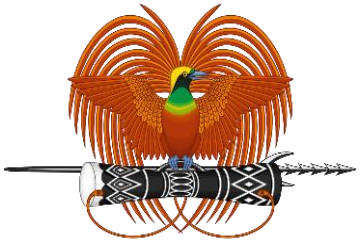
2023



Independent State of Papua New Guinea

# GOVERNMENT CLOUD POLICY

## TABLE OF CONTENTS

## ABBREVIATIONS

| | |
|---|---|
| GCP | Government Cloud Policy |
| DICT | Department of Information and Communication Technology |
| PNG | Papua New Guinea |
| NCSC | Nation Cyber Security Centre |
| DGA 2022 | Digital Government Act 2022 |
| CSP | Cloud Service Provider |
| GLC | Government Leased Cloud |
| IaaS | Infrastructure as a Service |
| PaaS | Platform as a Service |
| SaaS | Software as a Service |
| SLA | Service Level Agreement |
| TCO | Total cost of ownership |
| GovDC | Government Private Cloud or Data Centre |
| DTO | Digital Transformation Officer |
| ICT | Information and Communication Technology |
| IT | Information Technology |
| NEC | National Executive Council |
| CPA | Cloud Procurement Agreement |
| CPU | Central Processing Unit |
| AI | Artificial Intelligence |
| PNGSDP | PNG Sustainable Development Plan 2010-2030 |
| MTDP | Medium Term Development Plan |

## DEFINITIONS

| | |
|---|---|
| Public Bodies | Public bodies are as defined by the DGA 2022 including all public agencies with the exception of state-owned entities |
| PSICT Steering Committee | Public Service Information and Communications Technology Steering Committee as described in DGA 2022 |
| Government Cloud | Refers to Government Leased Cloud Infrastructure and Government Private Cloud Infrastructure as described in DGA 2022 |
| Private Cloud | Private Cloud Infrastructure as described in DGA 2022 |
| Cloud First Policy | means public bodies should use cloud services as their primary option |
| NEC Decision No. 39/2021 | A directive from the NEC for the development of the Government Cloud Policy |

## FOREWORD BY SECRETARY

It gives me great pleasure to introduce the PNG Gov Cloud Policy, which has been developed to guide public bodies in their adoption of cloud services. As we continue to modernize our public services, the adoption of cloud technology has become a priority for the government of Papua New Guinea.

The PNG Gov Cloud Policy outlines the framework that public bodies must follow when migrating services to the cloud. It provides guidance on important considerations such as data privacy and security, compliance requirements, and the selection of Cloud Service Providers (CSPs). By implementing this policy, we aim to ensure that public bodies are equipped with the necessary knowledge and tools to make informed decisions when adopting cloud services.

As a department we recognize the importance of the government's role in safeguarding our citizens' data privacy and security. We are committed to supporting public bodies in their journey towards cloud adoption, by providing guidance and ensuring compliance with relevant laws, regulations, and standards. We believe that this policy will not only enable public bodies to optimize their operations and service delivery but will also contribute to the growth of our digital economy.

As we embark on this journey towards a digital government, it is important to note that this policy complements the efforts we have made thus far. Our journey began in 2018 with the approval of the ICT Sector Roadmap 2018, which was aimed at transforming the ICT sector and leveraging technology to drive economic growth and improve service delivery. This was followed by the Digital Transformation Policy in 2020, which aimed to build a digitally enabled public service that is efficient, effective, and citizen-centric.

As a result of our continued efforts towards digital transformation, the Digital Government Act 2022 was approved, followed by the subsequent Digital Government Plan 2023-2027. This policy is an important component of the Act, as it outlines the guidelines and best practices for the use of cloud computing in the public sector. The policy also aligns with the government's broader digital transformation agenda and provides a framework for the secure and effective use of cloud computing in the delivery of public services.

I am proud to say that this is a home-grown policy which has been developed in house in consultation with stakeholders from various sectors, and I believe that it will play a crucial role in our efforts towards building a digitally enabled government that is responsive to the needs of our citizens. As we move forward, I encourage all public bodies to embrace this policy and ensure that they comply with the guidelines and requirements outlined in it. Together, we can build a truly digital government that delivers services in a transparent, efficient, and effective manner.

**STEVEN MAtAINAHO**
Secretary

## EXECUTIVE SUMMARY

The PNG Government Cloud Policy is a comprehensive framework that outlines the requirements for government agencies to adopt cloud computing services. The policy aims to leverage cloud technologies to enhance service delivery, reduce costs, and improve efficiency in the public sector. The policy is aligned with the government's Digital Transformation Policy and the Digital Government Act 2022, which set the stage for modernizing the public sector through the use of digital technologies.

The policy's primary objective is to provide guidance for government agencies on cloud adoption and implementation, ensuring that all public bodies have a consistent approach to the use of cloud technologies. The policy lays out the compliance requirements for public bodies, including data privacy and security, government policies and standards, industry standards, service level agreements, contractual obligations, and international standards and regulations. The Department of Information and Communications Technology (DICT) will provide support to public bodies in meeting these requirements.

The policy also outlines the benefits of cloud adoption, including improved service delivery, reduced costs, increased efficiency, and enhanced disaster recovery and business continuity. Cloud technologies offer scalable and flexible solutions that can meet the changing needs of the public sector. By leveraging cloud services, the government can improve access to information, promote transparency, and enhance collaboration among government agencies.

The PNG Government Cloud Policy is a critical step in the government's digital transformation journey. By adopting cloud technologies, the public sector can improve service delivery and efficiency, reduce costs, and enhance disaster recovery and business continuity. The policy provides a framework for consistent and compliant cloud adoption across all government agencies, supported by guidance and support from the DICT. The policy is aligned with the government's broader digital transformation agenda, supporting the country's vision of becoming a digital economy.

## 1.0 INTRODUCTION

The Government Cloud Policy (GCP) represents an important step forward in Papua New Guinea's (PNG) digital transformation, as it seeks to address some of the most significant challenges facing public bodies in their efforts to adopt and make use of cloud computing services. By providing clear guidance and direction to public bodies, the GCP will help to ensure that the adoption and use of cloud services aligns with the overall goals and objectives of the government. It will also help to prevent public bodies from adopting cloud services in a fragmented and uncoordinated manner, which can lead to increased costs and a lack of effective management of cloud computing resources.

To ensure the efficient and secure consumption of cloud services, public bodies should use the GCP to understand the available cloud services, determine the appropriate future usage of cloud services, and liaise with Department of Information and Communication Technology (DICT) as the coordinating agency. This will help to ensure that cloud services are used in a way that is financially sound, aligned with the goals of the government, and able to deliver improved service delivery to citizens across PNG.

In addition, the GCP emphasizes the importance of secure data exchange and shared services, which are key components of PNG's digital infrastructure. Through the use of public and private cloud services, public bodies will be able to take advantage of the benefits of cloud computing while also ensuring the security and integrity of their data. By working together with DICT and other stakeholders, public bodies will be able to leverage the power of cloud computing to drive innovation, improve efficiency, and enhance service delivery for the benefit of all citizens in PNG.

### 1.1 Policy Statement

The digital infrastructure in PNG, including the Government Leased Cloud (GLC), is critical for the delivery of high-quality digital services to citizens. GLC is as described under Section 25 of the Digital Government Act 2022[1](DGA 2022), to be established by DICT for the whole of government digital service delivery. The government recognizes the importance of modern, resilient, and widespread infrastructure with sufficient capacity for the development of the Digital sector in PNG. By expanding digital infrastructure such as GLC, the government aims to improve business continuity and the quality-of-service delivery in the public sector.

This policy is a crucial step towards achieving this goal by enabling the public sector to access cloud computing and other technologies facilitated by the cloud, such as Artificial Intelligence, Machine Learning, and the Internet of Things. This creates an environment that fosters development and innovation in an organic manner. The policy is designed to encourage greater adoption of cloud services in the public sector, promoting a more efficient approach to infrastructural investments and IT deployment.

[1] Digital Government Act certified on the 19 July, 2022 through NEC Decision No 41/2022

## 1.2 Purpose and Rationale

The policy establishes best practices for the consumption of cloud solutions and provides guidance to users on the use of cloud computing solutions. By adopting cloud services, public bodies will enjoy benefits such as on- demand access to computing resources, improved data management and analysis, and increased collaboration among staff members. The policy will also enable public bodies to securely process, share, store, and manage their data, while also promoting the adoption of innovative technologies such as Artificial Intelligence, Machine Learning, or the Internet of Things enabled by the cloud.

By promoting the use of cloud computing, the policy provides public bodies with greater access to services and information, reduces costs by eliminating the need for expensive on-premises hardware and infrastructure, and promotes a consistent framework for cloud adoption that promotes interoperability and reduces duplication of effort. The policy supports PNG's broader digital transformation goals by facilitating the growth of the digital economy and promoting the adoption of innovative solutions.

The Government Cloud Policy (GCP) is essential for PNG to leverage cloud computing services effectively across all public bodies. This policy framework provides guidance and coordination for public bodies in the adoption and use of cloud services, addressing data security, service quality, and vendor lock-in challenges (such as by using pay as you go pricing models). The policy establishes best practices for the consumption of cloud solutions and provides guidance to users on the use of cloud computing solutions.

## 1.4 Alignment

The GCP ensures that the adoption and use of cloud computing align with the overall goals and objectives of the government's digital infrastructure and services delivery to prevent public bodies from adopting cloud services in a fragmented and uncoordinated manner, reducing costs, and enabling more effective management of cloud computing resources across public bodies

The policy takes its cue from various government documents, including Vision 2050, National ICT Policy 2008, ICT Roadmap, 2018 APEC Digital Economy agenda, ICT Sector roadmap 2018 on digital framework, and PNG Digital Transformation Policy 2020[2] pilar 6 on Digital Infrastructure. It is empowered by the direction from the NEC Decision No. 39/2021[3] and Sections 25 and 26 of the Digital Government Act 2022 to coordinate and develop a Cloud Policy for the Government. The policy provides linkage to the DICT Corporate Plan 2020 - 2024, as per NEC Decision No. 252/2020, to achieve the desired outcomes of the Policy

Furthermore, this policy guides public bodies in their adoption and consumption of cloud services by incorporating emerging technologies and cybersecurity landscapes. The GCP

[2] Cloud policy is one of the policy scopes under Digital infrastructure

[3] Development of Government Cloud Policy was an NEC direction from the PNG Government.

also recognizes that not all public bodies may be able to use cloud services due to their specific requirements or the unavailability of suitable services. In such cases, the policy allows for the use of cloud services under the cloud service registry established by the DICT as per Section 25 (10) of the DGA 2022. This ensures that public bodies are using secure and reliable cloud services that meet the government's cloud standards and guidelines.

## 1.5 Mandate and Objectives

The GCP is a **"Cloud First Policy",** which means public bodies should use cloud services as their primary option. The "Cloud first" approach is followed by many governments and organizations worldwide. This approach encourages public bodies to adopt cloud services as the primary option. Cloud services provide several benefits such as increased flexibility, scalability, and cost savings. By making cloud services the default option, public bodies will have to consider cloud options before exploring other solutions, ensuring that they are taking advantage of the benefits of cloud services.

The development of the GCP in PNG was a directive of the NEC Decision No. 39/2021. The decision also re-affirmed the DICT as the coordinating agency for public sector cloud infrastructure and services specifications, as well as to deliver shared ICT services to all public bodies through a Virtual Cloud arrangement and to formulate a Government Cloud Policy. Additionally, all public bodies were directed to coordinate the planning and implementation of cloud-related services with the DICT and to take full advantage of cloud automation practices.

The DICT is further enhanced and mandated by the DGA 2022 as the central coordination agency to be responsible for coordinating all cloud-related activities in the PNG's public sector. In accordance with the DGA 2022, the DICT is tasked to establishing a GLC Infrastructure for connectivity of virtual private networks and digital services for all public bodies, as well as building a Government Private Cloud Infrastructure as part of the Government Private Network for delivery of digital services.

The GCP has seven objectives that guide public bodies in achieving optimal usage of cloud services: Security; Consistency & Alignment; Modernization; Procurement; Innovation, and; Optimal Commercial Outcomes. Seven principles will guide public bodies in the process and align with the government objectives:

i) making risk-based decisions when applying cloud security design services for the cloud;
ii) designing services for the cloud;
iii) using Government Leased Cloud (GLC) as the default;
iv) using the cloud as much as possible;
v) avoiding customisation and use cloud services as they come if not sure;
vi) taking full advantage of cloud automation practices; and
vii) monitoring the health and usage of cloud services in real time.

## 2.0 CLOUD OVERVIEW

The Cloud refers to numerous data centers managed by Cloud Services Providers (CSP) and located throughout the world that have installed hardware necessary for the purpose of providing cloud-based solutions accessible via the Internet. Cloud computing is a type of computing where servers, networks, storage, development tools, and even applications (apps) are enabled through the Internet. Whereas governments such as PNG, used to make major investments in data centers to buy equipment, train staff, and provide ongoing maintenance, many of these needs are handled by a CSP.

There are five key characteristics of cloud computing[4]:

i. **Internet Access**: Cloud computing resources are available over a network and can be accessed from a variety of devices and platforms where users "plug into" the data and applications via an internet connection giving anytime, anywhere access.

ii. **Measured Service**: Pay-as-you-go, where you only pay for what you use. Think about how a utility company meters how much water, electricity, or gas is used and charges based on consumption. The cloud is the same.

iii. **On-Demand Self-Service:** Where services can be requested and provisioned quickly, without the need for manual setup and configuration.

iv. **Shared Resource Pooling:** Where cloud services use a multi-tenancy model. This means a single application is shared among several users. So, rather than creating a copy of the application for each user, several users, or "tenants" can configure the application to their specific needs.

v. **Rapid Elasticity:** Cloud platforms allow organizations to scale its resource usage levels up or down quickly and easily as needs change.

Cloud Services offers many advantages such as lower costs, higher performance, faster delivery of IT services, better IT security, increased scalability of services and more reliable disaster recovery and business continuity.

[4] US National Institute of Standards and Technology (NIST).

## 2.1 Cloud Deployment Model

This section defines and describes the cloud computing deployment models;

### 2.1.1 Hybrid Cloud

The government has chosen to deploy a Hybrid cloud model that combines an on-premises datacenter with a Public Cloud, allowing data and applications to be deployed between them.

The government will leverage on the services offered by the public cloud and the use of private cloud or on-premises cloud infrastructure. The government's hybrid cloud deployment model allows for the utilization of both public and private cloud services to ensure high availability and data security. The public cloud can be used to leverage the benefits of cost-effectiveness and scalability while the on-premises datacenter can provide dedicated resources for secret data and other data and services that must be stored on premises.

With both deployment models, the government will take all necessary measures to ensure that the data sovereignty of PNG is protected and that data is stored, processed, and transmitted securely in accordance with established security standards and best practices.

### 2.1.2 Public Cloud

Public Cloud refers to a type of computing in which a service provider makes resources available to the public via the internet. These services may be free or sold on-demand, allowing customers to pay only per usage for the CPU cycles, storage, or bandwidth they consume. Connecting to a public cloud means that a person is using an Internet connection to access computing resources hosted on data centers managed by a third-party cloud service provider, rather than owning and maintaining these resources on site.

### 2.1.3 On Premise Infrastructure

On premises infrastructure is operated solely for a single organization, whether managed internally or by a third party, and hosted either internally or externally. Also called an internal or corporate cloud, this model may give businesses some of the benefits of a Public Cloud - including self-service, scalability, and elasticity - with the additional control and customization available from dedicated resources over a computing infrastructure hosted on-premises.

While in some circumstances on-premises datacenters could deliver strong levels of security and privacy through both agency’s firewalls and internal hosting, they are capital intensive to maintain and when not maintained properly the heavily protected data becomes much less protected. On premises data centers require the same staffing, management, and maintenance expenses as traditional data center ownership such as the one delivered in 2014 under Integrated Government Information System (IGIS) project.

### 2.1.4 Decision making on deployment Model

When considering which deployment model to use, public bodies should apply the following guidance based on data types as described under Section 45 of DGA 2022 and the forthcoming Data Governance, Protection and Privacy Policy:

i) For Public/Open Data and normal business workloads, agencies should use Cloud as the default model. Only by specific exception from DICT Secretary should other solutions be considered.

ii) For Confidential Sensitive) Data, agencies may use Cloud following a risk assessment including adhering to cloud standards, guidelines and satisfactory demonstration of security controls requirements laid out in Section 5.0 are adequately met.

iii) For Confidential (Highly Sensitive) Data, agencies may use Public Cloud subject to a risk assessment and following DICT review to ensure security controls requirements laid out in Section 5.0 are adequately met. Agencies should submit their risk assessment and controls information to DICT Secretary for review.

iv) For Top Secret Data, agencies should use On Premises Data center as the default model. Only by specific exception from DICT Secretary should other solutions be considered.

### 2.1.5 Cloud transition considerations

Incompliance with section 25 and 26 of the DGA 2022, public bodies should consider transitioning workloads[5] and data to cloud when:

- there is a major equipment/infrastructure refresh due;
- there is a major software refresh due;
- there is an emerging defined need for cross agency connectivity;
- there is an opportunity to consume an application through software as a service, or consolidate applications across agencies or a cluster;
- existing solutions do not meet agency, staff or customer needs; and
- systems have limited support from staff or suppliers or are becoming increasingly difficult to support.

[5]https://www.digital.govt.nz/digital-government/programmes-and-projects/cloud-programme/about-the-cloud-programme/

## 2.2 Cloud Service Deployment Models

Cloud technology is evolving and the cloud service models captured here are the current models used through public, private and hybrid clouds. Other cloud service deployment models are anticipated to emerge in the future.

Comparisons table from the Traditional (Legacy) ICT service deployment model to current Cloud service deployment models.

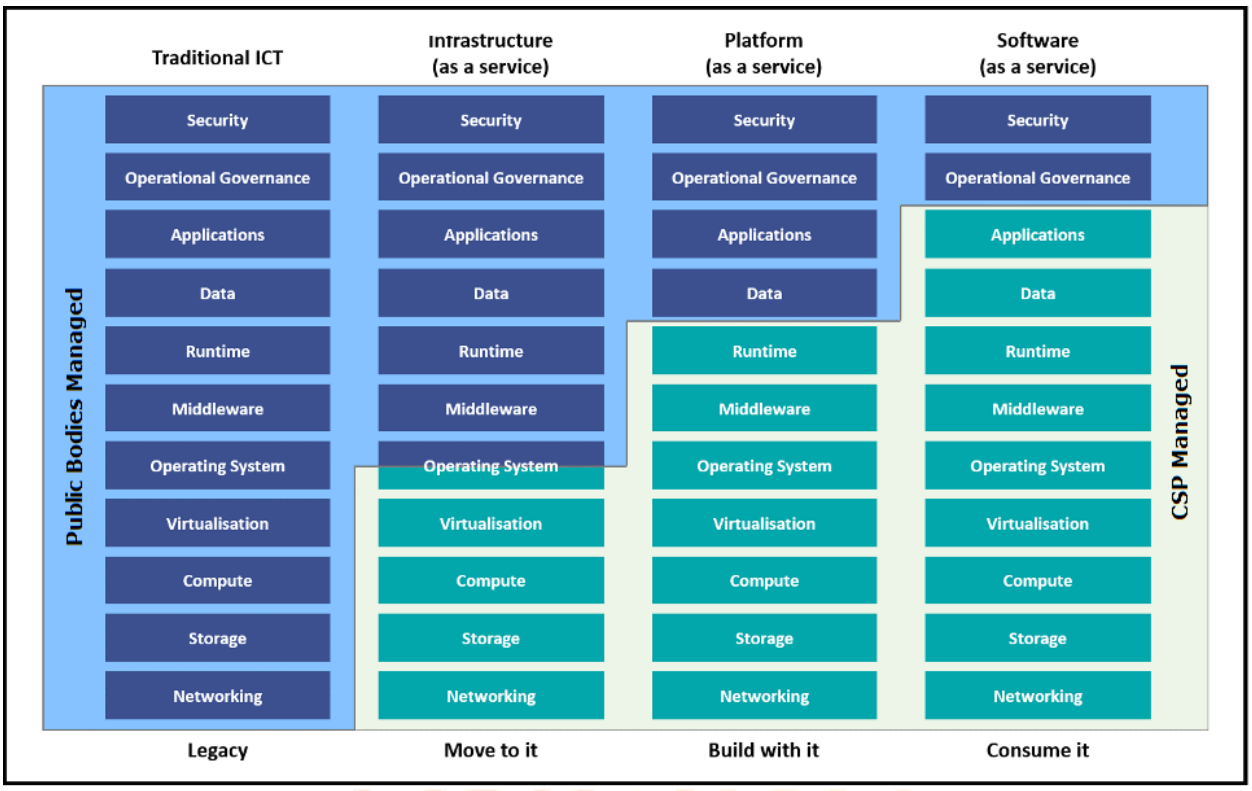



**Table 1**. The table depicts the traditional ICT service deployment model in comparison with the current Cloud Service Deployment Models.

### 2.2.1 Infrastructure as a Service (IaaS)

IaaS is a cloud service model that harnesses the integration of the traditional ICT model resources and infrastructure combined with specialized infrastructure services that are cloud based. The customer simply rents servers and data storage in the cloud rather than purchasing and maintaining its own infrastructure. It thus has the ability to control its own deployed applications, operating systems and a set of networking components if deemed necessary such as host firewalls. IaaS thus provides a government with the same technologies and capabilities as a Traditional (Legacy) ICT model, including full control over server instances.

Public bodies will be responsible for managing aspects such as databases, applications, runtime, OS, and security while the CSPs will manage the servers, hard drives,

networking, and storage. The CSPs (e.g., AWS, Azure, etc.) will control and manages the elemental cloud infrastructure, including the capabilities of the CSP to provide for the Cloud Computing networks, server, storage, processing, and other primary computing resources that will enable the deployment and running of arbitrary software that comprises applications and operating systems. Under IaaS, three services are offered as an optional service;

a. Full cloud Infrastructure
b. Hybrid Cloud Infrastructure
c. Disaster Recovery Infrastructure

The Public bodies will be given the opportunity to choose the infrastructures of their choice depending on their organizational needs.

### 2.2.2 Platform as a Service (PaaS)

PaaS allows government the ability to access a pre-defined environment for software development that can be used to build, test, and run applications. This service allows for the development, operation, and management of applications without the complexity of building and maintaining infrastructure. This will enable developers to focus on software development, as opposed to spending much time on writing extensive code or managing software updates or security patches. Examples of PaaS products include Google App Engine, web servers, and SQL servers. PaaS is implemented on the cloud through a virtual development platform and accessed via the internet over a web browser.

The Public bodies are given the privileges to deploy their own applications onto the CSP's cloud infrastructure by using software development tools and programming languages. The government will have no control or cannot manage the underlying cloud infrastructure such as storage, networks, operating systems, and servers however they will have control over the hosting configurations of the environment, including security and the applications they will deploy.

### 2.2.3 Software as a Service (SaaS)

With SaaS, the public bodies will have the opportunity to accesses a specific software application hosted on a remote server and managed by a third-party provider. Since everything is provided on a subscription basis, the application is accessed through a web browser, reducing the need for on-device software downloads or updates. On demand delivery of software applications, with CSP hosting and managing the application and its underlying infrastructure.

The CSP's runs applications on its cloud infrastructure that are made available to the government. Web browsers create accessibility to these applications and apart from security, the government will have no control or management privileges to underlying cloud infrastructure which encompasses storage, operating systems, servers, networks

and in less instances the provision of public bodies centric applications with its configuration settings.

## 2.4 Cloud Architecture

Cloud architecture refers to the overall design of a cloud computing environment, including the various components and their interactions. The architecture of a cloud system typically involves multiple layers and components, each with its own specific functions. The system typically involves multiple cloud components communicating with each other over a loose coupling mechanism such as a messaging queue.

The following are some of the key components and layers of cloud architecture:

- **Cloud infrastructure:** This layer includes the physical hardware and networking equipment, such as servers, storage devices, and switches, that are used to build the cloud system.
- **Virtualization layer:** This layer provides a software-based abstraction of the physical infrastructure, allowing multiple virtual machines (VMs) to run on a single physical server.
- **Cloud services layer:** This layer includes the various services and applications that are made available to users through the cloud system, such as storage, compute, and networking services.
- **Management and orchestration layer:** This layer includes the tools and services that are used to manage and orchestrate the various components of the cloud system, such as workload balancing, resource allocation, and service scaling.
- **Security and compliance layer:** This layer includes the various security and compliance measures that are implemented to protect the cloud system and the data stored within it.
- **Cloud platform layer:** This layer includes the various interfaces that are used by users to interact with the cloud system, such as web-based portals or APIs.

DICT will coordinate the design of the Government Cloud architecture depending on the specific needs and requirements of the organization or application. The goal is to create a system that is scalable, flexible, reliable, efficient, and secure, and that can meet the needs of PNG Government and applications in a cost-effective manner.

## 2.3 Cloud Benefits

Cloud services enable transformational opportunities across government operations, enabling the delivery of citizen focused services anywhere, anytime. Cloud allows the government the opportunity to harness the investment and transformational potential of cloud and enable the following benefits:

i. **Whole-of-government efficiencies:** Reducing the cost of developing and maintaining technology and reducing the duplication of capabilities across government.

ii. **Interoperability:** Efficiently manage information across public bodies and classifications including between the Protected and Unclassified domains where appropriate.

iii. **Competition:** Allows the Government to drive efficiencies through competition and easily move services between competitive and innovative offerings.

iv. **Interconnected Ecosystem:** The GLC is hosting majority of public bodies ICT infrastructure, making it the launchpad for public bodies looking to connect existing systems or workloads to GLC services through dedicated data network connectivity and cloud services. It enables public bodies to share and collaborate to reduce unnecessary duplication of ICT investment, or repetition of procurement and development processes.

v. **Flexibility:** Cloud allows business areas to rapidly tune their resource usage based on demand and eliminate the lead times that delay delivery. Businesses using cloud can leverage the latest technology innovations in the market as soon as they become available, enabling experimentation without big upfront investments. By consuming cloud services, the Government will have access to a range of programming models, operating systems, databases, and architectures as well as supplier services available through marketplaces provided by the public CSPs.

vi. **Collaboration:** As a community of public bodies, the GLC facilitates collaboration and sharing that is difficult to achieve when ICT and Digital service delivery is distributed.

vii. **Rapid Elasticity:** The on-demand model of Cloud allows public bodies to rapidly scale up and down their infrastructure in line with end user and developer needs, allowing the Government to keep up with growing and changing citizen demands.

viii. **High Availability:** ICT services running in the cloud can be architected to be highly available and resilient, ensuring fewer outages and less down time by leveraging constructs such as availability zones and autoscaling.

ix. **Real-time monitoring** of cloud services provides a clear picture of the health and status of the environments and can be used to drive behavior accordingly. Running services in the cloud makes our services more visible. It increases options for the delivery services with low-risk profiles, and applies greater focus and assurances around higher value information.

x. **Access to New Capabilities:** Cloud services provide the Government the foundations upon which to deploy more advanced capabilities such as artificial intelligence and machine learning, as well as access to continual updates and service improvements.

xi. **Automation:** Platform and application automation can enable greater ease of management across ICT environments as well as self service provisioning capabilities.

xii. **Focus on Service Differentiation:** Cloud consumption enables public bodies to transition away from the undifferentiated heavy lifting of managing infrastructure by consuming it as a service, allowing greater focus on transforming services for citizens.

xiii. **Greater Security and Resiliency**: Cloud environments can be configured to track changes using logging and can make use of the latest security features to reduce the likelihood of cyber-attacks and internal misconfiguration.

xiv. **Cost Avoidance**: Cloud services enable the Government to pay for resources used, on demand. This can enable upfront cost avoidance on infrastructure refresh and long-term cost savings as workloads are optimized in the cloud environment.

xv. **Business Agility:** Cloud services support more agile development and deployment practices, which can significantly reduce time to market if processes are updated to make use of rapid provisioning.

xvi. **Centralisation and Visibility:** Strong governance of cloud services can help to centralize ICT environments and provide clearer visibility of consumption and costs.

xvii. **Operational effectiveness**: Cloud services improve operational effectiveness through increasing availability and freeing up resources to focus on business delivery rather than maintenance. Right sized infrastructure reduces costs for maintaining idle resources. Cloud automation allows services to quickly restore after a failure and scale capacity up or down to meet demand.

## 2.5 Cloud Opportunities

Cloud opportunities that the government can leverage. The diagram depicts the cloud opportunities with the associated range of complexities around the services that are offered.

## 3.0 GOVERNMENT CLOUD MANAGEMENT

The PNG GCP is designed to promote a secure, reliable, efficient, and transparent cloud computing environment for the government of PNG. This section outlines the roles and responsibilities of the government, public bodies, and other stakeholders in the adoption and use of cloud services, and the DICT is responsible for coordinating the selection, procurement, and management of cloud services for the whole of government in accordance with the policy guidelines.

### 3.1 Department of Information and Communications Technology

The DICT has been mandated by the PNG government through the DGA 2022 to coordinate the development, implementation, and management of the cloud infrastructure and services across all public bodies. DICT will also be responsible for providing guidance and support to public bodies in the adoption and usage of cloud services, monitoring and evaluating the implementation of the policy, developing guidelines and standards, managing risks and issues related to the cloud, ensuring compliance, promoting capacity building, and facilitating partnerships with CSPs and other stakeholders. DICT's role is critical in ensuring the success of the implementation of GCP and in achieving the objectives outlined in the policy

The DICTs leading role includes but not limited to;

i. **Developing the policy:** The DICT will be responsible for leading the development of the policy, in consultation with relevant stakeholders, including public bodies, industry partners, and civil society groups.

ii. **Coordinating implementation:** The implementation of the policy will be as per Section 25 and 26 of the DGA 2022. This includes coordinating the implementation of the policy across public bodies, ensuring that it is being implemented in a consistent and coordinated manner as intended.

iii. **Advisory and Technical support:** The DICT will be providing guidance and support to public bodies in the adoption and use of cloud services, including best practices, training, and technical assistance in consultation with CSPs.

iv. **Promoting capacity building and awareness**: The DICT will be responsible for promoting capacity building and awareness-raising activities to support the adoption and use of cloud services by public bodies.

v. **Government Cloud Service Selection:** DICT will be responsible for building and coordinating the whole of government cloud selection in accordance with Section 25 and 26 of the DGA 2022.

vi. **Developing guidelines and standards:** The DICT will be responsible for developing guidelines and standards for the adoption and use of cloud services by public bodies accordance to Section 64 of the DGA 2022.

vii. **Managing risks and issues:** The DICT will be responsible for ensuring a secured holistic Government Cloud environment while the public bodies will play their part in managing risks in their own Virtual Private Cloud (VPC) environments. This will allow for scaling of Cloud Operations as well as services.

viii. **Facilitating partnerships:** The DICT will be facilitating partnerships and collaboration between public bodies, industry partners, and civil society groups and other stakeholders to promote and support the adoption and use of cloud services by public bodies.

ix. **Ensuring compliance:** The DICT will be responsible for ensuring that public bodies comply with the GCP and relevant laws and regulations in accordance with Part VI. - Enforcement of the DGA 2022.

x. **Monitoring and evaluation:** The DICT will be responsible for monitoring and evaluating the implementation of the policy, assessing its effectiveness, and making recommendations for improvement.

By fulfilling these responsibilities, the DICT will ensure that public bodies utilize government cloud in a highly efficient manner with a high standard for security, protect government data, and promote the adoption and use of cloud services by public bodies.

## 3.2 Public Bodies

Public bodies are responsible for consuming cloud services in coordination with the DICT and in accordance with the DGA 2022. By fulfilling their responsibilities and working closely with the DICT, public bodies can leverage the benefits of cloud computing to improve service delivery, reduce costs, and enhance the overall efficiency and effectiveness of government operations. To comply with the DGA 2022 and all relevant laws and regulations in PNG, public bodies must use cloud services in a manner that is consistent with their intended purpose, and ensure that they are used in accordance with the terms and conditions of the service agreement and according to the GCP.

Using cloud services in compliance with the policy and regulations, public bodies have a responsibility to empower their respective ICT divisions/branches. This is to ensure that all public bodies are in line with the digital transformation agenda led by the government. By doing so, digital infrastructure and services are delivered in a coordinated manner. This responsibility ensures that public bodies can optimize their use of cloud services and provide the best possible services to citizens while maintaining security and efficiency

Responsibilities of Public bodies:

i. **Compliance with Laws and Regulations:** Public bodies have a responsibility to comply with DGA 2022 and all relevant laws and regulations in PNG, including those related to data privacy, security, and protection.

**ii.** **Protection of Government Data:** Public bodies are responsible for the Protection of Government Data on their own Private Clouds (or VPCs), which are subsets of the overall GLC managed by the DICT. This includes ensuring the implementation of appropriate security measures and data protection protocols set by this policy including forthcoming Data protection and governance policy and legislation.

iii. **Adherence to Procurement Processes:** Public bodies have a responsibility to adhere to the procurement processes and standards enforced by the DICT as mandated by DGA 2022, including those related to the selection and use of cloud services.

iv. **Proper use of Cloud Services:** Public bodies have a responsibility to use cloud services in a manner that is consistent with their intended purpose, and to ensure that they are used in accordance with the terms and conditions of the service agreement and according to this policy.

v. **Regular Reporting:** Public bodies have a responsibility to provide regular reports to the DICT on their use of cloud services, including information on service consumption and performance, and any issues or concerns related to the services.

vi. **Capacity Building and Awareness Raising:** Public bodies have a responsibility to promote capacity building and awareness raising activities related to cloud computing, including training and support for their staff and stakeholders.

## 4.0 CLOUD SERVICE PROCUREMENT

Cloud service procurement will be in accordance with Public Finance Management Act (Amendment) 2018 and Digital Government Act 2022.

### 4.1 Government Cloud Selection Considerations

The decision on the selection of CSPs for the whole of government, will take into consideration existing government documents including Strategies, legislations, Policies and Security. In addition to those, other important lenses includes:

i. **Technical feasibility:** The government decision on selecting a CSP will be informed by a baseline assessment of the technical feasibility of implementing a government cloud, including evaluating the current infrastructure and identifying any potential technical barriers.

ii. **Cost-effectiveness:** The government decision on selecting a CSP will be inform by the costs associated with implementing and maintaining a government cloud, including infrastructure costs, staffing costs, and ongoing maintenance and support costs.

iii. **Vendor selection:** The government decision on selecting a CSP will be inform by carefully evaluating potential cloud service providers and select a vendor that can meet guidelines set by the government based on the specific needs and requirements of the government, including security, compliance, and service level agreements.

iv. **Data classification**: The government decision on selecting a CSP will be informed by the forthcoming data governance and protection policy and based on this policies data protection and classifications guidelines to ensure that data is stored and accessed appropriately based on its sensitivity and criticality.

v. **Integration with existing systems:** The government decision on selecting a CSP will be informed by the CSPs flexibility to accommodate the government needs to ensure that the government cloud is integrated with existing systems and applications used by public bodies to ensure a smooth transition and avoid disruption to operations.

vi. **User training and adoption:** The government decision on selecting a CSP will be informed by the CSPs customer support and training to provide adequate training and support to public body employees to ensure they are able to effectively use and adopt the government cloud.

vii. **Workload considerations:** The government decision on selecting a CSP will be informed by the public bodies workload considerations to support the workload requirements of public bodies. It involves identifying the workload characteristics, such as the size, complexity, criticality, and sensitivity of the data and applications to be migrated to the cloud.

## 4.2 Government Cloud Selection

Public bodies will work with DICT to deploy cloud infrastructure and services, with the opportunity to provide input and express their preferences. However, DICT through the PSICT Steering Committee will reserve the final say in making the ultimate decision on cloud selection, as mandated by the DGA 2022 and in accordance to the guidelines approved by the NEC.

Selecting the right cloud services is crucial to the success of the policy, as cloud services vary greatly in terms of their functionality, performance, security, and cost. Therefore, the selection, procurement and coordination of the Cloud will be done in accordance with Section 25 and 26 of the DGA 2022. Based on best practice, the Government will use the following guidelines to select one or more cloud service providers (CSP) that meets the specific needs of the PNG context:

i) **Compliance:** The government will select a CSP that is compliant with applicable Papua New Guinea laws and regulations.

ii) **Security:** The government will prioritize the selection of a CSP that adheres to international security standards, such as ISO 27001 to ensure the highest level of security for sensitive data.

iii) **Privacy:** The government will select a CSP that adheres to the highest privacy standards, such as the European Union's General Data Protection Regulation (GDPR) to protect the privacy of citizens' data

iv) **Data Sovereignty:** The government will select a CSP that allows government to determine where their data is stored, how it is secured, and who has access to it.

v) **Interoperability:** The government will prioritize the selection of a cloud service provider that supports open standards and protocols to ensure that cloud services can be integrated and used effectively across different government agencies.

vi) **Performance:** The government will select a CSP that offers high-performance to ensure that government services can be delivered efficiently and effectively.

vii) **Cost:** The government will prioritize the selection of a CSP that offers competitive pricing and cost-effective billing to ensure that government resources are used efficiently.

viii) **Availability:** The government will select a CSP that offers reliable and resilient services to ensure that government services are always available to citizens, within agreed SLAs.

## 4.3 Service-Level Agreements (SLAs) with CSPs

Agreeing service levels (in some cases through Service Level Agreements (SLAs)) is a critical component as this defines the expected level of service from CSP and ensure that public bodies receive the appropriate level of support and service.

The DICT on behalf of the government will review and negotiate, if required, the SLA with CSPs before engaging their services. This is to ensure that the SLA or other agreed services align with the PNG government agency's service requirements and expectations.

The SLAs will include the provisions for the following:

i) **Performance:** The SLA should define the expected level of performance for cloud services, such as network latency, response time, and availability. This should be based on the needs of the government agency, as defined by its service requirements.

ii) **Service Availability:** The SLA should specify the expected uptime of the cloud service and define the service credits or penalties that will apply if the service fails to meet this expectation. This should be aligned with the business continuity and disaster recovery requirements of the government agency.

iii) **Data Security:** The SLA, or other documentation such as security standards, should define the security requirements for government data stored or processed by the cloud service, and the measures that will be taken to ensure that data is protected. This should include provisions enabling public bodies to undertake data backup, data retention, and data recovery in case of a security breach. There should be clear recognition of the shared responsibility model and the responsibilities of the customer and the cloud service provider respectively.

iv) **Support:** public bodies should agree with the CSP the level of support that will be provided to public bodies using the cloud service, including the availability of technical support, customer service, and training.

v) **Compliance:** the SLA, or contract, should address regulatory requirements and compliance with applicable Papua New Guinea laws and regulations

vi) **Reporting and Monitoring:** Public bodies should understand and agree to monitoring and reporting arrangements and requirements for the cloud service, and where the CSP is providing an agreed reporting service this should include clarity on the frequency of reporting, the metrics that will be monitored, and the format of the reports.

vii) **Agreed service levels and expectations:** Public bodies in consultation with DICT should ensure clear and measurable service expectations are agreed, including through service level agreements (SLAs) where applicable, for cloud services, including on performance and availability, and DICT should ensure relevant

security standards and shared security responsibility model responsibilities have been identified

## 4.4 Cost Model Considerations

The cost model is a critical aspect that will be carefully planned and managed by DICT as the coordinating agency to ensure that the government maximizes the benefits of cloud computing while keeping costs under control. The government will be considering different cost models based on best practice that will help the government understand the cost implications of moving to the cloud so that the government make an informed decisions about which cloud services to procure and how to use them efficiently.

The government will consider the following key considerations to adopting a cost model:

i. **Total Cost of Ownership (TCO):** The cost model will consider the TCO of cloud services, including the cost of procurement, implementation, operation, and maintenance of cloud services. It will also consider the cost of data migration and integration with existing systems.

ii. **Consumption-Based Pricing:** Consumption-based pricing models to be used wherever possible to ensure the Government only pay for the cloud services they use. This will help to optimize costs and prevent wastage.

iii. **Cost Optimization:** The cost model to provide guidance on cost optimization techniques such as resource sharing, automated scaling, and rightsizing of cloud resources. This will help the Government to reduce their overall cloud costs.

iv. **Pricing Transparency:** The cost model will ensure pricing transparency by providing clear and consistent pricing information for cloud services. This will help the Government to make informed decisions about which cloud services to procure.

v. **SLA Requirements:** The cost model will consider the SLA requirements for cloud services and ensure that the cost of meeting these requirements is factored into the overall cost model.

vi. **Training and Support:** The cost model will include the cost of training and support for the Government staff to ensure that they are equipped with the skills and knowledge needed to use cloud services effectively.

## 4.5 Billing and Payment Considerations

Billing and payment are critical and will be carefully planned and managed. The billing and payment process for cloud services will be designed to ensure that government only pay for the cloud services it uses, and that the payment process is secure, transparent, and efficient.

The Government will consider the following key considerations for billing and payment of the cloud services:

i. **Consumption-Based Billing**: Public bodies will only be charged for the actual usage of cloud services. This will be achieved through consumption-based billing models, where the cost of cloud services is based on the actual usage of resources such as computing power, storage, and data transfer.

ii. **Transparent Pricing:** The Government will ensure CSPs provide clear and consistent pricing information for their services, including any taxes or fees that may apply. This will help the Government to make informed decisions about which cloud services to use and help to prevent unexpected charges.

iii. **Secure Payment Processes:** Payment processes for cloud services to be secure and compliant with relevant regulations and industry standards. This includes the use of secure payment gateways and the adoption of industry-standard security protocols such as Transport Layer Security (TLS)

iv. **Payment Methods:** CSPs to offer a range of payment methods to the Government including electronic payments and invoicing. This will help to ensure that the payment process is efficient and convenient for the Government.

v. **Payment Terms:** Payment terms for cloud services to be clearly defined and agreed upon by both parties. This includes the frequency of payments, the due date for payments, and any penalties for late payments.

vi. **Billing and Payment Management:** The DICT (DICT) will establish a billing and payment management system in collaboration with CSPs that will enable public bodies to monitor their cloud usage and expenses. This includes regular reporting and analysis of cloud usage, as well as tools for tracking and managing cloud expenses.

## 5.0 IMPLEMENTATION OF GOVERNMENT CLOUD

The implementation of the government cloud will be done in phases, prioritizing the public bodies that can achieve the quickest and greatest return on investment. The implementation will be done in accordance with the following steps:

### 5.1 Phase One: Assessment and Preparation

The first phase will involve conducting a thorough assessment of the current infrastructure, identifying areas that need to be upgraded, and preparing the public bodies for cloud adoption. The assessment will involve the following:

i) Identifying the public bodies' existing IT infrastructure, applications, data, and services to determine their readiness for migration to the cloud.

ii) Evaluating the current security controls and assessing whether they meet the minimum-security requirements including cloud standards set by the government.

iii) Developing a migration plan that outlines the steps to be taken to migrate to the cloud, including timelines, responsibilities, and milestones.

iv) Developing a training plan to ensure that public body employees have the necessary skills and knowledge to effectively use the cloud services.

v) Preparing a budget for the cloud migration, including the costs associated with infrastructure upgrades, staffing, and ongoing maintenance and support.

### 5.2 Phase Two: Cloud Adoption

The second phase will involve migrating public bodies' applications, data, and services to the cloud. This phase will involve the following:

i) Procuring cloud services from selected CSPs in accordance with the guidelines outlined in Section 4.0 and signing SLAs.

ii) Upgrading the infrastructure to ensure compatibility with the cloud services.

iii) Migrating data and applications to the cloud in a phased approach, based on the prioritization set out in the migration plan.

iv) Providing training and support to public body employees to ensure that they can effectively use the cloud services.

## 5.3 Phase Three: Optimization and Expansion

The third phase will involve optimizing and expanding the government cloud to ensure that it continues to meet the evolving needs of the public bodies. This phase will involve the following:

i) Reviewing the performance and usage of the cloud services to identify areas for optimization and improvement.

ii) Upgrading the infrastructure and software to ensure that the cloud services remain compatible with the evolving needs of the public bodies.

iii) Expanding the government cloud to additional public bodies as needed, based on the prioritization set out in the migration plan.

iv) Continuously monitoring the security of the cloud services to ensure that they remain compliant with the government's security requirements and standards.

## 5.4 Phase Four: Continuous Improvement

The final phase will involve continuous improvement of the government cloud to ensure that it remains aligned with the needs of the public bodies and the evolving technology landscape. This phase will involve the following:

i) Regularly reviewing the cloud services to identify areas for improvement and enhancement.

ii) Working with CSPs to identify new cloud services and technologies that can benefit the public bodies.

iii) Engaging with public body employees to identify their evolving needs and preferences for the cloud services.

iv) Updating the cloud services and infrastructure to incorporate new features and capabilities as needed.

## 6.0 SECURITY OF GOVERNMENT CLOUD

The security of government cloud is a critical concern for public bodies, as it involves the protection of sensitive and confidential data. Cloud governance refers to the set of policies, procedures, and processes that are put in place to ensure that cloud infrastructure and services are used in a secure, efficient, and cost-effective manner, and that the organization's goals and objectives are met.

The DICT is responsible for coordination and security of the use of cloud services across the whole of government, while public bodies are responsible for implementing appropriate security measures and ensuring compliance with government-mandated cloud standards, guidelines, and policies.

### 6.1 Cloud Security

The cloud security requirements are designed to promote a secure and efficient cloud computing environment for the government. By adhering to these requirements, public bodies can leverage the benefits of cloud computing while ensuring the protection of government data and in compliance with relevant laws and regulations.

It's important for public bodies to adhere to these requirements to ensure the protection of government data and compliance with relevant laws and regulations when using cloud computing services

Cloud Control Requirements:

i. **Data Classification:** Public bodies should classify government data in accordance to Section 45 of the DGA 2022 and forthcoming Data Governance, Protection and Privacy Policy and implementing appropriate controls to protect and secure the data.

ii. **Access Control:** Public bodies should have security measures in place to ensure that only authorized users have access to the cloud environment and its services.

iii. **Encryption:** Public bodies should ensure strong encryption must be used to protect government data both in transit and at rest using industry-standard encryption protocols. This has to be done in accordance with Section 52 and 53 of DGA 2022 for provincial governments and districts.

iv. **Vulnerability Management:** Public bodies should perform regular vulnerability assessments and penetration testing to identify and mitigate potential security risks

v. **Incident Management:** All Public bodies should ensure documented incident management process must be in place to respond to security incidents and data breaches and to ensure that they are promptly reported to relevant stakeholders such as DICT.

Cloud Accountability Requirements:

vi. **Compliance with Laws and Regulations**: Public bodies should ensure that all cloud services and operations are compliant with relevant laws and regulations in PNG, including those related to data privacy, security, and protection

vii. **Agreed Service Levels and Expectations:** Public bodies in consultation with DICT should ensure clear and measurable service expectations are agreed, including through service level agreements (SLAs) where applicable, for all cloud services, including on performance and availability, and DICT should ensure relevant security standards and shared security responsibility model responsibilities have been identified.

viii. **Audit and Reporting:** Public bodies should ensure that regular audits and reporting is conducted to ensure compliance with cloud policies and SLAs and to identify any areas for improvement.

ix. **Contract Management:** DICT will ensure that contracts with CSP must include clear terms and conditions related to service performance, data protection, and security.

x. **Training and Awareness:** Public bodies should ensure regular training and awareness activities are conducted to ensure that government employees and stakeholders are aware of their responsibilities related to cloud computing, and that they understand best practices for using cloud services.

All public bodies that use cloud computing services must adhere to these requirements to ensure the protection of government data and compliance with relevant laws and regulations. The DICT is responsible for managing the cloud environment in a secure and efficient manner, while ensuring that the cloud control and accountability requirements are met while each public body to manage its own Virtual Private Clouds (VPCs) when using cloud computing services.

### 6.1.1 Government On-premise Data Center

Government On-premise Data Center (GovDC) and VPCs are both private cloud solutions designed for different use cases. GovDC is a specific on-premise cloud infrastructure solution for public bodies that includes mini operational data centers for government agencies. In contrast, VPCs are virtual private clouds that can be used by any organization, including public bodies, that requires a private and isolated cloud environment.

By managing their own private clouds, public bodies can have greater control over their cloud environment and can customize the network settings, security policies, and resource allocation to meet their specific needs. However, they must adhere to the cloud standards, control mechanisms, and accountability requirements outlined by the

government to ensure the security and compliance of their cloud computing environment. outlined by the government to ensure the security and compliance of their cloud computing environment. This includes following access control measures such as authentication, authorization, and activity monitoring, as well as ensuring data encryption during transit and at rest.

Cloud Security requirements for GovDC:

i) **Cloud Security Architecture**: Public bodies should implement appropriate security controls to ensure the security of data stored in the cloud. Public bodies must provide a detailed description of the security architecture used to protect the data, including the security measures they have implemented to protect the data from unauthorized access or disclosure. The security architecture must be designed and implemented in accordance with the relevant PNG laws and regulations, as well as international best practices and standards

ii) **Security Monitoring and Response:** Public bodies should be able to detect and respond to security incidents in a timely and appropriate manner. Public bodies must implement appropriate measures to monitor their systems and networks for security incidents and respond to any such incidents promptly and effectively. Public bodies must have in place an incident response plan that outlines the steps to be taken in the event of a security incident.

**iii)** **Third-Party Audits:** Public bodies should be regularly audited by an independent third-party to verify compliance with applicable security standards and controls. The audit must be conducted at least annually and must include an assessment of the security architecture, security monitoring and response, and other security measures implemented by the public body. The Audit will be as per Section 16 and 17 of the DGA 2022.

iv) **User Access and Control:** Public bodies should implement appropriate measures to restrict access to the use of Government cloud to authorized personnel only. Public bodies must ensure that access to the Government cloud is granted only to authorized personnel and that the access rights are regularly reviewed and updated as necessary. Access to sensitive data must be restricted to only those personnel who have a need to know.

**v)** **Data Encryption:** Public bodies should ensure that all data stored in the cloud is encrypted and protected from unauthorized access. Strong encryption algorithms must be used to protect the data, and the encryption keys must be securely managed.

**vi)** **Data Retention and Disposal:** Public bodies should implement appropriate measures to ensure that data stored in the cloud is retained and disposed of securely. Public bodies must ensure that data is only retained for as long as necessary and is securely disposed of when no longer needed. Public bodies must also comply with any relevant data retention laws and regulations.

vii) **Data Backup and Recovery**: Public bodies should have appropriate measures in place to ensure that data stored in the cloud is backed up regularly and that a secure backup and recovery process is in place. The backup and recovery process must be tested regularly to ensure that it is effective.

viii) **Incident Reporting:** Public bodies should have a process in place to promptly report any security incidents or breaches to the DICT. The process must include steps to contain the incident and mitigate any damage, as well as to investigate the incident and take appropriate corrective actions

## 6.2 Data Security

The data on cloud will depend on the classification and sensitivity. Classification indicates the level of sensitivity of the data and determines the appropriate security controls required to manage the associated risks. The data on the cloud should be assessed and classified based on its sensitivity to ensure adequate protection against potential threats.

Data Ownership, Collection, Classification, Governance, Production, Storage, Access, sharing, and Security of the data on cloud will be subject to Section 36 and Part V of the DGA 2022.

Section 36 of DGA 2022 covers Open Data, while Part V of DGA 2022 covers; Electronic Data Governance Across Government, Classification of Electronic Data, Production, etc., of Electronic Data, Public Access to Electronic Data, Electronic Data Collection and Storage, Ownership of Data in Central Electronic Data Repository, Electronic Systems Integration, Electronic Data Register, Electronic Data Sharing, and Electronic Data in Provinces and Districts.

The government has recognized the need for Data Sovereignty on cloud and has taken appropriate measures. Hence, what data to be on cloud will be subject to section 2.1.4 of this policy.

## 6.3 Security Measures

Public bodies should have security measures in place to ensure that only authorized users have access to the cloud environment and its services. Access control measures for the government cloud are critical to ensuring the security of government data and services.

Following are access control measures:

i) **Access Control:** All government agencies should ensure that access control measures are in place to ensure that only authorized users are allowed access to the government cloud and services.

ii) **Authentication:** All government agencies should implement strong authentication measures, such as multi-factor authentication or biometric authentication, to ensure that only authorized users can access the government cloud and VPCs.

**iii)** **Authorization:** All Public bodies should ensure that there is an appropriate authorization process in place before granting access to users. This process should be based on the user's roles and responsibilities within the cloud environment and VPCs.

iv) **Access Rights:** Access rights should be limited to users based on their roles and responsibilities within the cloud environment and VPCs. This should be enforced through strict access control policies and monitoring.

v) **Activity Monitoring:** Public bodies should monitor user activities to ensure that they are not accessing unauthorized data or services. This should be done in collaboration with the DICT and CSPs.

vi) **Data Encryption:** All Public bodies should ensure that data encrypted during transit and at rest within the government cloud and VPCs. Open or public data should not by any means encrypted or restricted.

By implementing these access control measures, public bodies will ensure that their data and services are secure and protected from unauthorized access or malicious activities on cloud.

## 7.0 COMPLIANCE

Compliance of the cloud will be in accordance to the DGA 2022. Compliance requirements are an important consideration for the Government. DICT will provide guidance and support to public bodies in meeting compliance requirements.

Key compliance requirements that public bodies must ensure when implementing the policy to avoid penalties includes:

i. **Data Privacy and Security:** Public bodies must ensure that data is managed based on their sensitivity as prescribed under section 4.2 of this policy. This includes compliance with the DGA 2022, forthcoming PNG Data Governance and Protection Policy and legislation, and any other relevant laws and regulations related to data privacy and security.

ii. **Government Policies and Standards:** Public bodies must comply with relevant government policies and standards related to cloud services. This includes the ICT policies, standards and guidelines set by the relevant Government stakeholders.

iii. **Industry Standards:** Public bodies to adopt global industry standards and best practices such as ISO/IEC 27001 for information security management and ISO/IEC 27018 for protection of personal data.

iv. **Service Level Agreements (SLAs):** DICT to ensure that SLAs with CSPs are in place and comply with government policies and standards. This includes ensuring that SLAs address availability, performance, security, and data management requirements.

v. **Contractual Obligations:** DICT should ensure that contracts with CSPs comply with relevant laws, regulations, policies, and standards. This includes ensuring that contracts address data ownership, security, and privacy, and that they provide for appropriate audit and compliance reporting.

vi. **International Standards and Regulations:** If Public bodies use cloud services that involve cross-border data transfer, they must comply with relevant international standards and regulations as stipulated through mutual agreements between countries.

## 8.0 DISASTER RECOVERY & REGULAR REVIEW

### 8.1 Disaster Recovery

Public bodies should use CSP services to enable disaster recovery by public bodies in accordance with their disaster recovery plan, standards and policies in place. DICT will coordinate with public bodies to ensure that they have a disaster recovery plan, standards and policies in place.

Key considerations for disaster recovery includes:

i. **Disaster Recovery Planning:** Public bodies should have a disaster recovery plan that outlines the procedures to be followed in the event of a disaster or outage. This will include procedures for data backup and recovery, system recovery, and communications.

ii. **Data Backup and Recovery**: Public bodies should have a backup and recovery plan in place to ensure that government data is protected and recoverable in the event of a disaster. The backup plan to be regularly tested to ensure that it is effective.

iii. **Redundancy and Failover:** DICT should have a redundancy and failover mechanisms in place to ensure that government services remain available in the event of a disaster. This will include redundant data centers or servers, load balancing, and automatic failover.

iv. **Testing and Validation:** Disaster recovery plans and mechanisms should be regularly tested and validated to ensure that they are effective and can be executed quickly and accurately.

v. **Contractual Obligations:** DICT will ensure that public bodies have made arrangements for disaster recovery including specifying the expected recovery time objective (RTO) and recovery point objective (RPO) for government services. Public bodies should work with their CSP to architect their workloads appropriately to meet RTO and RPO.

vi. **Training and awareness:** DICT in collaboration with CSPs will be providing training and awareness to public bodies and

### 8.2 Regular Reviews

Regular reviews of the policy will be conducted on a need basis to ensure it remains relevant and aligned with national strategies, with input from stakeholders including public bodies, CSPs, and industry experts. The review process will focus on identifying opportunities for continuous improvement and assessing the effectiveness of policy

implementation. Communication strategies will also be used to ensure public bodies and stakeholders are aware of any changes to the policy.