control

Title	GEA-NZ Guide: Managing Shadow Cloud Services
Author	Phil Cutforth MBE MSc, AoG Enterprise Architect, GCDO Andrew Stephen, AoG Enterprise Architect, GCDO
Document Classification	UNCLASSIFIED

Revision History

Version	Date	Author	Description of changes
0.5	21/7/17	P Cutforth, A Stapleton	Final review, editing and proof-read. Beta Publish on PSI.
1.0	31/7/17	P Cutforth, Dr C Roberts	Approved for publishing.
1.01	28/9/17	A Stapleton, S Davies	Review for readability
1.02	4/5/2018	A Stapleton, A Stephen	Review for tone and consistency with other guidance

Document Approval

Approved as providing guidance in-line with AoG policy.

Name / Role	James Collier, Government Enterprise Architect, Department of Internal Affairs		
Signature		Date	

Contact us: Enquiries regarding this document are welcome to contact:

Government Enterprise Architect
Department of Internal Affairs
PO Box 805, Wellington 6140, New Zealand
email: gcio@dia.govt.nz

Overview

Purpose

The purpose of this guidance is to provide government agencies with a framework to address the use of "shadow cloud" in the context of Government's intent to accelerate the use of public cloud services.

Audience

This guidance is for anyone responsible for their agency's technology strategy or policies.

Structure

Part A of this guidance describes the context surrounding the use of shadow cloud and provides a view of benefits and risks. It is most useful for people involved in governing and managing digital services.

Part B describes the shadow cloud framework and has additional detail for practitioners, including recommendations for: developing policies, creating awareness and training programmes, gaining visibility of services already being used, assessing risks from using these services, enforcing policies, and monitoring, reporting and improving practices.

Learn more

Find the latest cloud guidance on digital.govt.nz, including briefing notes for accelerating the adoption of public cloud services, or talk to your Department of Internal Affairs (DIA) Relationship Manager.

Part A: Managing shadow cloud

Managing shadow cloud

This part provides an overview of the Shadow Cloud Management Framework for people involved in the governance and management of digital services.

What is shadow cloud?

Public cloud services are applications or services delivered over the internet that are offered for use or purchase to anyone who chooses to do so. "Shadow cloud" refers to public cloud services that employees use without organisational knowledge or approval.

Shadow cloud exists for many reasons. Agency employees who have used public cloud services in previous jobs or at home often see the opportunity to use them to enhance their work. They may not consider potential risks from the use of these services, such as SurveyMonkey or Dropbox.

Shadow cloud is one aspect of the user-led, ad hoc adoption of technology known collectively as "shadow IT." The use of personal mobile devices for business purposes is an example of shadow IT. Employees began using their own devices for work purposes without the knowledge or approval of their organisation's ICT function.

At first this was seen as dangerous and was discouraged. As the benefits of allowing this use became clearer organisations found ways to embrace it, manage it and to mitigate the risks that it might present. This is known today as "Bring Your Own Device" (BYOD) and is an accepted practice in most modern workplaces.

> ***The goal for managing shadow cloud should not be simply to minimise its risks, but to exploit its benefits.***

Unmanaged shadow cloud, like unmanaged shadow IT, can pose risks to agencies. But when properly managed it provides an opportunity to improve employee engagement, gain efficiencies, and manage the associated risks. The goal for managing shadow cloud should not be simply to minimise its risks, but to exploit its benefits.

To enable digital transformation it is important to recognise that shadow cloud adoption by employees is not only inevitable but also empowers employees to create business value. Forward-thinking CIOs are seeking more effective ways to partner with the business to better manage shadow cloud services.

Given the increasing importance of and dependence on technology, agencies should assess the extent of shadow cloud in their organisation, communicate the opportunities and risks, and identify appropriate steps to address the issue.

Drivers for shadow cloud adoption

Widespread use of shadow cloud services within an organisation might arise from perception that the ICT management function is slow to respond, slow to innovative, unwieldy or just doesn't understand business or project imperatives.

In response to this perception:

- business leaders have seen shadow IT as a way to innovate and improve their business. They see shadow cloud as delivering similar value through more powerful, efficient and less expensive options for business
- project teams adopt shadow cloud to achieve project goals and outcomes quickly, easily and cost-effectively
- staff and contractors use shadow cloud services to help their productivity (they are easy to acquire and use, require minimum learning time/effort, and can be procured with a credit card on a pay-as-you-go basis for just as long as needed).

> ***Shadow cloud is becoming seen to deliver real value through more powerful, efficient and less expensive options for business.***

In these scenarios the business unit or project team might bypass ICT management if they are perceived to be slow or inefficient. They may not take into account the need to manage information safely, comply with legislation and policies, and ensure that other ICT systems and networks can cope with the additional capacity required.

However, the CIO is ultimately responsible for ensuring that the enterprise uses technology safely, effectively and efficiently. The challenge for ICT is to help business units and project investment cases to deliver the desired business capability within timeframes and budgets. Embracing and governing the use of shadow cloud can help meet these expectations. A joint funding approach between business and ICT can help business units achieve their desired outcomes without stretching ICT budgets.

Benefits of managing shadow cloud

The key benefits realised from proactive management of shadow services typically include:

- better risk management through consistent security and assurance practices
- improved user experience by giving employees access to services that are familiar from outside the workplace
- greater innovation by encouraging digital culture practices of experimentation and innovation
- reduced duplication of cloud services used by employees procuring similar or the same services separately and without coordination.
- better information management by implementing an enterprise-wide approach to managing data across multiple cloud services.
- in some cases cost savings may be achieved as a result of better management and reduced duplication of services.

People are familiar and comfortable with using public cloud services at home and in their social lives. This leads to strong user motivation to integrate the same services into their workplace and use them for the benefit of their agency. By providing familiar cloud applications in the workplace we create a better end-user experience for both employees and customers, while also embedding a digital culture into work practices.

Government's digital transformation relies on agencies fostering rapid experimentation and innovation. Cloud services allow project teams to experiment, prototype quickly and learn fast. We must identify what risks are acceptable when planning prototype environments, and manage them appropriately. This can be managed by using segregated development environments and using sandboxing techniques, rather than by enforcing comprehensive risk and security management procedures and practices.

Government's digital transformation relies on rapid experimentation and innovation.

Business units benefit from the CIO's ability to help them achieve outcomes by proactively assessing and recommending user-friendly cloud services that meet the organisations' needs and risk appetite.

Risks from using shadow cloud

Easily consumed public cloud services such as SurveyMonkey, Trello and DropBox have blurred the lines between personal and business applications. While shadow cloud applications often have valid use cases, their increasing use has a number of implications, such as:

- data loss or compromise from poorly designed, poorly managed or malicious services exposing the organisation's data or infrastructure to unforeseen risk,
- data loss due to the information becoming distributed across multiple services and less accessible across the organisation (this can also lead to data loss through the cessation of service, the movement of employees and the loss of knowledge of where data is located)
- increased cost due to using multiple public cloud services for the same function, which can be costly to support and may not allow for volume pricing (other potential costs include restoration, recovery and remediation operations if a cloud service compromises organisational information or infrastructure).

People are increasingly using public cloud services for both business and personal purposes from agency networks, agency devices and approved personal devices (BYOD). Agencies may have had little visibility or control over what services are used, what data is stored in these applications and have few commercial assurances over availability of their data. This has led to uncertainty about the associated risks.

It is useful to acknowledge that a distinction can be drawn in the use of shadow cloud services by agency employees between business needs and personal use. This can be more difficult when social media is used for agency communications, marketing and media presence as well as personal use.

In practice, there may be at least four categories of use of public cloud services:

- individual personal use, no business context or content such as Facebook or TradeMe
- individual work use such as using a web-based 'to-do' application
- business unit use, but not sanctioned or managed by the agency such as the communications team using (possibly free) online event management or presentation builder services
- supported enterprise cloud services such as online survey services, approved for use across the agency and managed by the agency.

Taking a positive approach

Recognise that the benefits from use of well managed shadow cloud are a positive aspect of a digital culture.

The first step towards managing shadow cloud is to identify the extent of current use of shadow cloud and to communicate both the opportunities and risks this represents to senior leaders. Reflect this in appropriate policies, recommendations for managing the associated risks. Consider how you might streamline support services that make it easier to quickly and safely adopt new cloud services.

Apply this framework in a way that makes sense for your agency and expect incremental improvement.

Additional measures agency CIOs may take include:

- encourage business unit heads and others to ensure their employees take the necessary action to follow policies,
- create a 'cloud adoption' team inside the organisation from employees across multiple functions (for example Risk, IT, Finance, HR, Legal, and Procurement),
- Use the guidance from the Government Chief Digital Officer (GCDO) and this framework to develop an agency shadow cloud management plan and framework.

Embedding these good practices into your agencies will not be achieved overnight. Apply this framework in a way that makes sense for your agency and expect incremental improvement. Maturity takes time and practice.

Cloud services marketplace

Using the GCDO's marketplace for cloud services will further improve agency user experience and ease the adoption of public cloud services. The marketplace aims to reduce costs and the time taken for procurement and security certification of cloud services. It will also:

- provide a catalogue of recognised cloud services, simplifying downstream agency security and risk activities
- ease the cloud service lifecycle management requirements for agencies
- ensures demand, usage and costs can be monitored
- provide a view of service management information at a government and agency level, covering demand, consumption and supplier capability.

The marketplace is an alternative to agencies managing their own self-service application catalogue or portal, particularly where agency practices are not considered mature in this area.

Addressing common issues

Agencies should consider the following approaches to address common issues associated with shadow cloud.

A legitimate business process may be blocked or removed by accident during the triage phase. To manage this, work with the business unit to ensure their needs are met. Ensure risks are still acceptable and there is a plan to recover data and business outcome.

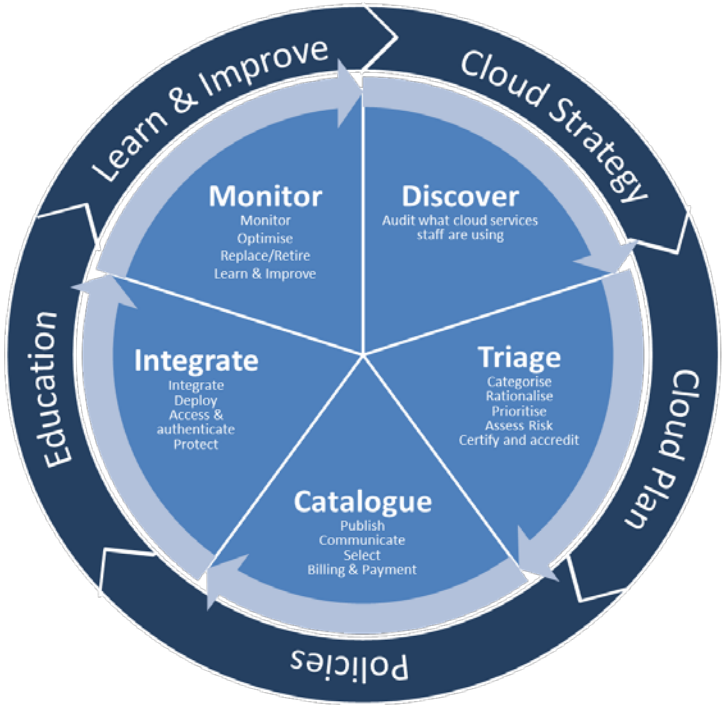
Not enough resources to conduct comprehensive risk assessments. Triage and prioritise identified cloud services based on business need, information value and potential impact to organisational processes. During triage you are unlikely to have the evidence needed for a full risk assessment, but this can be refined over time. Identifying, recording and accepting the risk of immature risk management practices in an initial period may be appropriate.

Users complain that the ICT or Risk team are slowing down the uptake of services. Assess business priority during the triage stage. Ensure your processes and approach are risk-based and internal processes are as streamlined as possible.

New shadow cloud services are constantly being added. Declare an amnesty on shadow cloud usage and seek to prioritise those shadow cloud services having the greatest impact on your business, for example have the most users, consume the most agency data, or have the highest procurement cost. If necessary, start with a strong cloud policy to reduce shadow cloud uptake while you tackle the backlog of unassessed services.

Fast-track process

The complete Shadow Cloud Management Framework consists of five governance and five management processes. These provide a complete and robust framework for ensuring an agency's use of public cloud services is appropriate and risks are managed.



Shadow Cloud Management Framework

Most agencies will already have widespread use of shadow cloud services. Starting with a fast track approach might be useful for proving the value of managing shadow cloud, gaining short-term benefit while the shadow cloud management capability is being developed, or as a scaled approach for smaller, more agile agencies.

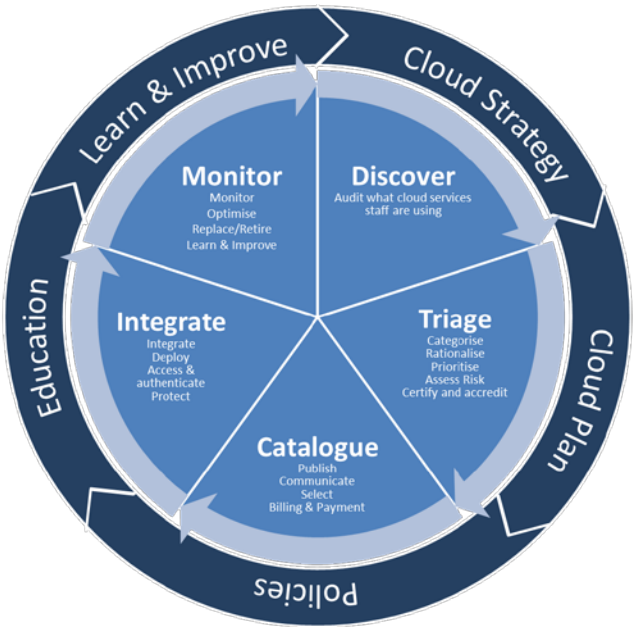
- Start with *discovery* and keep the *triage* and *catalogue* stages simple. Build categories over time and ignore duplication.
- Minimise the risk assessment effort during *triage* and use the information gathered during *monitor* to improve risk assessment.
- Use the information from the *monitor* stage to inform subsequent strategy and policy development later, or in parallel.
- Although the catalogue is a key enabler in a mature organisation, it can be considered as a later deliverable.

As your shadow cloud management capability matures, you can work towards a more complete use of the full framework in areas where it makes sense.

Part B: Shadow cloud management framework

Introduction

Agencies should aim to proactively manage shadow cloud across all business units and functions, for users at all tiers, and across all enterprise technology capabilities. Addressing shadow cloud will require many agencies to implement a new framework. The framework is composed of two ongoing processes: a governance process and a management process.



Shadow Cloud Management Framework

Applying a shadow cloud management model enables ICT teams to:

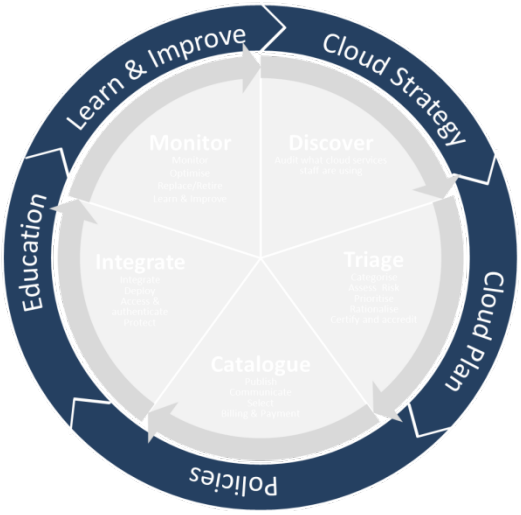
- improve agility by providing faster assessment and deployment of cloud services, such as through appropriately-scaled approval processes and a unified catalogue of cloud services
- support business and project teams' needs and timeframes, and investment case submissions
- provide better options by allowing agency users to participate in selection and management of cloud services
- better manage business systems and information through consistent application of enterprise IT and security profiles across all IT services, including cloud services (i.e. public cloud services are managed to the same level of trust and availability as in-house systems).

Governance

Cloud strategy

The *cloud strategy* should describe the organisation's strategic intent regarding use of cloud services. Shadow cloud should be included in the agency's ICT or cloud services strategy, though some agencies may wish to maintain a specific shadow cloud strategy. It could also be included in an application portfolio/lifecycle management strategy.

Cabinet requires agencies to have a *cloud plan*, which describes how agencies intend to use public cloud services to support major business improvements. This plan should show how cloud services will be used to enhance customer experience, improve effectiveness and efficiency, streamline operations, or create new delivery models.



Shadow Cloud Governance Cycle

Cloud plan and policies

Agencies should provide clear policies on the use of public cloud services for users, business unit managers, and project teams. This may be done by updating or amending existing agency policies, or introducing a specific policy for managing shadow cloud. Your shadow cloud policy should address the themes in this framework and make it easy for users to comply.

Other policies or plans that may be impacted by shadow cloud include:

- human resources codes of conduct
- assurance and risk management frameworks
- internet and social media policies
- information security policies
- BYOD and cloud computing policies
- acceptable use policies
- enterprise architecture frameworks and models.

Ensure ICT service management and delivery policies and procedures are amended to cater for public cloud services. Consider service management, incident reporting and management, procurement, disaster recovery, and business continuity policies.

Education, Learn and Improve

Awareness and education of staff are critical, particularly by using scenario-based examples (user stories) that make the policies relatable. Continuously monitor and respond to the changing ways your people use and procure services and applications that meet their needs.

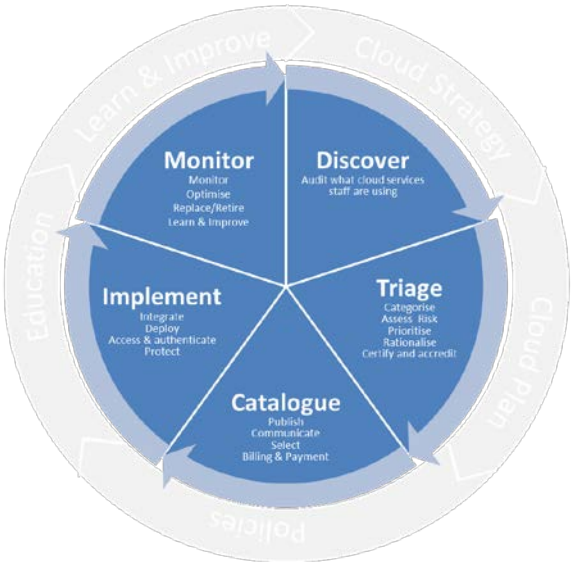
Give employees the information and tools they need to encourage responsible autonomy rather than proscriptive control.

Management

Discover

Begin by identifying the public cloud services that are being used by employees, who is using them, and from which devices and locations in your network. Include applications (SaaS), platform (PaaS) and infrastructure (IaaS) services if possible.

Discovery can be performed by reviewing firewall or router logs, using ad-hoc or automated tools, or through an online service or Cloud Access Security Broker (CASB).



Shadow Cloud Management Cycle

Discovery and monitoring of cloud services usage will enable ICT departments to establish demand profiles and prioritisation.

Full discovery may not be possible if employees are using public cloud services for business purposes from personal devices outside your agency network. By automating cloud service discovery as part of ongoing monitoring you will identify these services as soon as they are accessed from within your environment.

Triage

Triage has several elements and the depth and rigour applied to each stage vary based on an agency's maturity in a number of areas, particularly ICT security and risk management.

Categorise cloud services into the categories used for your existing application and service catalogue. You can also refer to the *GEA-NZ Enterprise Architecture Reference Taxonomies*. Where possible, identify, map and prioritise agency business requirements to identified cloud services. Mapping against the categorisation framework or taxonomy will assist in identifying where the agency may already have approved applications or capabilities in its application portfolio.

Prioritise services for further assessment based on the:

- demand and priority of the cloud service to business units and outputs
- nature of the information being processed or stored by the service
- criticality of the business processes relying on the cloud service.

The GCDO's *Cloud Computing: Information Security and Privacy Considerations* guide describes the attributes to consider in more detail.

Identify cloud services that can be left to business units to manage and which need to go through a formal ICT risk and adoption process. Identify the types of information or business functions are appropriate for use with each cloud service.

As an example, a cloud service used for team scheduling and collaboration, containing only information which can be lost or publically exposed without consequence, would not require a close scrutiny or control. Identify cloud services that can deliver value at low risk as candidates to be brought quickly into mainstream agency use.

Use the information gathered at this stage to plan on-boarding resourcing requirements.

Assess Risk

Understand your agency business priorities, risk appetite and tolerance. Assess risks using a consistent process such as the GCDO's *Risk Assessment Process*. The rigour applied to risk assessment should be appropriate to the business function being supported by the service. Certification and Accreditation may not be appropriate, affordable or even possible for services that are not tightly integrated with other agency ICT systems.

Cloud services likely to be used only for low risk business functions would not require the rigour and effort appropriate for a service handling personal, critical, or classified information. Services that require integration with existing agency ICT systems will require more effort than those that operate entirely independently. Include consideration of the viability of the cloud service provider and their third-party suppliers in your risk assessment.

When using third party frameworks guide risk assessment refer to the *New Zealand Information Security Manual*, Section 5.8, which provides guidance on interpreting the primary industry independent assurance schemes. Some third-party risk assessment frameworks are listed in 0.

Make sure that any residual risk is accepted following your agency's normal risk acceptance procedures.

Rationalise

Discontinue the use of, or substitute, high-risk or insecure shadow cloud services, replacing them with other approved services providing a similar function or outcome.

Using multiple services for the same business purpose might impact people's ability to collaborate or share information. Some services rely on the ability to share and collaborate in order to deliver value. Common examples of this type of service include case management, enterprise reporting or specialist applications.

When rationalising or consolidating services:

- understand the business functions that cloud services are being used to support (how important or visible are the agency services that these business functions deliver?)
- identify services that are widely used across the agency for low-risk business functions and consider keeping these services.
- identify services that are poorly designed or managed and pose unnecessary risk (look for: high cost, lack of IP ownership assurance, no data retention or backup, inability to migrate agency data to a new provider if required, and lack of or unproven DR/BCP capability),
- assess where shadow cloud could affect critical aspects of enterprise performance, such as security, privacy, strategic, or reputational threats, and consider removal/replacement of these services.

Where appropriate, consider a scaled grading or tiered classification scheme for cloud services which differentiates low- and high-assurance services, and clarifies the purposes for which services may be appropriately used. For example, low-assurance services might be used only for unclassified data, team collaboration or development of policies and other artefacts, whereas a high-assurance service might be appropriate for complex or critical business processes, contain personal or health information, or official information that has national security or economic implications.

Catalogue

Establish and publish a catalogue, either through a dedicated cloud services catalogue, or by adding them into the agency's existing application or software catalogues. Communicate the catalogue widely so that employees know where to look first when they need an application or tool.

Each entry in the catalogue should show the current approval status, the purposes for which the service has been approved, the cost for use of the service, including a margin if applicable, and known risks with the service, and purposes for which the service should not be used.

If agency resources are needed to provision or support the service it may be necessary to recover this cost. You may need to develop billing and payment models for cloud services. Decide which service may be purchased by employees individually, using a purchasing card or similar, and which might be better managed through more formal commercial arrangements. Overall cost and volume pricing may guide this decision.

Make sure that the procurement process is quick and easy to use otherwise employees might continue to bypass your processes altogether. Involve your agency procurement, accounting and policy teams when developing your cloud service procurement process.

Implement

Where possible, use the GCDO's marketplace for cloud services or consider establishing your own agency "app store" through which employees can choose or purchase pre-approved cloud services.

Some services will need to be integrated into your enterprise ICT environment. Integration requirements may include directory federation, network and firewall configuration, or automated data transfer. Such changes will need to follow your agency's change management processes, and might require architecture review or risk management approval. For common, well documented and low-risk changes you may be able to define standard changes which are pre-approved and may be fast-tracked through your change management process.

Implement agency-side security controls and Application Programming Interface (API) integrations for approved shadow cloud services used for enterprise-wide or critical business functions.

Acknowledge there will be exceptions, such as where a requirement to integrate would be too difficult or not financial viable for the cloud service, or the value of its information content is low, or the service does not deliver sufficient enterprise benefits to justify additional effort.

Optimise

Mainstream high-value cloud services as preferred enterprise capabilities. Where appropriate incorporate cloud services into the agency's application lifecycle management (ALM), software development lifecycle (SDLC), and security management tools, processes and procedures. Consider outsourcing cloud management to a cloud application security broker under the Telecommunications-as-a-Service shared ICT capability.

Monitor

As with any other enterprise business application, monitoring is an essential activity. Analyse real-time web traffic and logs in granular detail to monitor user activity, identify suspicious behaviour, and perform incident analysis, prevent data loss and inappropriate sharing of agency information, and block threats or malicious activity.

Retire or Replace

As with any agency ICT system or service, approved cloud services will have a lifecycle and will require replacing with better or more cost-effective equivalent services at some point. Be prepared to retire cloud services when no longer required, or they cease to meet business user's needs, or newer technologies surpass existing services. This tenet is one of the greatest advantages of public cloud services.

Maturity measurement

Understand your baseline shadow cloud management capability by measuring maturity of organisations shadow cloud Management Practices. Establish the capacity, maturity and workforce skills of the ICT department and associated outsourced service providers, as well as agency user education and culture.

Gain an understanding why employees are using shadow cloud to do their jobs effectively, and what value they put on the cloud service in achieving their work outputs and outcomes.

Implement scalable cloud service approval processes, such as no more than half-day effort required to approve minor, low-risk, services.

Review current employee policies, cloud and ICT strategies/plans and enterprise architecture within the organisation to assess whether these already adequately cover the shadow IT and shadow cloud concerns and requirements. (i.e. establish a current baseline).

A good level of maturity being reached in this subject will enable agency ICT teams to adopt a partnering approach where they are able to; proactively seek out new services that are a good fit with one or more of the business units; and actively engage with business units to identify good cloud solutions. Once a business unit has selected a service and agreed to pay for it, and understand the risks, help them step into the cloud promptly.

Selected references

5 Ways Shadow IT in the Cloud hurts your enterprise

6 Tips to help CIOs manage shadow IT

Accelerating the Adoption of Public Cloud Services (CAB Min (16) 03/16)

How the Service Broker Model Helps IT Meet Business Needs

Cloud Data Protection Guide

Shadow IT Blog

Cloud Computing: Information Security and Privacy Considerations

Cloud Security Alliance (CSA) research library

Code of Conduct for State Services

CSA Cloud Controls Matrix (CCM) with NZISM matrix map

GEA-NZ ICT Applications, Services, Business and Capability taxonomies

Shining Light on Shadow IT and how to ensure you get it right

The Age of Shadow IT Blog

US Federal Government System Classification Scheme (FIPS-199)

What should Public Sector CIOs do about Shadow IT