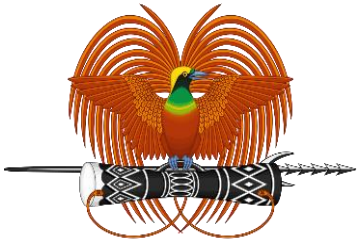
2023



Independent State of Papua New Guinea

DRAFT GOVERNMENT CLOUD POLICY 2023 (v2.1)

Table of Contents

INTRODUCTION

The Government of Papua New Guinea is making the strategic shift to cloud usage through the use of public and private cloud services. The Government Cloud Policy (GCP) provides guidance and direction to PNG Government Departments and Agencies in making use of Government Sanctioned Cloud (GSC) services.

Government Departments/Agencies and provincial governments must use this policy to ensure their consumption of cloud services is efficient, secure, and financially sound. In doing so, this policy will enable alignment, consistency, optimal commercial outcomes, reduced risk and improved service delivery to the citizens across PNG.

The GCP must be used by government agencies in understanding the available cloud services, determining the appropriate future usage of cloud services as well as liaising with the Department of Information and Communications Technology (DICT) as the coordinating agency mandated through the Digital Government Act 2022 (DGA 2022) under Section 25-26 and as per NEC Decision No. 39/2021, 40/2021 & 47/2021 in coordinating Cloud services, secure data exchange and shared services appropriately.

Policy Statement

Digital infrastructure such as GSC underpins the delivery of digital services. Rolling out widespread, modern, and resilient infrastructure with sufficient capacity is key to development of the ICT sector in PNG.

The PNG Government is determined to expand digital infrastructure such as GSC which underpins the delivery of digital services which will significantly improve business continuity and quality of service delivery in the public sector. This policy contributes to this goal by enabling the PNG Government (or public sector) access to cloud computing and other technologies enabled by the cloud, such as Artificial Intelligence, Machine Learning, or the Internet of Things among others. This is essential for the creation of an environment that spurs development and innovation in an organic way.

This policy represents a significant step aiming to drive greater uptake of cloud services in the public sector by adopting a Cloud computing to promote a better approach to infrastructural investments and efficient IT deployment in the public sector.

Purpose

Papua New Guinea (PNG) needs a whole of government cloud policy to provide a framework for the adoption and use of cloud computing services across all government agencies. Cloud computing has the potential to offer significant benefits to government agencies, including cost savings, improved scalability, and increased flexibility. However, without a clear policy framework, government agencies may face challenges related to data security, service quality, and vendor lock-in.

This whole of government cloud policy will address these challenges by providing best practices and coordination in relation to the consumption of Cloud computing solutions that the PNG Government departments and Agencies will use to support the processing, sharing, storage and management of their data. The policy also provides guidance to users of cloud computing solutions in the course of executing their duties as well as in the context of their private use of cloud solutions IT that may interface with certain government Departments/Agencies data.

Rationale

Over the last decade, organizations, people, billions of connected devices generate, process, and use data every day over the cloud infrastructure. Much of the Government data has moved online and as such a policy is needed to protect it.

Cloud Computing is not a new concept as many public agencies and private companies have been using cloud services to drive better business outcomes. Cloud computing delivers value to agencies through increased business flexibility, operational effectiveness and improved visibility across business services and ICT investments. The use of cloud technologies and techniques in ICT delivery provides the agility, flexibility, scalability, and robustness required to operate in a digital environment.

The cloud policy is aimed at addressing the challenges of acquiring and deploying IT systems in the public sector. Even though IT systems of some Government Departments and provincial governments have significantly advanced individually, some are still struggling to effectively digitize their operations due to lack of resources for acquiring and deploying appropriate computing resources while others have no dedicated ICT presence.

During the Digital Transformation Officers (DTOs) conference that was held in 2022, a Digital Government survey was conducted. During the analysis of the survey report we noted that out of the 58 agencies that have participated, less than 41% of the agencies have a dedicated had an IT division/section and more than 55% did not have an IT division/section. Note that this is only 58 agencies out of **xx** government agencies we have including provincial governments.

Based on the above challenges experienced currently by majority of government agencies and district and provincial governments, we have noted that most of these challenges falls under following challenges which includes but not limited to;

i. High cost of IT investments and poor sustainability of IT projects;
ii. Shadow IT environment that is tough to manage, difficult to operate and nearly impossible to secure;
iii. Inefficient and un-scalable IT environment;
iv. Poor interoperability of IT systems and inability to effectively share information and IT resources; and
v. Use of outdated systems where computer systems, applications, and software that are no longer widely used or supported, but are still in use by some government agencies due to historical reasons or functional requirements. These systems may

have been developed using outdated technology or programming languages, and may not be compatible with modern software or hardware,

vi. Lack of support for ICT in most of the government agencies especially in the district and provincial governments.

This policy will address these challenges faced by such agencies and governments and also guide those who have advanced in their use of cloud. The Policy will play an important role in enabling the development of the country by facilitating the growth of the digital economy. Key benefits of cloud computing are its potential to:

i. improve access to services and information, particularly in remote or underserved areas. By enabling government agencies to store and access data and applications in the cloud, cloud computing can help to overcome barriers to service delivery and promote greater efficiency and productivity through promotion of digital services offered by cloud.

ii. reduce costs by providing access to shared resources, eliminating the need for expensive on-premises hardware and infrastructure. This will be particularly beneficial for PNG, which faces budgetary constraints and limited resources for IT infrastructure.

iii. to provide a consistent framework for cloud adoption across government agencies, promoting interoperability and reducing duplication of effort. This is to ensure that government agencies are using cloud services in a coordinated and efficient manner, while also reducing the risk of vendor lock-in.

iv. to support PNG's broader digital transformation goals, such as the development of a digital economy and the promotion of e-government services. By providing a framework for the secure and effective use of cloud services, a Government Cloud Policy will help to build trust in digital technologies and promote the adoption of innovative solutions.

Alignment

This policy will ensure that the adoption and use of cloud computing services align with the overall goals and objectives of the government, and help prevent government agencies from adopting cloud services in a fragmented and uncoordinated manner. This will reduce costs and enable more effective management of cloud computing resources across government agencies.

Government Cloud policy takes its cue from the PNG Digital Transformation Policy 2020[1] *National ICT Policy 2008* and direction from the NEC Decision No. 39/2021[2] to develop a Cloud Policy for the Government. It provides linkage to the DICT Corporate Plan 2020 - 2024 as per NEC Decision No. 252/2020 to achieve the desired outcomes of the Policy.

[1] Cloud policy is one of the policy scope under Digital infrastructure

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

Furthermore, this Policy will guide government agencies in their adoption and consumption of cloud services by incorporating the emerging technologies and cyber security landscapes.

The Government Cloud Policy is 'Cloud first' meaning Government agencies must make use of cloud services as the default. Where private cloud services are not suitable or available for the agency's requirements/use, sanctioned cloud services such as GSC, recommended by DICT as the coordinating agency, can be used.

Mandate

The PNG GCP was developed in consistent with **NEC Decision No. 39/2021.** The government re-affirmed DICT as the coordinating agency for:

i. public sector cloud infrastructure and services specifications; and
ii. shared ICT services to all public bodies.

The government further directed the Department of Information and Communication Technology (DICT) to commence delivery of shared ICT services to all public bodies through a Virtual Cloud arrangement and commence formulation of a **Government Cloud Policy**. The government also directed all public bodies to coordinate the planning and implementation of all cloud related services with DICT and take full advantage of cloud automation practices within Government agencies.

The **NEC Decision No. 39/2021** is further enhanced by **Digital Government Act 2022 (DGA 2022) under Section 25-26** for DICT to establish a Government Leased Cloud Infrastructure for connectivity of virtual private networks and digital services for all public bodies and build a Government Private Cloud Infrastructure as part of the Government Private Network for delivery of digital services.

Objective

The Policy provides guidance and direction to enable Government agencies to achieve the following seven objectives:

i. **Security** – adhering to this policy guidance, regarding usage of cloud services will ensure Government agency assets and data are secured. Assuring citizens and agencies that their information and data stored in the cloud is secure, accurate and reliable is key to the success of all ICT policies.

ii. **Consistency & Alignment**– Government agencies receive common direction from DICT as the lead agency in the consumption of cloud service across the PNG Government agencies in accordance with governments strategic objectives and priorities such as National Development Goals, Vision 2050, MTDP III 2018-2022 and PNGDSP 2010-2030 allowing them to make consistent usage of the GSC services.

iii. **Modernisation** – The Policy guides government agencies in consuming cloud services to modernize their ICT and Digital service delivery in line with the Digital Transformation Policy 2020. This policy enables modernisation through lineage to update business processes for security, and consumption of cloud services. Seven principles that will guide agencies in the process and align with our objectives include;

a. make risk-based decisions when applying cloud security design services for the cloud;
b. design services for the cloud;
c. use government sanctioned cloud as the default;
d. use as much of the cloud as possible;
e. avoid customisation and use cloud services as they come if not sure;
f. take full advantage of cloud automation practices; and
g. monitor the health and usage of cloud services in real time.

iv. **Procurement** - DICT as the lead agency mandated through the DGA 2022 under Section 25 & 26, will coordinate the cloud procurement agreement (CPA) that will make responsibilities and accountabilities of Cloud service providers clearer.

v. **Innovation** – By enabling Government agencies to use new cloud capabilities such as Cloud computing, AI, machine learning, data analytics etc, and by leveraging cloud services, the Government agencies will be able to keep up with services released by industry, without having to build and maintain each capability. The DICT in collaboration with CSPs will develop a training schedule or through a portal to share knowledge and expertise of cloud products and services and will explore and develop shared platforms that different services can use, reducing duplication.

vi. **Optimal Commercial Outcomes** – Government agencies will contribute to optimizing Government commercial outcomes by using strategic partnerships with External and Internal cloud service providers (eg; AWS, Dataco, among others), for the whole of government cloud coordination.

CLOUD OVERVIEW

The Cloud refers to numerous data centers managed by Cloud Services Providers (CSP) (third party vendors) 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 Papua New Guinea, 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[3]:

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.

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.

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

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.

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

Cloud Deployment Models

This section defines and describes the three primary cloud computing deployment models deployed by Cloud Service Providers to their customers and Governments;

i. **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.

ii. **Private Cloud:** A Private cloud is cloud infrastructure 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, private cloud computing gives businesses many 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 Private clouds could deliver a higher level 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. Private clouds require the same staffing, management, and maintenance expenses as traditional data center ownership such as the one delivered in 2014 by IGIS.

iii. **Hybrid Cloud**: A hybrid cloud is a computing environment that combines an on-premises datacenter (also called a Private Cloud) with a Public Cloud, allowing data and applications to be shared between them. A Hybrid Cloud uses a combination of several different cloud environments. Hybrid cloud often includes a combination of public cloud and private cloud, frequently in combination with some on-premises infrastructure.

The government will leverage on the services offered by the public cloud and the use of private cloud or on-premises cloud infrastructure.

In this policy, the government deploy cloud in Hybrid model. The cloud infrastructure will be composed of Public and Private cloud (or GovDC) which is dedicated to GoPNG through a dedicated data network and cloud connectivity which will be managed by the DICT as the coordinating agency for the whole-of-government as per mandate through the DGA 2022 under Section 25 and 26. This will ensure that government agencies consume cloud infrastructure in a highly efficient manner with a high standard for physical security.

Cloud Service Deployment Models

There are three (3) main cloud service models that are used through public, private and hybrid clouds that the government will adopt. These include:

i. **Infrastructure as a Service (IaaS):** is a cloud service model that harnesses the integration of the traditional physical IT resources and infrastructure combined with specialized infrastructure services that are cloud based. In this context, 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 company or customer with the same technologies and capabilities as a traditional data center, including full control over server instances.

Government Agencies will responsible for managing aspects such as databases, applications, runtime, 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 government agencies will be given the opportunity to choose the infrastructures of their choice depending on their organizational needs.

ii. **Platform as a Service (PaaS):** This 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 government agencies 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 and the applications they will deploy.

iii. **Software as a Service (SaaS):** With SaaS, the government agencies 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 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 government agencies centric applications with its configuration settings.

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 agencies 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 GSC currently hosts the majority of Government department/agency ICT infrastructure, making it the launchpad for departments/agencies looking to connect existing systems or workloads to GSC (or Hybrid Cloud) services through dedicated data network connectivity and cloud services. It enables agencies 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 Government departments/agencies, the GSC 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 Government departments/agencies 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 Government departments/agencies 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.

Government Cloud Management

This section defines the responsibilities of the government, government agencies, and other stakeholders in relation to the adoption and use of cloud services. The PNG GCP provides a framework for the adoption and use of cloud services that is secure, compliant, cost-effective, and consistent across government agencies. This is to promote the efficient and effective delivery of government services and support PNG's broader digital transformation goals.

PNG Department of ICT

The Papua New Guinea Department of Information and Communication Technology will play a leading role in coordinating the development, implementation, and management of the cloud. As per mandated through the Digital government Act 2022 under Section 25 and 26, DICT will provide guidance and support to government agencies, monitoring and evaluation, coordination of implementation, development of guidelines and standards, management of risks and issues, ensure compliance, promote capacity building, and facilitation of partnerships.

The DICTs leading role will include 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 government agencies, industry partners, and civil society groups.

ii. **Coordinating implementation:** The implementation of the policy will be as per the Digital Government Act 2022 under Section 25 and 26, this includes coordinating the implementation of the policy across government agencies, ensuring that it is being implemented in a consistent and coordinated manner.

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

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 government agencies.

v. **Government Cloud Service Selection:** DICT will be responsible for building and coordinating the whole of government cloud selection as per the Digital Government Act 2022 under Section 25 and 26.

vi. **Developing guidelines and standards:** The DICT will be responsible for developing guidelines and standards for the adoption and use of cloud services by government agencies inconsistent with Section 64 of the DGA 2022.

vii. **Managing risks and issues:** The DICT will be responsible for identifying and managing risks and issues related to the adoption and use of cloud services, including issues related to security, privacy, compliance, and interoperability.

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

ix. **Ensuring compliance:** The DICT will be responsible for ensuring that government agencies comply with the Government Cloud Policy and relevant laws and regulations in consistent 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.

Cloud Service Decisions

DICT as the coordinating agency mandated by through DGA 2022 under Section 25 & 26, will provide guidance on the selection of cloud services including making cloud service decisions and the considerations that will influence service selection. All government agencies will liaise with DICT on the deployment of cloud infrastructure and services.

The following three lenses of Strategy and legislation, Policy, and Security will be considered to inform the Government cloud service decisions.

i. **Strategy & Legislative Lens**: is driven by the Goals and Strategic objectives of the Vision 2050, MTRS 2030, DGA 2022, Digital Government Plan 2023-2027 and MDP IV (draft). The cloud decision will take into consideration these strategy and legislative lens. Following are the set goals to achieved Goals and Strategic objectives of the Strategy and legislative lens:

   a. To establish and improve a nationally coordinated management and promotion of secure electronic government services, particularly Government to Government (G2G), Government to Business (G2B), and Government to Citizen (G2C) through federation with standardization principles and enable and trigger structured establishment and consequently promulgate PNG's digital economy.

   b. To build national infrastructure, including software and applications ecosystems required to facilitate digital government and other relevant ICT facilitated service delivery for the benefit of the citizens.

   c. To develop models, programs, and projects for digital government delivery.

d. To develop benchmarks, standards, guidelines and framework of interoperability for digital government applications, systems, processes and organizations.

e. To develop, operate and maintain a national e-government system which will enable seamless data collection, integration, shared services, and authentication.

ii. **Policy Lens:** is driven by the Digital Transformation Policy 2020 and National Cyber Security Policy 2021, NEC Decision No. 39, 40 and 47 of 2021 and further enhanced by the DGA 2022 under Section 25 and 26. These drivers give clear authority for DICT to be the coordinating agency:

a. for public sector cloud infrastructure and services specification, standards and implementations,
b. for shared ICT services to all public bodies,
c. to commence forthwith the delivery of ICT shared services to all public bodies through Virtual Private Cloud arrangement, and
d. commence formulation of PNG Government Cloud Policy
e. to coordinate the planning and implementation of all cloud related services.
f. for all public sector digital service implementation including alteration, and procurement of new ICT and digital infrastructure and services, effective of the date of this Decision,
g. to provide regular updates on the implementation of the decision that DICT be the coordinating agency in formulating Government Cloud Policy
h. to take a whole-of-government approach in the use of cloud infrastructure and services,
i. to secure government cloud to ensure high level of security and protection of highly sensitive/personal citizen data,
j. to develop practical guidance to help agencies develop knowledge, skills and abilities to choose, secure, adopt and manage cloud-based services,
k. to reduce duplication across government agencies and forgo the need for expensive custom based solutions of on-premises infrastructure,
l. to make risk-based decisions for government agencies when applying cloud security, and
m. to take full advantage of cloud automation practice within government agencies.
n. agencies must operate all private cloud services through GSC and/or GovDC

iii. **Security Lens**: is driven by Digital Government Act 2022, Cybercrime Code Act 2016, National Cyber Security Policy 2021, and government agency specific security plans. The cyber security drivers are:

a. Agencies must meet cyber security requirements outlined in the Cybercrime Code Act 2016 and PNG National Cyber Security Policy 2021.

b. Agencies must consider the protective marking of their data and implement security mechanisms that meet these data classification requirements.

Government Agencies

The responsibilities of government agencies in consuming cloud services in coordination with the DICT and in compliance with the DGA 2022 is designed to promote a secure, efficient, and transparent cloud computing environment for the government of PNG. By fulfilling their responsibilities and working closely with the DICT, government agencies will leverage the benefits of cloud computing to improve service delivery, reduce costs, and enhance the overall efficiency and effectiveness of government operations.

Responsibilities of Government Agencies:

i. **Compliance with Laws and Regulations:** Government agencies 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:** The protection of the Government data on the cloud will be in consistent with DGA 2022 and the Government agencies have a responsibility to ensure the protection and security of government data, including through the implementation of appropriate security measures and data protection protocols.

iii. **Adherence to Procurement Processes:** Government agencies 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:** Government agencies 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:** Government agencies 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:** Government agencies have a responsibility to promote capacity building and awareness raising activities related to cloud computing, including training and support for their staff and stakeholders.

Government Cloud Selection

Selecting the right cloud services is crucial to the success of the policy. Cloud services vary greatly in terms of their functionality, performance, security, and cost, and selecting the right services requires careful consideration of a range of factors.

The selection and procurement of the Cloud will be done in consistent with the Section 25 and 26 of the DGA 2022. Based on best practice, the Government will use the following standards to select a CSP:

i. **Security**: The government will select a CSP that adheres to international security standards, such as ISO 27001, and is compliant with applicable local laws and regulations.

ii. **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) and is compliant with applicable local laws and regulations.

iii. **Data Sovereignty:** The government will select a CSP that allows customers to ensure their data remains within the national jurisdiction and is compliant with applicable local laws and regulations.

iv. **Interoperability:** The government should select a cloud service provider that supports open standards and protocols and is compliant with applicable local laws and regulations.

v. **Performance:** The government will select a CSP that offers high-performance services and is compliant with applicable local laws and regulations.

vi. **Cost:** The government will select a CSP that offers competitive pricing and cost-effective billing models and is compliant with applicable local laws and regulations.

vii. **Availability:** The government will select a CSP that offers reliable and resilient services and is compliant with applicable local laws and regulations.

Cloud Service Providers (CSPs)

By working closely with the government and other stakeholders, CSPs can help to promote innovation, efficiency, and transparency in government service delivery, and contribute to the broader digital transformation of PNG.

The responsibility of cloud service providers (CSPs) towards the cloud policy in Papua New Guinea (PNG) is to ensure that their services comply with the relevant laws, regulations, and guidelines established by the government. This includes:

i. ensuring that their services meet the security and privacy requirements set by the government and that they provide the necessary support and assistance to government as they adopt and use cloud services.

ii. ensuring that their services are accessible and affordable for all government agencies and that they provide the necessary training and support to enable government employees to use their services effectively. They should also be transparent about their pricing and service levels and provide regular updates and reports on the performance of their services.

iii. willing to engage in dialogue with the government and other stakeholders to address any concerns or issues that arise in relation to the use of their services. They should also be willing to collaborate with other CSPs and technology providers to develop innovative solutions that can help to support the government's digital transformation goals.

iv. ensuring that their services are used in a manner that is secure, compliant, and aligned with the needs of government and its agencies.

SECURITY OF GOVERNMENT CLOUD

Cloud governance refers to the set of policies, procedures, and processes that are put in place to ensure that cloud computing resources are used in a secure, efficient, and cost-effective manner, and that the organization's goals and objectives are met.

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, government agencies can leverage the benefits of cloud computing while ensuring the protection of government data and the compliance with relevant laws and regulations.

The cloud control and accountability requirements ensure that government data is protected, and cloud services are used in a responsible and secure manner. These requirements are designed to promote compliance, transparency, and accountability in cloud computing, as well as to protect the interests of the government and its citizens.

Cloud Control Requirements:

i. **Data Classification:** All government data must be classified based on its sensitivity and criticality, and appropriate controls must be put in place to ensure that the data is protected and secured.

ii. **Access Control:** Access to cloud services and government data must be controlled and restricted based on the principle of least privilege, and user access must be regularly reviewed and audited.

iii. **Encryption:** Encryption must be used to protect government data in transit and at rest, using industry-standard encryption protocols.

iv. **Vulnerability Management:** Regular vulnerability assessments and penetration testing must be performed to identify and mitigate potential security risks.

v. **Incident Management:** A 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.

Cloud Accountability Requirements:

i. **Compliance with Laws and Regulations**: All cloud services and operations must be compliant with relevant laws and regulations in PNG, including those related to data privacy, security, and protection.

ii. **Service Level Agreements:** Clear and measurable service level agreements (SLAs) must be in place for all cloud services, including provisions for performance, availability, and security.

iii. **Audit and Reporting:** Regular audits and reporting must be conducted to ensure compliance with cloud policies and SLAs, and to identify any areas for improvement.

iv. **Contract Management:** Contracts with cloud service providers must include clear terms and conditions related to service performance, data protection, and security.

v. **Training and Awareness:** Regular training and awareness activities must be 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.

Government Agencies Cloud Security

In consistent with the Section 25-26 of the DGA 2022, Cloud Security requirements for Government Agencies:

i) **Cloud Security Architecture**: Government Agencies must implement appropriate security controls to ensure the security of data stored in the cloud. Government Agencies 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.

ii) **Security Monitoring and Response:** Government Agencies must be able to detect and respond to security incidents in a timely and appropriate manner. Government Agencies must implement appropriate measures to monitor their systems and networks for security incidents and respond to any such incidents promptly and effectively.

iii) **Third-Party Audits:** Government Agencies must be regularly audited by DICT or an independent third-party to verify compliance with applicable security standards and controls. The audit must be conducted at least once every two years and must include an assessment of the security architecture, security monitoring and response, and other security measures implemented by the DICT.

iv) **User Access and Control:** Government Agencies must implement appropriate measures to restrict access to the user of Government cloud to authorized personnel only. Government Agencies must ensure that access to the Government cloud is granted only to DTOs and its personals and that the access rights are regularly reviewed and updated as necessary.

v) **Data Encryption:** Government Agencies must ensure that all data stored in the cloud is encrypted and protected from unauthorized access. DICT will ensure that government agencies use strong encryption algorithms to protect the data and will be regularly reviewed and updated as necessary.

vi) **Data Retention and Disposal:** Government Agencies must implement appropriate measures to ensure that data stored in the cloud is retained and disposed of securely. Government Agencies must ensure that data is only retained for as long as necessary and is securely disposed of when no longer needed.

vii) **Data Backup and Recovery**: Government Agencies must 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.

viii) **Incident Reporting:** Government Agencies must have a process in place to promptly report any security incidents or breaches to DICT. DICT will ensure that any security incidents or

breaches are appropriately investigated, and appropriate corrective actions are implemented.

Data security

For the data security across the whole of government, standards and guidelines will be developed to guide the accessing of electronic data and the classification of electronic data. Correctly assessing the sensitivity and security of the data and information and classify, label and handling them safely is critical.

Data Classifications indicates the sensitivity of data and information and the need to defend against a broad range of threats to it. Each Classification will attract a level of security controls appropriate for managing the data and information risks involved.

The Data Calcification takes its cue from the NEC Manual[4] and DGA 2022[5] and aligns closely with international best practice and data security classification of other countries. Depending on the sensitivity of the data or information, this policy has classified the data into two categories;

i. **PUBLIC DATA**: Data/information which is not sensitive, and which is freely available to anyone is classified as "Public data/information". Security requirements for "Public" data/information are minimal. Such documents may be freely accessible but not modifiable by the public. Having access to the public data and information doesn't have any cause for improper handling. The Information or Data may include but not limited to their Mission, Vision and Goals, what they do, what services they provide, downloadable forms or documents, etc.

ii. **RESTRICTED DATA**: The Information or Data that requires security protection other than that determined to be Top Secret, Secret or confidential are classified into three categories based on its sensitivity;

    a. **Confidential Data**: Data and information that is somewhat sensitive. Unauthorized disclosure, modification, inaccuracy or incompleteness of confidential data and information may cause administrative embarrassment or difficulty or would be advantageous to a foreign power.

    b. **Secret Data:** Data and information which is highly sensitive. Unauthorized disclosure, modification, inaccuracy or incompleteness of secret data and information would be expected to cause serious injury to the interests or prestige of the nation or would be of great advantage to a foreign nation or might endanger a source. Adequate data and information security controls must be in place at all times to protect such data and information.

[4] Range of Security Clearance information available on the NEC Handbook

[5] Information available on Data Security and Data Governance in the Digital Government Act 2022

c. **Top Secret Data** : Information or Data that is very highly sensitive. The unauthorized disclosure of which would cause exceptionally grave danger to the Nation or would disclose the identity of the secret source of Data and information. Maximum security controls must be in place at all times to protect such data and information.

The classification of the electronic data and information aligns closely with that of the Digital Government Act 2022[6] and in bridge of this can be prosecuted under this Act. This classification will be further captured in Data protection, privacy, and governance policy and legislations.

Public Data

Information or data, that any person can access, use, and share, if disclosed or accessed without proper authorization, are unlikely to cause any harm or negative impacts to organizations, persons and/humanitarian actors[7].

Information & Data Sensitivity Classification	**Description**	**Sensitivity**
PUBLIC	Departments and Agencies data and information that is available for anyone to see and is often made available via the agencies websites, if the unauthorized disclosure, alteration, or destruction of the data could result in little or no risk to the government	LOW/NO

Restricted Data

Restricted data or information that is not openly accessible to the public. It is only accessible to authorized persons only. If disclosed or accessed without proper authorization, they are likely to cause minor to serious reputational damage to departments, National Interest, financial loss, legal actions, compromise of National Interest, etc. Maximum security controls must be in place at all times to protect such data and information.

Information & Data Sensitivity Classification	**Description**	**Sensitivity**

[6] Information available on Data Security and Data Governance in the Digital Government Act 2022

[7] A list of information and sensitive data available to the public both downloadable and available on website

CONFIDENTIAL DATA	Majority of the data and information that is created or processed by the public Sector. This includes routine business operations and services, if unauthorized disclosure, alteration, or destruction of the data could result in a moderate level of risk to the government.	**MEDIUM**
SECRET DATA	Very sensitive data and information that justifies heightened protective measures to defend against determined and highly capable threat actors. For example, if unauthorized disclosure, alteration, or destruction of the data could result in a high level of risk to the government.	**HIGH**
TOP SECRET DATA	PNG Government's most sensitive data and information requiring the highest level of protection from the most serious threats. For example, if the unauthorized disclosure, alteration or destruction of the data could result in a significant level of risk to the government.	**VERY HIGH**

The government is currently updating its data security to be consistent and aligned with other countries and to ensure it meet international standards. Therefore, this policy including PNG National Cyber Security Policy 2021, Digital Government Act 2022 and other data protection, privacy and governance policy and legislations will requires agencies to adhere to these standards and guidelines.

Access control

In consistent with the Section 25-26 of the DGA 2022, Cloud Security on access control:

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

ii) **Authentication:** All government agencies to ensure that there is minimum authentication in place. This is to ensure all users are authenticated before they are allowed access to the cloud environment and its services. The authentication process should include strong passwords, two-factor authentication, or biometric authentication.

iii) **Authorization:** All government agencies to ensure there is an appropriate authorization in place before granting access to a user after they have been authenticated. This is to be done based on the user's roles and responsibilities within the cloud environment.

iv) **Access Rights:** Access rights must be limited to user for accessing the cloud environment and its services based on the user's roles and responsibilities and should be enforced within the cloud environment.

v) **Activity Monitoring:** DTOs in collaboration with DICT and CSPs to monitor user activities and ensure that they are not accessing unauthorized data or services.

vi) **Data Encryption:** All government agencies to ensure data deemed RESTRICTED to be encrypted during transit and at rest.

CLOUD AVAILABILITY

Service-level agreements (SLAs)

Service Level Agreements (SLAs) are a critical as they define the expected level of service from cloud service providers and ensure that government agencies receive the appropriate level of support and service.

The DICT on behalf of the government will review and negotiate the SLA with CSPs before engaging their services. This is to ensure that the SLA aligns 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 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 for data backup, data retention, and data recovery in case of a security breach.

iv) **Support:** The SLA should specify the level of support that will be provided to government agencies using the cloud service, including the availability of technical support, customer service, and training.

v) **Compliance:** The SLA should define the regulatory requirements that the cloud service must adhere to, such as data privacy and protection laws, and the certifications and audits that the service must undergo.

vi) **Reporting and Monitoring:** The SLA should define the monitoring and reporting requirements for the cloud service, including the frequency of reporting, the metrics that will be monitored, and the format of the reports.

DICT will be coordinating the SLAs for the whole of government.

Disaster recovery

Disaster recovery is important as it ensures that government data and services remain available and functional in the event of a disaster or outage. CSPs to provide disaster recovery services as part of their offerings, However, DICT and government agencies will be required to ensure that they have a disaster recovery plan in place.

Key considerations for disaster recovery includes:

i. **Disaster Recovery Planning:** Each government agency will 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**: Government must ensure that the CSP 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:** Government must ensure that the CSP 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 disaster recovery requirements are included in the service level agreement (SLA) with the cloud service provider. The SLA will specify the expected recovery time objective (RTO) and recovery point objective (RPO) for government services.

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

CLOUD COSTS

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 develop 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.

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.

In consistent with the Section 25-26 of the DGA 2022, the government will consider the following key considerations for billing and payment of the cloud services:

i. **Consumption-Based Billing**: Government 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:** Cloud service providers 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 Department of Information and Communication Technology (DICT) will establish a billing and payment management system in collaboration with CSPs that will enable government agencies 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.

Department of ICT with the mandate from the DGA 2022 under Section 25-26 will be managing the whole of government cloud procurement, coordination, and advisory pertaining to cloud services. Public Finance management Act to be reviewed to incorporate payments of specialized services such as whole of government cloud services under 'utilities' or alternatively by the respective government agencies based on the established billing and payment management system established by DICT in collaboration with CSPs.

COMPLIANCE, MONITORING AND EVALUATION

Compliance requirements

Compliance requirements are an important consideration for the Government. DICT will provide guidance and support to government agencies in meeting compliance requirements. Compliance of the cloud will be in consistent with the Section 25 and 26 of the DGA 2022.

Key compliance requirements that government agencies must ensure when implementing the policy includes:

i. **Data Privacy and Security:** Government agencies must ensure that personal and sensitive information is protected when using cloud services. This includes compliance with the PNG Data Protection Act (draft)and any other relevant laws and regulations related to data privacy and security.

ii. **Government Policies and Standards:** Government agencies must comply with relevant government policies and standards related to cloud computing. This includes the Digital Government Act 2022, Cyber security Policy 2021, Digital Transformation Policy 2020, among other relevant laws and policies.

iii. **Industry Standards:** Government agencies to ensure that cloud services they use comply with industry standards and best practices. This includes standards set by DICT and based on international standards such as ISO/IEC 27001 for information security management and ISO/IEC 27018 for protection of personal data in the cloud.

iv. **Service Level Agreements (SLAs):** Government to ensure that SLAs with cloud service providers 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:** Government agencies must ensure that contracts with cloud service providers 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 government agencies use cloud services that involve cross-border data transfer, they must comply with relevant international standards and regulations or through mutual agreements between countries.

Policy reviews and updates

By regularly reviewing and updating the Government Cloud Policy, the Government can ensure that it continues to meet the needs of government agencies and aligns with best practices in cloud services. The Department of Information and Communication Technology (DICT) will play a critical role in supporting the policy review and update process and ensuring that government agencies are aware of any changes to the policy.

i. **Regular Review:** Based on Monitoring & Evaluation, the DICT policy will be reviewed on a regular basis to ensure that it remains relevant and up-to-date. This review will also consider changes in the cloud services market, evolving security threats, and changes in regulatory requirements.

ii. **Feedback from Stakeholders:** The review process will involve input from stakeholders, including government agencies, cloud service providers, and industry experts. This feedback will help to identify areas for improvement and inform updates to the policy.

iii. **Alignment with National Strategies:** The policy will be reviewed to align with future national strategies for ICT and digital transformation. This will ensure that the policy supports broader government objectives and contributes to the achievement of national goals.

iv. **Continuous Improvement:** The review process will focus on identifying opportunities for continuous improvement in the policy. This will include updates to guidance documents, training programs, and tools for managing cloud services.

v. **Implementation Monitoring:** The policy review will also consider the effectiveness of the policy in practice. This will involve monitoring the implementation of the policy by government agencies and assessing its impact on government operations and service delivery.

vi. **Policy Communication:** The policy review will include communication strategies to ensure that government agencies and other stakeholders are aware of any changes to the policy. This will include training sessions, workshops, and guidance materials.