Government Cloud Implementation Plan

The Gambia

Commissioned by the Ministry of Communications and Digital Economy

Document History

SN	Author	Version No	Release Date	Change Details
1	Consultant	1.0	26th April 2023	
2	Consultant	2.0	29th June 2023	Document updated with comments and suggestions from stakeholders

Table of Contents

1

Purpose, Application, and Related Documents

Purpose, Application, and Related Documents

Purpose

The purpose of this document is to guide the adoption and use of cloud computing technologies by Government of The Gambia (GoTG) institutions. The plan provides a roadmap for the government's transition to cloud computing, with a focus on both technology and non-technology related interventions.

Application

The implementation of this plan shall be subject to applicable policies and laws

Related Documents

This document should be read in conjunction with the following:

a) The Gambia Government Cloud Strategy

b) The Gambia Government Cloud Policies

2

Government Cloud Strategic Initiatives

The roadmap focuses on 4 thematic areas

Government of The Gambia (GoTG) will use Cloud services, shared and managed by one or many authorized and pre-identified Government Cloud service providers. IT infrastructure, software and information shall be device agnostic (laptops, smart phones etc), and provided as a utility via a ratified pricing model – on a pay by use basis or otherwise. Government Cloud services will be accessed via a network connection – in many cases traditional internet connectivity; and be supported by new delivery and supply models. The core of the Government Cloud landscape shall be facilitated by an online portal (Digital Marketplace) that enables dynamic scalability, service delivery agility, and easy service life-cycle management. Government Cloud implementation for GoTG shall not be a milestone achievement but rather an evolutionary program of work which shall be instrumental in changing the way GoTG institutions procure and operate IT for all stakeholder benefit

As the GoTG considers the adoption of the Government Cloud , it is imperative that the Principal Government Cloud service provider, supported by the MoCDE, establishes the foundations for strong governance, pragmatic policy implementation, continuous portfolio management and sustained organizational and IT transformation that is needed to support individual GoTG institutions on their Cloud journey. Additionally, there are a number of activities that can be started, to progress the evaluation of Cloud ready IT services and Cloud vendor offerings in the market. It will be prudent for the Principal Government Cloud Provider, to identify early candidates for Cloud migration (e.g., mature offerings including email, storage, and collaboration tools) to serve as model institutions and epitomize the idealized GoTG Government Cloud transition case study.

To ensure effective implementation of the Gambia Government Cloud project, 23 initiatives have been identified and grouped under 4 primary thematic areas which will be the central focus of the roadmap:

Thematic Areas

1. Cloud Governance and Trust
2. Cloud Adoption
3. Cloud Transition / migration
4. Cloud Change Management

The roadmap focuses on 4 thematic areas

Cloud Governance and Trust

Establishment of the appropriate legal and regulatory framework to guide and compel GoTG institutions to use and take advantage of the Government Cloud . Identify Government Cloud service providers, regulates costs of the services and also stipulates the services levels that must be maintained. It also involves implementation of foundational infrastructure and support frameworks to establish trust and confidence in the shared service centre to be operated by the Principal Government Cloud services provider .

Cloud Adoption

This involves the establishment of guidelines to enable GoTG institutions to self-assess their current state and determine both their short and long-term cloud service needs. This also involves institutionalizing key platforms to help these institutions embrace cloud services and autonomously adopt the Gambia Government Cloud .

Cloud Transition and Migration

Involves providing support to address the typical challenges faced by Government institutions moving from the traditional in-house IT operating model to reliance on a shared service centre and self-serviced digital market place. It also covers actual migration support, i.e., the process of moving existing applications, data, and workloads from on-premises infrastructure or other cloud providers to a specific the Gambia Government cloud environment

Cloud Change Management

This includes areas of institutional capacity support and soft services to optimize stakeholder engagement and involvement. Activities here help to maintain focus on the key objectives, manage expectations and minimize cost.

Government Cloud strategic initiatives

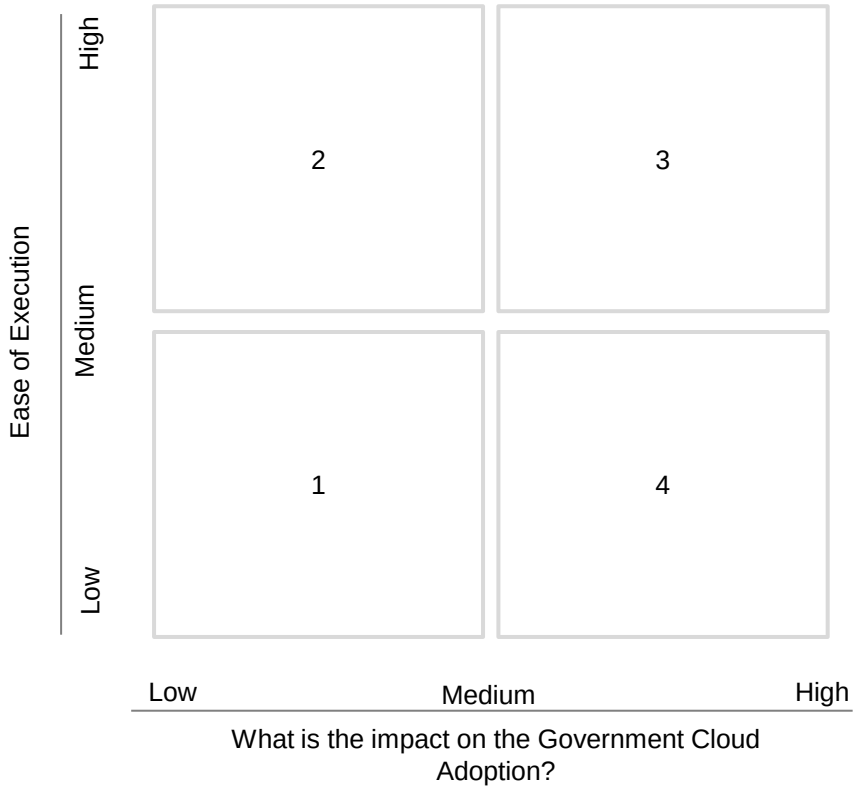
Cloud Governance and Trust	Cloud Adoption	Cloud Transition and Migration	Change Management
► Development of a Cloud Legal Methodology basis ► Endorse the Gambia Government Cloud Policy ► Establish of a Governance body ► Definition of architecture principles defined ► Analysis of Cloud risk analysis ► Redefinition of Financial management ► Redefinition of procurement and vendor/contract management redefined ► Establishment of Cloud Centre of Expertise ► Establishment of Compliance and certification framework ► Certification of Principal Government Cloud provider	► Establishment of Cloud alternative assessment guidelines ► Alignment of current cloud assets to policy ► Consolidation of infrastructure and repositioning of Gamtel as a CSP ► Establishment of a Cloud Digital Market place with new procurement rules in effect	► Establishment of Lifecycle methodology ► Identify First Cloud candidates ► Migration of First Cloud candidates / major agencies to IaaS ► Migrate all candidate assets to Cloud	► Establishment of sponsorship (Executive commitment) ► Establishment of communication plan ► Establishment of metrics for performance and cost ► Establishment of training program ► Workforce reconfiguration

Government Cloud strategic initiatives prioritisation (1/2)

Initiatives Mappings to the Opportunity Matrix

Ease of execution criteria

- Estimated duration required for implementation
- Level of change required to the status quo
- Cloud readiness
- Technology: Technical Complexity



Impact on Government Cloud adoption criteria

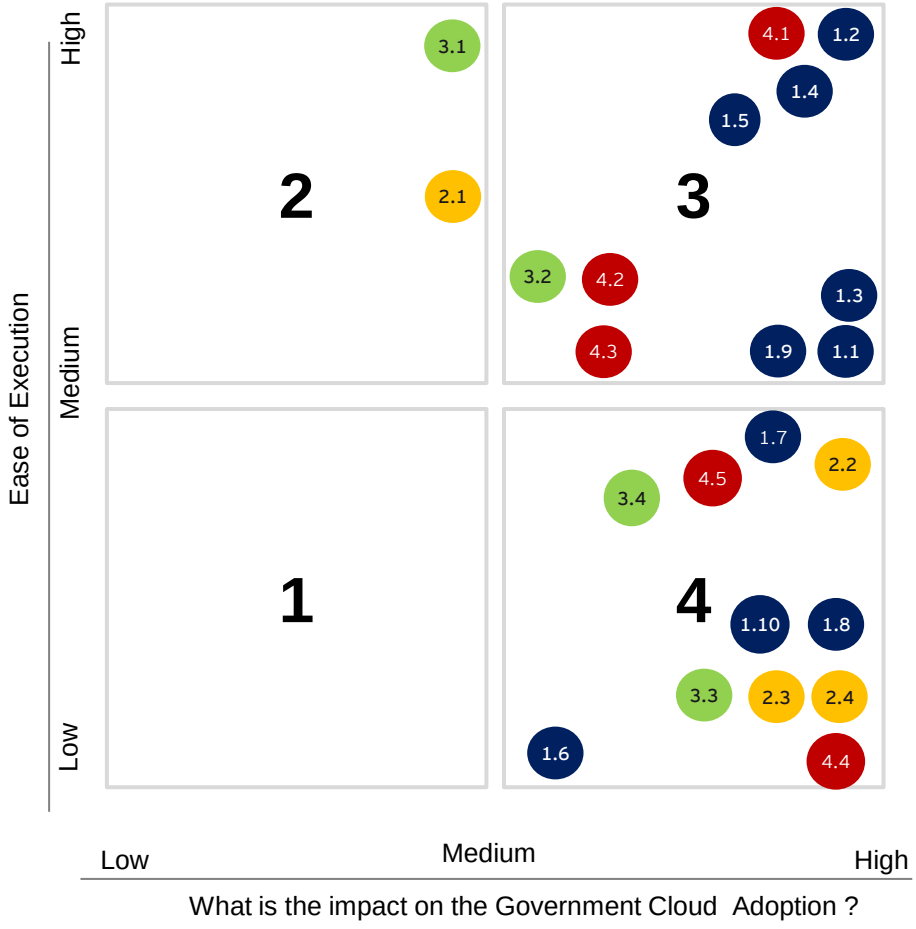
- Direct cost advantage
- Optimization or ease in management of resources
- Number of institutions impacted

Quadrant summary

1. Status quo – Difficult to execute, low advantage to cloud
2. Small Quick Wins – Easier to execute, low adoption advantage
3. Pursue - Easier to execute, high adoption advantage
4. Major Projects – Difficult to execute, high adoption advantage

Government Cloud strategic initiatives prioritisation (2/2)

Prioritization has been formulated based on assessment of identified initiatives under two broad criteria :"Ease of Execution" and "Impact on the Government Cloud adoption "



1 Cloud governance and trust

1.1 Development of a Cloud Legal Methodology basis
1.2 Endorse the Gambia Government Cloud Policy
1.3 Establish a Governance body
1.4 Definition of architecture principles
1.5 Analysis of Cloud risk
1.6 Redefinition of Financial management
1.7 Redefinition of Procurement and vendor/contract management
1.8 Certification of Principal Government Cloud provider
1.9 Establishment of Compliance and certification framework
1.10 Establishment of cloud Centre of Expertise

2 Cloud adoption

2.1 Establishment of Cloud alternative assessment guidelines

2.2 Alignment of current cloud assets to policy

2.3 Consolidation of infrastructure and repositioning of Gamtel as a private Government Cloud CSP

2.4 Establishment of a Cloud Digital Market place with new procurement rules in effect

3 Cloud transition and migration

3.1 Establishment of Lifecycle methodology

3.2 Identify First Cloud candidates

3.3 Migration of First cloud candidates / major institutions to IaaS

3.4 Migrate all candidate assets to Cloud

4 Change Management

4.1 Establishment of sponsorship

4.2 Establishment of communication plan

4.3 Establishment of metrics for performance and cost

4.4 Establishment of training program

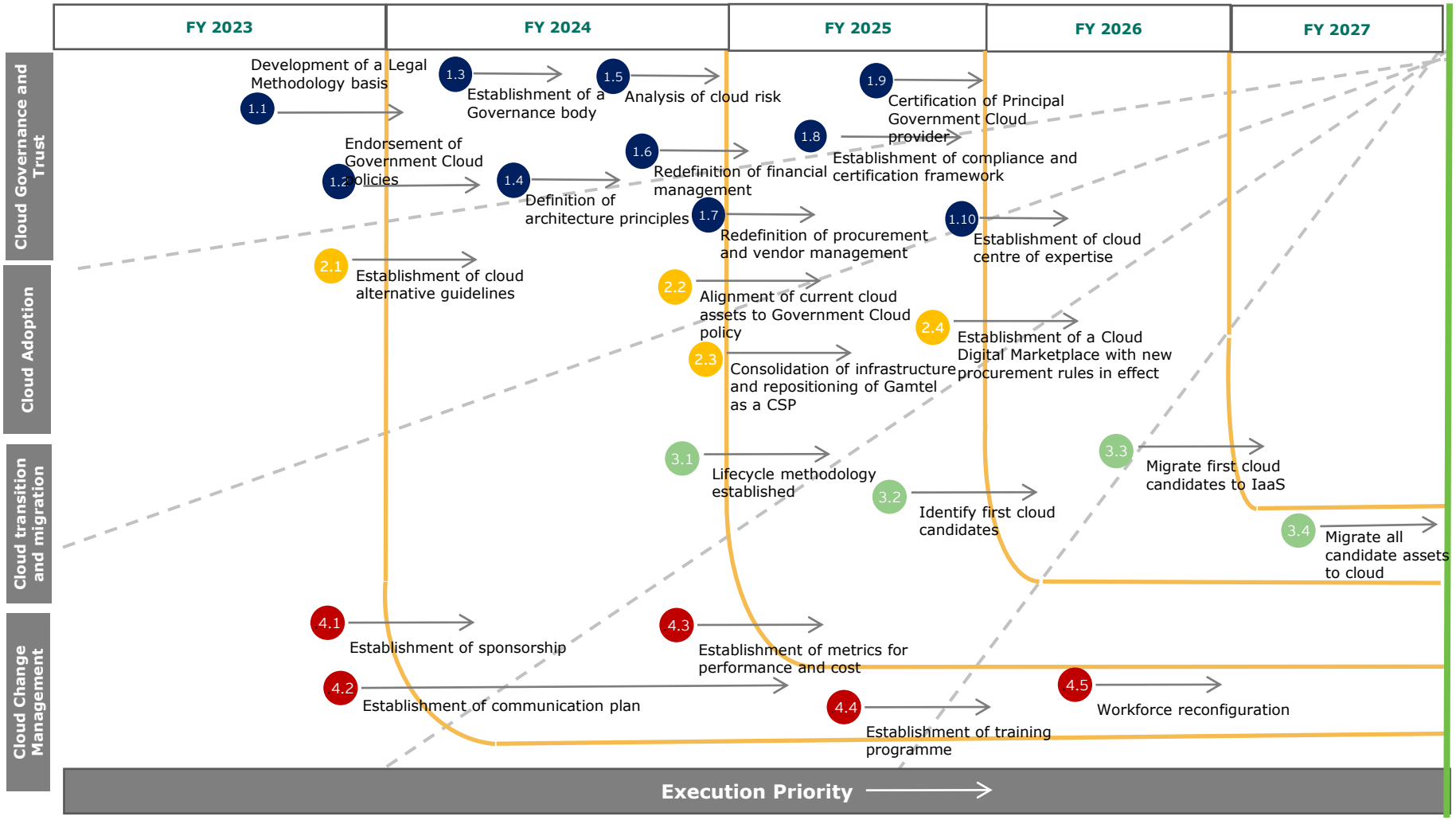
4.5 Workforce reconfiguration

3

Government Cloud Programme Implementation Roadmap

Government Cloud Implementation Roadmap

The figure below outlines a high-level roadmap to assist GoTG in charting and accelerating the Government Cloud journey for access to the incremental benefits of Cloud services as it moves toward a desired future state.



4a

Implementation Delivery Framework

Key Implementation Risks

Implementation Risks

	Risks	Probability	Impact
1	Cloud Governance and Trust		
	Inadequate relevant expertise and resources	High	High
	Evolving legal landscape	Medium	High
	Ambiguity and interpretation	Low	High
	Inadequate clarity and communication	Medium	High
	Resistance to change	High	High
	Decision making bottlenecks	High	High
	Inadequate scope and coverage	Medium	High
	Inadequate stakeholder involvement	Medium	High
	Limited scope of certification	Low	Medium
2	Cloud Adoption		
	Inadequate skilled personnel	High	High
	Resistance to change	High	High
	Inadequate evaluation criteria	Low	High
3	Cloud Transition		
	Appropriate change management	High	High
	Finance	High	High
	Interoperability challenges	High	High
	Other technical challenges	Medium	High
4	Change Management		
	Lack of executive support	Medium	High
	Ambiguous roles and responsibilities	Low	Medium
	Unavailability of baseline data to factor in determination of metrics	High	Low
	Funding	High	High
	Resistance to change	High	High
	Workforce morale and job satisfaction	Medium	High
	Disruption in team dynamics and collaboration	Low	Medium

Implementation Risks

	Risks	Mitigations	Owner
1	**Cloud Governance and Trust** ► Lack of relevant expertise and resources ► Evolving legal landscape ► Ambiguity and interpretation ► Lack of clarity and communication ► Resistance to change ► Decision making bottlenecks ► Inadequate scope and coverage ► Lack of stakeholder involvement ► Limited scope of certification	• Bridge skills and knowledge gap with private sector and consulting support • Scope of legal considerations should be holistic and take account evolving landscape including international laws • Adequate guidance and templates should be provided • Early stakeholder engagement, establishing sponsorship, and education • Funding prioritisation and early assessment of RoI • Scope of certification for Principal Government Cloud provider should be holistic and cover all critical areas	• MoCDE / MPS • MoJ • MoJ • MoCDE • PMO • MoCDE
2	**Cloud Adoption** ► Lack of skilled personnel ► Resistance to change ► Inadequate evaluation criteria	• Prioritise the funding and implementation of a Government Cloud Workforce development framework • Early stakeholder engagement, establishing sponsorship, and education • Evaluation criteria for CSP should be robust and without bias. Consulting support may be required	• MoCDE • PMO • MoCDE
3	**Cloud Transition** ► Appropriate change management ► Finance ► Interoperability challenges ► Other technical challenges	• Program sponsors should be proficient in change management practices to ensure smooth transitions, address resistance, and facilitate user adoption • Funding prioritisation of interoperability / integration system • Adopt an incremental approach and implement the cloud adoption process in phases. This allows for gradual changes, learning, and adaptation • Adequate planning and execution of migrations • Establishment of dual links and express routes to mitigate against network downtimes • All lessons from migrating first cloud candidates to be properly documented	• Project Sponsor • Project Sponsor • SISCo • Principal Government Cloud Provider • Centre of Expertise
4	**Change Management** ► Lack of executive support ► Ambiguous roles and responsibilities ► Unavailability of baseline data to factor in determination of metrics ► Funding ► Resistance to change ► Workforce morale and job satisfaction ► Disruption in team dynamics and collaboration	• Engage leaders who can effectively communicate the vision, benefits, and importance of the project to all levels. Their support will help drive the necessary changes and demonstrate commitment to the success of the cloud adoption • Identify non-executive change champions at the institutional level who can serve as advocates for the cloud adoption initiative • Identify key stakeholders, understand their concerns and expectations, and involve them in decision-making • Early sponsorship of institutional change impact assessments	• MPS • PMO

• PMO –Programme Management Office

4b

Implementation Delivery Framework

Delivery Framework/Project Governance Structure

Delivery Framework

Overview: The Gambia Government Cloud strategy implementation delivery framework has been developed to align with the following critical success factors:

1	**The cloud implementation must be driven from the top**	Ensure government support for the program all the way up to the Minister MoCDE: Having a dedicated sponsor at the top to drive transformation signals commitment
2	**Achievable Scope, Fast Pace**	Keep momentum throughout the implementation by driving to achievable milestones. Focus on value realisation and deliver demonstrable benefits quickly to maintain buy-in for the changes
3	**Metrics**	Define clear metrics and accountability. Screen initiatives for alignment to the vision of the Government Cloud initiative, outcomes and sustainability; have regular pulse checks to maintain control of value delivery
4	**Improved Service Delivery**	Focus on what is best for GoTG, tradeoffs must be made for all else. At every step, ask “How is this going to drive digital transformation for Gambia and improve government service delivery?”
5	**Transparent & Centrally Managed Programme**	Appoint a dedicated Project Management Office to standardise reporting and stakeholder communications.

Delivery Framework

Overview: Execution of GoTG's cloud aspiration will require a robust implementation framework to govern, coordinate, manage risks and unify stakeholder engagement

Early attainment of mobilisation priorities…

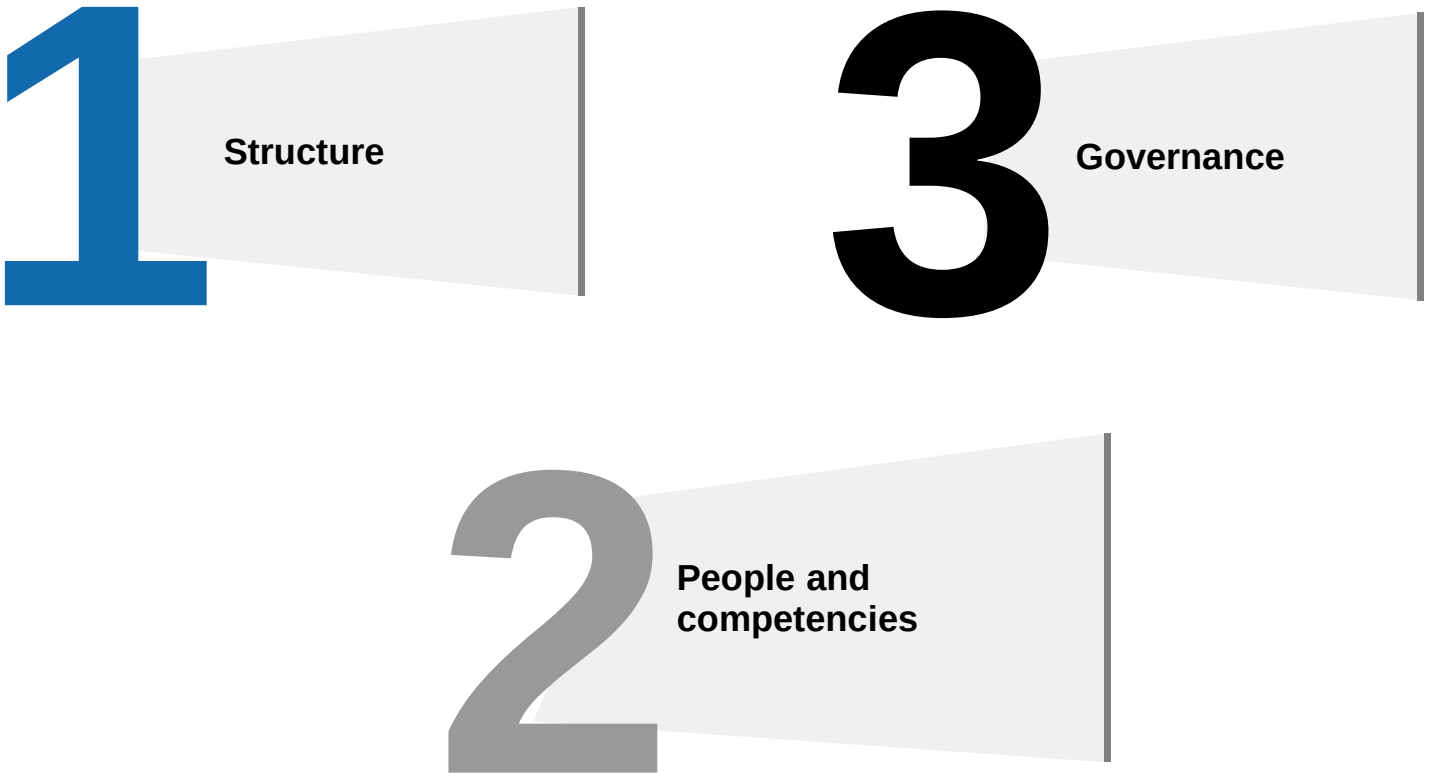
- Establish clear leadership, governance and charter across all initiatives
- Engage and align implementation team
- Define initiative workplans and teams
- Establish program workload plan
- Confirm funding availability and deliverables for first 12 months

…will require setup of effective and aligned implementing structure geared to results delivery

Proactive stakeholder management	Program Risk mitigation	Maintain programme momentum	Program tracking and reporting	Content Support
				
▪ Coordinate communications across GoTG agencies ▪ Align project managers with stakeholder feedback ▪ Build promoters and address detractors ▪ Identify gaps in the sponsorship spine	▪ Maintain program risk register ▪ Identify and mitigate execution risks ▪ Minimize program disruption ▪ Execute risk mitigations at Program level	▪ Lead progress communication to generate momentum and create excitement ▪ Reinforce messaging of successful implementation and get GoTG wide buy-in	▪ Track and monitor initiative level execution activities ▪ Enforce deadlines and deliverables ▪ Focus on results, issue resolution and decisions	▪ Drive projects with project teams to realize results

Delivery Framework

Overview: Instituting the PMO and Change Management office for execution of GoTG's cloud initiative should cover 3 main areas



Delivery Framework

Structure: In selecting optimal structures, the PMO must self evaluate by asking 2 key questions – readiness for change and magnitude of change

Organisational structure options for the Gambia Government Cloud Strategy Implementation

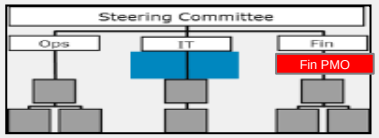
Lever 1

How ready for change is the GoTG?

- Amount of similar change experience
- Success with previous changes
- Depth of leadership team change and sponsorship experience
- Strength of change discipline and tools

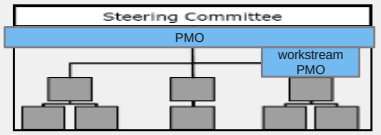
1. Accelerator model

- Accelerate benefits realization while building core changes capabilities



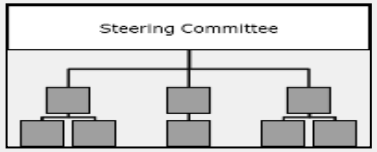
2. Transformer model

- Drive benefits realization across broad and complex change while building capabilities



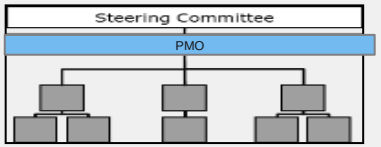
Delivery through the line

- Deploy and realize results through the line without a PMO



3. Orchestrator model

- Orchestrate complex change by leveraging existing capabilities



Lever 2

What is the magnitude and complexity of change?

- Span of progam impacted
- Changes to institutional-wide processes and systems
- Organization, decision rights, or KPI changes
- Behavioral and mindset changes

Delivery Framework

Structure: Selection of the “Orchestrator” model emerges from high-level assessment of GoTG’s readiness for change and the complexity expected from implementing the Government Cloud strategy

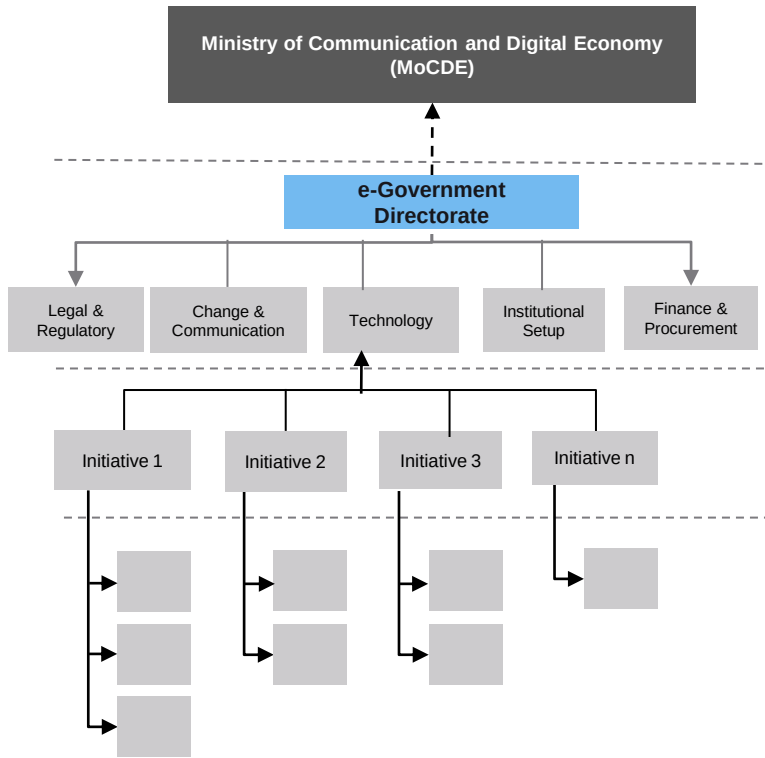
KEY: H – High; M – Moderate; L - Low

		Rating	Explanation
How ready for change is the GoTG?	**Does GoTG have a significant amount of similar change experience?**	**H**	• GoTG has executed several complex projects and multiple large-scale transformation and integration programs over the past years
	Has GoTG had success with previous change?	**M**	• Significant success recorded in past programs and change management processes have been successful
	Is there a depth of leadership team change and sponsorship experience?	**M**	• Government is mindful and committed to level of change required. However, it appears there is room for improvement in communicating the change to the rest of GoTG institutions
	Does GoTG have strong change discipline and tools?	**M**	• Capability exists to design and build implementation tools, but more work needs to be done to drive adoption and maintain institutional momentum across GoTG agencies
What is the magnitude and complexity of change?	**What is the size of government impacted by the change?**	**H**	• ~23 strategic initiatives and enablers impacting all GoTG agencies and support functions implying a large reach across government
	Are there significant changes to existing processes and systems?	**H**	• Changes to IT operating models; Financial Management, procurement and vendor management processes; and workforce reconfiguration is expected as new cloud service and deployment models are defined
	Are there extensive changes to organization structure, decision rights, or KPIs?	**L**	• Minimal IT organizational structure change and streamlining of decision rights to facilitate agility expected

Delivery Framework

Implementation of Governance Structure: Overall strategy rollout to be led by MoCDE project sponsor, supported with a cross functional and cross institutional Government Cloud Strategy Implementation Steering Committee

Implementation governance structure	High level responsibilities
MoCDE	Gambia Government Cloud delivery sponsor ▪ Responsible for ratification of the e-Government Directorate decisions as required ▪ Overall accountability for go/no-go decision on implementation of program MoCDE ▪ Makes decisions impacting the intent, realization outcomes, timing, resource allocation, or business case of specific cloud initiatives ▪ Review implementation progress and clear roadblocks ▪ Overall accountability for GoTG Government Cloud project delivery
Initiative sponsors	▪ Overall responsibility for Government Cloud implementation project delivery ▪ Drive change management across government during implementation ▪ Drive value realization, process efficiency and cadence to driver results delivery ▪ Plan and coordinate resource allocation and people effectiveness at program level while driving change agenda on behalf of MoCDE
Initiatives Owners	▪ Provide overall direction and guidance to implementing teams ▪ Clear roadblocks at initiative level ▪ Escalate roadblocks and issues to MoCDE ▪ Serve as change spine to drive change management initiatives
Team Members	▪ Responsible for day-to-day implementation of project/initiative activities ▪ Project Managers: accountable for team coordination and project cadence ▪ Team members: day to day activities and implementation cadence ▪ Provide regular reporting to the e-Government Directorate



Delivery Framework

People/Competencies: As minimum, the Programme Office (PO) staff will need to have strong capabilities in the following:

	Program Director	PO Lead	PO Officer
Leadership	▪ Strong manager of self and large teams (>15-50 staff strength) ▪ Strong negotiator and influencer ▪ Results oriented	▪ Established manager of self and smaller teams ▪ Leading with interpersonal skills and emotional intelligence	▪ Good interpersonal skills and emotional intelligence
Technical	▪ Trusted technology advisor to GoTG ▪ Analytical and data-driven decision making ▪ Detailed knowledge of Government Cloud project management and monitoring tools ▪ Big promoter of change management ▪ Skilled Conflict management expert	▪ Advanced knowledge of Government Cloud project monitoring and reporting including knowledge of tools, processes and policies ▪ Strategic alliances with GoTG agencies ▪ Good conflict management	▪ Accomplished user of Microsoft Office suite and other productivity tools. ▪ Results oriented and advanced knowledge of developing business cases and management level communications ▪ Strong data analysis and quantitative acumen
Other competencies	▪ Advanced communication skills and stakeholder management ability ▪ Senior designation within GoTG organization structure to liaise with institutional heads and SISCo	▪ Advanced communication skills and stakeholder management ▪ Senior designation within GoTG structure to liaise with GoTG institutional Sponsors and other Director level employees	▪ Strong communication skills ▪ Comfortable with managing stakeholders, including various heads at MDAs and below ▪ Attention to detail and resilience to monitor large long-term projects

Delivery Framework

People/Competencies: We have also established specific team roles to guide execution of major deliverables

	Program Director	PO Lead	PO Officer
Responsibilities	• Drives change agenda on behalf of SISCo • Decide when an initiative can move to next stage • Address issues that put substantial parts of the Government Cloud program delivery at risk • Provide coaching and training to key stakeholders and coordinates with key stakeholders • Flag and escalate key issues and risks to SISCo for resolution	• Tracks project progress of 7-10 projects • Ensure that value and project level milestones are met • Monitor project level interdependencies • Provides valuable expertise, experience and information; supports relevant analysis where necessary • Interacts directly with Initiative leads and project team • Flag issues that cannot be resolved at the project level to Sponsor & PO Lead	• Drive day-to-day monitoring of tasks and project activities • Manage and maintain project documentation including workplans, reports) • Proactively sets up project meetings in alignment with governance framework • Actively collects project implementation data for reporting to PO Lead and Program Director
Decision rights	• Make program-level decisions (e.g., implementation cloud initiatives within the strategy) • Make decisions on quality assurance • Decides which decisions need escalation to PSC and SISCo • Approve project recommendations	• Resolve issues with cross-functional Initiative leads and stakeholders • Assess activity and task level risks	

Delivery Framework

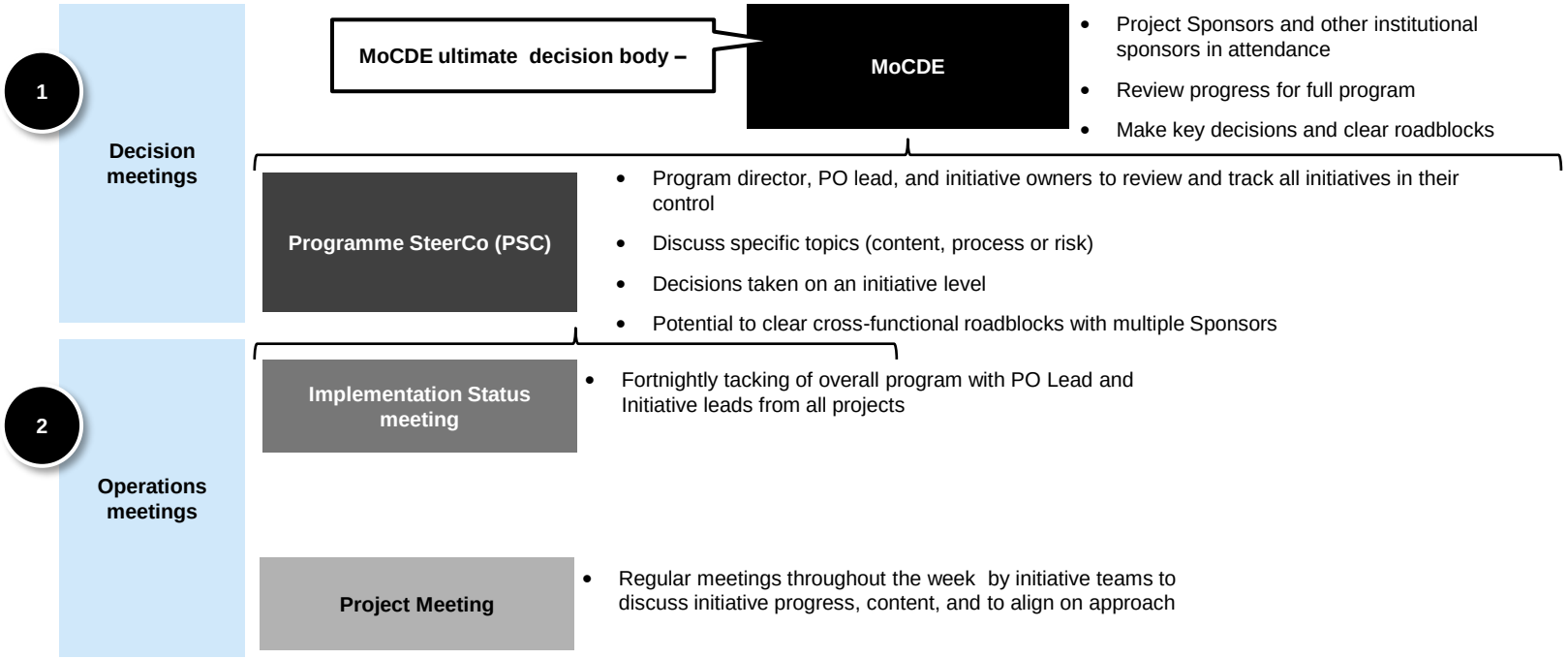
Governance: Members of the PMO will have clear operational and decision making responsibilities across program lifecycle

	SISCo	Program Director	PO Lead	Initiative / Institutional Cloud Sponsor	Initiative Owners	Initiative Teams	Other Subject Matter Experts
1 Direction Setting decisions							
Define governance ambition	I	A	C	R A	I	I	
Appoint CTO/ PMO lead & initial team	R A	I	I	I	I	I	
Define governance structure and guidelines				R A	I	I	
Approve governance staffing	R A	I	I	I	I	I	
Approve RACI, processes and deliverables		A	R	I	I	I	
Define meeting cadence		A	R	I	I	I	
Approve program business case	R A	I	I	I			C
2 Government Cloud Initiative Progress decisions							
Go/no go/iterate on initiative (Gate 0)	I	C	I	A	R	I	C
Go/no go/iterate on initiative (Gate 1)	I	C	I	A	R	I	C
Execute project task		C	I	C	A	R	C
Develop and execute project budget	I	I	I	A	R	I	C
Approve project plan		A		R	I	I	C
Execute day-to-day tasks					A	R	C
Communicate and report project progress	I	A	A	A	R	C	C
3 Define tools for project implementation		A	R	C	C	I	
Escalation decisions							
Decision to escalate issue to sponsor		A	R	I	C	I	
Decision to escalate issue to steerco	I	A	R	A	I	I	
Escalate initiative level roadblock				R A	I	I	
Escalate program level roadblock		R A	I	I	I	I	
Approve corrective action plans	R A	C	I	I	I	I	

R – Responsibility; A – Accountability; C – Consulted; I – Informed

Delivery Framework

Governance: The Government Cloud programme execution and oversight will be conducted by 3 key layers of meetings and touchpoints



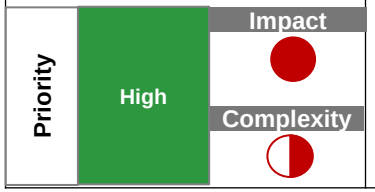
05

Detailed Initiative Charters

Detailed Charter – Development of a Cloud Legal Methodology basis

Cloud Governance and Trust

Initiative Owner	MoCDE	**Start date**	1 August 2023	**Duration**	6 Months
Initiative	**Activity**				**Deliverables**
Development of a Cloud Legal Methodology basis	▸ Develop legal framework to drive Cloud service adoption within agencies via adjustments to legislation and publication of appropriate guidelines. The following are key legal considerations: • Cloud services definition • Cloud services classification • Cloud services provision model • Mandatory or optional usage of cloud • Minimum requirements for CSPs (State-owned and Private • SLA for cloud services • Definition of Mission critical Information System (High Value Information Asset - HVIA) • Principles of financing of state owned CSPs together with cloud services costing and chargeback. • Cloud services pricing principles • Procurement principles of Cloud services (centralized, decentralized)				▸ Legal methodology document or guidelines with examples and templates
Objectives					**KPIs**
▸ To provide a structured and systematic approach to address the legal aspects of cloud computing (adoption and use) within the GoTG context.					▸ % of adjustments to relevant regulation
					Stakeholders
					▸ MoCDE ▸ Attorney Generals Chambers and Ministry of Justice ▸ Parliament ▸ Private sector representatives
					Dependencies
					▸ Establishment of sponsorship
					Risks
					▸ Lack or relevant expertise ▸ Evolving Legal Landscape ▸ Ambiguity and Interpretation



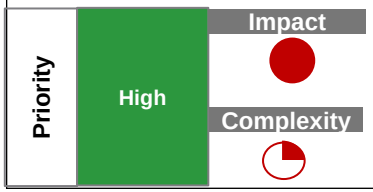
Refer to Annexure 1 for a full list of considerations

Keys *Low complexity/ impact* *Medium complexity/ impact* *High complexity/ impact*

Detailed Charter – Endorsement of Gambia Government Cloud policy

Cloud Governance and Trust

Initiative Owner	MoCDE	**Start date**	1 November 2023	**Duration**	2 months
Initiative	**Activity**				**Deliverables**
Endorsement of Gambia Government Cloud policy	► Stakeholder consultation of the draft Gambia Government Cloud policy to seek feedback and input ► Legal and regulatory review to assess the policy implications on relevant Gambian law, regulations and policies ► Update of the policy ► Executive approval by cabinet ► Communication of the endorsed policy to all GoTG entities and stakeholders involved in cloud adoption				► Documented and formalization of Gambia Government Cloud policy
Objectives					**KPIs**
► To establish a formal and authoritative framework for the adoption and use of cloud computing within GoTG					► Stakeholder endorsement and support for the policy ► Cabinet approval
					Stakeholders
					► MoCDE ► GoTG stakeholders ► The Presidency
					Dependencies
					Risks
					► Lack of Clarity and Communication ► Resistance to change



Keys *Low complexity/ impact* *Medium complexity/ impact* *High complexity/ impact*

Detailed Charter – Establishment of a Governance Body

Cloud Governance and Trust

Initiative Owner	MoCDE	**Start date**	1 February 2024	**Duration**	6 months
Initiative	**Activity**				**Deliverables**
Establishment of a Governance body	► Assess legal considerations to ensure that the establishment of a Government Cloud authority is consistent with relevant laws and regulations ► Nominate and mandate the Gambia ICT Agency (GICTA) as the Principal Government Cloud services provider ► Determine the organizational structure of GICTA as the Principal Government Cloud authority. Define the authority's reporting lines, decision-making processes, and relationships with other GoTG entities. ► Determine the resources required to establish and operate the government cloud authority. This includes financial resources, human resources, infrastructure, and technology. ► Secure the necessary budget and staffing to support the authority's activities effectively ► Appoint a leadership team to oversee the establishment and operations of Government Cloud ► Implement the necessary infrastructure, systems, and processes ► Obtain certification of Principal Government Cloud Service Provider as a IT Service Management Organization including ISO 27001, ISO 9001, and SOC 2				► Established Government Cloud Authority
Objectives					**KPIs**
► Establishment of a dedicated entity to oversee and govern the Gambia Government Cloud adoption, and management of cloud computing services ► Availability of a central authority responsible for providing guidance, establishing policies, ensuring compliance, and driving the strategic direction of cloud initiatives across GoTG entities.					► Established Government Cloud Authority with a governing board ► Approved budgetary allocation ► Certification as a Government Cloud services provider
					Stakeholders
					► MoCDE ► MoFEA ► Cloud Adoption PMO
					Dependencies
					► Adoption of Government Cloud Policy ► Development of a Cloud Legal Methodology basis
					Risks
					► Decision making bottlenecks ► Lack of expertise and resources ► Funding

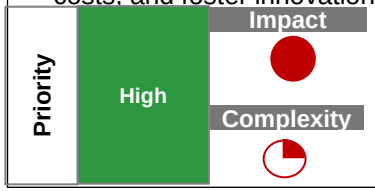
Priority High — Impact  Complexity 

Keys  *Low complexity/ impact*  *Medium complexity/ impact*  *High complexity/ impact*

Detailed Charter – Definition of architecture principles

Cloud Governance and Trust

Initiative Owner	Principal Government Cloud provider	**Start date**	1 May 2024	**Duration**	2 months
Initiative	**Activity**				**Deliverables**
Defininition architecture principles	► Define operational architecture principles including: 1. Events that would trigger a Cloud assessment 2. Development of interoperability requirements, including standards for integration of cloud services with in-house/hosted services 3. Performance requirements (e.g. scalability, elasticity, resilience, disaster recovery , auditing etc) that are required for regulatory and statutory compliance. This should be built into cloud management procedures including vendor management practices				► Gambia Government Cloud architecture principles
Objectives					**KPIs**
► To provide a strategic framework for designing and implementing cloud solutions within GoTG. ► To ensure that Government Cloud adoption in GoTG is aligned with set objectives, promote standardization, address security and risk management, enable scalability and interoperability, optimize costs, and foster innovation					► # of risk exposures recorded ► High standardisation of cloud services
					Stakeholders
					► MoCDE ► Principal Government Cloud Services Provider
					Dependencies
					Risks
					► Inadequate scope and coverage ► Lack of Stakeholder Involvement



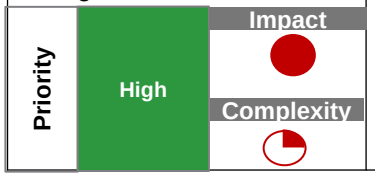
Keys *Low complexity/ impact* *Medium complexity/ impact* *High complexity/ impact*

Detailed Charter – Analysis of Cloud risk

Cloud Governance and Trust

Initiative Owner	Principal Government Cloud provider	**Start date**	1 July 2024	**Duration**	6 Months

Initiative	**Activity**	**Deliverables**
Analysis of cloud risks	► Identification of the potential risks and vulnerabilities specific to cloud adoption within the GoTG context. ► Evaluation of the identified risks in terms of their likelihood of occurrence and potential impact on GoTGs operations, data, and services. ► Develop risk mitigation strategies and controls to address the identified risks. In addition to the Gambia Government Cloud Policies, these strategies may involve technical measures, governance frameworks, contractual agreements, security controls, data protection mechanisms, disaster recovery plans and other measures. ► Establishment of mechanisms to monitor and manage risks throughout the lifecycle of the Government Cloud adoption. ► Provision of training and awareness programs to educate stakeholders involved in the Gambia Government Cloud adoption on risk management best practices, security protocols, and compliance requirements	► List of specific risks ► Risk mitigation strategies and monitoring mechanisms
Objectives		► **KPIs**
► Identification of cloud related risks specific to GoTG ► Determination of appropriate risk mitigation controls ► Secure and successful implementation of the Gambia Government Cloud , while safeguarding government data, protecting citizen privacy, and maintaining compliance with relevant regulations.		► # of reported exposures
		Stakeholders
		► MoCDE ► Principal Government Cloud Services provider ► Gambia Police Force
		Dependencies
		► Adoption of Government Cloud Policy
		Risks
		► Inadequate coverage



Keys *Low complexity/ impact* *Medium complexity/ impact* *High complexity/ impact*

Detailed Charter – Redefinition of Financial management

Cloud Governance and Trust

Initiative Owner	Principal Government Cloud provider	**Start date**	1 September 2024	**Duration**	12 months

Initiative	**Activity**	**Deliverables**
Redefinition of Financial Management	► Modify budgeting and funding models to enable institutions easily access the funds required to transition to and operate in the Gambia Government Cloud environment ► Develop costing models and supporting financial processes for: ◦ Understanding total cost of services ◦ Real-time tracking of service consumptions ◦ Vendor invoicing and payments ◦ Measurement of Cloud RoI ► Establishment of financial management capability within the Principal Government Cloud provider and GoTG entities.	► Budgeting and funding, and costing models ► Financial processes
Objectives		**KPIs**
► Effective and efficient allocation of resources to derive maximum value from the Government Cloud adoption ► To ensure financial transparency, optimization of resource utilization, assessment of ROI, support procurement activities, enable scalability and flexibility in the Government Cloud adoption		► % of cost savings achieved through the new financial management processes. ► Leadtime for accessing funding required to transition to and operate in the Gambia Government Cloud environment
		Stakeholders
		► MoFEA ► Principal Government Cloud Provider ► MoCDE
		Dependencies
		► Cloud Legal Methodology basis
		Risks
		► Resistance to change

Refer to Annexure 2 – Cloud financing paradigms

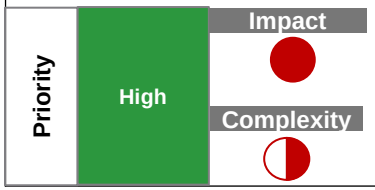
Keys *Low complexity/ impact* *Medium complexity/ impact* *High complexity/ impact*

Detailed Charter – Redefinition of Procurement and vendor/contract management

Cloud Governance and Trust

Initiative Owner	Principal Government Cloud provider	**Start date**	1 November 2024	**Duration**	12 months

Initiative	**Activity**	**Deliverables**
Redefinition of procurement and vendor/contract management	**Procurement** ► Modify the procurement management processes to enable GoTG institutions source Cloud services from the Cloud marketplace in line with Government Cloud policy ► Define Cloud vendor due diligence process ► Develop Cloud vendor certification requirement ► Develop a Cloud vendor evaluation framework **Vendor / Contract Management** ► Develop or identify procedures that will need to be enhanced for contract and vendor management including: • SLA monitoring • Contract management • Financial management of vendors • Vendor performance and compliance monitoring ► Development of guidance for GoTG agencies to implement or update their policies and procedures to reflect the move to the Government Cloud environment .	► Redefined procurement and contract management process ► Cloud vendor certification requirements document ► Cloud vendor due diligence guidance ► Cloud vendor evaluation framework
Objectives		**KPIs**
► To establish a streamlined procurement and contract management process that maximizes cost savings, efficiency, and effectiveness. ► To increase transparency and accountability in the procurement and contract management process.		► Level of compliance ► Leadtime for procurement and contracting processes
		Stakeholders
		► MoCDE ► Principal Government Cloud Services provider ► Public Procurement Authority
		Dependencies
		► Adoption of Government Cloud Policy ► Development of a Cloud Legal Methodology basis
		Risks
		► Resistance to change



Keys *Low complexity/ impact* *Medium complexity/ impact* *High complexity/ impact*

Detailed Charter – Establishment of Compliance and certification framework

Cloud Governance and Trust

Initiative Owner	Principal Government Cloud Provider	**Start date**	1 February 2025	**Duration**	12 months
Initiative	**Activity**				**Deliverables**
Establishment of compliance and certification framework	► Establish a framework for performing compliance and certification of vendors: • Define the scope of the certification framework with reference to the Government Cloud Policy • Identify key stakeholders who will be involved in the certification framework • Identify risks and threats associated with Government cloud services • Develop compliance requirements. These should be aligned with relevant standards and regulations • Define certification criteria based on compliance requirements • Develop a certification process aligned with the Government Cloud Policy. This should include application and assessment processes • Ensure the Principal Government Cloud Service Provider has the competence to oversee the certification process including accreditation of auditors and the issuance of certification. • Test and refine the certification framework				► Compliance and certification framework
Objectives					**KPIs**
► To ensure GoTG has access to Government Cloud services that meet their specific needs and requirement ► Establish a standardised process for evaluating risk and also reaping the benefits of Government Cloud services					► Level of compliance ► # of security incidence
					Stakeholders
					► Principal Government Cloud services provider ► MoCDE
					Dependencies
					► Government Cloud Risk Assessment ► Adoption of Government Cloud Policy
					Risks
					► Inadequate Coverage ► Interpretation and Consistency

Priority High — **Impact** ● **Complexity** ●

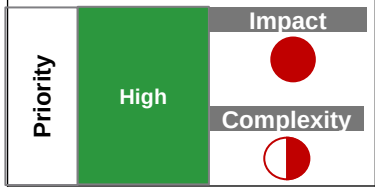
Keys ◔ *Low complexity/ impact* ◑ *Medium complexity/ impact* ● *High complexity/ impact*

Detailed Charter – Certification of Principal Government Cloud provider

Cloud Governance and Trust

Initiative Owner	MoCDE	**Start date**	1 June 2025	**Duration**	12 months

Initiative	**Activity**	**Deliverables**
Certification of Principal Government Cloud Service Provider	► Identify certification requirements specified by the relevant certification framework or program (e.g. CSA STAR Certification (Cloud Security Alliance Security Trust Assurance and Risk), ISO/IEC 27001: ISO/IEC 27001 , SOC 2 (Service Organization Control 2) and CIS (Centre for Internet Security) Benchmarks ► Prepare necessary documentation to demonstrate compliance with the certification requirements. ► Conduct a self-assessment to evaluate the cloud authority's readiness for certification. ► Engage an accredited assessor to ► Perform an on-site assessment by assessor ► Issue certification ► Establish a programme for ongoing compliance and audits	► Certification of the Principal Government Cloud Service Provider
Objectives		**KPIs**
► To provide the Principal Government Cloud Service Provider with the identity and credibility required to operate as an IT services organisation		► 100% of required certifications obtained
		Stakeholders
		► Principal Government Cloud Services Provider ► MoCDE
		Dependencies
		► Government Cloud Risk Assessment ► Endorsement of Government Cloud Policy ► Establishment of the Government Cloud Authority / Principal Government Cloud provider
		Risks
		► Limited Scope of Certification



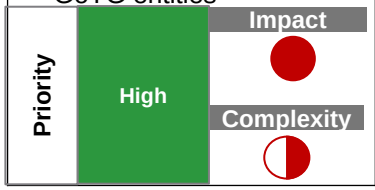
Keys *Low complexity/ impact* *Medium complexity/ impact* *High complexity/ impact*

Detailed Charter – Establishment of Centre of Expertise (CoE)

Cloud Governance and Trust

Initiative Owner	Principal Government Cloud Provider	**Start date**	1 September 2025	**Duration**	24 months

Initiative	**Activity**	**Deliverables**
Establishment of Centre of Expertise (CoE)	► Define the purpose, scope, and expected outcomes of the CoE, aligning them with the GoTGs Government Cloud strategy and policy goals. ► Conduct stakeholder analysis covering IT departments and cloud service providers to understand needs and expectations regarding the Gambia Government Cloud adoption and develop a stakeholder engagement plan. ► Define the structure, roles, and responsibilities of the CoE. Determine the decision-making processes, reporting lines, and coordination mechanisms within the CoE and with external stakeholders. ► Define the role of the private sector ► Identify the required expertise and skills for the CoE team. Minimum skills and certification requirements has been presented as Annexure 3. Consider the need for a mix of internal resources from GoTG institutions and external consultants or advisors. ► Determine the services and support the CoE will provide to government institutions. ► Establish collaboration mechanisms that foster collaboration and networking among GoTG institutions, cloud service providers, and other stakeholders. ► Develop a knowledge base and training programs ► Implement pilots to validate the CoE's approach, demonstrate value, and gather feedback. Collaborate with selected institutions (first cloud candidates) to transition to cloud, leveraging the CoE's expertise and support. ► Launch awareness campaigns and communication initiatives to promote the CoE's services, benefits, and success stories.	► Centre of Expertise established ► Training programs for Centre of Expertise team members developed and implemented
Objectives		**KPIs**
► Creation of a central cloud knowledge hub to guide, support, and provide best practices to GoTG institutions regarding the implementation and utilization of cloud technologies. ► Centralization of cloud-related expertise, streamline processes, and foster a culture of collaboration and knowledge sharing among GoTG entities		► # of government agencies and ministries supported by the CoE
		Stakeholders
		► Principal Government Cloud services provider ► GoTG Institutions ► Private sector subject matter experts ► MoCDE
		Dependencies
		► Establishment of the Principal Government Cloud provider ► Access to skilled personnel ► Resource allocation
		Risks
		► Availability of required skills



Detailed Charter – Establishment of Cloud alternative assessment guidelines

Cloud Adoption

Initiative Owner	MoCDE	**Start date**	1 November 2023	**Duration**	6 Months
Initiative	**Activity**				**Deliverables**
Establishment of Cloud alternative assessment guidelines	▸ Conduct an assessment of GoTG institutions to understand the needs, workloads, data sensitivity, unique operational requirements, security considerations, compliance obligations, and budget constraints . This analysis will help identify scenarios where alternative cloud approaches may be more suitable. ▸ Define guidelines to support institutions in assessing Cloud alternatives for their asset portfolio including cost, benefits and risk analysis ▸ Develop decision pathways for identifying the most appropriate service delivery model and deployment model for an asset in line with Government Cloud policy ▸ Leverage cost models developed under the financial management processes to provide tools for GoTG institutions to undertake the assessments ▸ Develop guidelines to review the implications of contracts for current IT assets that could be considered for Cloud adoption ▸ Conduct pilots to validate the feasibility and effectiveness of the cloud alternative guidelines. ▸ Develop a communication plan to raise awareness and disseminate the cloud alternative guidelines to GoTG agencies. ▸ Establish a mechanism for monitoring the adoption and effectiveness of the cloud alternative guidelines. Refer to Annexure 4 for a sample decision framework				▸ Cloud alternative assessment guidelines
Objectives					**KPIs**
▸ Establishment of guidelines to provide flexibility and options for GoTG institutions to choose the most suitable cloud deployment models based on their specific needs and requirements					▸ # of successful adoptions
					Stakeholders
					▸ MoCDE ▸ Principal Government Cloud provider
					Dependencies
					▸ Costing models
					Risks
Priority Medium — **Impact**  **Complexity** 					

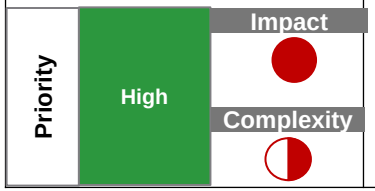
Keys  *Low complexity/ impact*  *Medium complexity/ impact*  *High complexity/ impact*

Detailed Charter – Alignment of current cloud assets to policy

Cloud Adoption

Initiative Owner	Principal Government Cloud provider	**Start date**	1 October 2024	**Duration**	12 Months

Initiative	**Activity**	**Deliverables**
Alignment current cloud assets to policy	► Provide training and awareness programs to educate GoTG institutions about the Gambia Government Cloud policy and the changes they need to make to align their cloud assets ► Issue a directive for GoTG institutions to align their current cloud assets to the Gambia Government Cloud policy. The directive must include timelines ► The CoE can provide guidance and also assist institutions with gap analysis, remediation planning, migration and integration planning, workforce reconfiguration and change management plans as part of the policy adoption at the institutional level. ► Establish monitoring mechanisms to track and evaluate the ongoing compliance of the cloud assets with the government cloud policy. This includes implementing monitoring tools, defining key performance indicators (KPIs), conducting regular audits, and establishing governance processes to ensure ongoing adherence to the policy	► Ongoing compliance monitoring and reporting guidelines for policy compliance developed
Objectives		**KPIs**
► To maximize the benefits of Gambia Government Cloud adoption while mitigating potential risks and ensuring compliance with relevant regulations and standards		► Rate of compliance
		Stakeholders
		► MoCDE ► Principal Government Cloud
		Dependencies
		► Endorsement of Government Cloud Policy and related regulations ► Development of legal methodology basis ► Establishment of the CoE
		Risks
		► Funding. ► Lack of skilled personnel



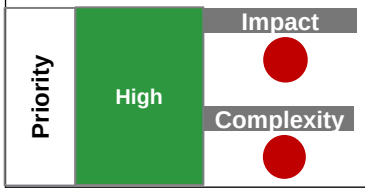
Keys *Low complexity/ impact* *Medium complexity/ impact* *High complexity/ impact*

Detailed Charter – Consolidation of infrastructure and repositioning of Gamtel as a resident private Government Cloud provider

Cloud Adoption

Initiative Owner	Principal Government Cloud provider	**Start date**	1 December 2024	**Duration**	12 months

Initiative	**Activity**	**Deliverables**
Consolidation of infrastructure and repositioning of Gamtel as a resident private Government Cloud provider	► Determine the baseline: Take stock of the current cloud assets within the GoTG ecosystem. This includes cloud services, applications, and infrastructure components being used. ► Identify new key IT projects. All IT projects are required to evaluate cloud options as part of the business case submission for funding. ► Determine demand requirements for HVIAs and key projects ► Assess the implications of positioning Gamtel as a resident cloud service provider leveraging the tier 3 data centre ► Assess the capacity of Gamtel's current portfolio ► Identify IT infrastructure whose custody and administration should be ceded to government cloud infrastructure operator in line with the Government Cloud strategy and Policy. ► Decide on the need to procure additional cloud infrastructure for Gamtel's operation (e.g. upgrade of the national data centre to tier 4) ► Gamtel to go through a certification process in line with the Gambia Government Cloud policy ► Execute MoUs to govern the arrangement between government cloud infrastructure operator and the institutions whose infrastructure has been transferred ► Assess the needs of Gamtel specific to cloud service delivery and develop a strategy and roadmap to transform it into a results-oriented service delivery organisation	► Cloud assets register ► Draft MoUs ► Transformation strategy and roadmap for Gamtel
Objectives		**KPIs**
► To rationalise and optimise the use of existing infrastructure ► Position Gamtel as a major resident cloud service provider ► Cost efficiency		► Certification of Gamtel as a Government CSP
		Stakeholders
		► MoCDE ► Principal Government Cloud Service Provider ► Gamtel
		Dependencies
		► Endorsement of Government Cloud Policy and related regulations ► Development of legal methodology basis
		Risks
		► Funding ► Resistance to change



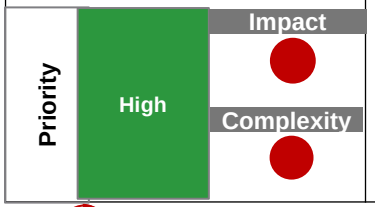
Keys: Low complexity/ impact; Medium complexity/ impact; High complexity/ impact

Detailed Charter – Establishment of a Cloud Digital Market place with new procurement rules in effect

Cloud Adoption

Initiative Owner	Principal Government Cloud Provider	**Start date**	1 September 2025	**Duration**	30 months

Initiative	**Activity**	**Deliverables**
Establishment of a Cloud Digital Market place	► Identify all key stakeholders to gather input and ensure involvement throughout the set up process ► Establish a framework for undertaking cloud vendor evaluation in line with the Government Cloud policy. This should consider identifying evaluation criteria for cloud vendor selection, include the minimum risk and compliance requirements per the Gambia Government Cloud policy ► Conduct market research and evaluate potential cloud service providers that can participate in the cloud marketplace. Consider factors such as their capabilities, security measures, compliance certifications, pricing models, and track record in serving government clients. Create a shortlist of qualified providers that align with the GoTG Government Cloud requirements ► Establish a governance and compliance framework for the cloud marketplace in-line with the Government Cloud policy ► Develop technical infrastructure required to support the marketplace. This would involve the following: ◦ Setting up a centralised / one-stop-shop digital services delivery platform or portal where GoTG institutions can browse, compare and select cloud services. ◦ The design of the interface and experience of the marketplace must be intuitive and user-friendly. Users should easily discover, evaluate, and procure the available cloud services. It must provide relevant information, documentation, and support resources to assist users in their decision-making and adoption processes. ◦ The platform should be capable of being accessed from multiple devices. ◦ Development of an integration mechanism(s) to connect with the CSPs APIs or platforms. Factors such as scalability, performance and security must be considered in the design of the infrastructure ◦ Establishment of an appropriate helpdesk and support framework ► Vendor Onboarding and Integration: Collaborate with Gamtel and the selected CSPs to onboard them onto the cloud marketplace. Establish master services agreements, and SLAs with the providers to outline the terms of their participation. Integrate the providers' services into the marketplace's technical infrastructure, ensuring seamless provisioning, management, and billing processes. ► Testing and Quality Assurance: Perform thorough testing and quality assurance of the cloud marketplace platform. Identify and address any issues or bugs before launching the marketplace. ► Provide training and support to GoTG institutions to promote the adoption of the cloud marketplace. Offer training programs, webinars, and documentation to familiarize users with the marketplace's features, security practices, and procurement processes. Address any concerns or questions from users and ensure their comfort and confidence in using the cloud marketplace. ► Launch the cloud marketplace and communicate its availability. ► Monitor the usage and adoption rates, gather user feedback, and make continuous improvements based on the feedback received.	► Cloud digital marketplace with supporting platform
Objectives		**KPIs**
► Offer cloud services to GoTG institutions as a utility ► To establish a one-stop-shop where GoTG institutions can compare and procure cloud services. ► Deployment of a digital service delivery platform to enable the delivery of cloud services		► Adoption rates ► Onboarding of at least 3 CSPs
		Stakeholders
		► MoCDE ► Principal Government Cloud Service Provider ► CSPs ► Gamtel
		Dependencies
		Risks
		► Funding ► Insufficient Evaluation Criteria



Keys *Low complexity/ impact* *Medium complexity/ impact* *High complexity/ impact*

Detailed Charter – Establishment of Lifecycle methodology

Cloud transition and migration

Initiative Owner	MoCDE	**Start date**	1 November 2024	**Duration**	12 months
Initiative	**Activity**				**Deliverables**
Establish Lifecycle methodology	► Define the scope of the lifecycle methodology ► Engage key stakeholders to gather their insights, feedback, and requirements to ensure their involvement and buy-in for the lifecycle methodology development. ► Develop a framework for the lifecycle methodology that outlines the key phases, activities, and milestones. Define the sequence of steps involved in the adoption process, such as assessment and planning, migration and deployment, testing and validation, operations and maintenance, continuous improvement and decommissioning. Map out the dependencies and interactions between each phase. ► Create templates, documentation, and guidelines to support the adoption process. ► Integrate security and compliance measures throughout the lifecycle methodology. ► Conduct a pilot implementation of the lifecycle methodology with a first cloud candidate(s) ► Develop training programs and support materials to educate government staff on the lifecycle methodology.				► Framework for lifecycle methodology
Objectives					**KPIs**
► To establish a structured and systematic approach to ensure successful planning, execution, and management of cloud adoption efforts of GoTG institutions. ► To mitigate risks, promote alignment with GoTGs objectives, and drive the realization of expected benefits from cloud technology.					► 100% success of pilot
					Stakeholders
					► MoCDE ► Principal Government Cloud provider
					Dependencies
					Risks
Priority: High; Impact; Complexity					.

Keys *Low complexity/ impact* *Medium complexity/ impact* *High complexity/ impact*

Detailed Charter - Identify First Cloud candidates

Cloud transition and migration

Initiative Owner	**Principal Government Cloud Provider**	**Start date**	**1 June 2025**	**Duration**	**6 months**
Initiative	**Activity**				**Deliverables**
First Cloud candidates identified	► Identify first IaaS model candidates that align well with the cloud environment. ► Use the Cloud Alternative guidelines as a basis to assess IT assets of candidate institutions. The priorities for assessing the assets should be taken from the Gambia Government Cloud strategy and Architecture principles, which defines the triggers for asset assessment (Refer to Annexure 4 for additional decision framework guidance) ► Develop a migration strategy that outlines the approach, timeline, and resources required for the migration process. Determine whether a lift-and-shift approach, where models are moved as-is to the cloud, or a re-architecting approach, where models are optimized for the cloud, is more appropriate. Consider any dependencies or integration requirements with existing systems ► Assess the resource requirements for the migration process, including cloud infrastructure, storage, compute resources, and network capacity ► Develop a migration roadmap for the first cloud candidate institutions identified				► Identification of model Cloud candidates
Objectives					**KPIs**
► Identification of first candidates for cloud migration to serve as a model cloud transition case studies.					► Identification of model Cloud candidate
					Stakeholders
					► MoCDE ► Principal Government Cloud provider ► Cloud Centre of Expertise ► Candidate institutions
					Dependencies
					Risks

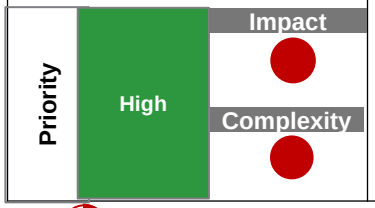
Priority	Impact	Complexity
Medium		

Keys  *Low complexity/ impact*  *Medium complexity/ impact*  *High complexity/ impact*

Detailed Charter – Migration of First cloud candidates / major institutions to IaaS

Cloud transition and migration

Initiative Owner	MoCDE	**Start date**	1 June 2026	**Duration**	24 months
Initiative	**Activity**				**Deliverables**
Migration of First cloud candidates / major institutions to IaaS **Objectives** ▸ Use candidate GoTG institutions as case studies in order to minimize the impact which would not be achieved if a 'big bang' change approach is utilized	*Phase 1:* ▸ Principal Government Cloud Provider nominates one major GoTG institution out of the first cloud candidates identified to serve as a case study and exemplary model institution of what GoTG institutions can expect to undergo ▸ Migrate majority of the infrastructure including non-production environments to IaaS offerings. ▸ Document all lessons learned *Phase 2:* ▸ Migrate remaining first cloud candidates' infrastructure, including non-production environments to IaaS offering where the best value for money and acceptable risk are met ▸ Decommission legacy infrastructure Refer to Annexure 5 – Refer to Annexure 5 for Cloud Security and Privacy consideration				▸ Transition of all first cloud candidates **KPIs** ▸ 80%+ infrastructure of first cloud candidates migrated to IaaS **Stakeholders** ▸ MoCDE ▸ Principal Government Cloud Service Provider ▸ Cloud Centre of Expertise ▸ First cloud candidates **Dependencies** ▸ Cloud Digital Marketplace established **Risks** ▸ Appropriate change management ▸ Finance ▸ Interoperability Challenges ▸ Other technical challenges (data loss, service disruptions, or extended downtime)



Keys Low complexity/ impact | Medium complexity/ impact | High complexity/ impact

Detailed Charter – Migration of all candidate assets to Cloud

Cloud transition and migration

Initiative Owner	MoCDE	**Start date**	1 March 2027	**Duration**	48 Months
Initiative	**Activity**				**Deliverables**
Migration of all candidate assets to Cloud	► All candidate assets identified by agencies have transitioned to their selected Cloud service delivery model ► Legacy assets should be decommissioned				► All priority assets transitioned to cloud
Objectives					**KPIs**
► All candidate assets for transition to the cloud will be successfully migrated and tested, with end-users fully trained and able to effectively use the cloud-based assets.					► Number of candidate assets successfully transitioned to the cloud
					Stakeholders
					► MoCDE ► Principal Government Cloud provider ► Cloud Centre of Expertise ► GoTG institutions
					Dependencies
					► Digital Marketplace established and operational
					Risks
Priority: High Impact Complexity	Refer to Annexure 5 – Refer to Annexure 5 for Cloud Security and Privacy consideration				► Appropriate change management ► Finance ► Interoperability Challenges ► Technical challenges (data loss, service disruptions, or extended downtime)

Keys *Low complexity/ impact* *Medium complexity/ impact* *High complexity/ impact*

Detailed Charter – Establishment of Sponsorship

Cloud change management

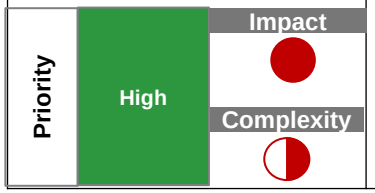
Initiative Owner	MoCDE	**Start date**	1 October 2023	**Duration**	6 months
Initiative	**Activity**				**Deliverables**
Establish of sponsorship	▸ Identify key sponsor from MoCDE for GoTG Government Cloud adoption and transition ▸ Identify key sponsors for each GoTG institutions				▸ Sponsors identified
Objectives					**KPIs**
▸ To establish influential individuals or entities within GoTG who can drive and support the adoption of cloud technologies at various levels ▸ To secure high-level support and guidance, mobilize resources, address concerns, and create a conducive environment for successful cloud adoption within GoTG					▸ Principal sponsor for the Government Cloud adoption programme identified ▸ All other sponsors identified
					Stakeholders
					▸ MoCDE
					Dependencies
					Risks
					▸ Lack of Executive Support ▸ Ambiguous Roles and Responsibilities

Keys *Low complexity/ impact* *Medium complexity/ impact* *High complexity/ impact*

Detailed Charter – Establishment of a Communication Plan

Cloud change management

Initiative Owner	MoCDE	**Start date**	1 November 2023	**Duration**	6 months
Initiative	**Activity**				**Deliverables**
Establishment of a communication plan	► Map out stakeholders ► Develop clear, consistent, and compelling messages about the benefits, objectives, and impact of the Gambia Government Cloud adoption. ► Determine the appropriate communication channels ► Establish a timeline for communication activities, considering key milestones and events related to the Gambia Government Cloud adoption process. ► Develop strategies to engage stakeholders throughout the cloud adoption journey. ► Address potential risks, concerns, and mitigations related to cloud adoption in the communication plan. ► Establish metrics and feedback mechanisms to assess the effectiveness of the communication plan.				► Communication plan
Objectives					**KPIs**
► To ensure effective communication, engagement, and collaboration among stakeholders, while building trust, managing expectations, and ensuring a successful transition to cloud with GoTG.					► Level of engagement and feedback from stakeholders
					Stakeholders
					► MoCDE ► Principal Government Cloud provider
					Dependencies
					Risks



Keys *Low complexity/ impact* *Medium complexity/ impact* *High complexity/ impact*

Detailed Charter – Establishment of metrics for performance and cost

Cloud change management

Initiative Owner	MoCDE	**Start date**	1 October 2024	**Duration**	6 Months
Initiative	**Activity**				**Deliverables**
Establish metrics for performance and cost	► Identify the key performance indicators (KPIs) that will be used to measure the performance and success of the Gambia Government Cloud adoption program ► Determine cost metrics (This may include metrics such as cost savings achieved measured by TCO, or RoI from the cloud initiative ► Establish baseline and targets ► Determine the data collection mechanisms and sources needed to track the identified metrics ► Engage with relevant stakeholders to ensure their understanding and involvement in the KPIs and cost metrics				► Key Performance Indicators
Objectives					**KPIs**
► To effectively monitor, measure, and evaluate the progress, success, and impact of the Gambia Government Cloud adoption initiative					**Stakeholders** ► MoCDE ► Principal Government Cloud provider
					Dependencies
					Risks ► Unavailability of baseline data

Priority High — Impact — Complexity

Keys Low complexity/ impact; Medium complexity/ impact; High complexity/ impact

Detailed Charter – Establishment of Training program

Cloud change management

Initiative Owner	MoCDE	**Start date**	1 March 2025	**Duration**	12 Months
Initiative	**Activity**				**Deliverables**
Establishment of training program	► Design a GoTG Government Cloud Workforce Development Framework. At a minimum the framework should cover competency models; capacity development programmes; certification programs; and assessment and evaluation tools ► Establish bi-lateral training partnerships with principal Government Cloud providers in other countries who are running similar models ► Establish training partnerships with private sector, including CSPs and consultants ► Sensitise and train GoTG institutions on the use of the Government Cloud Workforce Development framework ► Rollout training programmes				► Government Cloud Workforce Development framework
Objectives					**KPIs**
► To address specific skill gaps ► To equip GoTG workforce with the necessary knowledge, skills, and expertise to effectively plan, implement, and manage the cloud adoption programme ► To ensure that GoTG workforce have the capabilities required to leverage the full potential of cloud computing					► Endorsement of the Government Cloud workforce development framework ► # of capacity development partnerships established
					Stakeholders
					► MoCDE ► Principal Government Cloud provider ► Cloud Centre of Expertise
					Dependencies
					Risks
	Refer to Annexure 3 for standard list of skills and certifications required for the Gambia Government Cloud adoption				► Funding ► Resistance to Change

Priority **High** **Impact** **Complexity**

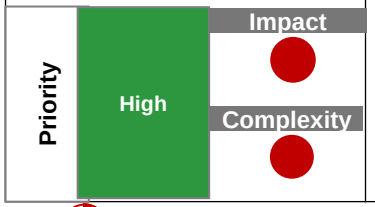
Keys *Low complexity/ impact* *Medium complexity/ impact* *High complexity/ impact*

Detailed Charter – Workforce reconfiguration

Cloud change management

Initiative Owner	MoCDE	**Start date**	1 April 2026	**Duration**	12 months

Initiative	**Activity**	**Deliverables**
Workforce reconfiguration	▸ Government institutions to conduct cloud skills gap assessments (using the competency models and skills assessment tools in the Government Cloud Workforce Development Framework) ▸ Government institutions to conduct change impact assessment as part of migration strategies ▸ Government institutions to develop Change Management plans and resourcing strategies ▸ Government institutions to rollout the required workforce changes in line with the Government Cloud Policy	▸ Skills gap reports ▸ Change management plan
Objectives		**KPIs**
▸ Reconfigure the workforce to align with the Government Cloud implementation project objectives, reduce skill gaps, eliminate redundancies, and improve efficiency and effectiveness.		▸ Reduction in skill gaps ▸ Improvement in workforce efficiency and effectiveness
		Stakeholders
		▸ MoCDE ▸ Principal Government Cloud provider ▸ Candidate institutions
		Dependencies
		▸ Gambia Government Cloud Workforce Development Framework
		Risks
		▸ Resistance to change ▸ Workforce morale and job satisfaction ▸ Disruption in team dynamics and collaboration



Keys *Low complexity/ impact* *Medium complexity/ impact* *High complexity/ impact*

06

Annexures

Annexure 1 – Establishment of Gambia Government Cloud Regulatory Environment: Regulatory Considerations

Annexure- 1: Regulatory Considerations (1/2)

*General provision with reference to sub-statutory legal act which provides the methodology document or guidelines and examples/ templates/ more detailed description.

No	Legal Considerations	Implementation Structure
1	Establish or share IT services and Cloud services definition legislative regulation.	*Legislative Regulation
2	Establish shared IT services (e.g. Colocation) and Cloud services classification (e.g. IaaS, PaaS, SaaS)	*Legislative Regulation
3	Establish Cloud services provision model definition, private sector and state owned cloud services providers or only one of them.	*Legislative Regulation
4	Establish mandatory or optional usage of cloud services Legislative Regulation	*Legislative Regulation
5	Identify prerequisites, which are to be met, in order for the state owned cloud services provider and private sector cloud services providers to be allowed to provide the cloud services with reference to the more detailed policy with the requirements.	*Legislative Regulation
6	Obligations to have the SLA for cloud services defined with the reference to the methodology / guidelines / templates of SLA definition.	*Legislative Regulation
7	Mission critical Information System (High Value Information Asset -HVIA) definition and mission critical Information System classification together with the reference to the methodology of mission critical IS identification and classification (e.g. based on the impact level if the data confidentiality, availability or integrity would be affected)	*Legislative Regulation
8	Establish the principles of financing of state owned cloud services provider(s) and their activity of cloud services provision together with the reference to the methodology of cloud services costing and chargeback.	*Legislative Regulation
9	Establish State owned cloud services provider's services pricing principles, if institutions would be paying for the cloud services, together with the reference to the methodology of cloud services pricing.	*Legislative Regulation
10	Establish State owned cloud services providers' governance model and principles together with the reference to a more detailed description of the State owned cloud services providers' governance model.	*Legislative Regulation
11	Establish the procurement principles of Cloud services (centralized, decentralized) and institutions responsible for centralized procurements, etc.) with the reference to policy of cloud services procurement.	*Legislative Regulation

Annexure- 1: Regulatory Considerations (2/2)

No	Legal Considerations	Implementation Structure
12	Document requirements for state owned cloud services providers operations (e.g. responsibilities matrix (split of responsibilities between the state owned cloud services providers and institutions, who would be using the services, per type of the cloud services, services demand management / IT resources planning and etc.)	Institutional standards and guidelines
13	Document methodology and guidelines with templates for SLA definition of cloud services used by public sector institutions.	Institutional standards and guidelines
14	Document methodology/ policy for mission critical IS identification and classification	Institutional standards and guidelines
15	Document requirements for Cloud services providers' (including state owned cloud services providers and private sector cloud services providers) Data centers facilities	Institutional standards and guidelines
16	Document methodology/ policy of cloud services, which are provided by state owned cloud services providers, costing and chargeback.	Institutional standards and guidelines
17	Document methodology/ policy for cloud services, which are provided by state owned cloud services providers, pricing, if the institutions are to pay for the cloud services provided by the state owned cloud services providers.	Institutional standards and guidelines
18	Document State owned cloud services providers' governance model and governance policy	Institutional standards and guidelines
19	Document policy for cloud services procurement (centralized, decentralized) and institutions responsible for centralized procurements, etc.)	Institutional standards and guidelines
20	Document methodology for state information resources infrastructure migration to the cloud, including the description of approach and detailed activities	Institutional standards and guidelines
21	Identify priority state information resources, which infrastructure should firstly be moved to Government Cloud .	Institutional standards and guidelines

Annexure 2 – Cloud Financing Paradigms

Annexure- 2: Cloud Financing Paradigms (1/2)

Cloud Financing Option	Alternative A	Alternative B
Cloud Financing Model	Model where institutions are not paying for the cloud services provided by Government Cloud services providers.	Model where institutions are paying for the cloud services provided by Government Cloud services providers.
Calculation and control of compensation overpayment as government support	Considerations to calculate exact value of compensation needed to cover expenses of state-owned Government Cloud service providers and execute efficient control of compensation overpayment methods.	Payments for state-owned Government Cloud services providers are done by many different cloud services recipients, calculation of payable compensation may be more complicated with this method.
Encouragement of rational use of provided cloud services	The irrational use of cloud services by recipients may occur because the budgeting and acquisition of services are done by state-owned Government Cloud service providers. Optimisation of service acquisition cost may not be a priority to service recipients.	The rational use of cloud services are encouraged because the institutions pay directly for cloud services, they therefore use them more rationally, because they need to get annual budget setup and approved for cloud services.
Cloud services acquisition opportunities	Exploitation of cloud service acquisition opportunities by services recipient are not hampered. This is because service acquisition does not depend on pre-planned limited resources but on real business needs such as on demand computing.	Cloud services acquisition opportunities of cloud services recipient depends on the organisations pre-planned limited resources.
Cloud services administrative burden	Cloud services administration burden and costs are lower. This is because there is no need to conclude agreements with cloud service recipients, invoice clients and manage payments.	Cloud services administrative burden are higher due to the need to conclude agreements with each single cloud services recipient, invoice clients individually and manage payments.
Opportunities of applying flexible software licensing	Better preconditions exist to treat state-owned Government Cloud service providers. Services provision to institutions categorised as a single economic entity in the public sector is less cumbersome. Thus, according to global licensing practices, it creates opportunities to apply more flexible software licensing conditions for acquired software services.	Opportunities for applying more flexible software licensing conditions for acquired software would be cumbersome as the fact of paying for provided cloud services occurs. Most software providers treat it as a commercial practice of providing cloud services.

Annexure- 2: Cloud Financing Paradigms (2/2)

Cloud Financing Option	Alternative A	Alternative B
Complexity of implementation	Relatively easier to implement as compared to the model where each cloud services recipient needs to pay for cloud services. This requires fewer changes in legal environment and less additional methodical and technical tools.	Relatively more difficult to implement as compared to other models when all cloud services provision costs are covered centrally. In this case more changes in legal environment and additional methodical and technical tools would be needed.
Assumptions of increasing performance efficiency of IT services recipients and reducing administrative burden of citizens and economic entities	Conditions exist to increase performance efficiency of cloud service recipients and reduce administrative burden of citizens and economic entities. Institutions would not be financially restricted to use cloud services as much as they need to achieve these goals.	Conditions to increase performance efficiency of cloud services recipients and reduce administrative burden of citizens and economic entities are not created as institutions have to pay for cloud services if they want to computerize processes or services and thus they have to budget more resources for cloud services acquisition. Ensuring the needed budget is often complicated due to the established practice of public finances planning
Risk of politicizing operating activities	Higher risk of politicizing activities, because obtaining financial resources for operating activities is in most cases dependent on political decisions that are not always optimal from financial, economic and administrative perspectives.	Lower risk of politicizing activities, because obtaining financial resources for operating activities depends more on factual financial needs of institutions than on centralized political decisions.
Cloud users' satisfaction due to financial terms of cloud services provision	Higher satisfaction of institutions due to financial terms of cloud services provision is expected as institutions would not have to share additional costs due to insufficient use of state owned IT infrastructure of Government Cloud services providers.	Lower satisfaction of institutions due to financial terms of cloud services provision is expected as institutions would have to share additional costs due to insufficient use of IT infrastructure of Government Cloud services providers owned by the state or the definition of a more complex model for justifying costs.

Annexure 3 – Required Skills for Cloud Adoption

Annexure- 3: Key skills required for cloud adoption (1/2)

While embarking upon cloud journey it is critical to gain related understanding on respective domain. The table below lists the minimum key skills required for the different teams across the Principal Government Cloud provider and GoTG IT teams to be successful in cloud adoption. It does not consider current state cloud skills maturity of existing IT teams.

Role	Required Understanding/ Learning
IT Senior Management Team	• Establish and agree on a common understanding on Cloud Fundamentals, Trends, Futuristic Technology, Pros and Cons of Cloud Computing, Business and IT Benefits of adoption cloud
Data Center Management	• Common understanding of different cloud deployment models e.g. Public, Private, Hybrid and related considerations • Skills upgrade to cover implementation, management and maintenance of DC components (e.g. IT Infrastructure) in hybrid cloud environment • Common understanding on Cloud Interoperability
Network management	• Understanding on implementing, monitoring and managing network configuration and consumption in hybrid cloud environment (for example, Configuring Virtual Private Network on Cloud) • Understanding of Software Defined Network and hands on expertise
Security Operations / Quality Assurance	• Understand IT security considerations in hybrid cloud environment • Capability to review security measures taken on-premises and also Cloud Provider's end • Capability to interpret / understand Cloud Service Provider Audit Reports and correlate / identify potential risks related to services availed from GoTG institutions • Understand the key quality parameters applicable in hybrid cloud environment and define KPI accordingly to achieve high quality
Service Continuity and DR	• Understand Service Continuity and DR perspective in Hybrid Cloud environment e.g. Review / revise existing RPO/ RTO, understand DRaaS model
Business Analyst & System Analyst	• Capability to map the requirement to related cloud services
App Design & Dev. Teams	• Understand cloud Platform as a Service model • Build understanding on DevOps tools and methodology
DB Design & Administration	• Gain related understanding on DB Cloud Administration
Helpdesk Support (including End User Support)	• Gain understanding on support model, methodology and procedure of Cloud Service Provider • Lean ITSM practices based on leading standards e.g. ITIL, COBIT etc.
Procurement Management	• Gain understanding on cloud pricing and billing model • Gain understanding on cloud accounts management • Gain understanding on provision cycle/period of cloud services • Gain understanding on cloud services contract model

Annexure 3- Key skills required for cloud adoption (2/2)

Competencies of the existing team on topics related to Cloud can be further enhanced through the following certifications across basic, advanced and specialized levels

Basic level Certification
To gain fundamental understanding and knowledge about Cloud Computing and related services

- CompTIA "Cloud Essentials"
- EXIN "Cloud Computing Foundation"
- Arcitura's "Certified Cloud Professional (CCP)"
- Cloud That's "Fundamentals of Cloud Computing Certification (Level 1)"

Advance level Certifications
The certification that demonstrate individual's knowledge about Cloud Provisioning and Administration, Cloud Bursting, Cloud Interoperability, Strategic Policy Design for Cloud Usage and Compliance, Disaster Recovery and Business Continuity Strategies for the Cloud, as well as Performance Measurement and Monitoring

Cloud Credential Council's
- Professional Cloud Administrator
- Professional Cloud Security Manager
- Professional Cloud Service Manager
- Professional Cloud Solutions Architect
- CompTIA Cloud+

Arcitura's
- Certified Cloud Technology Professional
- Certified Cloud Architect
- Certified Cloud Security Specialist
- Certified Cloud Governance Specialist
- CSA's Certificate of Cloud Security Knowledge (CCSK)

Technology/ Platform Specific Certifications
To gain understanding/experience on your cloud service provider specific certificates

- Microsoft Azure Fundamentals
- Architecting Microsoft Azure Solutions
- AWS Certified Solutions Architect
- Oracle Certified Master, Database Cloud Administrator
- Oracle Certified Professional, Database Cloud Administrator
- ORGANIZATION Certified Solution Architect – Cloud Computing Infrastructure

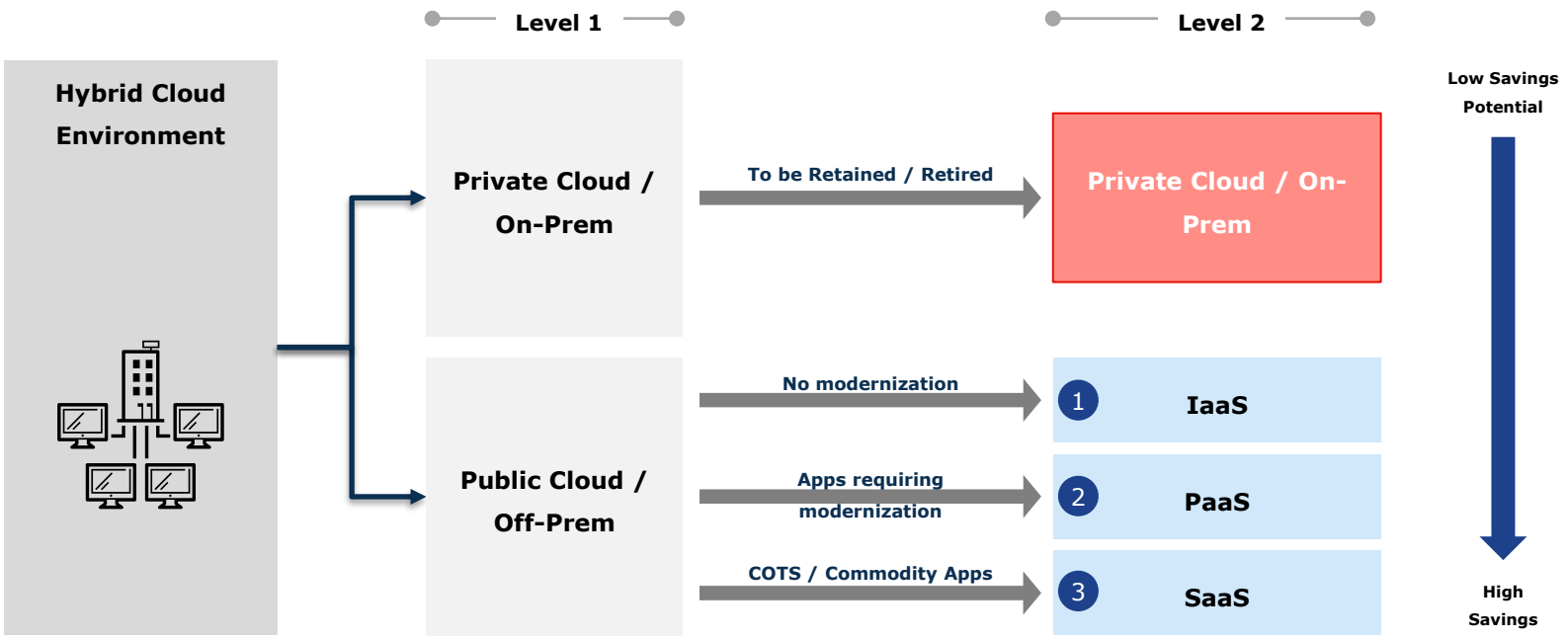
**Given Certification list is not exhaustive*
**Source: http://itcertificationmaster.com/it-certifications/cloud-certifications/*

Annexure 4 – Decision framework for Migration based on service, technical and cloud suitability parameters

Annexure- 4: Decision framework for Migration/ Modernization based on service, technical and cloud suitability parameters

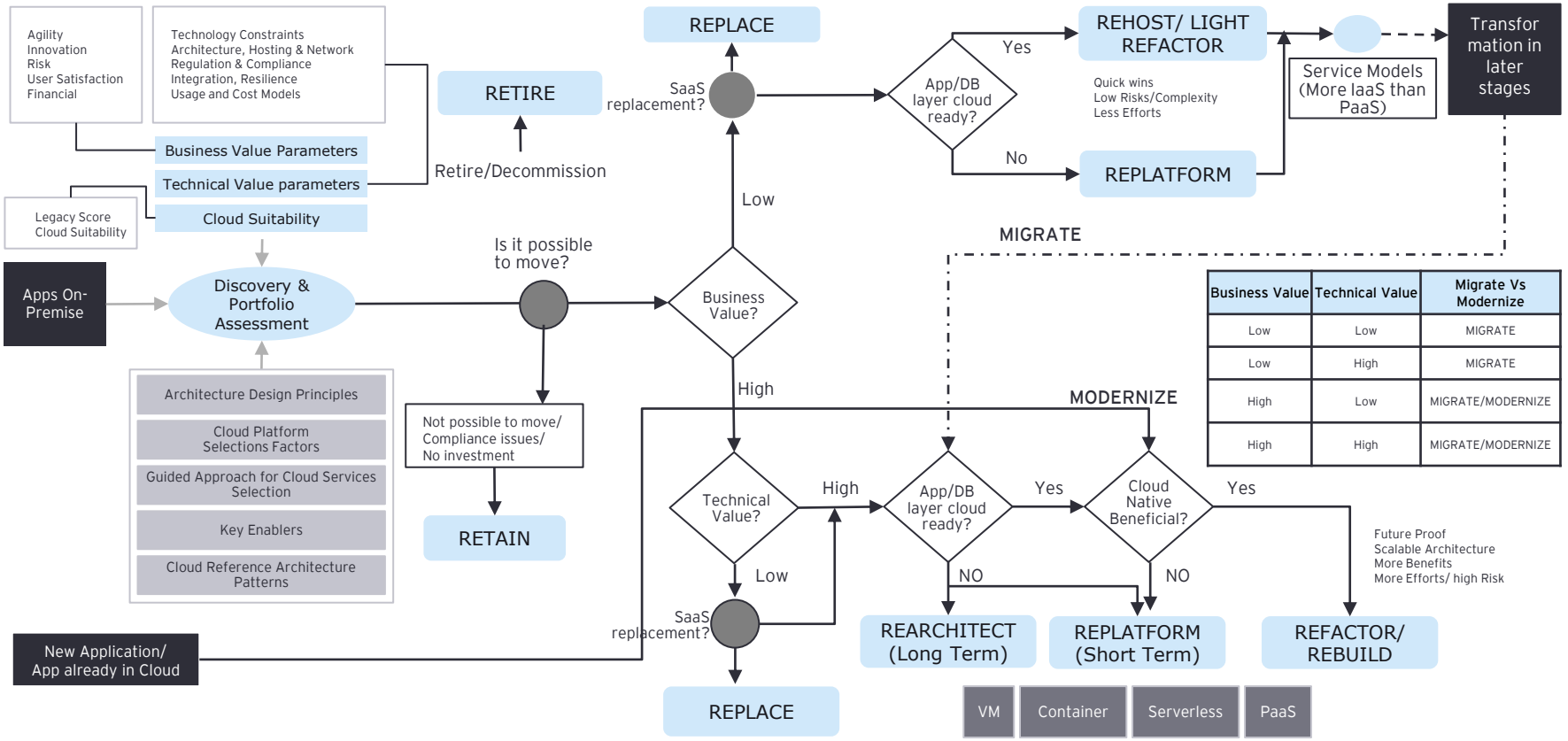
Based on Gambia's Government Cloud Strategic Proposition, different cloud service models and deployment will be required for varied considerations – data classification, security amongst other cloud policies.

The migration plan is therefore based on the notion of a hybrid cloud at least in the interim period – with few applications staying on premise and few others eligible for migration to cloud. Aligned to leading practice, the optimal strategy from a cost point of view is to leverage IaaS option wherever possible, and if there is sufficient time, explore PaaS and SaaS options.



Decision framework for Migration/Modernization based on service, technical and cloud suitability parameters

The decision framework aims to provide GoTG institutions with a step-by-step guide to help them make informed decisions about their cloud migration. The framework presents a decision-making criteria based on institutional needs, technical requirements, security, compliance, and costs

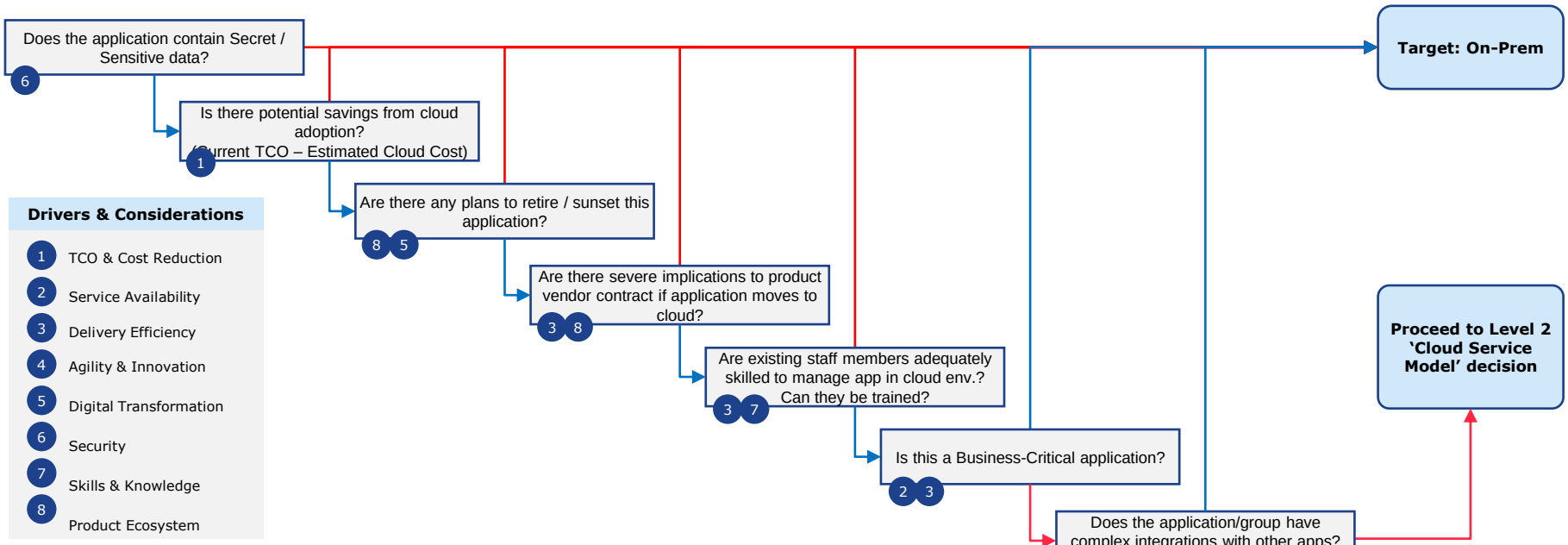


Deciding Cloud Deployment / Service Model for GoTG institutions (1/4)

Level 1: Decision Framework

The cloud decision framework is defined based on the optimal migration strategy / approach for the Government of The Gambia and is summarized below and covers two major levels of decisions – (1) Level 1: 'Cloud Deployment Model' and (2) Level 2: 'Cloud Service Model'

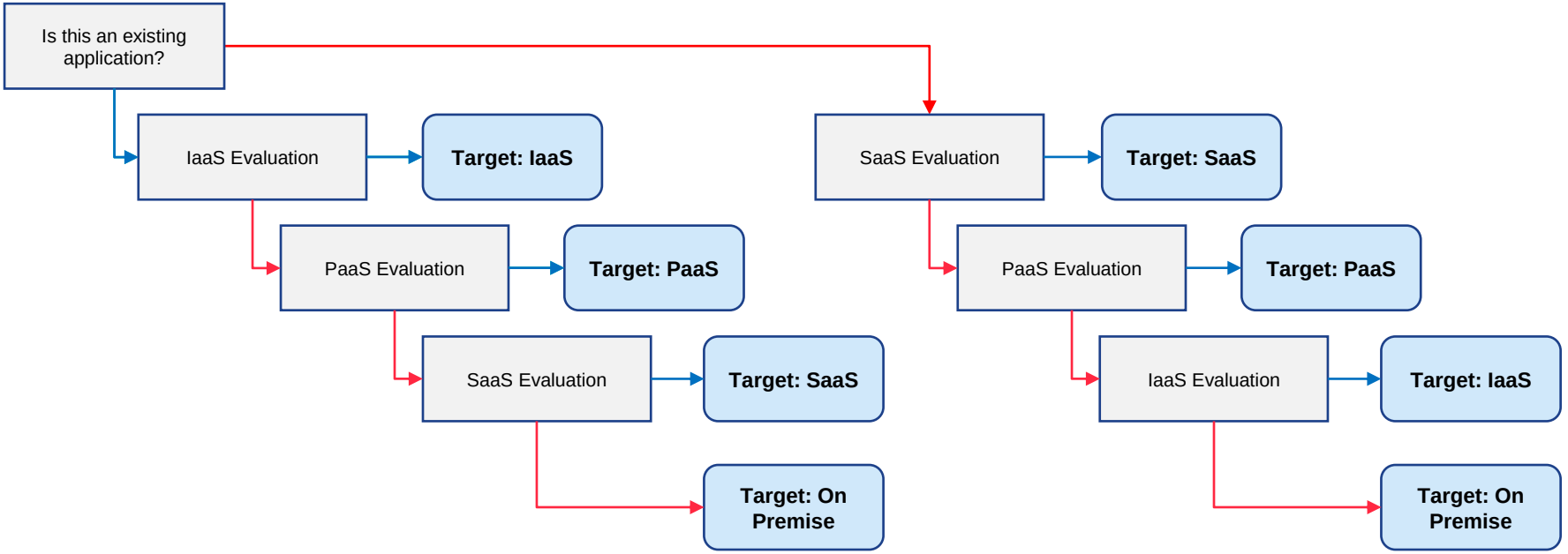
Level 1: Cloud Deployment Model



Note: Evaluated at Technology Band level where data is unavailable (high level analysis of sample applications representative of the band)

Deciding Cloud Deployment / Service Model for GoTG institutions (2/4)

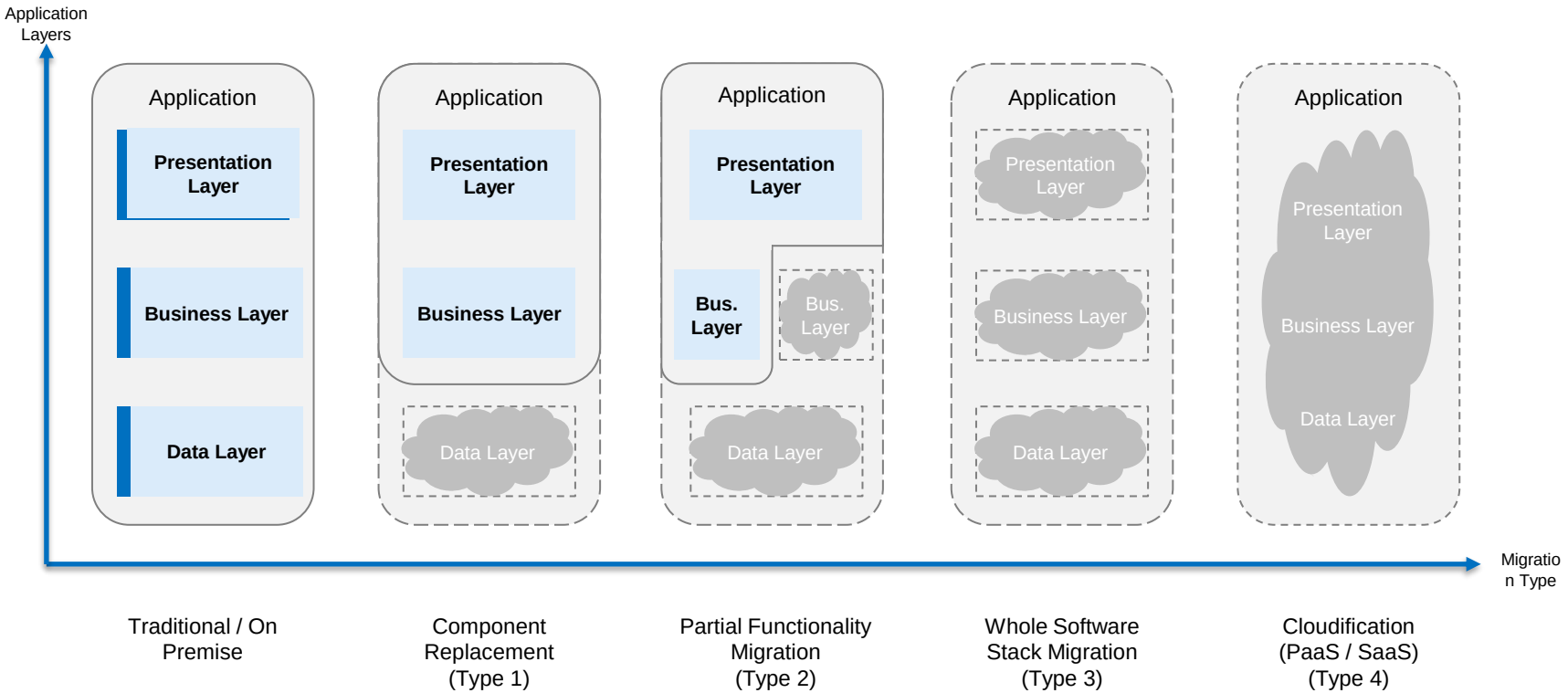
Level 2: Decision Framework (Cloud Service Model)



Note: Evaluated at Technology Band or Application level, as feasible

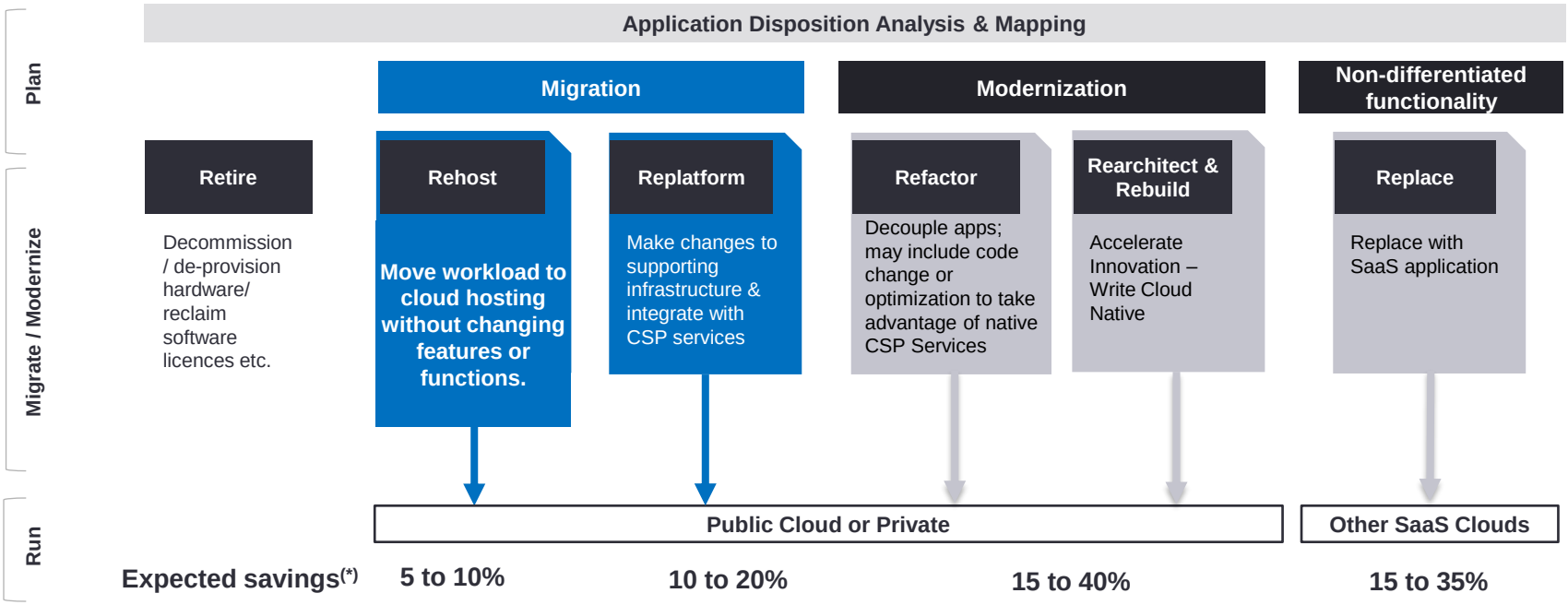
Deciding Cloud Deployment / Service Model for GoTG institutions (3/4)

The below outlines Cloud migration types for Level 2 based on application components type.



Deciding Cloud Deployment / Service Model for GoTG institutions (4/4)

GoTG institutions constrained by current infrastructure can adopt a Migration followed by Modernization approach



Phase 0 | **Phase 1** | **Phases 2 & 3**

Annexure 5 – Cloud Security considerations

Annexure 5 - Why is security critical for the Gambia G- cloud

95%	Cloud security failures happening due to customer's fault and not providers (by 2022)
60%	A majority (over 60%) of cloud security professionals cite data loss and data privacy were their biggest concerns
19%	Stolen or compromised credentials were the leading cause behind data breaches in 2022
38%	Globally, cyberattacks rose in 2022 compared to 2021
277 days	Average time it took for organizations to identify and contain a data breach in 2022

Why GoTG should focus on cloud security ?

1. Use of cloud to store classified and sensitive data does not mean complete transfer of security responsibilities to cloud service provider. Cloud security is a shared security model between the enterprise and IaaS/PaaS/SaaS provider.

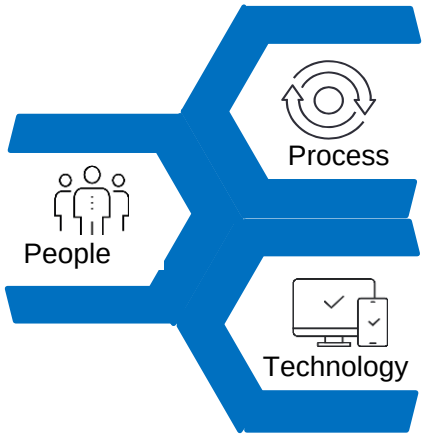
2. With workloads moving from on-premise to multiple IaaS and PaaS environments along with multiple SaaS applications, the complexity of data environments increases significantly making it a prime target to attack through the loopholes missed.

3. Strict government regulations protecting citizens data/privacy (examples: GDPR, ECOWAS Data and Privacy Act etc) with high penalties imposed for data breach is another reason to ensure robust cloud security.

4. Security breaches will erode confidence in the Gambia Government Cloud and negatively impact adoption .

Source:
- IBM and Ponemon Institute.26 Jan 2022
- Gartner, Inc. Gartner
- 2022 Hacker powered security report
- 2022 cloud security report
- IBM's Cost of a Data Breach Report 2022

Annexure 5 - Security Coverage



People

- **Security roles & responsibilities:**
  Different roles to effectively secure cloud resources
- **Security awareness & training:**
  Educating employees about cloud security with respect to individual roles and responsibilities
- **Personnel security:**
  Ensuring both internal and third party (vendor/cloud service provider) personnel are trustworthy

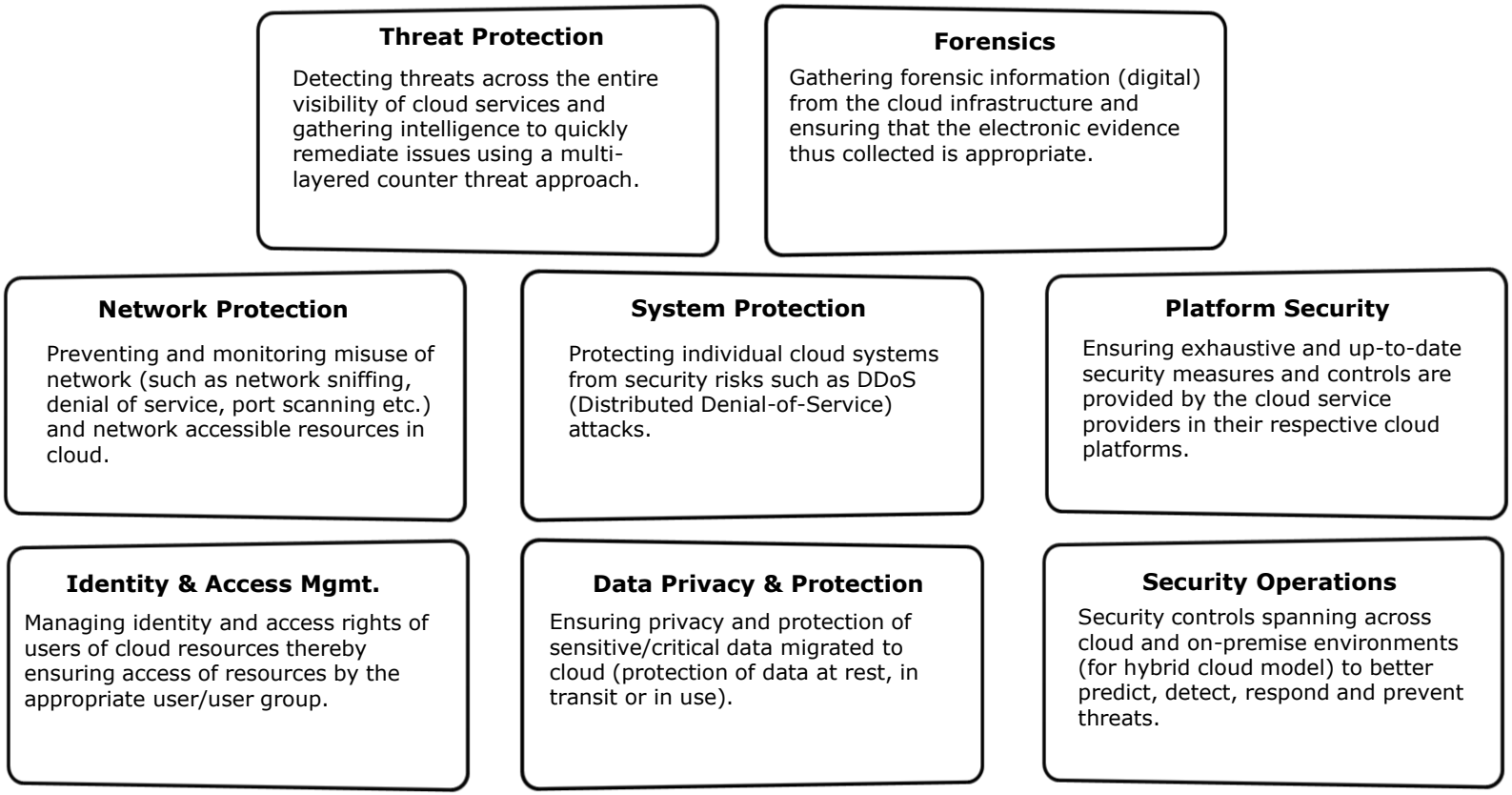
Process

- **Cloud Minimum Security Baseline:**
  Benchmarking most critical aspects of cloud security
- **IT Procurement:**
  Cloud security requirements for any procurement
- **Cloud Security Governance:**
  Ensuring cloud security strategy and policy updates are adhered to
- **Cloud Security Guidelines:**
  Guidance to business/IT teams regarding all aspects of cloud security
- **Cloud Security Assessment:**
  Objectively measuring effectiveness of security procedures
- **Cloud Security Risk Management:**
  Day-to-day management of cloud security

Technology

- **Identity & Access Mgmt.:**
  Mgmt. of identities and access rights of personnel using cloud resources
- **Data Encryption:**
  Technology to encrypt data at rest, in transit or in use
- **Key Management:**
  Technology to manage security keys (encryption, SSL keys)
- **Network Protection:**
  Technology to manage network security
- **Backup, recovery & archive:**
  Tools to back up critical data in the event of catastrophe

Annexure 5 - Security Building blocks



Annexure 5 - Security and Privacy on the Gambia G- Cloud

Key Considerations

IT security threats and issues poses specific challenges to business. GoTG must apply same diligence to application and data security as they do to physical and infrastructure security. If an application is compromised, it can create financial liability and reputation damage

***Security Risks Mitigations**	► **Data at Rest and Transit** need to be encrypted ► **Personally Identifiable Information** related data should be protected/ masked ► **SSL/TLS certificates should be implemented** at application level ► **Audit Trail** should be implemented at Database level ► **Institutional-wide Information Security Procedures** (detailed) should be defined to ensure baseline security standard at application/ data layer ► Ensure **effective governance, risk and compliance processes** exist (e.g. ISO IEC 38500 standards) ► Get level of access of **institutions operation and compliance reports** (conducted by independent auditor) ► Manage security terms in the **cloud service agreement** ► Understand the security requirements of any **exit process** ► Consider BSA Cloud computing Scorecard (global policies) while selecting Cloud Data Centre location
****Security as a Service** (SECaaS)	► Secure **Key/ Encryption** Management ► **Application Security** Assessment ► **SSL/TLS** Certificate Manager ► **Identity and Access** Management ► **DDOS** Protection Services ► Web Application **Firewall**

*Listed Security risks Mitigation should be common across all GoTG institutional applications
**Listed security services are not exhaustive, GoTG need to explore more on this based on various other factors including deployment models etc.

Annexure 5 - Security and Privacy on the Gambia G- Cloud

Application Security Considerations

Deployment Type	Key Considerations
IaaS	► Application security policy should closely mimic the policy of applications hosted internally by GoTG institutions ► GoTG should focus on network, physical environment, auditing, and authorization & authentication considerations. ► Appropriate data encryption standards should be applied in the handling of data and to user interaction (e.g., secure browsing) by the application in line with GoTG Government Cloud policy. ► System assurance principles, and development and testing methods that minimize the risk of introducing vulnerabilities in the code, should be applied even more rigorously than for on premises application, since some application will reside outside of the GoTG's security perimeter. ► CSPs must use hardware-based trusted computing security measures such as Intel TXT
SaaS	► Application-tier security policy constraints are mostly the responsibility of the service providers and are dependent upon terms in the contract and SLA. GoTG must ensure that these terms meet their confidentiality, integrity and availability requirements. ► It is Important to understand the service providers patching schedule, controls against malware, and release cycle. ► Scaling policies help deal with fluctuating loads placed on the application. Scaling policies are based on resources, users and data requests. ► Typically, GoTG institutions will only be able to modify parameters of the application that have been exposed by the service providers. These parameters are likely independent of application security configurations; however, GoTG should ensure that their configuration changes augment but not inhibit the service providers security model. ► GoTG should have knowledge of how their data is protected against administrative access by the provider. In a SaaS model, GoTG will likely not be aware of the location and format of the data storage. ► GoTG must understand the data encryption standards which are applied to data at rest and in motion. ► GoTG needs to be aware of how sensitive data, as defined in their data classification, is being handled in general and by configuration options

Annexure 5 - Security and Privacy on the Gambia G- Cloud

Application Security Considerations

Deployment Type	Key Considerations
PaaS	► GoTG will have responsibility for application deployment and for securing access to the application itself. ► CSPs will have the responsibility for properly securing the infrastructure, operating system and middleware. ► GoTG should focus on network, physical environment, and auditing, authorization, and authentication considerations. ► Appropriate data encryption standards should be applied in the handling of data and to user interaction (e.g., secure browsing) by the application. ► System assurance principles, and development and testing methods that minimize the risk of introducing vulnerabilities in the code, should be applied even more rigorously than for an on-premises application, since the application will reside outside of the GoTG's security perimeter. ► Appropriate data encryption and key management standards should be applied. ► GoTG needs to define how sensitive data, as part of their data classification, is being handled in general and by configuration options provided by utilized PaaS services. ► In a PaaS model, GoTG may or may not have knowledge of the format and location of their data. It is important that GoTG has knowledge of how their data may be accessed by individuals with administrative access.

Annexure 5 - Security and Privacy on the Gambia G- Cloud

Multi Tenancy Architecture Risks

What is the threat posed by multi-tenant architectures?

- Lack of data isolation due to configuration issues with the virtual resources
- Loss of critical information
- Service unavailability

How can GoTG minimize this threat?

Carefully evaluate the security capabilities and integrated functionality of each service model

SaaS: Evaluate service levels, security, governance, and compliance & liability expectations

IaaS or PaaS:

- System administrators must effectively manage security in collaboration with cloud service providers
- Supplement virtualization techniques with security measures for compute, storage, and network security enforcement and monitoring
- Restrict access to other tenants' actual or residual data, network traffic etc.

Annexure 5 - Security and Privacy on the Gambia G- Cloud

Data Privacy Security Risks

What is the threat posed by multi-tenant architectures?

- Fraudulent activity such as identity theft, email spamming, and phishing
- Trade-off between making information more accessible and protecting IP and PII (personally identifiable information)

How can GoTG minimize this threat?

- Conduct a risk assessment to evaluate legal, reputational and technical risks
- Require vendor to encrypt, isolate and separate data, and deploy intrusion prevention mechanisms
- Ensure transparency of vendor operations for effective oversight over system security and privacy
- Require vendors to commit to the location of cloud data centers
- Use the services of legal advisors who understand international privacy laws while creating framework agreements with CSPs

Annexure 5 - Security and Privacy on the Gambia G- Cloud

Data Loss and Leakage Security Risks

What is the threat posed by multi-tenant architectures?

- Lack of clear knowledge of what data is being transmitted across the network and being stored in the cloud
- Lack of data access standards , procedures and periodic monitoring
- Non-existent or largely ineffective security awareness and education

How can GoTG minimize this threat?

- Ensure isolation of systems, networks, management, provisioning, and personnel (e.g. read-only mode, robust key management, network segmentation, etc.)
- Ensure compatibility with cloud vendors' customer support processes, procedures, tools and support hours
- Establish adequate requirements for data recovery & backup in SLAs to ensure business continuity
- Create easily measurable and enforceable SLAs tailored to handle data loss incidents
- Enforce specific provisions to address data leakage reporting requirements, incident reporting and penalties

Annexure 5 - Security and Privacy on the Gambia G- Cloud

Reliance on Legacy Network Perimeter Control

What is the threat posed by multi-tenant architectures?

- Intrusion Detection / Prevention Services
- Data Leakage Protection / Prevention
- Traffic analysis and blocking

How can GoTG minimize this threat?

- Understand expected data flows to/from/between systems utilizing cloud technologies
- Understand the use of Software-Defined-Networking and virtualized appliances that can be custom-configured, such as IDS/IPS, DLP, virtual firewalls
- Consider use of virtual private cloud instances and create your own logical network with custom rules

Annexure 5 - Security and Privacy on the Gambia G- Cloud

Malicious Insider Security Risks

What is the threat posed by multi-tenant architectures?

- Knowledge of vulnerabilities in an institutions underlying information systems infrastructure
- Insider attacks often go unpublicized and even undetected

How can GoTG minimize this threat?

- Study vendor's processes, procedures and security mechanisms
- Ensure segregation of duties and grant minimum access required to individual or groups
- Deploy IAM solutions, intrusion detection systems and vulnerability management tools
- Regularly monitor usage logs and conduct audits in order to protect sensitive and confidential data assets
- Conduct pre-hiring background checks
- Include strict clauses in employment contracts prohibiting intentional sabotage of informational and other assets
- Train employees to identify and report risks
- Clearly define contingency plans and processes to notify key stakeholders about any security breaches

Annexure 6 – Case studies

What have others done with regards to Government Cloud?

Annexure 6 – Case studies

What have others done with regards to Government Cloud?

Aspect	United Kingdom	Oman	Ghana	Nigeria
Governance Structure	A cloud governance framework is in place with detailed policies regulating procurement of ICT and cloud services to public sector are in place. Clear rules and regulations mandating when public sector bodies can use public service providers are set. Cloud services are payable, prices are transparent, buyers' and suppliers' duties are well specified.	Cloud services governance is ensured via general ICT policies and procedures of Oman's Information Technology Authority (ITA), which are adequate. ITA manages service portfolio in accordance with public sector needs and feedback from customers.	The portfolio of IT projects are centrally reported at all times and are available to a governance body to make sure that progress (performance, costs and adoption) is known and under control. The National Information Technology Agency drives and monitors the move to and adoption of the Government Cloud. It implements the governance model which controls IT procurement, working closely with the Public Procurement Authority.	Nigeria's cloud governance functional module consist of the bodies charged to implement the operational module. Mainly the National Information Technology Development Agency (NITDA) coordinate activities across governance bodies, set overall cloud related priorities, and provide guidance to agencies whiles the Bureau of Public Procurement (BPP) operationalize governmentwide procurement regulation for Cloud services.
Pursued strategy	UK Government Cloud strategy is clearly geared towards an open cloud-first and cloud-native market ecosystem where public service bodies can purchase cloud services from competing private sector vendors using simplified procedure and avoiding public procurement bureaucracy. In addition, the Government as a Platform (GaaP) concept is used to promote and encourage reuse of public services and avoid duplication of work, waste of resources.	Compared to the UK Government Cloud , Oman solution is much more controlled and homogenous, there is no competitive marketplace involving private sector cloud providers. The new digital strategy of Oman stresses the need to foster private ICT sector, hence some private providers may appear in the future.	The Ghana Government Cloud strategy is centred on an open essential cloud program overseen by the National Information Technology Agency (NITA) that is the custodian of the shared services centre. Suppliers and alternate Government Cloud service providers under a simplified central governance, form a united IT service delivery and management structure for government.	The Federal Government of Nigeria is pursuing a cloud-first strategy. Local cloud service providers are the fist choice of consideration while deploying and assessing computing resources in the public sector and by SMEs that provide computing services to the public sector.

Annexure 6 – Case studies

What have others done with regards to Government Cloud?

Aspect	United Kingdom	Oman	Ghana	Nigeria
Marked spend	£1,696,137,364 - current total (ex VAT) of reported Government Cloud sales, November 2016 - 56% of total sales by value and 64% by volume, from all reported Government Cloud sales to date, have been awarded to SMEs ; 77% of total sales by value were through Central Government; 23% through the wider public sector	No official public data, most likely around 100M USD.	No official public data, most likely around 300M USD.	No official public data, most likely around 500M USD.
Underlying Architecture	As UK Government Cloud services are provided by private sector companies, the architecture varies – some agencies use Amazon AWS, others use Microsoft Azure and so on. The general trend is, that the ultimate providers are big, world-class cloud players, which foster brokerage and consulting services ecosystem around them. Common standards and guidance documents are available for GOV.UK (PaaS, implementing GaaP) platform, as well as deployment environment. Digital service standards are published.	Oman Government Cloud is architected and built using open standards and open source approach and components, namely OpenStack as the main cloud technology. Customers use IaaS, PaaS and SaaS services, so far there are no cloud-native solutions. Cloud platform design and virtualization layer foresees usage of various hypervisors and IaaS-level technologies.	Government of Ghana adopted an 'Essential Cloud' Policy meant to replace the traditional in-house and distributed IT infrastructure of GoG to provide consolidated, integrated, reliable and secure government IT service delivery. The Open Group Architecture Framework (TOGAF) was leveraged as a basis for enterprise architectural development	Data unavailable
Security and Data Classification	Comprehensive security guidance and principles are published as well as security classifications (three levels – official, secret, top secret) aimed to protect confidentiality and integrity of any government information and data. Some private providers accredited for top secret level.	Comprehensive security guidance and principles are published as well as security classifications aimed to protect confidentiality and integrity of any government information and data.	Ghana National Data Sharing Policy details the Security classifications of government data. Information is classified as either restricted, shareable or open.	Nigeria defined a clear data classification framework in its National Cloud Computing Policy. It clarifies what types of data can be stored on each type of system and also guides institutions when considering any type of cloud either within or outside Nigeria.

Annexure 6 – Case studies

What have others done with regards to Government Cloud?

Aspect	United Kingdom	Oman	Ghana	Nigeria
Digital Marketplace Structure	UK Digital Marketplace lists thousands of cloud and digital specialist service providers, all of them pre-screened and verified, having framework agreements for simplified procurement of services. Each provider lists openly priced services and supplies other relevant information for public sector bodies to make appropriate decisions.	Cloud services are available for purchase via Government Cloud self-service portal, prices are published. Public sector entities use cloud services provided by ITA. Buyers' and suppliers' duties are well specified through Master Services Agreement.	Ghana's Digital Marketplace is expected list pre-approved cloud services providers	Nigeria partnered with the Bureau for Public Procurement (BPP) and other critical stakeholders to establish a "Digital Marketplace" which encompass a series of framework agreements with pre-approved cloud services suppliers and maintain a database of services in an online portal that can be accessed by procuring entities
Number of Government Cloud providers	19249 Government Cloud services (hosting – 2735, software – 6563 and support – 9951) at the time of reporting. Some providers offer several services. Important note: providers can be from other countries, not only UK.	At the moment ITA is the only government cloud provider, however Oman pursues a strategy aimed to attract private cloud vendors to the market.	The National ICT Agency (NITA) is the principal Government Cloud Service provider (CSP) amongst others (e.g. Microsoft Azure, AWS etc) contracted by the government agencies provide cloud services in Ghana.	Data unavailable