Government Cloud Policy

The Gambia

Policy Designation: Government Sector

Issue Date: [To be inserted]

Effective Date: [Insert date sign off is obtained]

Accountable Owner: [Principal G-Cloud Provider]

Commissioned by the Ministry of Communications and Digital Economy

Contents

Document History

SN	Author	Version No	Release Date	Change Details
1	Consultant	1.0	20 April 2023	
2	Consultant	2.0	29June 2023	Updated with comments and suggestions from stakeholders

Section 1: Background and Context

The delivery of Government services to meet citizen needs continues to drive a large range of ICT use cases amongst Government of The Gambia (GoTG) institutions, which must balance legacy platforms with more responsive services. To better address these needs, the e-Government 2020-2024 strategy recognizes the need to make a strategic shift to cloud consumption through the use of public, private, community or multi- cloud services. To achieve this, GoTG will deploy a robust cloud computing infrastructure (multi-cloud) that provides agility, scalability, cost savings, and enhanced security. Adopting cloud computing will help the GoTG maintain IT service excellence during a period of increasing demand for digital services and timely access to emerging technologies.

As GoTG institutions move their data, applications, and services to the cloud, data security, and privacy is a concern. There is also a need to consider compliance with regulatory requirements. Therefore, a well-defined government cloud policy is essential to ensure the secure and effective use of cloud technology in the public sector.

This policy document outlines GoTG's objectives, guidelines, and requirements for G-cloud adoption, including cloud governance, data protection, security, interoperability and procurement, among other aspects. By establishing a clear and comprehensive Gambia -Government Cloud policy, GoTG can realize the benefits of cloud technology while also ensuring the protection of sensitive data and the delivery of quality services to both GoTG institutional consumers and citizens.

Section 2: Key Facts

The Gambia Government Cloud Policy is predicated on the following facts:

ICT for Development

The emergence of the information age has brought to the fore, the important role that information, knowledge and technology can play in facilitating socio-economic development. The Gambia National Development Plan recognises this and therefore emphasises the use of ICT in achieving rapid economic growth and wealth creation, and for improving socio-economic well-being of Gambians. More specifically, the plan amongst other things seeks to make The Gambia a “Digital Nation” and “a modern information society”. It proposes initiatives that will lead to enhanced ICT infrastructure and services to support inclusive and sustainable development. In keeping with modern practice, cloud computing is fundamental to achieving rapid digitalisation.

Adoption of modern technologies in realising the objectives of the National e-Government Strategy 2020 - 2024

The National e-Government Strategy 2020- 2024 sets out 4 strategic objectives which will make the whole government more accountable and transparent. The objectives shall leverage advances brought upon by technological innovations to drive the success of digitizing GoTG in keeping with internationally accepted best practices and standards for e-Government. More specifically, the adoption of cloud computing services is emphasised. Other include internet of things, big data, mobile innovations, etc.

The need to use common ICT infrastructures for e-Government services

The use of Common ICT infrastructures is necessary for e-Government services to be provided securely and seamlessly by GoTG. As efforts are made to match demand for infrastructure with the challenge of growing data variety and volume, applications, and services, it is important to use common infrastructures to reduce the repeated use of resources, enhance interoperability and to minimize critical infrastructure risks. The use of cloud computing technologies is considered a key enabler to achieving common ICT infrastructures and implementing virtualization. In view of this, the National e-Government Strategy 2020 – 2024 provides for the setting up of a Government Cloud Computing Infrastructure.

Enabling the broadening of Open Data usage in The Gambia

To promote good governance, transparency and accountability, citizens engagement, innovation and economic growth among others, The National e-Government Strategy 2020 – 2024 seeks to broaden the use of Open Data. Actions such as the development of an open data sharing portal and ensuring there is open access to digital, scientific and cultural information is proposed. Open data and cloud adoption are closely linked and often go hand in hand. Cloud computing provides an ideal infrastructure and platform for hosting, managing, and distributing open data.

Development of an Enterprise Architecture for e-Government

In keeping with good practices, the National e-Government Strategy 2020 – 2024 seeks to establish an enterprise architecture (EA) for e-Government in The Gambia. An EA will play a crucial role in the successful implementation of the identified e-government initiatives. It provides a strategic framework and methodology for designing, planning, and managing IT infrastructure, systems, and services of GoTG institutions. Implementing an e-Government EA largely hinges on a cloud computing friendly environment.

The value that cloud computing can create for Government of The Gambia.

The National Development Plan, and The Gambia ICT for Development (ICT4D) Policy statement 2018-2028 both recognises ICT infrastructure development as key pillars in realising the national digital transformation agenda. More specifically e-Government strategy 2020-2024 emphasises the adoption of cloud technology. MoCDE and other stakeholders believe that cloud computing can bring the following benefits to GoTG:

Domain	**Benefit**
Information system agility / Rapid scaling of capacity	► Rapid provisioning of systems and shared resources allowing for elastic demand and capacity ► Infrastructure is provided as a service ► Increased response to business needs with near instantaneous increases or reductions in computing resources ► Quicker deployment times ► Provide greater choice
Cost savings	► Leveraging economies of scale in ICT acquisitions across government entities will lead to reduced overall ICT expenditure ► Reduction in IT staff cost
Infrastructure usage and management	► Optimisation of infrastructure usage through resource pooling or multitenancy ► Improved backup/ disaster recovery
Enhanced security and continuity	► Streamlined management of infrastructure risk ► Increased information security protection and resilience ► Leveraging the opportunity to deploy an integrated security and business continuity framework, infrastructure, and services.

Innovation	► Access to top end IT capabilities, better services and collaboration
Governance principles	Cloud computing also supports the governance principles of providing: greater Cybersecurity, Data Protection – including security and privacy, Interoperability of standardized data systems, and Portability of standardized virtual compute and storage resource pools. This promotes greater assurance that information systems will not be easily compromised, will not be confined by proprietary vendor technologies or information systems, and through data systems.

Section 3: Guiding Principles

The guiding principles for The Gambia Government Cloud Computing Policy include the following:

1 **"Cloud First" Policy Thrust:** To realise the full benefit of cloud computing through adoption and usage, government agencies are expected to consider cloud infrastructure, applications, and services as the first option in new procurements or existing technology refresh. All policies, regulation, and legislation applicable to government cloud adoption in The Gambia should ensure cloud options take pre-eminence over on-premises alternatives except in cases where the latter has greater advantages.

2 **Simplified, connected and integrated government:** The Government Cloud shall form part of the government ICT infrastructure backbone that will enable both government and citizens have accessible, efficient, cost-effective, and seamless e-government services. Government institutions should be able to share information via interoperable cloud services, supporting collaboration and facilitating the development of integrated government services.

3 **Accessibility to multiple-choices -online service delivery:** The cloud-service offering will be provided as a utility, and in a form that allows for multiple options for government institutions to pick and choose, and dynamically scale, to achieve optimal utility.

4 **High agility, scalability and mobility**: Government cloud computing resources should be available in real time and on demand.

5 **Security, trust & confidence in Government Cloud service delivery:** The model will emphasise continuous management of government institutions security requirements, real and perceived and to ensure that key controls are in place to mitigate risks. It must incorporate appropriate security standards and best practice to foster trust and confidence.

6 **Protection of Information:** All government information assets should be adequately protected against cyber threats

7 **Economies of scale, effective & efficient governance process**: The model will reap meaningful benefits. Cloud computing has the potential to deliver savings for the GoTG. The journey to this outcome will require significant compromise and transformation including the decommissioning of IT assets and workforce reconfiguration, as this is where the real savings reside. The model incorporates a suitable Governance framework with associated guidelines for stakeholders to follow and abide by in relation to Cloud service and general IT system usage. The governance process will be centrally managed.

8 **Strategic ICT Delivery:** ICT functions within government agencies should work to deliver strategic objectives and enhance service delivery, while dedicating minimal resources to the management of physical assets.

9 **All inclusive & compatible Government Cloud service delivery and utilization:** The Government Cloud model will be all inclusive and encompass ecosystem players including institutions with existing resources, CSPs and cloud services consumers both in the public and private sector. The model must be structured to avoid duplications within the ecosystem.

10 **Partnership through collaboration and reliability:** The cloud policy will be all inclusive and promote strong collaborations amongst stakeholders. This will drive uptake and use of Government Cloud services in The Gambia.

11 **Digital Inclusion, Accountability & Responsiveness:** The Government Cloud policy will seek to bridge the digital divide essential to ensure an effective e-government and a thriving digital economy. The model must foster digital inclusion, equal access, and equal opportunity for all stakeholders to participate and benefit from the opportunities Government Cloud services provide.

Section 4: Rationale for The Gambia Government Cloud Policy

The delivery of Government services to meet citizen needs continues to drive a large range of ICT use cases amongst Government of The Gambia (GoTG) institutions, which must balance legacy platforms with more responsive services. To better address these needs, the e-Government-2020 to 2024 strategy recognizes the need to make a strategic shift to cloud consumption through the use of both public and private cloud services. To achieve this, GoTG will deploy a robust cloud computing infrastructure (private, and public) that provides agility, scalability, cost savings, and enhanced security. Adopting cloud computing will help the GoTG maintain IT service excellence during a period of increasing demand for digital services and timely access to emerging technologies.

As GoTG institutions move their data and applications to the cloud, data security and privacy is a concern. There is also a need to consider standardisation, and compliance with regulatory requirements. Therefore, a well-defined government cloud policy is essential to ensure the secure and effective use of cloud technology in the public sector.

The Gambia Government Cloud policy seeks to establish a framework that guides the adoption and use of cloud computing within government agencies. It seeks to ensure consistency, security, cost-efficiency, and interoperability across government agencies, while leveraging the benefits of cloud computing in public service delivery.

Section 5: Purpose and Application

This policy outlines GoTG's objectives, guidelines, and requirements for Government Cloud adoption, including cloud governance, data protection, security, interoperability, and procurement, among other aspects. By establishing a clear and comprehensive Government Cloud policy, GoTG can realize the benefits of cloud technology while also ensuring the protection of sensitive data, and applications, and the delivery of quality services to both GoTG institutional consumers and citizens.

As The Gambia matures in the adoption of cloud computing technology, the development of a 'Cloud Computing Act' can be considered. In the absence of a 'Cloud Computing Act', the application of this Policy shall be subject to applicable Policies, Regulations and Legislations related to ICT/Digital Infrastructure in The Gambia such as those related to but not limited to the following:

- Information and Communications Act (IC Act) 2009 (to be succeeded by a new IC Act 2023)
- Data Protection and Privacy Policy and Strategy - no Act / law yet adopted,
- National Data Protection and Privacy Bill 2021
- Cybercrime bill 2021
- Consumer Protection Act 2014,
- The Gambia Information & Communication Technology Agency (GICTA) Act 2019
- The Gambia E-Government Strategic Plan 2020-2024,
- The Gambia ICT for Development (ICT4D) Policy Statement 2018-2028
- Gambia National Cybersecurity Policy & Strategy 2020-2024,
- Critical Information Infrastructure Protection (CIIP) Policy Framework

Section 5: Scope of Policy

The Gambia Government Cloud Policy has been developed through a cross-sector collaboration. It takes into account the strategic intents of ICT4D Policy Statement 2018-2028; the e-Government strategy 2020-2024; and the Government Cloud Strategy 2023.

This policy is applicable to all stakeholders whose participation will be critical to the success of Government Cloud adoption in The Gambia. It is specifically applicable to the following:

1. All levels of government (national and local)
2. All organs of State

Section 6: Vision

Towards the use of common ICT infrastructure to reduce the repeated use of resources, ensure interoperability, and to minimize critical infrastructure risks for Government of The Gambia.

Section 7: Policy Objectives

This Government Cloud policy align with the National Development Plan (NDP); ICT for Development (ICT4D); and e-Government strategy (e-Govt 2020-2024) and objectives, while also addressing the unique challenges and opportunities associated with cloud adoption in the public sector.

Specifically, the Gambia Government Cloud policy objectives seeks to achieve the following:

1. Provide clear guidance and direction on GoTG's journey to cloud and the use of cloud services by GoTG institutions
2. Operationalization of a Government Cloud platform and services in the public sector by 2027
3. Clear direction to drive adoption of cloud computing by GoTG institutions, which will serve as an enabler for rapid scaling of Government digitalization.
4. Decrease in government ICT expenditure by leveraging of economies of scale in cloud-technology acquisitions across GoTG entities through the adoption of a coordinated and standardized approach.
5. Establishment of robust guidelines to ensure the security of GoTG's data and services in the cloud.
6. Establishment of a clear and sustainable approach to developing qualified human resources for the operation of Government Cloud.

Section 8: Definitions

Terms used in this Policy have the following meanings:

Cloud adoption / Cloud transition The process or strategy to promote the migration of computing services from on-premises or traditional infrastructure to cloud based infrastructure in way that is efficient and sustainable

Cloud computing A computing model for on-demand and real time network-accessed pool of configurable and rapidly provisioned computing resources (servers, storage, networks, applications, etc.) required by and available to public institutions to carry out their businesses and operations

Cloud First Policy A guiding principle, that prioritizes the use of cloud computing solutions for IT infrastructure, applications, and services.

Cloud infrastructure Virtual infrastructure consisting of hardware and software components (e.g., servers, storage, networks, and virtualisation software) – that are needed to support the computing requirements of a cloud computing model.

Cloud migration This is a subset of cloud adoption, and involves the process of moving existing applications, data, and workloads from on-premises infrastructure or other cloud providers to a specific target cloud environment.

Cloud Service Providers (CSPs) A local or international company that offers cloud computing services.

Critical information infrastructure All ICT resources that are fundamental to the effective operation of public institutions in the Gambia

Cybercrime Unlawful acts, involving the use of information and communication technologies, which affect the confidentiality, integrity, availability and survival of data and ICT systems

Cybersecurity The practice and measures to protect critical ICT systems (networks, devices, programs, and data) from attack, damage, or unauthorized access

Data Electronic representations of information in any form suitable for communication, interpretation, or processing by human beings or by automated means

Data centres Centralized locations where computing and networking equipment is concentrated for the purpose of collecting, storing, processing, and distributing or allowing access to large amounts of data

Data classification The process of categorizing data according to its sensitivity and value and assigning appropriate security controls and access policies

Data portability The ability to access data in a structured, commonly used, and machine-readable format, and transfer it for their own purposes

Data protection The measures taken to safeguard personal and confidential information against unauthorized access, theft, or loss

Data sharing The capability to make the same data resource accessible to multiple applications or users

Encryption The process of converting data or information into a code to prevent unauthorized access by human and/or computer systems

eXtensible Access Control Markup Language (XACML) A standard for fine-grained access control that provides a flexible and extensible framework for policy-based authorization across different cloud environments

Government data Data produced or commissioned by government or government-controlled entities

Government institutions Ministries, Departments, and Agencies of Government

Interoperability The ability of different systems and services to connect, exchange and consume data regardless of the origin, developer, or interface

Metadata A set of data that describes other data and processes.

OAuth A way to get access to protected data from an application. It's safer and more secure than asking users to log in with passwords

On premise Computer systems that are located within the physical confines of public institutions in The Gambia

Open Cloud Computing Interface (OCCI) OCCI is a set of open standards for cloud computing that provide a common API for managing cloud resources across different cloud platforms

OpenID Connect (OIDC) OIDC is an identity layer on top of the OAuth 2.0 protocol that enables single sign-on (SSO) authentication across different cloud services and platforms

Open data Data that is made freely available to everyone for use, re-use and sharing for any purpose, subject to ensuring protection of privacy, confidentiality, and security in line with the regulations

Open standards Standards made available to the general public and are developed (or approved) and maintained via a collaborative and consensus-driven process. Open standards facilitate interoperability and data exchange among different products or services and are intended for widespread adoption (adopted from ITU-T)

Personal data Information relating to an identifiable, natural person, by which this person can be identified, directly or indirectly

Principal Government Cloud Service Provider Institution with will operate as an IT services organisation with the mandate to set the overall direction, including the determination and ratification of government's cloud objectives, future vision, business case, and the sequencing strategy for delivering the components of the Government Cloud solution, including the Government Digital Marketplace and Data Centre Consolidation

Government Cloud Infrastructure Operator Public or Private sector organisation, appointed by GoTG to run and operate the National Data Centre and any government owned cloud infrastructure.

Representational State Transfer (REST) lightweight architectural style for designing web services that allows different applications and cloud services to communicate and exchange data using standard HTTP protocols.

Security Assertion Markup Language (SAML) Standard protocol for exchanging authentication and authorization data between different systems and cloud services.

Sensitive data Data that must be protected from unauthorized access to safeguard the privacy or security of an individual or organisation

Simple Object Access Protocol (SOAP) Messaging protocol that enables communication between different applications and cloud services by defining a standard message format and protocol.

Software A set of instructions, data, or programs used to operate computers (and similar equipment) and execute specific tasks

Secure Sockets Layer (SSL) An SSL certificate is a digital certificate that authenticates a website's identity and enables an encrypted connection.

Vendor lock-in A situation in which public institution using the services of a cloud service provider cannot easily transition to competitor's cloud service

Section 9: Review and Reporting

3.1 Review

This Policy shall be reviewed at least once every 3 years.

3.2 Reporting

Ministry of Communications and Digital Economy (MoCDE), and the Principal Government Cloud Services Provider shall receive reports on the implementation and compliance with the provisions of this Policy.

Section 10: Related Documents

This Policy should be read in conjunction with the following

a) Recovery Focused National Development Plan
b) The Gambia ICT4D 2018-2028 Plan
c) The Gambia e-government strategy 2020 to 2024
d) The Gambia Government Cloud Strategy 2023

Section 11: Cloud Computing Service and Deployment Models

Cloud and internet hosted solutions may seem the same to the end user but are by nature different. Often, IT vendors may present their solution as cloud-enabled, or cloud based to benefit from the current interest in cloud but will not be able to display the basic Cloud characteristics – therefore limiting the potential benefits.

The characteristics identified in Table 2 serve as a mechanism to identify typified Cloud solutions:

Characteristics of Cloud				What this means
Reduced capital and operating expenditure	Demand/capacity alignment	Scales quickly	Capabilities scale rapidly commensurate with demand. To the consumer, the availability of capabilities appears to be unlimited and can be appropriated and released in any quantity at any time.	Unanticipated spikes in system demand caused by a policy change, emergency change or special events can easily be accommodated resulting in high solution availability.
		Elastic Demand	The provider's resources (people, processes and components and infrastructure) are highly leveraged and can be pooled to serve multiple consumers (depending on the Deployment Model). Resources can be dynamically assigned and reassigned according to consumer demand.	Economies of scale and reduced operating costs can be achieved by acquiring services from cloud providers without the trade-offs in operating unit agility imposed by traditional ICT consolidation strategies.
		Consumption-based	Mature Cloud capability providers charge exclusively on capability consumption. No consumption results in no charge. Higher consumption results in a	An operating unit pays only for capabilities it is using at a given time. The result is lower opportunity costs when compared to systems with dynamic usage that run

Characteristics of Cloud				What this means
			higher charge. Resource usage is monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilised service.	on fixed capacity infrastructure.
	Improved delivery velocity	Ubiquitous	Must be available to authorised users over the Internet and/or secure private networks and accessible by heterogeneous platforms (e.g., mobile phones, tablets, laptops, workstations)	Services are always available to consumers regardless of location or device (depending on application capability). This enables access by authorised users and personnel from anywhere at any time.
		Solution packaged	Customer can consume the capabilities without the need to own, manage or understand the underlying resources used to create and support the capabilities.	Significant reduction in the amount and complexity of technologies that agencies must consume resulting in reduced ICT implementation and operations effort and personnel.
		Provisioned quickly	A consumer can unilaterally provision and release capabilities as needed without requiring human interaction with each service provider often measured in minutes or hours.	Agencies can bring new capability online quickly and evaluate options without significant time and expense. Unneeded services and capacity can be shut down with no residual financial footprint.
		Published Interfaces/API	Providers publish service-based APIs that allow customers and other vendors to access functionality within their offering.	Hybrid solutions can be easily integrated, cloud to cloud and cloud to on premise allowing selective replacement of legacy systems over time.

Table 2: Characteristics of Cloud services

11.1 Cloud service models

Cloud service models are progressive encapsulations of technology that deliver targeted “packages” of IT capability (operate, develop, use). Packaging contributes almost all of the effort reduction potential within the IT organization as the components within each package are fully managed and maintained by the Cloud service provider including upgrades, patches, enhancements, and refreshes.

Figure 2 shows the distribution of IT capability that exists within the Cloud service models.

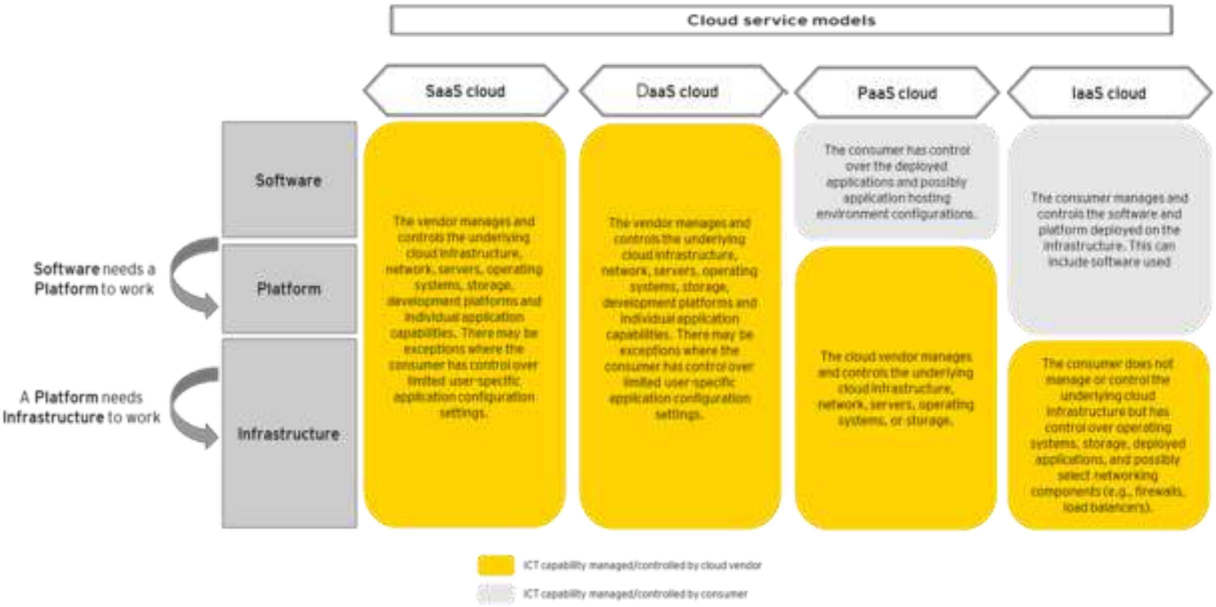

Cloud service models
SaaS cloud
DaaS cloud
PaaS cloud
IaaS cloud
Software
Platform
Infrastructure
Software needs a Platform to work
A Platform needs Infrastructure to work
The vendor manages and controls the underlying cloud infrastructure, network, servers, operating systems, storage, development platforms and individual application capabilities. There may be exceptions where the consumer has control over limited user-specific application configuration settings.
The vendor manages and controls the underlying cloud infrastructure, network, servers, operating systems, storage, development platforms and individual application capabilities. There may be exceptions where the consumer has control over limited user-specific application configuration settings.
The consumer has control over the deployed applications and possibly application hosting environment configurations.
The cloud vendor manages and controls the underlying cloud infrastructure, network, servers, operating systems, or storage.
The consumer manages and controls the software and platform deployed on the infrastructure. This can include software used
The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly select networking components (e.g., firewalls, load balancers).
ICT capability managed/controlled by cloud vendor
ICT capability managed/controlled by consumer

Figure 2: IT capability distribution within Cloud service models

There is a specific use for each service model and a process should be undertaken to identify what model is the most appropriate to adopt for a particular asset within the IT estate. The process starts by considering what ensues if a business process or application is customized, will there be a significant ROI? Where the response is limited or no ROI will be generated from the customization, then the SaaS and DaaS models should be adopted. Where an ROI is identified, then PaaS or IaaS can be considered for the service delivery model, depending on several factors including the cost-effectiveness of maintaining a suite of development tools, services, and libraries to support their in-house IT development capability. Table 3 describes the service models, when they are best adopted, what are examples of current vendor solutions and what this means for the beneficiary organization.

	Best use of model	Examples of vendors solutions	What this means
Software-as-a-Service (SaaS) The **capability** provided to the consumer is to use complete software applications provider's applications running one cloud infrastructure and accessible from various client devices through a thin client interface such as a Web browser (e.g., web-based email) The **consumption model** for SaaS is predominately unit based on users.	Used for business process and application areas that are viewed as commodity or generate little to no ROI when customised. Organisational processes must then be re-aligned to the SaaS capability.	This service model is widely used across application areas including: - Cloud9 (Analytics) - Google (Email, Collaboration, Productivity) - Oracle (CRM, HCM, Finance) - SalesForce.com (SFA, Marketing, CRM, Finance) - SAP (HCM, Finance, CRM, Marketing, Service Management) - Workday (HCM, Finance) - Cash and Treasury Management such as Kyriba Enterprise Software - IFMIS systems like Oracle Financials	Agencies have the opportunity to standardise and simplify their processes to leverage lower cost off-the-shelf solutions (e.g., Email and Collaboration, Salesforce Automation, Customer Relationship Management, Records Management). SaaS packages will also enable mobility and flexibility of the workforce as they are web-enabled. Finally, SaaS will significantly improve the opportunity for agencies to collaborate between each other, or with the community.
Data-as-a-service The capability provided to the consumer is access to a wide range of data sets and data-related functionalities over the internet. It involves the outsourcing of data management and delivery to a third-party provider, who maintains and delivers the data to consumers on-demand. It can be a standalone service or a sub-service of IaaS, SaaS or PaaS. The **consumption model** for DaaS typically involves a pay-per-use or subscription-based approach (e.g. volume of data consumed, number	The versatility and availability of diverse data sets make DaaS valuable for organizations seeking to enhance decision-making, gain insights, and leverage external data to drive innovation. Examples of use case include: Market research, geospatial analysis, social media and	This service model is fairly mature and readily available from global vendors including: Snowflake, Oracle Data Cloud, Salesforce Data Studio, Acxiom, Experian , and Dun & Bradstreet. Some traditional IaaS, SaaS, and PaaS services providers also provide DaaS, for example: Amazon Web Services (AWS) -provides DaaS through the Amazon Data Exchange; , Microsoft Azure provides DaaS offerings through services such as Azure Data Share; Google Cloud Platform (GCP) offers DaaS solutions through	Availability of DaaS offering in the market means agencies have the opportunity to scale their data access and usage based on their requirements in a cost-effective way. This scalability and flexibility will also enable institutions to adapt to changing institutional requirements faster. DaaS will also eliminate the need for institutions to spend time and resources on data collection, aggregation, cleaning, and maintenance. This will save time and resources

	Best use of model	Examples of vendors solutions	What this means
of API calls, recurring fee arrangement etc)	sentiments analysis, financial and risk analysis, healthcare analytics, IoT data integration, and regulatory reporting	services like BigQuery, a fully managed data warehouse, and Cloud Data Fusion	
Platform-as-a-Service (PaaS) The **capability** provided to the consumer is to deploy onto the cloud infrastructure consumer-created applications using prior programming languages and tools supported by the provider (e.g., java, python, .NET) The **consumption model** for PaaS is unit based on users and resource consumption (e.g., number of records, number of reports etc.)	Used to develop and deploy areas of differentiation across business processes, custom applications, and integration. There must be a significant ROI identified to deliver a differentiated service in the manner instead of using SaaS.	This service model is the least mature and includes ERP vendors who have introduced partial PaaS offerings to create a migration path for existing customers: - Google App Engine - IBM BlueMix - NetSuite SuiteCloud - Oracle Cloud Platform - Salesforce.com - Heroku - SAP Hana Cloud Platform - Windows Azure	Agencies have the opportunity to deliver services by composing applications from platforms and components available in the cloud (e.g., Reporting and analytics, database management, development environment). One of the opportunities for instance would be for the agencies to increase its digital presence in the community by providing a one-stop-shop transaction platform that agencies could join over time to provide their services.
Infrastructure-as-a-Service (IaaS) The **capability** provided to the consumer is to provision scalable processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software. This can include software used to deliver PaaS and SaaS.	Heavily customised production systems Fulfil temporary capacity needs. E.g. pre-production systems that are utilised for specific purposes. E.g. software development testing	This service model is fairly mature and readily available from global vendors including: - Amazon Web Services - Dimension Data (Public and ICON) - IBM SoftLayer Enterprise* - HP Helion	The maturity and breadth of the IaaS offering in the market means agencies have the opportunity to move to IaaS and start to derive benefits that can be realised immediately including improved disaster recovery scenarios, business continuity options and backup and retrieval. Key assets to target include non-production and non-mission critical systems in the immediate future, and highly customised, highly

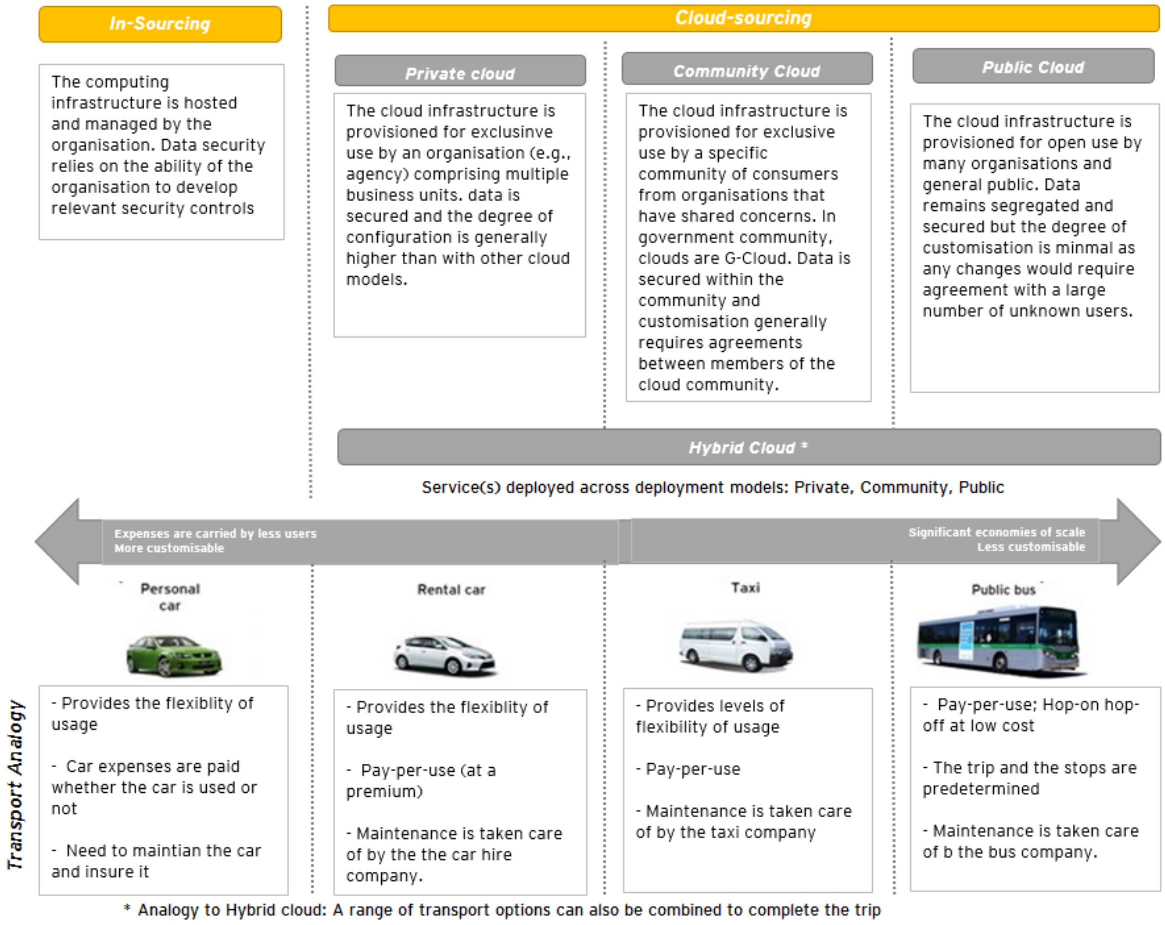
	Best use of model	Examples of vendors solutions	What this means
The **consumption model** for IaaS is unit based on asset utilisation or sizing (e.g., compute, storage, network bandwidth, etc.)			availability, steady demand applications in the longer term.

Table 3: Cloud service models and their use

While the majority of an MDA’s IT estate can be delivered leveraging one of the three Cloud service models, there are instances where moving to a Cloud based service would not be considered a cost-effective option. On-premises systems running on fixed asset infrastructure that is fully depreciated, systems with a fixed workload or low maintenance costs are factors that may contribute to a system not being a suitable candidate for moving to the Cloud. As these factors can change over time e.g., infrastructure refresh, the consideration of whether an asset is Cloud-ready needs to be an iterative process.

11.2 Cloud deployment models

Cloud deployment models are instances of Cloud services that are made available to specific groups of consumers. There are two primary models – public and private – and two derived models – community and hybrid. Figure 3 describes the four deployment models and provides a transport analogy to further highlight the differences between the models.



The computing infrastructure is hosted and managed by the organisation. Data security relies on the ability of the organisation to develop relevant security controls

The cloud infrastructure is provisioned for exclusinve use by an organisation (e.g., agency) comprising multiple business units. data is secured and the degree of configuration is generally higher than with other cloud models.

The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organisations that have shared concerns. In government community, clouds are G-Cloud. Data is secured within the community and customisation generally requires agreements between members of the cloud community.

The cloud infrastructure is provisioned for open use by many organisations and general public. Data remains segregated and secured but the degree of customisation is minmal as any changes would require agreement with a large number of unknown users.

Service(s) deployed across deployment models: Private, Community, Public

- Provides the flexiblity of usage

- Car expenses are paid whether the car is used or not

- Need to maintian the car and insure it

- Provides the flexiblity of usage

- Pay-per-use (at a premium)

- Maintenance is taken care of by the the car hire company.

- Provides levels of flexibility of usage

- Pay-per-use

- Maintenance is taken care of by the taxi company

- Pay-per-use; Hop-on hop-off at low cost

- The trip and the stops are predetermined

- Maintenance is taken care of b the bus company.

* Analogy to Hybrid cloud: A range of transport options can also be combined to complete the trip

Figure 3: Cloud deployment models

Compartmentalization and customization concerns as outlined below drive deployment model decisions.

► Compartmentalization

There are circumstances where MDAs require high compartmentalization due to the extreme impact of sensitive information leakage and/or regulatory requirements. Compartmentalization may include separate virtual or physical instances of a service to be provisioned for the exclusive use of an organization. In extreme cases, such as the US CIA IaaS Centre operated by Amazon, physical compartmentalization may include separate facilities and personnel.

► **Customization**

There are circumstances where services that are developed for broad consumption lack a specific capability deemed critical requiring a unique version of the service to be deployed for the exclusive use of the organization. Customizations may necessitate the Cloud service provider to deploy and manage a separate instance of the service for a specific MDA or community of government institutions. They may also require the MDAs to take on the overhead and complexity of building and operating their own Cloud service.

Figure 4 below illustrates the inversely proportional relationship between the cost benefits of economies of scale and the need for high degrees of compartmentalization and/or customization.

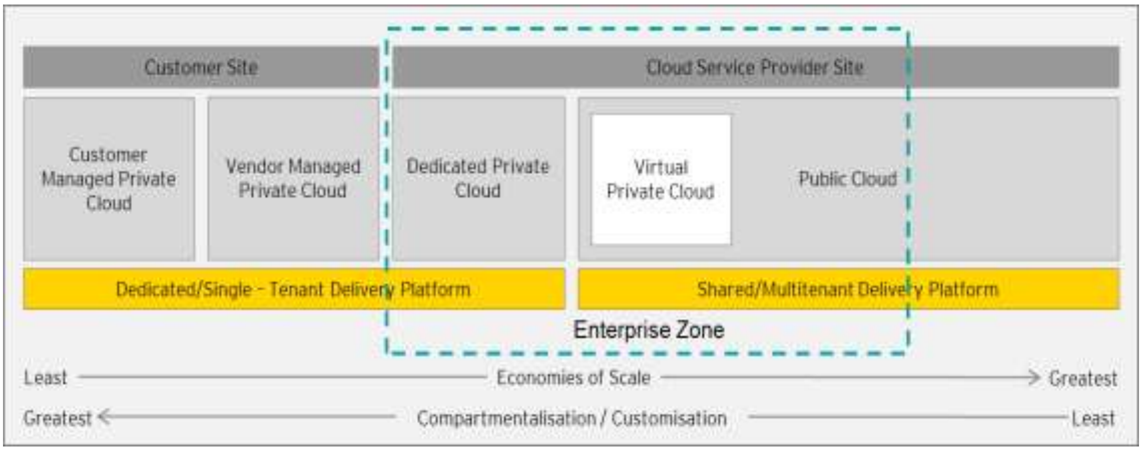

Customer Site
Cloud Service Provider Site
Customer Managed Private Cloud
Vendor Managed Private Cloud
Dedicated Private Cloud
Virtual Private Cloud
Public Cloud
Dedicated/Single - Tenant Delivery Platform
Shared/Multitenant Delivery Platform
Enterprise Zone
Least
Economies of Scale
Greatest
Greatest
Compartmentalisation / Customisation
Least

Figure 4: Levels of deployment model adoption (Original source: IDC Cloud Taxonomy 2012)

Most MDAs will choose to stay within the “Enterprise Zone” to maximize economies of scale. Public/private hybrid deployments are becoming common in organizations where they have adopted Cloud services for the majority of their IT estate.

It is worth noting that IT organizations with a “build your own” culture, or who errantly assume there is more absolute risk in a vendor managed Cloud, will naturally tend towards the left-most segments. ‘Essential Cloud’ policies must be implemented with methods to identify and avoid this pitfall. Customer managed private Clouds are options only for very large, diverse, and technically advanced enterprises for the following reasons:

1. Customer developed and managed services must conform to the characteristics (identified in Table 2) in order to be considered Cloud. Services that do not conform to the characteristics are traditional online ‘IT shared services’. While operating online shared services may be appropriate in certain circumstances, the economic and strategic benefits of Cloud will not be realized.

2. Advanced technology consumption is the responsibility of the internal provider who becomes the Cloud service provider. Capability packaging (IaaS, DaaS, PaaS, SaaS) must be achieved for consumers to realize benefits (reduced realized complexity and improved velocity).
3. The consumer portfolio of the internal Cloud service provider must be diverse enough to mitigate the risk of having to acquire and operate fixed cost technology assets while offering consumption-based services to internal consumers (No consumption = No cost). Amortized economies of scale must be delivered in order to lower opportunity costs.

11.3 A market assessment of Cloud industry and future directions

According to a report by Gartner, global spending on public cloud services is forecasted to grow at 20.7% to total $591.8 billion in 2023. This includes spending on software as a service (SaaS), infrastructure as a service (IaaS), and platform as a service (PaaS) offering provided by cloud service providers.

Both in Gambia and globally, the Cloud market is changing rapidly as new vendors emerge and there will likely be several expansion and consolidation cycles over the next decade. This reality emphasizes the need for customers to develop strong vendor assessment and management processes in addition to enhanced contracting skills in order to mitigate risk and manage market churn.

Software companies including large, entrenched players like Amazon, Microsoft, Oracle, IBM and SAP are now driving the transition to Cloud. The delivery model improves their development productivity, increases business stakeholder satisfaction, and reduces value proposition erosion caused by misuse or misapplication of their products by IT practitioners and/or System Integrators.

Going forward, there will be fewer and fewer organizations that release new capability by traditional in-house IT delivery methods.

11.4 Market view of cloud service models

There are 3 primary cloud services models (further explained in section 7.1). The current market view of these service models in Gambia and globally is discussed below.

11.4.1 Market view of Software as a Service (SaaS)

Software as a Service (SaaS) is the most mature segment of the market and has seen the highest adoption of the Service Models globally. SaaS provides complete software applications that can be adopted by organizations with little or no IT delivery effort. SaaS solutions do offer a degree of flexibility by way of configuration that affords customers with the ability to specify presentation preferences, process exceptions, and some light workflow modifications. Configuration is done by the vendor making SaaS services easy to acquire directly by business stakeholders.

The SaaS market is growing significantly in the niche application market and will continue to see expansion as benefit awareness grows and Cloud becomes more mainstream. Typical SaaS service offerings currently being offered in Gambia are office productivity products such as word-processing and spreadsheet software, email and collaboration tools, Customer Relationship Management tools, marketing tools, Human Capital Management, Finance applications and some generic Enterprise Planning Resource (ERP) tools. Key providers of SaaS cloud services mainly include Microsoft in addition to numerous other global entities with a smaller presence in the Gambian market.

Typically, public sector adoption of SaaS lags the private sector largely due to the perception that heavy customization is required across all process areas or that SaaS solutions are inherently insecure. This is however changing rapidly. This market segment is dynamic and represents the biggest challenge to traditional tender-based procurement programs often used by governments. New methods that facilitate continuous and more agile qualification of vendors must be instituted to ensure that public sector agencies have access to a robust set of offerings.

11.4.2 Market view of Data-as-a-Service (DaaS)

Data as a Service (DaaS) is a relatively mature service model and has been in existence for several years. However, compared to other cloud service models like Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), DaaS has gained less widespread adoption and visibility in the market.

IaaS, PaaS, and SaaS have seen significant market growth and have a larger number of providers and offerings. On the other hand, DaaS has gained traction more gradually, with its adoption primarily driven by consumers seeking specific data-related solutions or aiming to leverage external data sources for analytics and decision-making.

The maturity of DaaS varies across sectors and use cases, with some sectors being more advanced in adopting DaaS than others. Adoption in the public sector is fledgling and mainly driven by the growing recognition of the value of data in informing policymaking, improving public services, and enhancing transparency. Governments worldwide have launched open data initiatives, making public data sets available to the public and businesses. DaaS is facilitating the sharing and dissemination of these open data sets, allowing access and utilization for various purposes, such as research, civic innovation, and development of public applications.

Whiles there is a strong case for DaaS adoption in the public sector, ensuring the privacy and security of data when utilizing external DaaS providers can be a significant concern. Also, integrating DaaS solutions with existing systems and ensuring interoperability can be complex, requiring careful planning, data mapping, and system integration efforts

11.4.3 Market view of Platform as a Service (PaaS)

PaaS is generally the least mature and most dynamic segment of the Cloud market. The primary use of PaaS is the development and deployment of custom applications, the implementation of differentiated business processes and integrations across mixed IT ecosystems. In short, if business needs cannot be addressed with SaaS, it will likely be done in PaaS.

Globally, ERP and traditional software vendors have created confusion in the space by introducing partial PaaS offerings. PaaS includes several sub-categories including Cloud ERP, Database as a Service, Identity as a Service and Analytics as a Service (e.g IBM Watson). Each sub-category addresses an application or functional area that requires customization to be put to use.

PaaS services are almost always acquired by IT and development teams but variants are emerging that can be acquired and used by typical organization end-users without IT intervention. The PaaS market segment is changing rapidly however care must be taken to acquire PaaS services that clearly meet the need and mission of the organization as changing PaaS vendors is no small feat. Currently in Gambia, there are no PaaS offerings.

11.4.4 Market view of Infrastructure as a Service (IaaS)

Infrastructure as a Service (IaaS) is also a relatively mature segment and is the most used service in the public sector. This is largely due to the ability of government agencies to leverage IaaS to mitigate performance and reliability risks. Non-production and temporary environments are the most common early targets as these are clearly much lower risk. IaaS is almost always acquired by the IT function within an organization.

IaaS can also be used by niche or specialty software developers to create highly customized Cloud based applications for their customers. Netflix's Video Streaming Service (available locally in The Gambia) re-developed their platform to run on Amazon Web Services (AWS) in order to gain rapid scale of compute and storage. In very rare cases, IaaS is used by enterprise customers to develop custom Cloud applications however, most organizations forgo the complexity, effort and expense of bespoke Cloud applications in favour of deploying directly on PaaS.

IaaS is available from a number of global vendors and a growing number of national, regional and local companies in Gambia. Notable names in this space within the Gambian market include Gamtel amongst other global service providers. Amazon is the largest global vendor with international government customer experience. Their AWS offering is used by government agencies across the UK and the US (including the US Central Intelligence Agency).

IaaS vendors can be managed via traditional tender-based procurement processes. However, methods that facilitate continuous qualification will allow for the inclusion of the increasing pool of local and regional providers as they mature.

Generally, pricing of IaaS has been dropping steadily as vendors realize amortized economies of scale and competition in the segment increases, but also as the core inputs (storage and compute power) also continue to fall. Packaged and modular offerings (Integrated Systems) have become the focus of major hardware vendors as IaaS providers seek turn-key expansion options and lower operating costs. This will also translate into further cost-savings for consumers.

a. Pricing

Globally, IaaS pricing has been dropping steadily as vendors realize amortized economies of scale and competition in the segment increases. Amazon has continually passed lower prices on to customers without provocation to do so.

Pricing of SaaS solutions is also dropping as higher use creates more competition and the customers become more educated. Marketplaces are emerging that give customers the ability to compare offerings from multiple vendors creating higher visibility and greater negotiating power.

PaaS pricing varies widely largely due to the number of permutations and options involved. It is too early to make accurate predictions about future directions on pricing.

The growing number of DaaS providers in the market has intensified competition, leading to competitive pricing strategies. Providers are adjusting their pricing models to attract customers, differentiate themselves, and gain market share. This competition can result in more competitive pricing, innovative pricing structures, and potential cost savings for organizations.

Aside from storage and compute power costs, IaaS, PaaS DaaS, and SaaS pricing are also influenced by the administrative cost of physical data centre facilities. Cost of power and utilities for cooling and other data centre amenities are comparatively higher in Gambia. Cloud services based in Gambia may then tend to struggle with more competitively priced options who may have achieved even further economies of scale beyond other base costs.

Care must be taken when comparing pricing across all service models as contractual terms relating to SLAs, service throttling, scaling thresholds, and custom services can vary widely across the consumer base (See Appendix 3).

b. Interoperability considerations

Cloud deployments will likely include offerings from multiple vendors and will include capabilities provided through multiple Service and Deployment Models. While standards to ensure interoperability across vendor offerings are emerging, they are not yet adopted. Pragmatic mechanisms must be put in place to ensure system cohesion and to mitigate vendor lock-in risk. Vendor lock-in-risk is a major concern for public sector entities such as MoCDE and various MDAs, because of the size and scale of Government administration. GoTG will be prudent to consider open-source solutions where feasible to maximize interoperability and also lighten the burden on the public purse.

c. Security considerations

Cloud adoption rates continue to soar, yet some executives remain sceptical that the benefits of endorsing a predominantly Cloud approach outweigh the risks.

Some of the more pervasive concerns in the Gambian context gathered as a result of both Public and Private sector engagement include:

- Belief that communicating information over a public network will increase the risk of cyber-attack resulting from a lack of awareness on cloud operational models and the benefits that cloud services offer the typical consumer
- Conviction that providers offering the same infrastructure to multiple clients in multiple locations will be unable to maintain segregated confidentiality
- Anxiety that transmitting their information across international boundaries will expose them to diverse legal and regulatory requirements in jurisdictions with which they are unfamiliar and hence the preference to have in-house or at least within Gambia deployments

These concerns are understandable, particularly given one of the traditional principles that have served as the foundation of information security: take control of your environment. It may feel counterintuitive for a government organization to surrender control of its IT infrastructure and information to a third party; however, it may be one of the most effective ways to rapidly secure the ecosystem.

Cloud security for both government and private managed infrastructure can be assured through adherence to cloud security standards. These standards are a set of guidelines, best practices and regulations that aim to ensure the security of data stored on the cloud. The security measures and controls are designed to protect unauthorised access, disclosure and alteration of data stored on the cloud. Common examples include ISO 27001/27002, National Institute of Standards and Technology (NIST) SP 800-53, SOC 2 auditing standards developed by the American Institute of Certified Public Accountants, and the General Data Protection Regulation (GDPR) developed by the European Union (EU) to govern the processing and protection of personal data. Adherence to these cloud security standards can help the GoTG evaluate the security of its own cloud infrastructure and other CSPs to ensure that data is protected in the Government Cloud.

- **Trusted design** – A Cloud ecosystem with trusted design has the right controls in place to safeguard and protect the underlying computing and information assets. The controls are designed to address the key areas of risk and are strong enough to match the threats to the environment. Both the provider and consumer are responsible for designing effective Cloud controls to manage risk in their respective environments.
- **Trusted execution** – A Cloud ecosystem with trusted execution has the right controls in place and is operating effectively per the trusted Cloud design. The controls are working as intended and are strengthened when risk indicators rise. The provider generally has responsibility for control execution while the consumer is accountable for governing and verifying the control objectives are met.

- **Trusted certification** – A Cloud ecosystem with trusted certification has been independently tested and verified that the controls are in place, functioning as designed, operating effectively and have been attested to by a certifying body. The provider has responsibility for attaining the trusted certification status while the consumer reviews and understands the scope and relevance of the certification on the consumed service.

Vendors have become even more sensitive to concerns over privacy due to recent revelations of widespread collection and interrogation of data on internet systems but also by incidences of security breaches. Customers realise that all online systems, whether Cloud based or on premise, are at risk. Security conscious consumers are taking steps to encrypt confidential information across their entire IT ecosystem, be they in-house or cloud based. Advances in end device security including on device encryption are becoming common place as manufacturers respond to the growth of online enterprise ecosystems.

d. Impact on general IT management practices and organization

Economies of scale that once justified consolidating IT services and operations within and across agencies have been dwarfed by the massive economies of scale and lower usage costs available from Cloud providers. Guiding organizations, CTOs and CIOs must shift focus to helping businesses and institutions leverage Cloud to operate more effectively and become the facilitators of new opportunities enabled by Cloud. Going forward:

1. New governance methods are needed to proactively enable evaluation, procurement, consumption and management of capabilities in the Cloud. Processes that strike the right balance between agency/operating unit autonomy, benefits realization, and risk mitigation are essential.
2. New lifecycle management processes are needed especially for PaaS and SaaS. Rapid application development and integration leveraging PaaS is the mission of the new Cloud-IT organization.

Mixed IT systems will exist for some time. Strategies must align ongoing business initiatives with a rapidly changing Cloud landscape.

11.5 Mobile Cloud Computing (MCC)

As technology evolves, there is a growing trend towards mobile technology which offers enormous convenience and flexibility. Mobile cloud computing offers the ability to access and utilize cloud-based resources and services through mobile devices such as smartphones and tablets. It leverages the power of cloud computing to store, process, and retrieve data and applications on the go, without being limited by the capabilities of their mobile devices.

The general use cases of MCC range from social media, interactive experiences, healthcare, security, commerce etc. Common use cases in in the government sector include the following:

Mobile Government Services: Government agencies can provide mobile applications that allow citizens to access government services and information conveniently from their mobile devices. This includes services like submitting forms, paying bills, accessing public records, scheduling appointments, and receiving real-time updates from government agencies etc

Mobile Workforce Enablement: Government employees are able to access cloud-based applications, data, and collaboration tools from their mobile devices. This empowers them to work remotely, access critical information on the go, and collaborate with colleagues and stakeholders from anywhere.

Mobile Citizen Engagement: Through mobile apps or cloud-based platforms, citizens can provide feedback, report issues, participate in surveys, and engage in discussions on public policies

Mobile Emergency Management: Mobile applications can provide real-time alerts and updates to citizens, enable two-way communication between emergency responders and affected individuals, provide access to emergency resources and evacuation routes, and facilitate coordination and collaboration among response teams through cloud-based platforms.

Mobile Analytics and Decision Support: Mobile cloud computing enables government agencies to access cloud-based analytics and decision support tools from mobile devices.

The high mobile phone ownership (93 per cent of households)[1] rain The Gambia creates a unique opportunity for GoTG to exploit the potential of MCC in the adoption of cloud services. Special MCC initiatives may be necessary to drive cloud adoption and usage whiles improving internet service delivery and effectively managing the risks associated with mobile computing.

[1] World Bank, The Gambia Digital Economy Diagnostic Report

Section 12: Policy Pillars

12.1 Governance Structure

Cloud governance describes the process of procuring, managing and controlling the use of cloud resources and services within an organisation. It establishes a working framework that defines who has access to resources and how they can use them and provide guidelines on cloud service procurement. It involves defining roles and responsibilities, establishing metrics and standards, and implementing frameworks and tools to monitor and manage cloud usage. Cloud governance is essential for governments adopting cloud computing to mitigate risks, optimize costs, and ensure compliance with regulations and industry standards.

GoTG needs a cloud governance structure and policy in place for several reasons:

- **Successful Adoption of Government Cloud**: Governance guidelines provide a framework for effective management of cloud programmes and oversight of cloud services, which is critical for successful adoption of the Gambia Government Cloud. At the heart of cloud governance is an operational structure, with defined roles and mandates to advance the vision of cloud adoption in the public sector.
- **Data Security:** The government has a responsibility to protect the confidential and sensitive data it handles, such as citizens' personal and financial information. Cloud governance ensures that appropriate security measures are in place to protect data.
- **Compliance:** Government agencies are subject to various laws and regulations regarding the handling and protection of data. Cloud governance ensures that these legal and regulatory requirements are met.
- **Cost Management:** The government needs to be accountable for public spending and proper management of financial resources. Cloud governance helps control costs through efficient management of cloud resources.
- **Transparency:** Government needs to be transparent about its activities and decisions, including the management of cloud data and resources. With cloud governance, cloud activities can be audited and monitored, increasing transparency.
- **Interoperability:** Cloud governance ensures that cloud services are interoperable and compatible with other systems, making it easier for different government agencies to work together and reducing system fragmentation.

Operations Categories

The Gambia Government Cloud Governance Operational Structure depicts the framework for governing cloud computing operations. The operational categories shall include The Principal Cloud Service Provider, and Cloud Working Groups.

Principal Government Cloud Service Provider - The Gambia ICT Agency (GICTA) will be assumed as the Government ICT services organisation, with responsibility as the Principal Government Cloud Services Provider. GICTA as established by the ICT Agency Act 2019 will set the overall direction, including the determination and ratification of government's cloud objectives, future vision, business case, and the sequencing strategy for delivering the components of the Government Cloud solution, including the Government Digital Marketplace and Data Centre Consolidation.

Working groups - The Working groups will bring together IT officers co-opted from government institutions categorized under the following working groups:

- *Security Working Group:* This group shall be responsible for ensuring the security of the government cloud infrastructure and data. They will develop security policies, conduct security audits, and manage the security of the cloud environment.

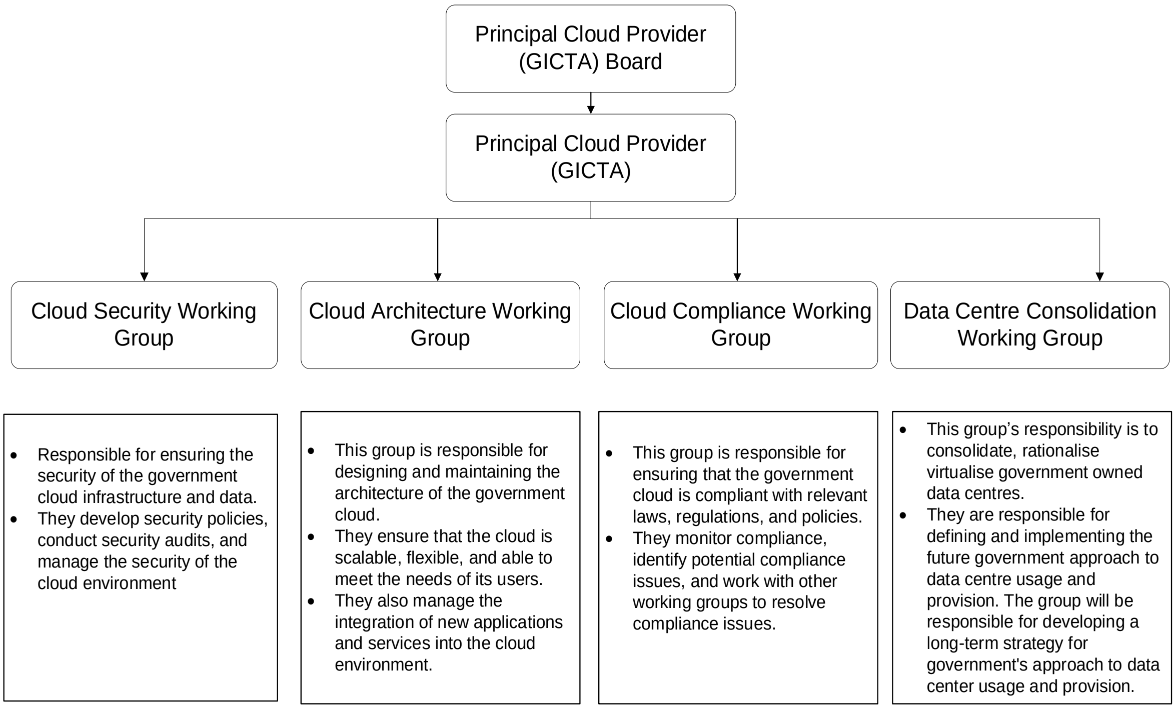
- *Architecture Working Group:* This group is responsible for designing and maintaining the architecture of the government cloud. It will ensure that the cloud is scalable, flexible, and able to meet the needs of its users. The group will also manage the integration of new applications and services into the cloud environment.

- *Compliance Working Group*: This group will be responsible for ensuring that the government cloud is compliant with relevant laws, regulations, Standards and policies within and outside The Gambia. They will monitor compliance, identify potential compliance issues, and work with other working groups to resolve compliance issues.

- *Data Centre Consolidation Working Group:* This group's responsibility is to consolidate, rationalise virtualised government owned data centres. They will also be responsible for defining and implementing the future government approach to data centre usage and provision. The group will also have a broader responsibility of developing a long-term strategy for the government's approach to data centre usage and provision. This role will also involve exploring new technologies and best practices to ensure that the government's data centre infrastructure remains up-to-date and effective in meeting the needs of various government agencies and departments

Governance Framework

The governance structure depicts the institutional structures responsible for ensuring that the delivery of government cloud services within GoTG is done effectively, efficiently, and in compliance with applicable laws and policies.


Principal Cloud Provider (GICTA) Board
Principal Cloud Provider (GICTA)
Cloud Security Working Group
Cloud Architecture Working Group
Cloud Compliance Working Group
Data Centre Consolidation Working Group

- Responsible for ensuring the security of the government cloud infrastructure and data.
- They develop security policies, conduct security audits, and manage the security of the cloud environment

- This group is responsible for designing and maintaining the architecture of the government cloud.
- They ensure that the cloud is scalable, flexible, and able to meet the needs of its users.
- They also manage the integration of new applications and services into the cloud environment.

- This group is responsible for ensuring that the government cloud is compliant with relevant laws, regulations, and policies.
- They monitor compliance, identify potential compliance issues, and work with other working groups to resolve compliance issues.

- This group's responsibility is to consolidate, rationalise virtualise government owned data centres.
- They are responsible for defining and implementing the future government approach to data centre usage and provision. The group will be responsible for developing a long-term strategy for government's approach to data center usage and provision.

Figure 1: Government Cloud Governance structure

Policies

1. The operational categories for Governing Government Cloud in Gambia shall cover a The Principal Cloud Service Provider Board, The Principal Cloud Service Provider and Cloud Working Groups.
2. Working groups – Security, Architecture, Compliance and Data Centre consolidation. The groups shall be constituted by representatives of GoTG institutions who are custodians of Critical Information Infrastructure/High Value Information Assets.
3. The cloud governance structure can be reconfigured as government cloud adoption evolves and to the extent that any updates are consistent with the vision for Government Cloud adoption in by GoTG.

12.2 Procurement

Cloud Procurement is a key strategic step towards an optimal and cost-effective cloud platform. Government cloud procurement requires careful consideration of data security, privacy, compliance with regulations, and transparency.

Key Considerations for Procuring Cloud Services

Before government institutions makes any cloud procurement, the following issues should be considered during the procurement cycle:

- *Master Services Agreement (MSA)* – For standardisation and to manage risks in a master services agreement must be signed with cloud services providers operation in the Government Cloud digital marketplace. The agreement must incorporate all regulatory and policy considerations as it pertains to Government Cloud adoption. All specific institutional level agreements will derive its form from the MSA.
- *Private vs public* - Government agencies must consider the data sensitivity, regulatory compliance requirements, and security implications of using public or private cloud services
- *Ownership of data* – The Principal Government Cloud Service provider must ensure that GoTG retain ownership of data and that cloud providers do not have unauthorized access to or control over the data. The ownership of data must be specified in in Master Services Agreements, and government must be able to retrieve data at any time.
- *Vendor Lock-in and exit criteria* – The Principal Government Service Cloud provider must consider vendor lock-in and exit criteria when selecting and accrediting cloud provider. The contract must include exit clauses that specify the conditions and procedures for transferring data and applications to another provider.
- *SLAs and Penalties* – Service level agreements (SLAs) must be included in the contract to ensure that the cloud provider meets the government's requirements for availability, performance, and security. The contract must also specify penalties for non-compliance with SLAs.
- *Support agreements* – Government agencies must ensure that the cloud provider provides adequate support and maintenance for the services. The contract must include support agreements that specify the level of support, response times, and escalation procedures.
- *Vendor testimonials* – The Principal Government Cloud Service Provider must review vendor testimonials and references to assess the CSP's experience and

reputation. The testimonials must be verified, and the government must ensure that the provider has a track record of delivering high-quality services.

- *Fit Gap analysis* – The principal Government Cloud Service Provider must conduct a fit gap analysis to assess the suitability of the cloud services for their requirements. The analysis must evaluate the functionality, security, scalability, and compatibility of the services with the government's existing infrastructure.
- *OPEX calculations* – Government agencies must consider the operating expenses (OPEX) associated with the cloud services, including licensing fees, maintenance costs, and support fees. The OPEX must be compared to the cost of operating the services in-house to determine the cost-effectiveness of the cloud services
- *Ministry and citizens readiness* – Government agencies must ensure that the relevant ministries and citizens are ready to adopt cloud services. This may include training programs, awareness campaigns, and communication plans to ensure that the transition to cloud services is smooth and successful.

Buyer Guide and Seller Guide in the Gambia Government Cloud Digital Marketplace

In The Gambia, Cloud based purchases by government institutions and sales will be done over the Gambia Government Cloud Digital Marketplace. The Digital Marketplace is the online platform that allows public sector organizations to procure cloud-based services from approved vendors. The platform serves as the single point of access for cloud services that meet GoTG's security and data protection standards, and the key considerations defined in this cloud policy.

Government agencies seeking cloud services including infrastructure as a service (IaaS), software as a service (SaaS), data as a service (DaaS), platform as a service (PaaS), and specialist cloud services such mobile cloud (General Purpose MCC or Application Specific MCC solutions), will procure such services from vendors listed on the Gambia Government Cloud Digital Marketplace.

To use the Marketplace, public sector organizations can browse the services offered and select the services that meet their requirements. The Marketplace provides information on pricing, service level agreements, and vendor qualifications to help organizations make informed decisions. Once a service is selected, the organization can enter into a contract with the vendor through the Marketplace.

Cloud Service Providers (CSPs) can apply to sell on the Government Cloud Digital Marketplace. The various cloud services are welcomed to be listed on the Gambia Government Cloud Digital Marketplace:

a. Could hosting services
b. Cloud Software
c. Cloud support services

When applying to sell on the Gambia Government Cloud Digital Marketplace, vendors will provide the following documents to the Principal Government Cloud Services Provider for processing:

a. Document defining the service – This should cover the following themes
    I. Description of the service
    II. Data backup and restoration levels, including business continuity and disaster recovery plans
    III. Support provided for onboarding and offboarding processes
    IV. Service constraints, such as maintenance windows and level of customization permitted
    V. Service level agreements (SLAs) for performance, availability, and support hours
    VI. Post-sales support
    VII. Technical requirements
    VIII. Outage and maintenance management
    IX. Hosting options and locations
    X. Data access upon exiting the service
    XI. Security measures
b. Service-specific terms and conditions – Vendors will not be able to modify the service terms and conditions once the framework is active
c. Document outlining pricing information – the document should encompass
    I. The price of the service, comprising unit prices, volume discounts, and expenses for data extraction
    II. Any excluded items that are not covered in the price
    III. Pricing details for additional services offered.

Regulations for Purchasing Cloud Services (Focus on Cloud Service Models)

The Gambia Public Procurement Authority (GPPA) sets out the regulations for government procurement. The GPPA in collaboration with the Principal Cloud Provider (GICTA) will set out the following regulations in relation to cloud service models:

- *Cloud First* **-** The Principal Government Cloud Service Provider will establish a Cloud First Policy which ensures that public sector organizations will consider cloud technology as the first option when procuring new or existing infrastructure, applications or services. The policy will require government agencies to consider and assess cloud options before procuring on-premises alternatives.

- *Cloud Security Principles framework* -The Cloud Security Principles framework will provide guidance for managing risks associated with cloud computing. This framework will cover security principles that should be considered when evaluating and selecting cloud services, such as data protection, personnel security, and secure development. It provides a comprehensive set of guidelines for managing risks associated with cloud services and ensuring that they are used securely.

- *Government Cloud framework (Government Cloud Marketplace)* - This framework offers a pre-approved list of cloud service providers and services that have met the GoTG's strict security and performance standards.

Policies

1. All institutions of state shall consider cloud infrastructure, applications, or services as the first option for new procurements or exiting technology refresh. Cloud options should be considered and assessed before procuring on-premises alternatives.
2. The Principal Government Cloud Service Provider shall establish the Gambia Government Cloud Digital Marketplace which will serve as the online marketplace for cloud services
3. The Principal Government Cloud Service Provider shall be guided by this policy and the Procurement law in selecting and approving CSPs who will provide Government Cloud services.
4. The Principal Government Cloud provider shall ensure that government cloud service offerings cover the following as a minimum: IaaS, DaaS, SaaS, PaaS, and Mobile Cloud Computing solutions.
5. The principal cloud provider shall ensure the availability of both public cloud and private cloud options.

6. To ensure standardisation for Government Cloud procurement agreements, the Principal Government Cloud Service Provider in consultation with the Attorney Generals Chambers and Ministry of Justice, shall execute Master Services Agreements with each Government Cloud services provider. The agreement must incorporate all regulatory and policy considerations as it pertains to Government Cloud adoption.
7. The Government Cloud MSAs shall be the frame of reference for all institutional level agreements.
8. The Principal Government Cloud Service Provider, in Consultation with the Data Centre Consolidation working group, shall ensure signing of MoUs with government institutions who have significant IT infrastructure installations (e.g., data centres) to cede their custody and administration to the selected government cloud infrastructure operator. As part of these institutional arrangements, the selected government cloud infrastructure operator shall meter and monitor their IT service patronization and credit them appropriately till the initial capital expenditure is recovered.
9. Procurements of Government Cloud services shall be conducted on the Gambia Government Cloud Digital Marketplace. Buyers and Sellers shall refer to the Buyer and Seller Guide for guidance on the Digital Marketplace
10. As a pre-conditions to the Government Cloud procurement, The Procurement Act,2014 will be reviewed to ensure compliance to policies and regulations pertaining to the following:
    - Criterion for the selection and evaluation of cloud service providers (CSPs)
    - Service-level agreements (SLAs) with CSPs
    - Compliance by CSP
    - Data ownership and access
    - Transparency and accountability

12.3 Data Classification

Cloud data classification is the process of categorizing data according to its sensitivity and value and assigning appropriate security controls and access policies. This is essential to ensuring the security and privacy of government data in cloud-based (public or private) environments. Once the data types are identified, they can be assigned a classification level, such as confidential, sensitive, or public.

Various MDAs within The Gambia will have varied data types and therefore will require different level of technical safeguards. The classification level is used to determine the appropriate security controls and access policies that should be applied to the data.

National Electronic Data Classification Framework

An electronic national data classification framework is currently lacking in the Gambia. Individual institutions, however, have their own internal mechanisms for classifying electronic data. A unified National Data Classification Framework for The Gambia is essential for effective management of government data in electronic form. It helps ensure consistency, protection, compliance, efficiency, and interoperability - all critical factors in the modern digital age.

GoTG's electronic data will be classified using the following framework

Category	Description	Appropriate Technical Safeguards
Classified	GoTG's most sensitive information requiring the highest levels of protection from the most serious threats. This type of data is considered sensitive to national security and thus requires additional safeguards.	Storage in Government private cloud where available and resident in Gambia or on-premises storage.
Sensitive	Very sensitive information that justifies heightened protective measures to defend against determined and highly capable threat actors. This data is classified as "sensitive" because the loss of confidentiality, integrity, or availability of the data could have serious, adverse, and material	Information is suitable for Government private cloud; or public cloud hosted in Gambia and subject to robust security controls

Category	Description	Appropriate Technical Safeguards
	effects on the data subject or related entities.	
Internal	Information that is required by government agencies as well as Gambians in government service delivery. Internal information may be shared within Gambia but should not be shared outside of the country (overseas).	Suitable for private or public cloud, subject to robust security controls on the underlying data but minimal controls on anonymized datasets
Public	Information that can be disclosed to anyone within or outside The Gambia. It would not violate government's confidentiality obligations. Knowledge of this information by the general public would not expose or threaten the national security of government and does not require extremely high assurance of protection from all threats	Suitable for private or public cloud

Policies

1. All government agencies shall refer to the Electronic Data Classification Framework to identify the types of data it has and the appropriate technical controls that may be required for migration to cloud services.
2. The Principal Government Cloud Service Provider in collaboration with the Gambia Information Commission will ensure that government agencies comply with the Electronic Data Classification Framework and that the appropriate safeguards / controls are in place
3. All DaaS offerings are subject to applicable law and the Electronic Data Classification framework
4. All open-data initiatives shall be subject to applicable law and the Electronic Data Classification framework

12.4 Data Sovereignty

Data Sovereignty determines the ability of a country to exercise legal control over data stored within its borders, regardless of the ownership of the data. It is relevant in the context of cloud computing, where data may be stored on servers located in different countries or regions. This raises questions about which country's laws and regulations apply to the data and who has legal access to it.

In practice, this means that an organisation must ensure that data is stored in compliance with the laws and regulations of the country in which it is located. This may require choosing a cloud provider with data centres located in the same country as the organization or implementing specific security measures to ensure compliance. Countries may have different regulations regarding the collection, storage, and use of personal data, ensuring compliance with these regulations is essential to protect the privacy and rights of individuals whose data is stored or processed.

The Gambia does not have a framework or policy to protect government information and to exercise legal control. The draft Data Protection and Privacy Policy only addresses transborder personal data flows and rights of data subjects. The policy however does not make provision for privacy, security, and intellectual property of national data. There is no policy on how government data is processed or stored in foreign jurisdictions.

Key considerations:

- ► *Data residency:* One of the most important considerations for data sovereignty is where the country's data is geographically located. This is because different countries have different laws and regulations governing the storage and use of data. It is important to ensure that data is stored in a location that complies with this policy and Gambia's data protection laws.

- ► *Access:* When government stores data in the cloud, it is important to ensure that it has control over who can access it. GoTG must ensure that a CSP has robust security measures in place to protect government data from unauthorized access, and that government can control access to its data.

- ► *Data Usage:* Another key consideration is how your data will be used by a CSP. Gambia will carefully review the terms and conditions of any cloud service it is considering, to ensure that the provider will not use government data in ways that are contrary to Gambia's data protection laws. This might include restrictions on the types of data that can be stored in the cloud, or requirements for explicit consent before certain types of data can be used.

- ► *Administration:* As the owner of the data, government will have control over the administration of the data in the cloud. This means having the ability to manage and delete data as needed, as well as ensuring that the CSPs have appropriate backup and recovery mechanisms in place to protect the data in the event of a disaster.

Policies

1. **Data Ownership:** GoTG shall be the sole owner of all data stored in the Government Cloud
2. **Geographic restrictions:** In the absence of any law on data residence:
   a. All government data categorized as 'Classified' shall be stored and processed within The Gambia, on a government private cloud or on-premises.
   b. All government data categorized as 'Sensitive' shall be stored on Government private cloud or public cloud hosted in Gambia and subject to robust security controls
3. **Access:**
   a. Data in the Government Cloud shall be encrypted and protected with access controls that restrict access to authorized personnel only. This includes limiting access to data centres, implementing multi-factor authentication, and logging and auditing all access attempts.
   b. Agreements with CSPs authorized to operate in the Government Cloud digital marketplace shall include terms that provide GoTG unrestricted access and control of GoTG data.
4. **Data retention and deletion:** All data stored in GoTG Government Cloud environment shall be subject to GoTG policies and regulations for electronic data retention and deletion
5. Data stored and or processed on the Government Cloud shall be subject to data protection and privacy rules and laws found in; the Information and Communications Act ('the ICA') in 2009; Data Protection and Privacy legislation; Information and Communications Technology Agency Act 2019 ('the ICTA Act'); The Gambia Consumer Protection Act 2014 and where applicable, the Economic Community of West African States ('ECOWAS') Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS.

12.5 Security

Security is a critical consideration in government cloud environments due to the sensitive nature of the data that is often stored and processed. Cloud environments can be vulnerable to a variety of security threats, including data breaches, cyber-attacks, and insider threats. Therefore, information security standards and controls in a cloud environment is critical to ensure that data is protected from unauthorized access, modification, or destruction.

Key policy considerations

The Gambia Information Communication Act (ICA), 2009[2] ; The Cybercrime Bill[3] together with the National Cybersecurity policy (2020 – 2024) provides the legal and policy framework for government information security and should be a key frame of reference for the Gambia Government Cloud. To ensure adequate security of the Gambia Government Cloud environment, the policy design is guided by the following considerations:

- *Roles:* The Principal Government Cloud service provider and the CSPs shall be responsible for cloud security.
- *Data classification and handling:* The levels of security controls provided in the Government Cloud environments should be consistent with how data is classified, based on its sensitivity and criticality. Therefore, the intersection between the Government Cloud Security policies and the Data Classification policies is recognized in the policy.
- *Access control:* How users are authenticated and authorized to access the Gambia Government Cloud resources must be clearly spelt out. Access revocation, and monitoring to detect and prevent unauthorized access is be determined.
- *Encryption:* Encryption of data transit and at rest and the minimum standard for encryption is considered.
- *Disaster recovery and business continuity:* Restoring cloud resources in the event of a disaster or disruption is vital. Roles and responsibilities of all stakeholders involved in disaster recovery, disaster recovery planning, business continuity

[2] Part III of Chapter III provides for the misuse of computer and cybercrime, including, data and system interference, computer related fraud and forgery, illegal access, and illegal interception

[3] A cybercrime bill has been developed but yet to be passed into law

standards and infrastructure availability are essential for the Gambia Government Cloud.

.

Cloud Security Guiding Principles

To ensure that the Gambia Government Cloud platform and services are secure and meet leading standards of reliability and privacy the following guidelines may be followed:

- *Data in transit protection:* All government data transmitted over networks should be protected using encryption and other security measures to prevent interception or tampering from or outside the Gambia.
- *Asset protection and resilience*: All GoTG cloud technology assets, including hardware, software, and data, should be protected against loss, theft, and damage. Government agencies must ensure that appropriate backup and recovery procedures are in place to ensure that systems can be restored quickly in the event of a disaster.
- *Separation between customers:* Personal data should be kept separate to prevent unauthorized access or leakage. This can be achieved through logical separation or physical isolation of personal data.
- *Governance framework:* The Cloud Governance Framework will provide security oversight of the service. The governance framework depicts a governance structure headed by The Principal Cloud Service Provider Board, with functional authority residing with the Principal Government Cloud Service Provider. The Principal Government Cloud Service Provider must ensure there is a documented framework for security governance and risk management, with policies governing key aspects of information security, relevant to the service.
- *Operational security:* Government agencies must establish appropriate controls to ensure that the service is operated securely. The controls shall cover access, monitoring and logging, incident management, and vulnerability management.
- *Personnel security:* All personnel who operate within GoTG's cloud environment should be screened and trained to ensure that they are trustworthy and have the necessary skills and knowledge in accordance with the National Government Cloud Workforce framework to operate the service securely.
- *Secure development*: Security should be incorporated into all stages of the software development life cycle to ensure that services are designed and implemented securely.

- *Supply chain security:* The security of third-party vendors and suppliers listed on the Gambia Digital Marketplace should be assessed and monitored to ensure that they are operating securely and in accordance with the Governemnt Cloud policy.
- *Secure user management:* All users of cloud services should be authenticated and authorized appropriately. Password policies, access controls, and other security measures should be in place to ensure that user accounts are protected.
- *Identity and authentication:* Strong authentication mechanisms should be in place to ensure that only authorized users can access the service. As a minimum, they should include multi-factor authentication, and biometric authentication.
- *External interface protection*: All external interfaces, including APIs, web services, and other communication channels, should be secured to prevent unauthorized access or tampering.
- *Secure service administration:* Appropriate controls should be in place to ensure that the service is administered securely. This may include access controls, monitoring and logging, and other security measures.
- *Audit information and alerts for customers:* GoTG institutions should be provided with audit information and alerting mechanisms to ensure that government is aware of any security incidents or breaches affecting their data.
- *Secure use of the service:* Citizens should be provided with guidance on how to use the cloud-based service securely. This may include recommendations for password policies, data protection, and other security measures.

Policies

Standards

1. The Principal Government Cloud service provider shall be ISO 27001/27002 and ISO 22301 certified
2. All CSPs providing Government Cloud services shall be ISO27001/27002 and ISO 22301 certified

Data classification and handling

3. The level of security provided shall be commensurate to data classifications and the safeguards for handling and storing data in the Government Cloud Data Classification Policy.

4. Processing and storage of personal data on the Government Cloud must be consistent with the Government Cloud policies on Data Protection including compliance to the rules and regulations on data protection found in The Gambia Information Communication Act (ICA), 2009; the legislations on cybercrime ; National Cybersecurity policy (2020 – 2024) , ECOWAS Act on Data Protection; EU General Data Protection Regulation (GDPR) and any other international law as applicable

Access Control

5. Access to Gambia Government Cloud resources must be based on the principle of least privilege.
6. All users accessing the Gambia Government Cloud resources must be identified and authenticated using a robust, multi-factor authentication (MFA) mechanism.
7. The Gambia Government Cloud platform must be monitored real-time for unauthorized access attempts. Access control violations must be investigated.
8. Access must be promptly terminated when users are no longer authorized to access the Gambia Government Cloud resources

Mobile Cloud Security

9. Only GoTG-approved mobile devices, compliant with the Gambia Government cloud security standards, shall be used for mobile cloud computing.
10. A Mobile Device Management (MDM) solution shall be implemented to enforce security policies, manage device configurations, and enable remote management, monitoring, and control of mobile devices.
11. Mobile devices accessing cloud services shall connect via secure networks, such as encrypted Wi-Fi or virtual private networks (VPNs), to ensure data confidentiality and integrity.
12. Mobile devices shall be regularly updated with the latest security patches and firmware updates to address vulnerabilities and protect against emerging threats.

Encryption

13. All GoTG data stored in the cloud must be encrypted at rest using industry-standard encryption algorithms.
14. All GoTG data transmitted over public networks, such as the Internet, must be encrypted using secure transport protocols, such as SSL/TLS. Data transmitted between cloud instances must also be encrypted using appropriate encryption algorithms.
15. Access to encryption keys must be granted based on the principle of least privilege

Auditing

16. The principal Government Cloud service provider and CSPs operating in the Government Cloud digital marketplace shall be audited annually. SOC -2 must be the minimum auditing standard for providing assurance that appropriate controls to protect customer data have been implemented

Disaster Recovery and Business Continuity

17. All Government Cloud CSPs must have a documented business continuity plan that outlines the steps to be taken in the event of a disruptive event.
18. All Government Cloud CSPs must have a documented incident response plan that outlines the steps to be taken in the event of a security incident or data breach.
19. The principal Government Cloud Service Provider must have a robust backup and recovery solution that ensures that data hosted on government owned Government Cloud platforms is protected and can be quickly restored in the event of an outage or disaster. The backup solution should include regular backups of data to an off-site location, as well as procedures for testing the integrity of backup data.
20. Periodic testing of disaster recovery procedures must be done by both the principal Government Cloud services provider and all CSPs. Testing should include simulations of various disaster scenarios and procedures for restoring service and data.
21. The Gambia Government Cloud infrastructure must be designed to ensure high availability. This may include redundant hardware, load balancing, and failover mechanisms. Availability level must be consistent with the Government Cloud SLA policy.
22. Local network traffic should be via a WAN, with the internet as a back-up

12.6 Data protection

Data protection refers to the measures taken to safeguard personal and confidential information against unauthorized access, theft, or loss. It is essential in government cloud services as sensitive information such as citizen data, classified government information, and confidential reports are often stored and accessed in the cloud. A robust framework as it pertains to government cloud services is necessary to ensure the confidentiality, privacy, compliance, and protection of the reputation of GoTG and citizens.

The Gambia does not currently have a comprehensive data protection framework in place to protect personal data and to ensure that the processing of personal data is carried out according to defined standards. A Data Protection and Privacy Policy and a Personal Data Protection and Privacy Bill have been drafted, but both are yet to be enacted into law.

Nevertheless, the Information Communication Act (ICA) 2009, provides for the processing of personal data and the protection of privacy. It sets out the principles to be followed by MDAs when processing personal data.

There is a lack of policies or standards on data quality, including its provenance, accuracy, timeliness, and completeness, as well as policies on ownership and licensing of government data. There are no common data governance frameworks/data sharing protocols, and data is not centrally hosted, with each MDA holding its data in institutional databases.

Key considerations

To ensure a comprehensive approach to data protection covering all aspects of data processing, from collection to disposal within The Gambia, the following must be considered:

- *Regulations***:** The Personal Data Protection and Privacy Bill must provide a harmonized legal framework for protection of personal electronic data relating to collection, processing, transmission, storage and use before passage into law. It must be expanded to include provisions on Data Governance.

  GoTG Institutions using the Government Cloud must comply with all relevant data protection policies and regulations that apply to their operations when processing personal data. These should include the Gambia Data Protection and Privacy Policy; Information Communication Act (ICA) 2009, and other international regulations such as The ECOWAS Act on Data Protection and the EU General Data Protection Regulation (GDPR).

- *Standards:* Institutions within The Gambia should adhere to industry-standard data protection practices. As a minimum, security standards including OAuth, Secure Sockets Layer (SSL) and Transport Layer Security (TLS) must be adopted to prevent unauthorized access. Standards such as ISO/IEC 27001; and Payment Card Industry Data Security Standard (PCI DSS) must also be adhered to.

- *Procedures:* A GoTG data governance framework must be designed and should include clear and comprehensive procedures that cover all aspects of data handling, including data collection, storage, processing, sharing, and disposal. These procedures should be regularly reviewed and updated to ensure that they remain relevant and effective.

- *Data minimization***:** GoTG institutions should only collect and store data that is necessary for their operations and should avoid collecting excessive data. Data should also be kept up-to-date and accurate.

Policies

1. The Personal Data Protection and Privacy bill, when enacted into law shall be the legal framework that govern the collection, storage, and use of data in Government Cloud environment. All Data protection measures including data collection, storage, processing, sharing, and disposal in Gambia shall comply with this law.
2. Institutions using the Government Cloud shall comply with the ECOWAS Act on Data Protection and the EU General Data Protection Regulation (GDPR) and any other international law as applicable
3. All CSPs must comply with ISO/IEC 27001 and Payment Card Industry Data Security Standard (PCI DSS) where applicable before given accreditation to operate in the Government Cloud Digital Market place
4. For the purpose of protection of electronic data categorized as 'Classified' or 'sensitive' government data, GoTG institutions shall use only Private cloud providers, resident in The Gambia and accredited by the Principal Government Cloud Service Providers in accordance with the Government Cloud policies on Data Classification and Data Sovereignty as well as any data residency and data sovereignty laws[4]
5. All agreements with CSPs operating in the Government Cloud Digital Market place must include a clause that guarantees GoTG as the sole owner of data stored in the cloud environment. Government has complete control over the data, including the right to know where it is stored and processed, and the ability to retrieve, modify or delete it as necessary.
6. Processing of metadata on personal information in the Government Cloud environment shall comply with privacy provisions as contained in the Gambia Data Protection Act

[4] Data residency and data sovereignty laws are currently non-existent in the Gambia

12.7 Interoperability

Technology interoperability refers to the ability of different technology systems, software, or devices to work together and exchange data seamlessly. Interoperability guidelines as it pertains to cloud describes a roadmap and a group of best practices to ensure seamless communication and data exchange between different cloud environments.

Interoperability should be a critical element of GoTG's e-Government agenda because it will enable the integration of different systems and technologies, improve efficiency, reduce costs, and drive innovation within the GoTG IT estate. It will also enable the exchange of data and information between different technologies, which is crucial for government decision-making, analysis, and reporting.

To achieve technology interoperability, standards and protocols are required to ensure that different systems and technologies within the GoTG IT estate can communicate with each other effectively. In addition, technology providers within the Gambia Government Cloud ecosystem must adhere to these standards and work together to create a more open and integrated technology ecosystem. This will enable GoTG institutions leverage the benefits of different technologies and create more value for citizens and stakeholders.

There is an absence of a National Enterprise Architecture and Interoperability framework for GoTG. Mapping of all platforms and data registers maintained by GoTG institution is also lacking, while the proliferation of systems is approached in a siloed manner. Current cloud deployments include offerings from multiple vendors with capabilities provided through multiple service and deployment Models are not interoperable. While standards and protocols required to ensure interoperability across vendor offerings are emerging, they are not yet adopted in The Gambia.

Key considerations

To ensure interoperability for government cloud computing in the Gambia it is important to consider the following:

- *Government Interoperability Framework:* To promote a common approach to interoperability across government agencies, reduce complexity and duplication, and ensure that public services are delivered more efficiently and effectively, a GoTG interoperability framework must be developed. As a minimum, the GoTG interoperability framework must define technical standards for data exchange and communication protocols, as well as governance processes for managing interoperability across all GoTG entities. It may also address issues such as security, privacy, and data protection.

- *Standards and Protocols:* Common standards and protocols must be adopted across GoTG institutions to ensure effective interoperability between systems and technologies. Examples of such standards include HTTP, TCP/IP, XML, JSON, and RESTful APIs

- *Use of open standards:* GoTG should adopt open standards for communication, data exchange, and application development.
- *Use of APIs:* A unique, standard, and well-designed way of communication

between the environments in the cloud. This will help integrate the individual apps from GoTG institutions.

- *Adopt common data formats and portability*: GoTG institutions at all levels must use a common data format for documents. This will help in making data portable across environments. The data should be able to move between the environments without major changes.

- *Implement security standards:* Government should design and create security standards as a safeguard against unauthorized access. This can include some standards such as OAuth, SSL, and TLS.

- *Support multi-cloud environments*: Government should be able to seamlessly deploy applications across different environments and cloud providers**.**

- *Documentation:* Integrations of the environments, the deployment of the applications, and all the services within cloud environment must be documented.

Policies

1. All GoTG institutions using Gambia Government Cloud services shall comply with the GoTG Interoperability Framework.
2. CSPs accredited to operate in the Government Cloud Digital marketplace shall provide platforms and services that support data and applications portability.
3. The following minimum standards and protocols apply:
   a. Open Cloud Computing Interface (OCCI)
   b. Security Assertion Markup Language (SAML)
   c. OpenID Connect (OIDC)
   d. eXtensible Access Control Markup Language (XACML)
   e. Simple Object Access Protocol (SOAP)
   f. Representational State Transfer (REST)
   g. OAuth
   h. SSL
   i. TLS

3. Adoption of the browser as the key interface - All public sector information systems deployed on the Government Cloud platform are to be accessible through browser-based technology; other interfaces are permitted but only in addition to browser-based ones

4. GoTG institutions must only use CSPs that support portability of data and applications across different CSPs and provide API documentation to enable easy integration with other cloud services

5. Data must be stored in open and standard formats that can be easily accessed by other cloud services
6. Integrations in the Government Cloud environment, deployment of applications, and all services must be documented by the Principal Government Cloud services provider
7. Non-compliance with this policy may result in sanctions, including suspension or termination of use of the cloud computing services
8. The interoperability policy will be reviewed annually by the Principal Government Cloud Service Provider to ensure it remains current and effective

12.8 International Implications

Government Cloud adoption can be a complex process and requires careful consideration including a variety of international implications. GoTG must take a holistic approach to ensure that adoption of the Gambia Government Cloud complies with all relevant laws and regulations, protects the security and privacy of stakeholders, and is compatible with cloud services used by other governments and stakeholders.

Policy considerations

Some of the key international considerations that would shape the Gambia Government Cloud adoption include the following:

- *Regional integration:* The adoption of government cloud services in the Gambia can play an important role in facilitating regional integration. As a member of ECOWAS, ECOWAS' policies on Technology should be an integral part of Gambia's technology blueprint. The role of the Gambia Government Cloud in the realization of integration programmed of ECOWAS must be considered. Cloud services can provide a platform for collaboration and information sharing with member countries, enabling more efficient and effective communication and collaboration.

- *Interoperability and standardization*: One of the key objectives of the Gambia e-Government strategy is improvement of the delivery of public services. Governments can use cloud services to provide citizens with access to information and services across national borders, which can help break down barriers and promote regional and international integration. Government Cloud also provides a more secure platform for sharing sensitive information and data between governments. This can help build trust and cooperation between the Gambia and its partners and promote greater transparency in international affairs.

  To realize this benefit, GoTG must ensure that the Gambia Government Cloud platform is compatible with cloud services used by other governments and stakeholders. This may involve adopting industry-standard protocols and formats.

- *Compliance with international laws and regulations:* GoTG must ensure that the Gambia Government Cloud adoption complies with all relevant international laws and regulations. This may include compliance with data protection regulations, cross-border data transfer rules, and intellectual property laws.
  Regulation and policy relating to cross-border data flow in The Gambia is lacking. The draft Personal Data Protection Bill of the Gambia, 2021 makes provision for the transfer of personal data outside the jurisdiction of the Gambia. The Bill still awaits enactment into law. As a member of ECOWAS, Gambia is subject to the ECOWAS Data Protection Regulation (EDPR). The EDPR sets out rules for the transfer of personal data across borders, including requirements for obtaining data subjects' consent, ensuring adequate data protection measures are in place, and providing data subjects with adequate information about the transfer. Compliance with the General Data Protection Regulation (GDPR) is also

important to guide cross-border data flow with European Union member states.

- *Security and privacy concerns:* It is vital to ensure that the adoption of the Gambia Government Cloud does not compromise the security or privacy of GoTG and other stakeholders. This may involve implementing strong security controls through the enforcement of the Government Cloud security policy and ensuring that data is stored and processed in a way that protects privacy.
  For the security of international data flow, it is advisable to implement a Secure Socket Layer (SSL) as a security encryption measure, while the information is being transferred. This limits the risk of hackers to read the information. Also depending on the end-users or websites that the information is interchanged with, an IP Whitelist can be set up, for granting them access and privileges.

- *Data sovereignty*: It is important to consider where GoTG data is stored and processed and to carefully select host countries to ensure that it is kept within its jurisdiction. The Government Cloud Data Sovereignty rules/policies and the Data Classification Policy limits the storage and transfers of ‘Classified’ and ‘Sensitive’ data to other jurisdictions due to concerns about sharing state secrets or other sensitive data types. Therefore, adequate mechanisms need to be taken before the cross-border transfer of GoTG data and selection of Government Cloud hosting locations.

- *Vendor lock-in:* The risks of vendor lock-in when selecting a Government Cloud Service Provider must be considered and appropriate safeguards put in place to ensure easy switch of CSP if necessary.

- *Political and cultural factors:* Political and cultural factors that may affect the adoption of the Gambia Government Cloud must be considered. This may include factors such as national security concerns or concerns about the use of foreign technology.

Policies

1. All cross-border data transfers should be adequately protected and access to the data restricted to authorized personnel only and be based on contractual arrangements that include clear and enforceable data protection provisions.
2. Transfer of GoTG data categorized as ‘Classified’ or ‘Sensitive’ based on the Government Cloud Data Classification policy must have legal basis and must comply with the Gambia Data Protection rules.
3. Processing, storage, and transfer of data to countries within the ECOWAS subregion must comply with ECOWAS Data Protection Regulations.
4. All cross-border data flows must comply with relevant international data protection standards such as the GDPR.

5. Government data can only be hosted outside the boarders of the Gambia to the extent that the Government Cloud Data Classification Policy permits it.
6. To the extent that the law of Gambia permits it, GoTG data can only be hosted in designated countries. The Principal Government Cloud Service Provider in conjunction with the Gambia Data Protection Agency will decide on designated host countries. Factors such as availability of favourable laws on data protection, and data sovereignty should be considered.
7. CSPs should sign contracts that specify their obligations to host data in specified countries, to protect the data of GoTG and citizens of Gambia, comply with Gambian laws and regulations.
8. All GoTG data, resident, and non-resident, hoste on public and private cloud platforms should be encrypted both in transit and at rest
9. As a minimum, all cross-border data transfer must be done using secure transport protocols, such as SSL/TLS. Data transmitted between cloud instances must be encrypted using appropriate encryption algorithms.

12.9 Consumer protection

Generally, the adoption of government cloud services raises several policy considerations related to consumer protection, which includes citizens who use government services or interact with government agencies. It is vital to consider the impact of Government Cloud adoption on citizen's data protection and privacy rights. It is important to ensure that citizens have control over their data, and that their data is secure, accessible, and reliable. Transparent and accountability for Government Cloud adoption policies and the provision of effective remedies for any issues that may arise is also critical.

Key policy considerations

Currently, The Gambia has a Consumer Protection Act, which is generally designed to protect consumers from unfair and misleading market conduct. The Act also provides for the establishment of a Consumer Tribunal and connected matters. What may be lacking in the Act is the absence of provisions for consumer protection as it pertains to cloud. The following are key consumer protection policy considerations for Government Cloud adoption in Gambia:

- *Consumers:* The primary consumers of the GoTG Government Cloud services will be GoTG institutions. However, citizens will also interact with GoTG institutions and consume government services hosted on the cloud and therefore must be included in scope of Consumer protection policies as it pertains to the GoTG Government Cloud.

- *Transparency and accountability*: There is a need for transparency about the Government Cloud adoption policies and the provision of clear information about how Gambian citizens' data is being used and protected in the cloud. GoTG must be accountable for any breaches or data loss that may occur as a result of the Gambia Government Cloud adoption.

- *User consent:* Citizens' consent in storing their personal data in the Gambia Government Cloud is important. In some jurisdictions citizens are given the options to control their data, such as the ability to access, delete or transfer their data from the cloud.

- *Data access and portability:* The feasibility of giving citizens the right to access their data stored in the cloud and to port their data to another service provider if they wish to do so is vital.

- *Data security and privacy:* GoTG must ensure that citizens' personal data is protected when stored in the cloud. This includes implementing proper security measures such as encryption, access controls, and data backups to prevent unauthorized access, modification, or disclosure of data in line with the Government Cloud policies on Data Protection and Security. It is important to establish procedures for reporting security incidents and breaches, and for notifying affected consumers

- *Service quality and reliability:* The principal Government Cloud service provider must ensure that cloud services are reliable, available, and meet the quality expectations of both GoTG institutional consumers and citizens. Service level agreements and support services to institutional consumers who experience service disruptions or issues must be robust.

- *Complaints and redress*: The Principal Government Cloud service provider should provide both institutional consumers and citizens with clear channels to lodge complaints about cloud services and seek redress for any harm caused by data breaches or other issues related to cloud adoption.

Policies

1. The rights of the GoTG Government Cloud consumers and the responsibilities of service providers including the Principal Government Cloud Service Provider shall be consistent with the provisions in the Gambia Consumer Protection Act 2014, and the Government Cloud policies on Data Protection, Security, and SLAs.
2. The consent of citizens' will be obtained before storing their personal data in the GoTG Government Cloud subject to applicable laws.
3. Citizens should have the right to control their data and to access, delete or transfer their data from the cloud platforms subject to applicable law.
4. Citizens should have the right to access their data stored in the Government Cloud platform.
5. In line with Government Cloud Security Policy, the Principal Government Cloud Service Provider and accredited CSPs operating in the Government Cloud digital marketplace must have effective disaster recovery and business continuity plans in place, covering among other things a clear incident response and reporting to handle security incidents and breaches. This plan should include procedures for notifying citizens, investigating incidents, and mitigating their impact.
6. The Principal Government Cloud service provider shall establish clear Channels including a helpdesk where institutional consumers and citizens can lodge complaints about cloud services or government services hosted on the Government Cloud and seek redress for any harm caused by data breaches or other issues related to cloud adoption.
7. The Principal Government Cloud services provider must ensure that Government Cloud services and government services hosted on the Government Cloud are reliable, available, and meet quality expectations of GoTG institutions and citizens' as far as the cloud infrastructure is concerned. SLAs should also provide quality standards and support services to consumers who experience service disruptions or issues.
8. CSPs should disclose all relevant information about their services, including their terms and conditions, privacy policies, security measures, data ownership and control, and any other pertinent details that may affect GoTG

12.10 Service Level Agreements (SLAs)

A cloud service level agreement (SLA) is a contractual agreement between a cloud service provider (public or private) and its customers that outlines the terms and conditions of the service provided. The SLA defines the standards for performance, availability, and other parameters of the cloud service, as well as solutions and penalties in case the provider does not meet them. The purpose of the SLA is to establish a clear agreement between the provider and the customer about the quality of service that is expected and to ensure that the provider will meet the agreed performance levels. The SLA also helps establish accountability and responsibility between both parties and provides a basis for monitoring and measuring provider performance over time.

The SLA normally involves a promise to a service user that the service availability SLO (Service Level Objective) should meet a certain level over a certain period. Failing to do so then results in a penalty.

The Principal Government Cloud Service Provider will be responsible for ensuring CSPs comply with defined SLA guidelines and requirement. The Chief IT officers within the various government agencies will advise if some modifications are needed based on changing consumer needs and regulations. Noncompliance to defined SLAs might lead to a partial refund of the service subscription fee paid for that period or additional subscription time added for free.

Key considerations

When developing the SLAs for cloud vendors listed on the Gambia Government Cloud Digital Marketplace, the Principal Cloud Provider must ensure that cloud services meet the highest performance and availability standards, and to provide a framework for addressing SLA breaches. To ensure that Government Cloud services are aligned with the needs of GoTG institutions and meet the required levels of performance, security, and availability, the following must be considered as minimum standards when selecting appropriate SLAs for cloud services:

- *Service levels*: SLAs should define the service levels that the service provider must meet, including SLOs for uptime, response times, and resolution times. These should be realistic and achievable and should be regularly reviewed and updated.

- *Availability:* SLAs should define the uptime or availability of the service and the consequences of failing to meet the specified uptime. This includes defining service level objectives (SLOs), downtime credits, and response and resolution times.

- *Data sovereignty:* SLAs should address the geographic location of data storage and processing and the applicable data protection laws in those locations. This includes specifying data center locations, data transfer mechanisms, and any restrictions on data storage and processing. This should be consistent with relevant Government Cloud policies.

- *Security:* Security controls and measures that the service provider must implement to protect data and GoTG systems. This includes access controls, encryption, monitoring, and incident response procedures.

- *Compliance:* The SLAs should specify the applicable laws, regulations, and industry standards that the service provider must comply with. This includes privacy laws, security regulations, and other legal requirements that govern the handling of GoTG and Citizens data.

- *Change controls:* SLAs should define the change control process for any changes to the service or system. This includes defining the approval process, testing requirements and notification procedures.

- *Help desk support*: SLAs should define the hours of operation for help desk support and the response and resolution times for support requests. This includes specifying support channels (e.g., phone, email, chat) and escalation procedures.

- *Penalties*: The SLA should include provisions for penalties or credits in the event of non-compliance with the SLA

- *Reporting and monitoring*: SLAs should define reporting requirements for service performance, security incidents, and other key metrics. This includes specifying the frequency, format, and content of reports, as well as access rights to monitoring tools and data.

- *Exit strategy*: SLAs should define the process for terminating the service and transferring data and systems to another CSP. This includes defining the notice period, data migration requirements, and any costs associated with termination.

Policies

1. Availability: CSPs must provide at least 99.9% availability for their services. Providers must have systems in place to monitor and report on their availability.
2. CSPs must provide response times that are consistent with the expectations of each GoTG institution.
3. CSPs must ensure that their services are secure and meet the standards required by customers. Providers must have appropriate security measures in place, such as firewalls, intrusion detection and prevention systems, and data encryption.
4. CSPs must comply with all applicable data protection laws and regulations in Gambia. Providers must have appropriate data protection measures in place, such as data encryption, access controls, and backups.
5. Violation of this policy may result in disciplinary action, up to and including compensation to government, citizens, or termination of the contract with the CSPs.

12.11 Audit

Cloud audit is critical to ensuring the security, privacy, and compliance of cloud-based systems and data. It entails a comprehensive evaluation of the security and compliance posture of a CSPs. A cloud audit involves review of the CSPs policies, procedures, and controls, as well as their compliance with relevant Government Cloud policies, specific SLAs, laws, and regulations. The purpose of a Government Cloud Audit is to provide assurance to government agencies and departments that their CSP is meeting their security and compliance requirements, and that their data is being protected appropriately.

CPS must ensure that they are being audited annually by an independent cloud auditor of a recognized charter. The audit shall include but not limited to:

a. Assessments of the following:
    I. physical security
    II. network security
    III. access controls
    IV. data encryption, and
    V. incident response capabilities
b. The audit shall also evaluate the CSP's compliance with the Gambia Government Cloud policies, regulations such as the Data Protection Act, Cybercrime Act, and other industry standards, such as those established by the Cloud Security Alliance or the International Organization for Standardization.
c. The audit may identify areas of weakness or gaps in the CSPs security controls, which can then be addressed through remediation actions.

Criteria for Conducting cloud audit in Gambia

1. *Compliance with data protection and privacy laws:* The CSP should comply with all relevant data protection and privacy laws and regulations, including those related to data retention, transfer, and disclosure.
2. *Security policies and procedures:* The CSP should have comprehensive security policies and procedures that are documented and communicated to all CSP employees. These policies and procedures should cover areas such as access control, incident response, and data encryption.
3. *Network security:* The CSP should have adequate network security controls in place to protect against unauthorized access, malware, and other cyber threats. This should include firewalls, intrusion detection and prevention systems, and regular vulnerability scanning.
4. *Physical security:* The CSP should have appropriate physical security measures in place to protect against unauthorized access to its data centres, such as biometric access controls, security cameras, and security personnel.
5. *Disaster recovery and business continuity:* The cloud service provider should have a disaster recovery and business continuity plan in line with the Government Cloud policy, that includes backup and recovery procedures, redundancy measures, and testing protocols.
6. *Service level agreements (SLAs):* The CSP should meet or exceed the SLAs specified. This should include availability, uptime, and response time guarantees.
7. *Audit logs and reporting:* The CSP should maintain detailed audit logs that record all system activity and provide regular reports to the government agency or department that detail compliance with security controls and SLAs.
8. *Personnel security:* The CSP should perform background checks on all employees, contractors, and third-party service providers who have access to government data in the cloud.

Policies

1. The Principal Cloud Service provider must conduct regular cloud audits to ensure that CSPs meet security and compliance requirements.
2. Audit reports shall be filed with the Principal Cloud Provider by the end of the first quarter of the ensuing year.
3. Cloud audits shall be conducted by trained and qualified auditors who have experience with cloud computing and security and belongs to a recognized charter.

4. Cloud audits must follow established audit guidelines stated in this policy, and others provided by the Cloud Security Alliance (CSA) or the International Organization for Standardization (ISO).
5. Government agencies and departments shall ensure that their use of cloud services is compliant with relevant laws and regulations, and that their CSPs comply with the same requirements.
6. The Principal Government Cloud Service provider shall establish a process for addressing any security or compliance issues identified during cloud audits, including remediation and follow-up verification.

12.12 Cloud Certification

Certifying CSPs is necessary to ensure that services offered to the Government of Gambia and its agencies meet certain standards of security, reliability, and regulatory compliance. For CSPs to be listed on the Gambia Government Cloud Digital Marketplace, they will need to be certified by the Principal Government Cloud service provider.

Key Considerations

To ensure that government CSPs operating within The Gambia meet the highest standards for security, compliance, and reliability, there are several key considerations:

1. CSPs must meet the minimum Government Cloud policy requirements and other regulatory requirements and standards for data protection, security, privacy, sovereignty etc. Compliance will be verified and certified by an independent third-party auditor.
2. Data Sovereignty: CSPs must commit to ensure that data categorized as ‘Classified’ or ‘Sensitive’ is stored and processed within the jurisdiction of The Gambia. This is important to maintain control over government data.
3. Security and Privacy: CSPs must have robust security measures in place to protect against data breaches, unauthorized access, and cyber-attacks. They must also have policies in place to protect user privacy, including data access and sharing.
4. Reliability and Availability: CSPs must have the ability to provide reliable and available services, with little to no downtime or service interruptions. This is critical for the smooth operation of Government Cloud consumers.
5. Customer Support: CSPs must have a good track record of providing adequate customer support, including prompt response times and resolution of issues. They must also have the capacity to provide training and resources to help users make the most of their cloud services.
6. Interoperability: CSPs services should be easily integrated with existing Government IT infrastructure used by government agencies and other organizations. This is important for maintaining continuity and reducing disruption during the migration to cloud services.
7. Disaster Recovery and Business Continuity: CSPs must have effective disaster recovery and business continuity plans in place to ensure that data and services can be quickly restored in case of natural disasters, power outages, or other disruptions.

CSP Certification Process

1. Application Submission: The first step in the certification process is for the CSP to submit an application for certification to the Principal Government Cloud Service Provider. The application should include details on the cloud services offered, the location of the data centre(s), the security management system in place, disaster recovery plan, and service level agreement.
2. Audit: After receiving the application, the Government Cloud Service Provider will appoint an independent auditor to evaluate the CSP's compliance with the certification criteria. The auditor will review the CSP's security management system, disaster recovery plan, service level agreement, and other relevant documentation.
3. Evaluation: Based on the audit findings, the auditor will evaluate the CSP's compliance with the certification criteria. If the CSP meets the certification criteria, the Principal Government Cloud Service Provider will issue a certificate of compliance. If the CSP fails to meet the certification criteria, the auditor will provide a detailed report to the Principal Government Cloud Service Provider explaining the areas where the CSP needs to improve.
4. Certification: Once the CSP meets the certification criteria, GICTA will issue a certificate of compliance, and the CSP will be added to the list of certified cloud service providers on the GICTA website.

Policies

1. The Principal Cloud Provider shall establish a Cloud Vendor Certification Framework for CSPs incorporating local requirements and international standards.
2. CSP shall have a security management system that complies with international standards such as ISO/IEC 27001
3. Compliance of CSPs shall be periodically reviewed against regulations and standards and accompanying certifications independently tested
4. The Principal Government Cloud Service Provider shall maintain a list of certified cloud service providers on the Digital Marketplace. Cloud Service Providers that fail to meet the certification criteria or that fail to maintain compliance with the certification criteria will be subject to revocation of their certification and delisted from the Cloud Digital Marketplace. The Principal Government Cloud Service Provider will maintain a list of certified cloud service providers on the Digital Marketplace
5. CSPs security controls shall be evaluated based on local and international standards (e.g. ISO/IEC 27k, ISO/IEC 22301, ISO/IEC 20000, ISO/IEC 38500)

12.13 Workforces and Skills

The development and adoption of Government Cloud technology in The Gambia will require a skilled workforce with the appropriate expertise and knowledge to effectively design, implement, and manage cloud-based systems. GoTG recognises the need to develop a skilled workforce to support the adoption of cloud computing in the government and public sector.

Policy Considerations

- *Immediate and sustained investment in skills development:* The IT departments of MDAs in the Gambia, play an integral role in the management of the ICT estate of the institutions, delivery of services to the public and the provision of security to the essential ICT systems and information of GoTG. Immediate and sustained investment in GoTG workforce is critical to the enhanced quality, security, and impact of e-Government. Without it, the goal to optimise GoTG's technology infrastructure in keeping with the e-Government strategy and the successful proliferation of the Government Cloud adoption will not be fully realised.

- *Impact on workforce:* As GoTG institutions adopt and migrate to cloud platforms, the impact of these migrations on the workforce needs to be examined. Specifically, there is need for GoTG institutions to identify potential skills gaps that emerge as a result of transitions to cloud-based infrastructure and services, and, where necessary, equip existing staff with additional skills and knowledge to keep up with the growing trend of technology options available to procure and deploy.
- Also, the impact of moving legacy IT estate to the cloud on staff roles needs to be considered, including potential for job losses. Workforce reconfiguration will be required for the successful adoption of Cloud services:
  - There will be specific need for skills at government managerial levels who understand the opportunities and challenges
  - There will be less demand for traditional IT skills such as hardware and system management, application development
  - There will be more demand for skills including business analysis, enterprise architecture, portfolio and program management, services provisioning, and management, change management, vendor and contract management, relationship management, innovation and problem-solving

- The size of agency IT departments/teams will be reduced over time as the management of infrastructure is outsourced to CSPs.

- *Skills requirements:* Overall, the transition, management, and operation of Government Cloud services in the Gambia require a combination of technical, managerial, and operational skills, as well as strong communication, collaboration, and leadership skills:

  1. Technical expertise: cloud computing, networking, security, data management, and automation.
  2. Security knowledge: security protocols, risk management, compliance, and governance. A thorough understanding of security requirements and regulatory compliance is critical.
  3. Portfolio and Project management: Effective portfolio and project management skills are essential for overseeing the implementation of cloud services, ensuring that project timelines and budgets are met, and monitoring project progress.
  4. Change and Communication management: Managing change effectively is crucial for ensuring that the adoption of cloud services runs smoothly. This requires a strong understanding of the impact of change on people, processes, and technology.

     Effective communication skills are essential for managing stakeholders, negotiating with vendors, and ensuring that project goals and objectives are met.
  5. Vendor and Contract management: Managing vendor relationships is crucial for ensuring that Government cloud services are delivered on time, on budget, and to the required quality standards and SLAs are properly monitored and enforced.
  6. Analytical skills: Analytical skills are essential for assessing the performance of Government cloud services and identifying areas for improvement.
  7. Relationship Management: Collaboration skills are important for working with stakeholders within and GoTG institutions to ensure that cloud services are meeting their needs.
  8. Leadership: Leadership skills are critical for managing and motivating a team of professionals responsible for managing the operations of the cloud services

- *Integrated approach to Government Cloud skills development:* A national framework for ICT skills development in the Gambia is currently lacking. To sustain the availability of cloud skills within government, an integrated skills development plan and programme, designed to facilitate the building of competencies that will enable the workforce within GoTG have the fundamental skills and certification in the management and operations of cloud technologies will have to be adopted.

  It is important for the Government Cloud skills development framework to focus on multiple models for workforce transformation. The capacity development approach should straddle development initiatives for traditional IT and non-IT personnel, emerging talent (including non-IT personnel), professional certification programs, study tours, apprenticeship programs, and exchange programs. The role of the private sector in skills development must also be considered.

Policies

1. The principal Government Cloud services provider in collaboration with the MoCDE shall be responsible for the design and operation of a National Government Cloud Workforce Development Framework. The framework shall consist of a set of guidelines and best practices to help GoTG institutions develop and maintain a skilled workforce capable of managing and operating the cloud services effectively. The framework would provide a roadmap for GoTG institutions to identify the skills and knowledge needed to successfully transition to cloud services and to develop and train their workforce to acquire those skills.

2. GoTG institutions shall develop resourcing strategy as part of their change management programs for transition to the Government Cloud. Individual institutions will need to identify their current capability to establish a baseline around the core skill sets required to manage service providers, as opposed to the more traditional ‘operator’ role that currently exists.

3. GoTG shall ensure minimal job losses as a result of cloud adoption. Employees should only be fired when reskilling and redeployment options have been exhausted.

4. The Principal Cloud Provider shall provide a sandbox environment for IT professionals to practice acquired skills

5. Training on mobile cloud computing security, including best practices for data protection, secure access, password management, and incident reporting shall be included in the list of approved training initiatives

12.14 Data Portability

Data portability allows government agencies and users to move their data from one cloud service provider (CSP) to another without any constraints or vendor lock-in. It enables users to retain control over their data and avoid being tied to a single CSP, which could result in limited options and increased costs.

Data portability is usually of most concern for SaaS cloud services, since the service, content, data schemas, and storage format are under the control of the cloud service provider and government agencies will need to understand how the data can be imported into the service and exported from the service. For IaaS and PaaS services, it is typically the case that the government agency will be in control of the content and schemas for the data, with the service offering basic storage capabilities such as a file system or object store.

Data portability is a critical feature of cloud computing for the GoTG for several reasons such as the following:

- Data portability will help avoid vendor lock-in and will allow GoTG maintain control its data and applications, making it easier to migrate between cloud service providers or cloud models.
- Data portability will provide cost savings by enabling GoTG institutions move data between CSPs. By taking advantage of best pricing or higher quality services, institutions can optimize spending and reduce overall costs.
- Data portability will facilitate interoperability between within the public sector by allowing institutions to easily share data with each other. This can improve the efficiency of government services, reduce duplication of effort, and enable faster decision making.
- Data portability will also allow GoTG have greater control over its data.

Policy Considerations

Data format: It will be important to ensure that government data is stored in an open, interoperable format that can be easily transferred between different cloud service providers or environments. Standard formats such as CSV, JSON, or XML can help ensure compatibility.

Data access: Full access to data hosted on the Government Cloud, including the ability to download and export it at any time must be a key consideration in negotiation terms with CSPs. This can help ensure that institutions have the flexibility to move data between CSPs or environment as needed.

Contractual obligations: Agreements with Government Cloud must include provisions for data portability, including the ability to transfer data to other CSPs or to an on-premises environment.

Interoperability: All services by Government Cloud Service Providers must be interoperable with other cloud services and environments. This will help ensure that data can be easily moved between different environments as needed.

Data security: Secure transfer of data between different CSPs or environments, should be a key consideration to prevent data breaches or unauthorized access to sensitive data.

Data privacy: Data must be protected in accordance with relevant laws, regulations, and policies related to data privacy and security, even when data is being transferred between different CSPs or environments.

Policies

1. MoCDE shall develop an Open Data framework for sharing data.
   The framework should provide guidelines to GoTG institutions on storing data in open, interoperable formats that can be easily transferred between different CSPs or environments. Standard formats such as CSV, JSON, or XML should be used.

2. Master services agreements with Government Cloud service providers shall include provisions that ensure data portability. This may include the ability to transfer data to another provider or to an on-premises environment, as well as provisions for data access and export

3. The principal Government Cloud Service Provider shall conduct regular testing and validation of data portability processes of CSPs to ensure that they work as intended and that data is transferred correctly between different cloud service providers or environments.

4. This policy shall be consistent with the Government Cloud Security, and Data Protection Policies

12.15 Enforcement

Enforcement guidelines will be critical to ensuring that the Government Cloud policies are being followed, the policies objectives are being realised, security risks are being mitigated, standardization is being promoted, and clarity is being provided.

The Principal Government Cloud Service Provider will be the primary enforcer of the policies with the authority to apply sanctions for non-compliance. The Principal Cloud Provider shall collaborate with the Cloud Working Groups constituted by various GoTG institutions in enforcing the policies.

Policies

1. The Principal Government Cloud Service Provider shall define the roles and responsibilities of stakeholders involved in cloud service delivery, including government agencies, CSPs, and end-users. The Principal Government Cloud Service Provider will also establish processes and procedures for ensuring compliance with the Government Cloud policies.
2. The Principal Government Cloud Service Provider shall establish clear criteria for the selection of CSPs, based on their ability to meet the requirements of Gambia's cloud policies. The criteria shall be transparent, and providers will be required to demonstrate compliance before being accredited.
3. The Principal Government Cloud Service Provider shall ensure that contractual obligations with CSPs are in place, clearly outlining their responsibilities and obligations under Gambia's cloud policies. These contracts shall include SLAs, security and privacy requirements, and compliance monitoring. The contracts shall be regularly reviewed to ensure that they remain up-to-date and relevant.
4. The Principal Government Cloud Service Provider shall conduct regular audits and monitoring of CSPs to ensure compliance with contractual obligations and Gambia's cloud policies. This shall include the implementation of technical and operational controls, and the monitoring of cloud provider's security posture. The audits shall be conducted by qualified auditors, and the results shall be reported to the Cloud Governance Board.

5. The Principal Government Cloud Service Provider shall establish incident response and reporting procedures for CSPs, outlining the steps to be taken in the event of a security or privacy incident. This shall include reporting to government institution and the public if required. CSPs shall be required to report incidents promptly and transparently.
6. The Principal Government Cloud Service Provider shall impose penalties and sanctions on CSPs that fail to comply with contractual obligations and Gambia's cloud policies. These penalties shall include financial penalties, suspension or termination of contracts, or exclusion from future government contracts. Penalties and sanctions shall be enforced consistently and fairly.
7. The Principal Government Cloud Service Provider shall collaborate with industry groups through workshops and media outlets to promote awareness and understanding of Gambia's cloud policies. This shall include the publication of policies to ensure stakeholder awareness. The government shall also engage with industry groups to identify emerging trends and technologies that may impact Gambia’s Government Cloud policies.

Section 13: Monitoring and Evaluation (M&E)

Realization of the expected outcomes of The Gambia Government Cloud Adoption will require consistent monitoring and evaluation of outcome indicators as detailed in the Government Cloud Implementation Plan. 2 major monitoring and evaluation activities will be carried out periodically. These are impact assessment and periodic performance assessments will be carried out as follows:

I. Impact assessment and evaluation will be carried out after five years of implementation to assess its contribution to achieving the digital agenda of Government of The Gambia and inform future e-Government planning processes.

II. Implementation of monitoring will be carried out on an annual basis to establish whether the implementation is on schedule and assist in correcting deviations (if any) and bring the implementation back on course.

Section 14: Waivers and Expectations

Any waivers or exceptions to the provisions of this Policy require the approval of the Ministry of Communications and Digital Economy.

Section 15: Policy Designation

This Policy is for public use and shall be made publicly available.

Section 16: Effective Date

The effective date of this Policy is _______________.

Section 17: Accountable Owner

The Chief Executive Officer of the Principal Gambia Government Cloud Service Provider is the accountable owner of this Policy.