Tonga Cloud First Policy

Tonga Enterprise Architect for Developing and Supporting ICT Infrastructure

September 06, 2021, Version 0.2.

Change history

Version	Date	Summary of changes
0.2	06.09.2021	Draft for approval

Document status

Draft	
For approval	
Approved	X

Authors

Name	Role
Ilja Livenson	Cloud Computing / Migration Specialist
Dr Uuno Vallner	Enterprise architect

Table of Contents

1. Policy statement

The Tonga Government is committed to modernizing government information and communication technologies (ICTs) in accordance with the strategy set by Tonga Digital Government Strategic Framework (TDGSF)[1] and will lead by example in using cloud computing services to reduce costs, increase security, increase productivity, and develop excellent citizen services.

The goals of the Cloud first approach are:

- Reducing the cost of government ICT by eliminating duplication of solutions and fragmentation in the technology environment;
- Increasing security of the systems by providing clear guidelines for selecting the hosting solution in accordance with data security requirements;
- Increasing productivity and agility off the ICT solutions in the public sector;
- Achieving business continuity by standardizing infrastructure management;
- Providing a clear model of engagement with the private sector for hosting the public sector's ICT solutions.

In order to achieve this, all government agencies of Tonga affected by this policy will evaluate cloud-based services when undertaking all ICT procurements. The decision on the appropriate ICT delivery model will be based on an assessment of each application, incorporating fitment of purpose, cost benefit analysis and achieving value for money over the life of the investment.

This document sets out general guiding principles for a "cloud first" approach for government ministries and agencies to consider in adopting cloud computing solutions as a primary part of their information technology planning and procurement.

1.1. Entities affected by this policy

This policy is applicable to all government entities with an exception of National Reserve Bank of Tonga and entities primarily responsible for the national security and defense:

- Ministry of His Majesty's Armed Forces;
- Ministry of Internal Affairs;
- Minister for Police, Fire & Emergency Services.

It is also highly recommended for commercially registered entities that are fully or partially owned by the Tonga government as well as the private sector to leverage this policy and create similar internal Cloud First policies for their respective organizations.

[1] Digital Government Strategic Framework 2019-2024. Kingdom of Tonga, 2019, p 50

1.2. Who should read this policy

ICT leadership of all Ministries and Government Entities.

2. Overview of Cloud Computing

Government of Tonga adopts National Institute of Standards and Technology (NIST) definition for cloud computing[2]. The section below provides a short summary of the characteristics of the cloud systems as well as their service and deployment models.

2.1. Key characteristics

Cloud computing leverages several elements including scale, virtualization, resilience, cost efficiency, service orientation, agility, etc. These elements are combined under the NIST definition into five key characteristics:

- **On-Demand Self-Service** – customers are able to provision resources (e.g. a virtual server or email account) without any interaction with the service provider.
- **Broad Network Access** – customers are able to access resources over networks such as the Internet using a ubiquitous client (e.g. a web browser) from a range of client devices (e.g. smartphones, tablets, laptops).
- **Resource Pooling** – the service provider's computing resources are pooled to serve multiple customers. Typically, virtualization technologies are used to facilitate multi-tenancy and enable computing resources to be dynamically assigned and reallocated based on customer demand.
- **Rapid Elasticity** – resources can be quickly provisioned and released, sometimes automatically, based on demand. Customers can easily increase or decrease their use of a cloud service to meet their current needs.
- **Measured Service** – customers pay only for the resources they actually use within the service. Typically the service provider will supply customers with a dashboard so that they can track their usage.

2.2. Service models

Software as a Service (SaaS): The capability provided to the consumer is to use the Cloud Service Provider's (CSP's) applications running on a cloud platform and infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g. web-based email). The consumer does not manage or control the underlying cloud platform and infrastructure including network, servers, operating systems,

[2] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings. Examples may include, but are not limited to:

- Government applications
- Internet services
- Virtual desktops
- Enterprise Resource Planning (ERP) systems
- Customer Relationship Management (CRM) systems
- Communication software (email, instant messaging)

Platform as a Service (PaaS): The capability provided to the consumer is to deploy onto the cloud infrastructure of the CSP consumer-created or acquired applications, these applications are created using programming languages and tools supported by the CSP. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations. Examples may include, but are not limited to:

- Application development
- Database and database management (DBMS)
- Middleware (Web MQ, WebSphere, etc.)
- Testing and developer tools
- Directory Services

Infrastructure as a Service (IaaS): The capability provided to the consumer is to provision processing, storage, networks and other fundamental computing resources. It's up to the consumer to decide what software is deployed and operated, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control on select networking components (e.g. firewalls). Examples may include, but are not limited to:

- Mainframes
- Mid-tier Servers
- Storage
- IT Facilities/Hosting Services
- Virtual Machines

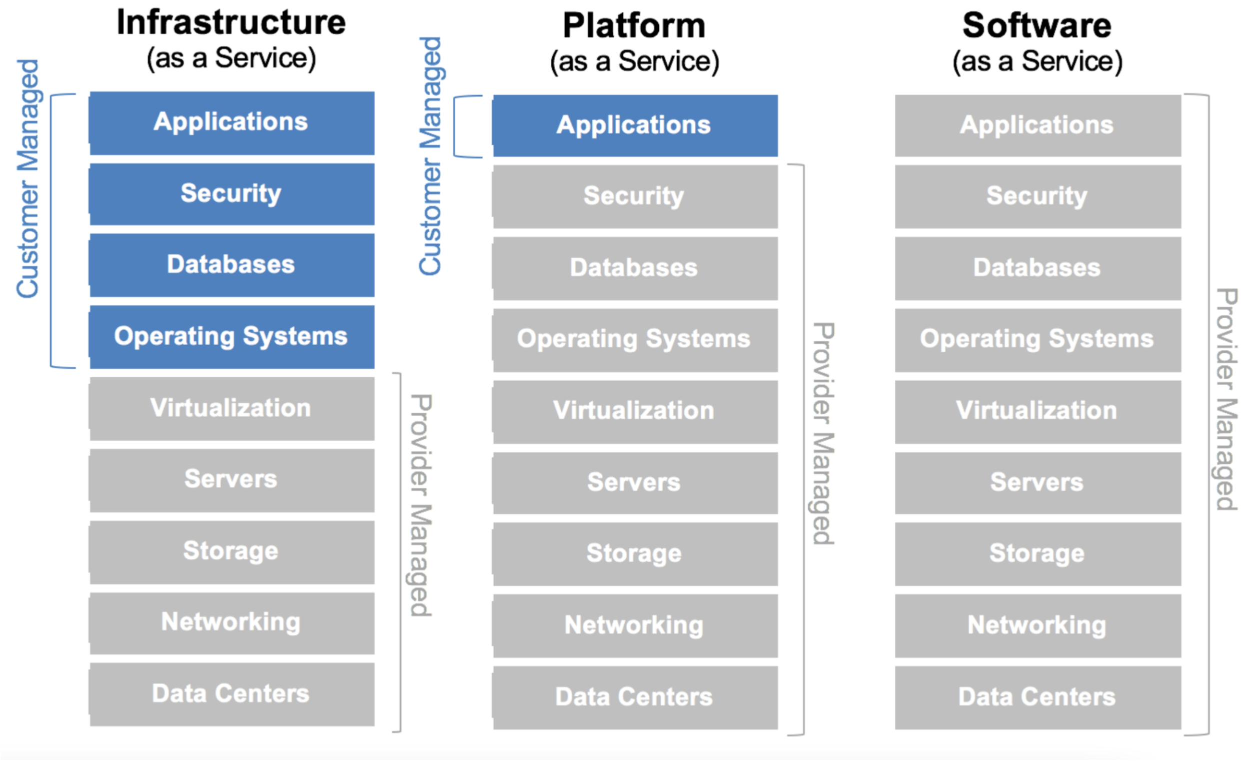


Figure 1: Cloud computing service models

Depending on the selected service model, users of the Cloud services will outsource certain portions of the IT value chain to the CSP. Figure 1 provides an overview of the scope covered by each of the service models. For instance, in the Software as a Service (SaaS) model, the CSP will provide a software application targeted towards end-user software clients, available via Cloud. As part of this offering, the CSP will be covering the platform architecture layer which entails development of environments, database management systems, libraries, compilers and other testing tools needed to develop and implement the applications. Additionally, the CSP will be providing the physical infrastructure layer which typically includes the facility layer (heating, ventilation, air conditioning, power, etc.) and the hardware layer (servers, storage, network components, etc.) as well as the virtualized infrastructure layer which includes software elements (hypervisors, virtual machines, virtual data storage), used to realize the infrastructure upon which a Cloud computing platform can be established.

Similarly, the Platform as a Service (PaaS) model covers the platform architecture layers as well as the infrastructure layer, both the physical and the virtualized one. While for Infrastructure as a Service (IaaS), the CSP will be providing the virtualized and the physical infrastructure layers.

2.3. Deployment models

Cloud computing has three primary deployment models, with most of the countries adopting a composition of these three. Each of these deployment models can offer the different service models explained above, the main difference lies primarily in the level of control and ownership the CSP assumes versus the ownership of the user (consumer).

	Private cloud	**Community cloud (e.g. Government cloud)**	**Public cloud**
Users	Used by a single organization	Used by a community of consumers	Used by the general public
Operating model	Owned and operated by the organization itself, a third party or combination of both	Owned and operated by one or more organization of the community or a third party	Owned and operated by a business.
Location	May exist on and off premises	May exist on and off premises	Exists on the premises of Cloud provider
SLA/Uptime	No guarantees, data redundancy is self-managed	Guaranteed by provider, data redundancy is managed by provider	Guaranteed by provider, data redundancy is managed by provider
Timeline	Longer timelines due to deployment and testing	Faster timeline, plug and play model	Faster timeline, plug and play model

Private Cloud: The cloud infrastructure is provisioned for exclusive use by a single organization, comprising multiple users (e.g. business units). It may be owned, managed, and operated by the organization, a third party (e.g. a CSP), or a combination of these. The physical location may be on or off premise. There are no guarantees on SLAs/Uptime and data redundancy is managed by the entity itself. Solutions development on private Clouds typically consume more time as all the deployment and testing needs to be done in-house.

Common examples of a private Cloud for the Governmental sector are the entity's own Clouds, that are typically serving the entity or an exclusive collection of entities.

Community Cloud: The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared/aligned interests (e.g., mission, cyber security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or a combination of these. The physical location may be on or off premise. The SLAs/Uptime are guaranteed by the service provider and the data redundancy is managed by the provider as well. This model offers a "plug and play" model which allows for faster timelines for deployment of new solutions.

A common form of community Cloud for the Public sector is a Government-owned community Cloud, which is often cited as "G-Cloud" or "Gov-Cloud". This is a Cloud typically fully owned by a Government, and provisioned for the exclusive use of Governmental entities. Operations for this Cloud could be done by a Governmental entity, a third party (e.g. a CSP) or a combination of these. It is typically located inside the country, mainly to protect data sovereignty.

Public Cloud: The cloud infrastructure is provisioned for open use by a variety of entities. It may be owned, managed, and operated by a business, academic, or government organization, or a combination of these. It exists on the premises of the cloud provider. Public Cloud is typically served by global players (e.g. AWS, Google Cloud, Microsoft Azure) as well as by local players (e.g. local telecom and ICT players). The SLAs/Uptime are guaranteed by the service provider and the data redundancy is managed by the provider as well. This model offers a "plug and play" model which allows for faster timelines for deployment of new solutions.

Hybrid Cloud: The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g. cloud bursting for load balancing between clouds). A multi-Cloud approach, a similar model, is a composition of two or more distinct cloud infrastructures but without necessarily connectivity or orchestration between them. Such an approach is globally endorsed.

3. Introduction to Cloud First Policy

A Cloud First Policy is a policy meant to define and typically stimulate Public sector migration from traditional IT solutions to Cloud-based models.

3.1. How Cloud computing helps public sector

Globally, multiple Governments have been adopting Cloud computing. This is mainly to benefit from advantages Cloud computing bears, particularly in terms of efficiency improvements, enhanced agility, reliability of services, more robust cyber security and increased innovation.

Efficiency improvement: In its essence, Cloud computing is about resource pooling and sharing across different applications and entities, leading to an increased utilization of the assets. This increase in utilization means that more value is derived from the assets, which optimizes the current state and reduces the need for future capacity expansions, which translates into cost effectiveness.

Migration of infrastructure to Cloud typically results in ~30% savings in terms of total cost of ownership. Additionally, Cloud computing serves as a catalyst which can accelerate the implementation of Data Center Consolidation initiatives. Similar efficiencies can be seen in applications and platforms, particularly when taking the aggregation of demand that will occur into consideration. This aggregation helps streamline the demand, removes duplications and realizes synergies from scale. In summary, Cloud computing will help entities to shift focus from technology itself to higher-value activities.

Enhanced agility and reliability: By leveraging scalability of Cloud computing, entities are typically able to improve services' responsiveness, particularly in cases of fluctuating demand. Unlike traditional IT which is typically built upon a fixed capacity against a forecasted demand, Cloud solutions offer the users the flexibility to scale up and scale down depending on the demand, which improves the overall user experience with minimal additional investments required while minimizing the service disruptions and outages that could occur. Additionally, Cloud computing – through its dynamic and streamlined approach – will help end users improve the overall time to market. For example, while traditional IT solutions would typically require an elongated period to take care of the development, integration, testing and implementation, a commercially available Cloud solution typically serves the same purpose with a "plug and play" approach. Cloud computing provides a more interoperable and portable environment for data and systems that would help achieve seamless communication between the different entities.

More robust cyber security: Beyond achieving a more efficient, innovative and agile environment, Cloud computing helps to improve overall cyber security. By following best-in-class cyber security protocols in the network communication, Cloud services typically offer a high level of cyber security that is difficult to be attained by Governmental entities themselves. In fact, leading Cloud Service Providers have shown to invest significantly into cyber security-related R&D activities.

Increased innovation: Cloud computing is by nature a driver of innovation for the whole ecosystem. This innovation covers the primary scope of Cloud solutions (infrastructure, platform, software) and is an enabler to transform the way Governmental entities deploy services.

For example, Cloud has already helped transform several private sectors (the way we order a cab, the way we order food, communication with other people, meetings, etc.), all are now online and available anytime anywhere with a simple connection to the internet. It is inevitable that this knowledge and past successful experiences of Cloud computing will be transferred into Governmental processes. In fact, because of limited initial investment required, Cloud computing helps Governmental entities adopt the "start small" entrepreneurial approach to investments, which in turn means more willingness to deploy innovative solutions without having to go through several rounds of budget approvals.

Cloud computing will help **rationalize Government IT spend**. Entities are now facing major challenges when it comes to procuring IT services (e.g. long procurement cycles). Cloud computing will help reduce the time to market significantly through streamlining the procurement process and adopting a "marketplace" for Cloud services.

In the current set-up, the individual Governmental entities have a responsibility regarding cybersecurity. On the contrary, cloud computing will enable a more coherent and robust cyber security framework through adopting best practices in cyber security across Governmental entities, in which the responsibility of the cybersecurity will be shared between the customers and the CSPs.

3.2. Implementation of the Cloud First Policy and its benefits

A Cloud First Policy is a policy that covers Governmental entities and aims at accelerating the deployment of Cloud computing services of these entities when making new IT investment decisions. This objective is achieved by mandating these entities to consider Cloud options every time a new IT investment decision is made, in line with the policy guidelines, processes and governance as defined in the Cloud First Policy. The purpose of the policy is to improve efficiency and effectiveness and minimize Total Cost of Ownership of Governmental entities, while enhancing cyber security of information by adopting the right Cloud model for each goal (in line with the data classification laws, policies and regulations of the Government and other relevant regulations). It also enables interoperability and hence improved communication between participating entities.

3.3. Considerations for the Cloud First Policy

Potential government investments in Cloud computing for the public sector should be evaluated on a case by case basis. Each case should be assessed from 1) a cybersecurity perspective to make sure it satisfies the national cyber security requirements, 2) a technical perspective to ensure its technical viability and 3) a commercial perspective to ensure it represents the most cost-efficient solution available.

A **Government Cloud Service Provider** is a government owned community cloud (**G-Cloud**). A **Commercial Governmental Cloud Service Provider** is any commercial cloud provider (global or local) that meets the cybersecurity requirements to host non-sensitive or open data.

Security perspective

When considering migration to Cloud services, security is a key aspect for evaluation and is governed by regulations and laws issued by Tonga. Therefore, the policy mainly takes into account the input of data security and protection and builds upon it the decision-making tree for the policy. All security regulations and frameworks must be reviewed when designing or implementing any cloud solutions to ensure their compliance with security controls and requirements. Existing and drafted regulations and frameworks:

- Electronic Transaction Act[3]
- [4]Tonga Telecommunications Commission Act
- Tonga Interoperability Framework[5]
- National Cybersecurity Framework[6]
- Cybersecurity Act[7]
- Data Privacy & Protection bill[8]

[3] Electronic Transactions Act 2014

[4] http://www.paclii.org/to/legis/consol_act/ttca385

[5] Tonga Interoperability Framework (TIF). Version 0.8, 2021

[6] National Cybersecurity Framework (in preparation)

[7] Cybersecurity bill (in preparation)

[8] Data Privacy & Protection bill (in preparation)

Technical perspective

Another aspect that should be considered when migrating to Cloud is its technical viability. For example, solutions that are highly sensitive to latency may be better off hosted locally on premise, especially when the Cloud services solutions don't present the same technical features.

Commercial perspective

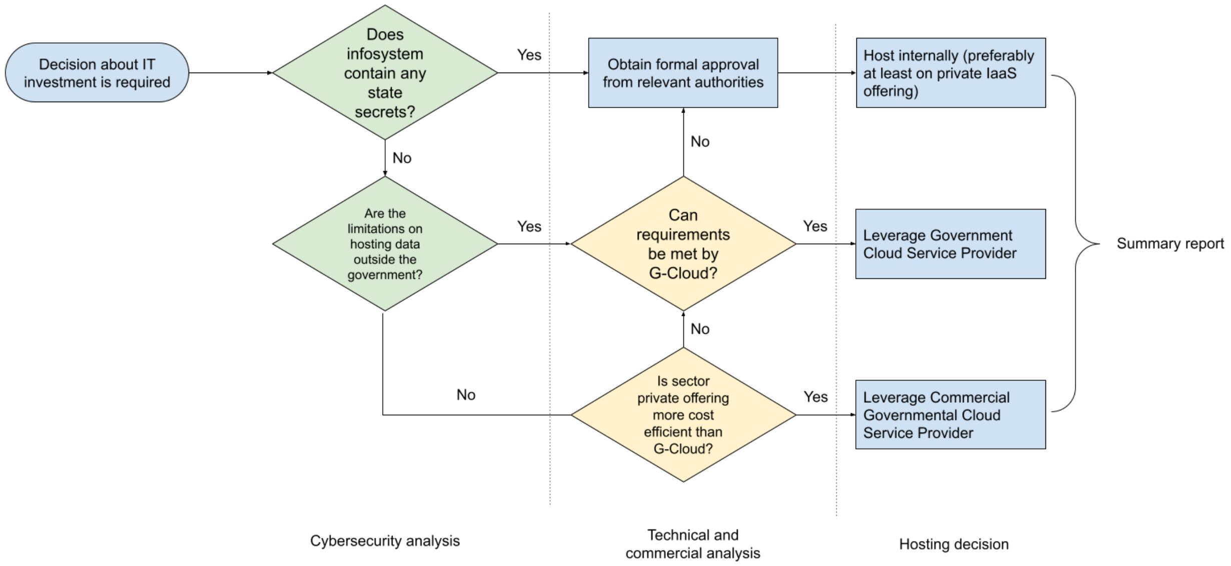
Cloud computing has significant potential in terms of economic benefits to the migrating entities. However, the economic aspect (quantified by the Total Cost of Ownership) needs to be assessed on a case-by-case basis. For example, applications that are highly customized and specific to the end-user may at times be more expensive to migrate to Cloud compared to the 'as-is' situation.

In summary, every case should be treated separately and should be rigorously evaluated as such, based on the three dimensions highlighted above.

4. Tonga's Cloud First Policy

4.1. Policy guideline

When making new IT investments, entities covered by this policy are required to consider Cloud computing options and must adopt the following multi-faceted approach as illustrated in the figure below:



Decision about IT investment is required
Does infosystem contain any state secrets?
Yes
No
Obtain formal approval from relevant authorities
Host internally (preferably at least on private IaaS offering)
Are the limitations on hosting data outside the government?
Yes
No
Can requirements be met by G-Cloud?
Yes
No
Leverage Government Cloud Service Provider
Summary report
No
Is sector private offering more cost efficient than G-Cloud?
Yes
Leverage Commercial Governmental Cloud Service Provider
Cybersecurity analysis
Technical and commercial analysis
Hosting decision

Start: All new IT investments which are to be made by one of the entities which are included in the scope of the Cloud First Policy need to go through the process. A 'New IT investment' includes procurement of new hardware and software, renewal of hardware and renewal of present software licenses. It is noteworthy that the entities falling under the scope of this policy must abide by the laws, regulations and controls related to data classification and other regulations regarding the location of hosting their data in any way.

Stage Gate 1: If an infosystem contains data that is classified as containing state secrets, a formal request to the DTD should be submitted in order to host the solution internally.

Stage Gate 2: Limits on data hosting -> G-Cloud or internal hosting.

Stage Gate 3: No limits and G-Cloud is more cost efficient -> G-Cloud.

Stage Gate 4: No limits but G-Cloud cannot provide service or is less cost efficient -> Commercial.

4.2. Analysing requirements

Security analysis: assess if the security requirements, which are based on the governing data classification law in the Tonga, authentication requirements and other specific security measures and regulations, are met by the Cloud model under consideration.

Technical analysis: assess the technical aspect of the Cloud migration or deployment case, to ensure that the Cloud solution will achieve the desired outcomes (e.g. for cases of latency-sensitive applications, integration with legacy systems, etc.). This should be done in coordination with the Digital Transformation Department (DTD) under the Prime Ministers' Office.

Commercial analysis: assess the commercial aspect of the Cloud adoption case to ensure that it yields a positive business case, i.e. that the selected Cloud computing model (Commercial Government Cloud, Government owned community Cloud or self-hosted) offers the most cost-effective option for each specific case. This should be done in coordination with the Digital Transformation Department.

4.3. Prioritization of Cloud solutions

Entities should consider the following priority in terms of service model when selecting a Cloud solution:

a) Software as a Service (SaaS) is the preferred option as it maximizes the benefits brought by Cloud.

b) Platform as a Service (PaaS) when SaaS is not possible.

c) Infrastructure as a Service (IaaS), when SaaS and PaaS are not feasible.

Additionally, with the aim of achieving a more efficient, more utilized IT in the Tonga Government sector, entities covered by the scope of this policy are no longer required to buy or build new data center infrastructure (e.g. data center, servers or other, storage media, network equipment, uninterruptible power sources).

4.4. Format of the formal request

When requesting an exception to host solution internally, the following should be provided:

- Summary of the planned information system.
- Legal requirements to the hosting entity.
- Financial analysis of required investments for 5 years.
- Technical requirements to the platform and assessment of G-Cloud platform fit.

4.5. Format of the summary report

When a hosting decision is made, to foster improvements to G-Cloud, the following information should be provided to the Digital Transformation Department (DTD) under the Prime Ministers' Office.:

- Decision path on the diagram.
- If applicable: cybersecurity, technical and commercial analysis.

5. Governance structure

A well-defined governance structure must be in place to ensure smooth implementation and optimal results. The following roles are used to govern the Cloud First Policy:

Role	Description	Entity
Policy body	Defining objectives, scope and governance of the Cloud First policy.	Prime Minister's Office (Digital Transformation Department)
Cloud operator team	Drives cloud adoption. Operates the main G-Cloud service. Assists with analysis of IT solutions from technical and commercial perspectives.	Digital Transformation Department
Security body	Reviews and monitors cloud cybersecurity controls, assists with development of regulations and laws affecting entities in scope of the Cloud First Policy.	Digital Transformation Department
Cloud Service Providers	Provide cloud services to the public sector. Government and commercial entities.	Digital Transformation Department
Enablers	Assist with adoption of the Cloud First Policy	Digital Transformation Department & relevant

		Government agencies
End users	Entities targeted by the Cloud First policy	Government agencies