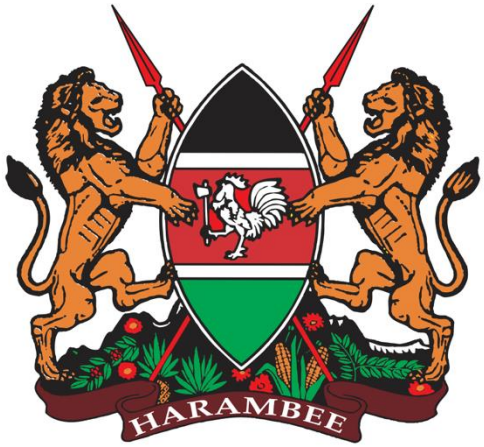

REPUBLIC OF KENYA

MINISTRY OF INFORMATION, COMMUNICATIONS AND THE DIGITAL ECONOMY

KENYA CLOUD POLICY

2024

Definition of Terms

- **Availability**: Ensuring timely and reliable access to and use of information
- **Change:** Refers to the addition, modification or removal of people, process and technology that could affect Cloud Policy.
- **Cloud Adoption:** Refers to the process by which organizations integrate Cloud Computing services and technologies into their operations, infrastructure and workflows.
- **Cloud Service:** Refers to computing services, software and infrastructure delivered over the Internet by Cloud Service providers to use as on as a pay as you go basis.
- **Cloud Infrastructure:** refers to the physical and virtual resources that make up the foundation of cloud computing services.
- **Cloud Computing:** Refers to a model for enabling access to computing resources (servers, storage, applications) through on-demand and can be rapidly provisioned and released with minimal management effort or cloud service provider interaction.
- **Cloud Policy:** A set of guidelines, rules, and procedures that govern the use, deployment, and management of cloud computing resources within an organization.
- **Cloud Service Provider:** Refers to an organization that offers cloud computing services and resources to individuals, organizations and businesses.
- **Confidentiality**: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
- **Community Cloud:** Refers to a cloud computing model that is shared by multiple organizations with similar interests, such as industry-specific regulations, compliance requirements, or business objectives.
- **Cybersecurity:** The practice of protecting computer systems, networks, devices, and data from unauthorized access, cyberattacks, and data breaches.
- **Data –** Information translated into a form more convenient to transmit or process.
- **Data Localization:** Refers to the regulatory requirement that data about a nation's citizens or residents is initially collected, processed or stored within the boundaries of a particular "jurisdiction", such as a country or a geographic region like a regional economic community or bloc.

- **Data Silos:** Refers to isolated or segregated collections of data within an organization that are not easily accessible or shared with other parts of the organization.
- **Data Sovereignty**: Refers to the powers of a country or a state over data created within its jurisdictions.
- **Data Redundancy:** Refers to the duplication of data within a system, database, or organization.
- **Data Residency:** Refers to the geographical location where data is stored and processed, encompassing the regulations and practices that govern data location, data movement and data security.
- **Disaster Recovery:** refers to the process of restoring and recovering IT infrastructure, systems, and data following a disruptive event or disaster, such as natural disasters, cyberattacks, hardware failures, or human errors.
- **Government Cloud Service Provider:** These are cloud computing organizations, that offer cloud services tailored specifically for government agencies and public sector organizations.
- **Hybrid Cloud:** This is a cloud computing environment that combines elements of both public and private clouds, allowing organizations to leverage the benefits of both deployment models.
- **Information –** Data analyzed and summarized in an easy form to interpret and draw conclusions from.
- **Innovation:** Refers to the process of creating new ideas, products, services, processes, or business models that add value, solve problems, or meet unmet needs.
- **Interoperability:** refers to the ability of different systems, devices, or applications to communicate, exchange data, and work together effectively to achieve common goals or objectives.
- **Integrity** - Refers to the accuracy and completeness of data from modification.
- **ISO**: Stands for the International Organization for Standardization. It is an independent, non-governmental international organization that develops and publishes voluntary international standards for various industries, sectors, and domains.
- **Jurisdiction:** Refers to the limits or territory within which authority maybe exercised.
- **Kenya Cloud Policy:** Refers to cloud first and sovereignty policy prioritized to the adoption and use of cloud computing solutions.

- **Localization:** refers to the process of adapting products, services, content, or experiences to meet the cultural, linguistic, regulatory, and market-specific preferences and requirements of a particular region, country, or target audience.
- **Private Cloud:** It is a cloud computing model that is dedicated exclusively to a single organization, providing secure and scalable IT infrastructure and services for internal use.
- **Public Cloud:** A type of cloud computing model that offers computing resources and services over the internet to multiple users or organizations on a pay-as-you-go basis.
- **Restricted Data:** Sensitive or confidential information subject to legal, regulatory, or organizational restrictions on access, use, and disclosure.
- **Risk Assessment:** A process of evaluating the potential risks involved in a projected activity or undertaking.
- **Risk Management:** The process of identifying, assessing, prioritizing, and mitigating risks to an organization's objectives, assets, projects, or operations.
- **Risk Mitigation:** The process of taking actions to reduce the likelihood or impact of identified risks to an acceptable level.
- **Secret Data:** Refers to highly sensitive or confidential information that is subject to strict controls and protection measures to prevent unauthorized access, disclosure, or misuse.
- **Sensitive information**: Refers to data that must be protected from unauthorized access to safeguard the privacy or security of an employee or the Authority.
- **Scalability:** Refers to the ability of a system, network, or application to handle increasing workloads, traffic, or demand without sacrificing performance, reliability, or efficiency.
- **Sovereignty:** Refers to the supreme authority and power of a governing entity, such as a nation-state or government, to govern itself, make decisions, enact laws, and exercise control over its territory, people, and resources without external interference or influence
- **Third Party:** Refers to a person or body that is recognized as being independent.

Acronyms

AU - African Union

BETA - Bottom-up Economic Transformation Agenda

CapEx – Capital Expenditure

CSC - Cloud service customer

CSP - Cloud service provider

DPA - Data Protection Act

GDC - Government Data Center

GoK - Government of Kenya

IaaS - Infrastructure as a service

IT - Information Technology

ITU - International Telecommunication Union

ISO - International Organization for Standardization

IEEE - Institute of Electrical and Electronics Engineers

ISP - Internet Services Provider

MCDA- Ministry, County, Department, Agency

MICDE – Ministry of Information, Communications and The Digital Economy

MISS - Minimum Information Security Standards

NCSS - National Cyber Security Strategy

NIST - National Institute of Standards and Technology

NGO – Non-Governmental Organisation

OpEx – Operation Expenditure

ODPC - Office of the Data Protection Commissioner

PaaS- Platform as a service

PII - Personally Identifiable Information

PS – Permanent Secretary

SaaS- Software as a service

SLA -Service level agreement

SWOT - Strength Weakness Opportunity and Threat

TCO - Total Cost of Ownership

VM – Virtual Machine

Contents

1. CHAPTER ONE: INTRODUCTION

1.1 Background

The Kenyan government recognizes the pivotal importance of Digital Transformation in cultivating a contemporary, flourishing, and inclusive society. This involves embracing emerging technologies to improve efficiency and productivity in disseminating information and services. The storage and connectivity of data play a crucial role in ensuring prompt, cost-efficient, and secure access to information. Acknowledging this, the Kenyan government intends to shift towards Cloud Infrastructure and Solution Services to supplement its traditional data storage and computing framework, thus establishing a more robust, efficient, cost-effective, and secure environment.

The Ministry of Information, Communications and the Digital Economy has been tasked with establishing digital governance frameworks for effective utilization of emerging technology. This initiative aligns with the African Union (AU) agenda 2063, Kenya Vision 2030, ICT Masterplan 2022-2032 and the Bottom-up Economic Transformation Agenda (BETA).

The policy aims to prioritize the adoption of cloud-based information and communication technologies, covering infrastructure, hardware, software, information security, licensing, storage, data provision, as well as services such as security, development, virtualization, databases, or any other technology where cloud solutions are deemed equivalent to alternative technological solutions.

Cloud computing is increasingly recognized as a vital aspect of digital transformation and innovation. The primary definition of cloud services lies in technology, optimal cost, maturity, reliability, sustainability, performance, and enhanced security.

Innovations driven by cloud computing offer significant potential benefits, often necessitating the movement of data across international boundaries. Balancing the facilitation of seamless data flow with the imperative to safeguard privacy, individual and public safety, and national security poses a challenge.

Existing legal frameworks constrain cross-border data flows. Adoption of this policy will align with legal principles as outlined in the Data Protection Act, (2019). It is recommended that all entities adhere closely to these legal directives when determining the appropriate cloud storage locations for their data flows.

1.2 Purpose

The purpose of this policy is to:

i. Ensure the seamless transition from traditional on-premises data center practices to Cloud Computing technology.
ii. Facilitate cross-border transmission, fostering interoperability and strengthening collaboration across nations.
iii. Complements other relevant existing cloud computing regulation.

1.3 Scope

This policy applies to all entities operating in Kenya and any entity utilizing data residing or emanating from Kenya.

While the policy encourages widespread cloud adoption, entities may be exempted upon approval by the cloud adoption committee.

On scenarios where data may be stored or transmitted between two or more sovereign states, it is recommended that the entities comply with Data Protection Act(2019) and attendant regulations.

1.4 Rationale

This Cloud Policy is a strategic approach prioritizing cloud-based solutions over traditional on-premises infrastructure when considering new IT projects or initiatives.

The successful adoption of cloud services is anticipated to yield several key outcomes:

i. **Cost savings:** Utilizing cloud infrastructure reduces expenditure on purchasing, setting up and maintenance. This streamlines technology operations and enhances service efficiency.
ii. **Service Enhancement:** Cloud solutions enable entities to seamlessly address service demands, with technology that support agility to meet requirements without interruption.

iii. **Innovation:** Cloud adoption allows for the swift and secure deployment of applications, leveraging modern technologies and frameworks.

iv. **Improved Cybersecurity:** Cloud solutions bolster resilience against cybersecurity threats, offering enhanced cybersecurity and privacy protection.

v. **Scalability:** Moving to the cloud ensures that infrastructure remains future-ready, enabling organizations to embrace the latest technologies rather than relying on outdated platforms.

vi. **Enhanced collaboration**: Cloud solutions facilitate effective collaboration by enabling easy data sharing across entities and jurisdictions fostering greater productivity and creativity in delivering online services.

vii. **Global reach:** Cross-border data transmission enables entities to expand their reach beyond local boundaries, tapping into international opportunities.

2 CHAPTER TWO: OVERVIEW OF CLOUD COMPUTING

2.1 Introduction

As Kenya embarks on its journey towards digital transformation, the adoption of cloud computing emerges as a strategic imperative to drive innovation, enhance service delivery, and optimize resource utilization across agencies and organizations. Cloud computing is a concept that refers to services, applications, and data storage delivered online through powerful file servers interconnected through the internet infrastructure. It allows consumers and businesses to use applications without installation and access their data and information at any computer with internet access. This technology allows for much more efficient computing by centralizing data storage, processing and bandwidth.

2.2 Policies and Legal Framework

For cloud computing to achieve its objectives towards the digital transformation of the nation, it must be underpinned by a robust policy and legal framework to address regulatory requirements, safeguard data privacy and security, and mitigate associated risks. The current landscape of the policy and legal framework that underpin cloud computing includes:

i. **Constitution of Kenya 2010**

   This is the supreme law of the Republic and binds all persons and all State organs at all levels of government. The policies and laws should conform to the provisions of the Constitution.

ii. **Data Protection Act, CAP. 411C**

   This is the primary statute on data protection in Kenya which gives effect to Article 31 (c) and (d) of the Constitution of Kenya, 2010 (right to privacy).

iii. **National ICT Policy of 2019**

   The Kenya National ICT Policy outlines the policy of the Government of Kenya in relation to the design, development, acquisition, deployment, operation, support and evolution of public and private ICTS. It defines the current and forward-looking position of the government on various areas of the evolving and emerging technology landscape in Kenya.

2.3 The need for Cloud Policy

The cloud computing landscape is robust and needs adequate policy and legal framework to ensure. The Kenya's existing policy and legal framework is inadequate and doesn't address all the issues and challenges related to cloud computing hence the need to come up with a comprehensive cloud policy. While general ICT principles are outlined, there may be gaps in addressing the traditional on-premise challenges and opportunities associated with cloud computing. The establishment of a Cloud Policy in Kenya presents an opportunity to address gaps in the existing policy and legal framework related to cloud computing. By defining clear objectives, enhancing the legal framework, and promoting best practices, Kenya can position itself as a leader in cloud computing, driving innovation, efficiency, and competitiveness in the digital economy.

The Kenya Cloud Policy builds upon the foundational principles and objectives outlined in National ICT Policy, which serves as the overarching framework guiding ICT development and governance in the country. This policy acknowledges the importance of leveraging cloud computing technologies to accelerate digital transformation, enhance service delivery, and drive economic growth, while ensuring alignment with existing legal frameworks and regulatory requirements.

2.4 Current State

Most organizations typically host their data and systems on-premise by managing their own IT infrastructure within dedicated server rooms or facilities located within their premises. Here's an overview of how organizations host their data and systems on-premise and the challenges they may encounter:

i. **Personal Computers:** Some organizations due to lack of centralized storage, host their data and applications on personal computers.
ii. **Dedicated Server Rooms**: Many organizations maintain dedicated server rooms equipped with servers, storage devices, networking equipment, and other IT infrastructure to host their data and systems on-premise. These server rooms are often managed by internal IT teams or outsourced IT service providers.
iii. **Data Centres:** Some organizations operate their own data centres to host & manage data and systems for multiple departments or branches within the organization. These data

centres are equipped with advanced infrastructure and security measures to ensure reliable and secure hosting of critical government data and systems. These Data Center are owned and operated by the specific organizations and mostly host their own data.

iv. **National Data Centres:** The government has also invested and implemented Data Centres that are hosting MCDA's data. These Data Centre's include Ruaraka GDC and Konza National Data Center.

v. **3rd party owned Data Centres:** Some organizations are hosting their data or collocating with 3rd party Cloud Service Providers both locally and international.

Currently there is no legal framework to direct organization to adopt Cloud hence some organizations are still investing in server rooms and data centres in a bid to host their applications. Even with the heavy investment of constructing server rooms and data centres, organizations still face challenges ranging from unreliable/poor connectivity, lack of technical capacity and infrastructure, backup challenges, unsecure data hosting, unreliable service level agreements, power surge and UPS failure among others.

2.5 Challenges

i. **Limited Resources**: Many organizations face challenges related to limited resources, including budget constraints, huge maintenance cost, skilled IT personnel shortages, and outdated infrastructure. Limited resources may hinder their ability to invest in modern IT infrastructure, security solutions, and staff training.

ii. **Security Risks**: On-premise hosting exposes organizations to security risks, including physical security breaches, unauthorized access, data theft, and cyber attacks. Ensuring robust security measures, such as access controls, encryption, and intrusion detection systems, is essential to mitigate these risks.

iii. **Data Silos**: Hosting data and systems on-premise may result in data silos, where data is fragmented and stored in isolated systems or applications within individual organizations. Data silos can hinder data sharing, collaboration, and interoperability between organizations, impacting decision-making and service delivery.

iv. **Scalability and Flexibility**: On-premise hosting may lack the scalability and flexibility of cloud-based solutions, making it challenging for organizations to accommodate growing

data storage and processing demands or adapt to changing requirements. Scaling infrastructure resources may require significant investments in hardware upgrades and expansion.

v. **Disaster Recovery**: Organizations must implement robust disaster recovery strategies to mitigate the risk of data loss or system downtime. On-premise hosting requires organizations to establish redundant infrastructure, backup systems, and recovery procedures to ensure uninterrupted service delivery in the event of disasters or disruptions.

vi. **Compliance and Regulatory Requirements**: Organizations must comply with various regulatory requirements, data protection laws, and government policies governing data management and security. Ensuring compliance with these requirements while hosting data on-premise requires diligent monitoring, auditing, and adherence to established standards and protocols.

vii. **Lack of collaboration:** On premise hosting hinders sharing of information, collaboration and innovation hence slows down organization's decision as well limiting opportunities to adopt to new technologies and improve service delivery and efficiency.

As technology advances and business priorities evolve, organizations must explore cloud solutions and other strategies to optimize their IT infrastructure and address the challenges associated with on-premise hosting.

2.6 International Best Practices.

Most countries have developed and adopted cloud policies prioritizing cloud-based solutions over traditional on-premise infrastructure for new IT initiatives and investments. This strategy aims to capitalize on the benefits of cloud computing, such as scalability, flexibility, and cost-effectiveness, to accelerate digital transformation, enhance competitiveness and improve service delivery.

With the advent of Cloud Service Providers venturing into cloud solutions and having invested heavily, cloud solutions have become cost-effective and the first choice for many organizations. These Cloud Service Providers (CSP) are governed by international standards such as ITU, ISO/IEC 27001, NIST, etc. hence ensuring a safer cloud-based environment and reducing the risk of security problems.

Government cloud policies strive for a balance between data control and security, ensuring personal and national data protection while fostering innovation. This necessitates exploring mechanisms for national sovereignty alongside international cooperation, allowing countries to retain control over their data while leveraging the global benefits of cloud computing.

Governments focus their cloud computing policies on several key areas to ensure responsible innovation in this rapidly developing field. This cloud policy will therefore consider the following:

i. **International Governance Frameworks**: Exploring the need for, and potential development of, international legal and regulatory frameworks specific to cloud computing service and deployment models. This will therefore, provide guidance on establishing clear guidelines for data privacy, security and national control in a globalized environment.
ii. **Codes of Conduct for Responsible Use**: Developing codes of conduct for all stakeholders (MCDA, industry players and NGOs) is crucial. These codes will promote responsible use of cloud computing services across all sectors, ensuring ethical practices and mitigating potential risks.
iii. **Data Interoperability and Portability**: Addressing data interoperability and portability challenges, both domestically and internationally, is essential. This will facilitate seamless data exchange within and across borders, fostering collaboration and innovation while ensuring data remains accessible and secure.
iv. **Global Standardization**: Promoting global harmonization of cloud computing standards will ensure compatibility and security across borders.

2.6.1 Data Location Concepts

The widespread utilization of distributed cloud data processing infrastructures by Cloud Service Providers (CSPs) to deliver services globally necessitates a clear understanding of how local data protection laws impact data transfers. This is particularly crucial when considering the transfer of data beyond the national borders or legal jurisdiction that governs the applicable data requirements.

Cloud computing adds another layer of complexity to data privacy. Three connected ideas - data localization, sovereignty and residency all play a role in data control. A good cloud policy needs to address all three for strong data security.

i. **Data Localization**: This refers to legal restrictions that mandate data to be stored or processed within a specific geographic location. The primary motivation for data localization policies is to ensure national control over sensitive data and potentially boost domestic data security expertise.

ii. **Data Sovereignty**: This principle focuses on a nation's legal control over data stored within its borders, even if the data is physically located elsewhere. Data Sovereignty ensures that data remains subject to the laws and regulations of the data owner's country, regardless of its physical location.

iii. **Data Residency**: Data residency refers to the physical location where data is stored, regardless of ownership. It's essentially about where the data's "home" is within the cloud. Understanding data residency is crucial for determining the applicable laws and regulations, as well as potential security risks associated with the data storage location. However, data residency alone doesn't guarantee control over how the data is used or accessed.

2.7 Cloud Services & Deployment Models

2.7.1 Service Models

Cloud computing offers various service models as illustrated below:

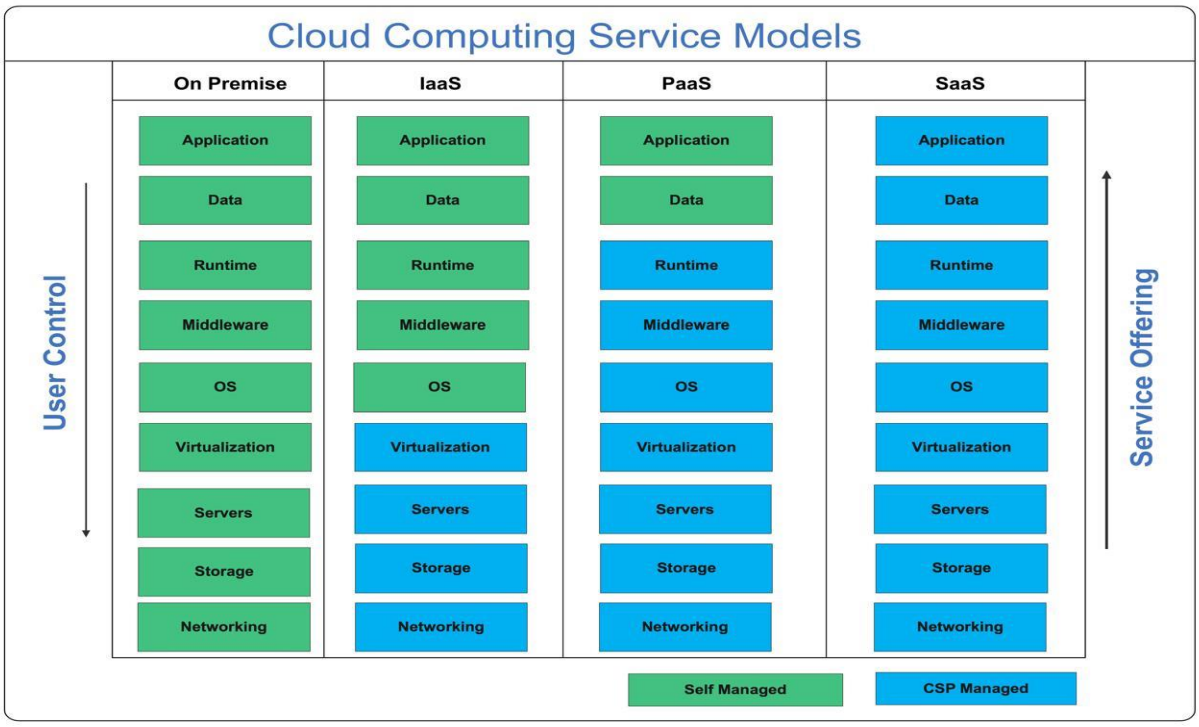

Figure 1: Cloud Computing Service Models

i. Infrastructure as a Service (IaaS):

This category offers fundamental cloud computing services, enabling the rental of IT infrastructure such as servers, virtual machines (VMs), storage, networks, and operating systems from a cloud provider on a pay-as-you-go basis.

ii. Software as a Service (SaaS):

Software as a service delivers software applications over the internet, typically on a subscription basis. With SaaS, cloud providers host and manage the software application and its underlying infrastructure, including maintenance tasks like software upgrades and security patching. Users access the application via the internet, often through a web browser on their mobile devices or computers.

Examples of SaaS applications include email services, social media platforms, and cloud-based file storage solutions.

iii. Platform as a Service (PaaS):

Platform as a service offers cloud computing services that furnish an instant environment for building, testing, deploying, and overseeing software applications. PaaS aims to simplify the process for developers to swiftly create web or mobile applications, without the need to handle the setup or management of underlying infrastructure such as servers, storage, networks, and databases required for development.

2.7.2 Deployment Models

In addition, this policy also acknowledges the following deployment models for cloud services:

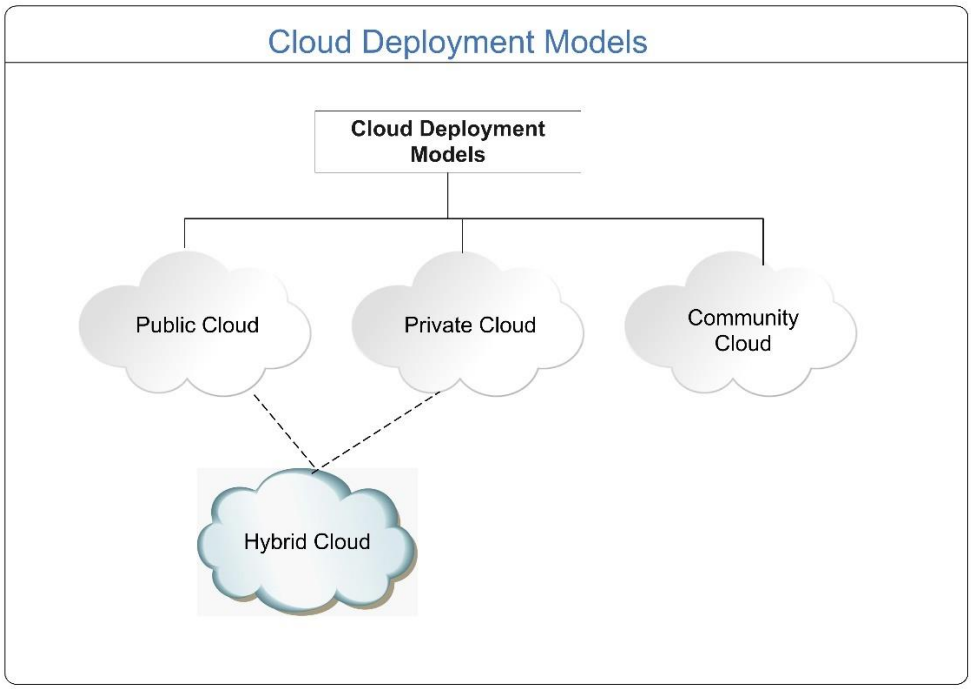

Figure 2: Cloud Computing Deployment Models

i. Public Cloud:

This model offers is widely adopted model offers readily available and scalable resources from a cloud service provider (CSP) over the public internet. Public cloud can be thought as a vast utility grid, offering computing resources on-demand, similar to how electricity is delivered to homes and businesses. Public cloud solutions are ideal for agencies seeking a cost-effective and flexible

option with minimal upfront investment. While offering a high degree of scalability and accessibility, the public cloud may present security considerations for highly sensitive data due to the shared infrastructure environment.

ii. Private Cloud:

This model provides a dedicated cloud environment for a single organization, such as the Kenyan government. Private clouds can be hosted on-premises within a government data center or managed by a CSP in a dedicated off-premises environment. A private cloud can be likened to a secure, gated community, offering exclusive access to computing resources for government agencies. This model provides a high degree of control and security, making it suitable for sensitive data and applications. However, private clouds typically require more upfront investment in infrastructure compared to the public cloud model.

iii. Hybrid Cloud:

Combining two or more distinct cloud infrastructures (private, community, or public), this model remains separate entities interconnected by technology enabling data and application portability. Hybrid clouds offer enhanced flexibility, diverse deployment options, and assist in optimizing existing infrastructure, security, and compliance.

iv. Community Cloud:

This model is tailored for exclusive use by a specific community of consumers from organizations with shared concerns such as mission, security requirements, policy, and compliance considerations. Ownership, management, and operation can be undertaken by one or more organizations within the community, a third party, or a combination thereof, and may exist on or off premises.

3 CHAPTER THREE: POLICY STATEMENT

3.1 Objectives

The Kenya Cloud Policy shall mandate all entities to prioritize cloud-based solutions when making ICT investments (procurement of hardware, software, renewal of existing software licenses, revamping existing ICT infrastructure including Data Centers). This prioritization aims to achieve the following key objectives:

i. To accelerate adoption of green cloud computing technology
ii. To reduce Total Cost of Ownership of ICT infrastructure
iii. To ensure robust Cybersecurity measures on data hosted on cloud.
iv. To enable collaboration and interoperability among entities.
v. To promote Data Residency and Sovereignty.

3.2 Statements

When making new IT investments, entities covered by this policy are required to consider the below stages:

a) A 'New ICT investment' includes procurement of new hardware and software, renewal of hardware and renewal of present software licenses. It is noteworthy that the entities falling under the scope of this policy must abide by the laws, regulations and controls related to data classification and other regulations regarding the location of hosting their data in any way.
b) If data is classified as top secret or secret, the government cloud service providers should be relied upon only if the technical and cybersecurity requirements are met. In the case that the government cloud service providers do not meet the technical and the cybersecurity requirements, the entity can then seek approval to host internally.
c) If data is not classified as top secret or secret, entities should utilize the deployment model of Government Cloud Service Providers only if the security, technical, and commercial requirements are met. With regards to the data classification, data classified restricted

should seek approval to host internally. For open data, should be hosted in Government Cloud Service Providers.

d) If the security, technical, and commercial requirements cannot be met by Government Cloud Service Providers entities should assess solutions from 3rd party cloud service provider subject to approval.

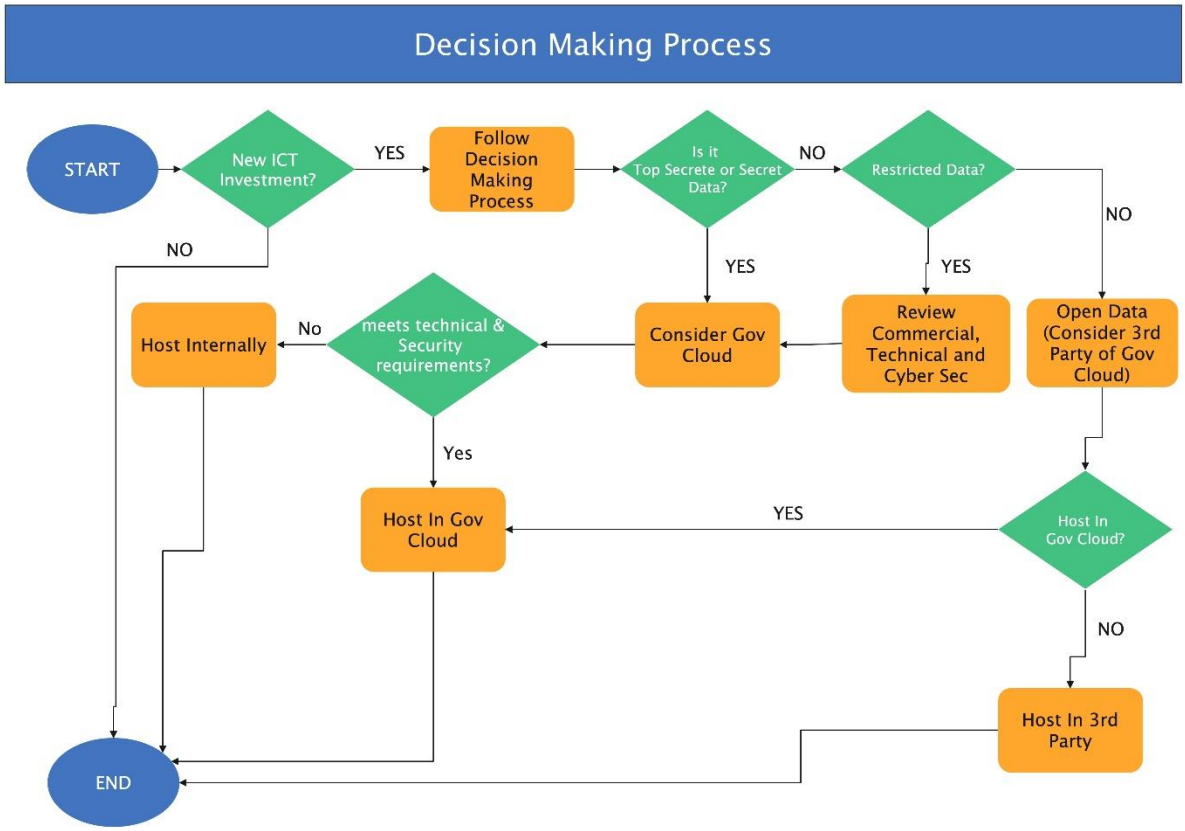

Figure 3: Decision Making Process

The Cloud policy shall:

i. Promote adoption of green cloud computing technology to enable entities to access on-demand scalable resources, such as compute power, storage, and networking allowing organizations to rapidly scale up or down based on demand.

ii. Optimize IT resource utilization across agencies and eliminating duplications in IT expenditures achieved through:

a. Use of pooled cloud computing resources from a certified cloud service provider.
b. Shift Kenyan entities from capital expenditures (CapEx) to operational expenditure (OpEx)

iii. Leverage on cloud service providers' expertise in cyber security standards

iv. Facilitate seamless data sharing and collaboration between entities and jurisdiction.

v. Promote Data Residency, Sovereignty and Localisation.

vi. The Kenya cloud policy shall prioritize the selection of accredited Cloud Service Providers (CSPs) that provide a centralized and redundant data storage, disaster recovery and data backups to foster operations continuity.

4 CHAPTER FOUR: IMPLEMENTATION AND GOVERNANCE

4.1 Implementation Strategy

4.1.1 Migration Strategy

Entities will need to consider their existing organizational environment when adopting new delivery models. The transition to an as-a-service model will potentially have significant change implications. Moving to a cloud environment will require entities to reconsider business design and enterprise architecture.

Adoption of a cloud service should be seen as integral to a wider business reengineering process, rather than solely an IT-related task. Commencing early engagement across the entity to discuss the change implications of transitioning to an as-a-service model will facilitate entities in more effectively leveraging associated opportunities to enhance business efficiency.

4.1.2 Considerations for Cloud Policy

The evaluation of potential government investments in cloud computing for the public sector will be conducted on a case-by-case basis. Each case will undergo assessment from three key areas:

Cybersecurity

Ensuring compliance with national cybersecurity requirements is paramount. All cloud solutions must be evaluated to guarantee data security and protection in accordance with regulations and laws issued by the governing body for cybersecurity

Technical

The technical viability of each migration to cloud services will be thoroughly assessed. Solutions must meet specific technical requirements, with consideration given to factors such as latency sensitivity and the availability of required features.

Commercial

The economic benefits of cloud computing will be considered, with a focus on assessing the Total Cost of Ownership (TCO) for migrating entities. The commercial aspect will be evaluated on a case-by-case basis, taking into account factors such as customization needs and comparative costs.

4.1.3 Contract Terms

Industry best practices for cloud computing contracts require entities to address the following aspects when formulating a cloud computing contract:

i. **Selecting a Cloud Service:** The critical first step in procuring cloud services will be to choose the appropriate CSP and deployment model (refer to Chapter 2).

ii. **Cloud Service Provider (CSP) and End-User Agreements:** Terms of Service and all agreements required by the CSP or contracting entity will need to be fully integrated into the cloud contracts.

iii. **Service Level Agreements (SLAs):** SLAs will need to define performance with clear terms and definitions, demonstrate how performance will be measured, and establish enforcement mechanisms to ensure SLAs are met.

iv. **CSP and Entity Roles and Responsibilities:** There will be a need for careful delineation of responsibilities and relationships between entities and CSPs to effectively manage cloud services.

v. **Standards:** The use of the ISO 22123 IT cloud computing standard.

vi. **Security:** Entities will need to clearly specify the requirements for CSPs to maintain the security and integrity of data existing in a cloud environment. At a minimum, this should be in conformance with ISO 27017, Security Techniques, a code of practice for information security controls based on ISO/IEC 27002 for Information Security, Cybersecurity and Privacy protection.

vii. **Privacy:** If cloud services host "privacy data," entities must adequately identify potential privacy risks and responsibilities and address these in the contract. At a minimum, this should be in conformity with The Data Protection Act (DPA) 2019 and ISO 27018, Security Techniques, a code of practice for the protection of personally identifiable information (PII) in public clouds acting as data controllers and processors.

viii. **Legal Discovery:** Entities will need to ensure that all data stored in a CSP environment is available for legal discovery by allowing all data to be located, preserved, collected, processed, reviewed.

ix. **Electronic Records (E-Records):** Entities must ensure CSP's understand and assist entities in compliance with the Access to Information Act 2016 and Access to Information (General) Regulations 2023 and obligations under this law.

4.1.4 **Skills and Capabilities**

The migration to a new system, regardless of the delivery model, will necessitate an assessment of the Entity's workforce capability. The skills and capabilities required to deploy ICT as a service with a cloud-based solution may see a decrease in demand for certain system maintenance/software skill sets and an increase in demand for business analysts, portfolio/programme managers, app developers, and vendor/contract managers. Entities will be able to call upon the CSP for assistance with such retraining/reskilling, and this may be addressed as part of the contract.

There will also be implications for Entity skills and capabilities requirements through the implementation of cloud services. For example, where 'commercial off-the-shelf' solutions are used and business practices need to be amended.

4.2 Governance

To ensure smooth implementation and achieve optimal results, a clearly defined governance structure is essential. Six primary roles have been identified to govern the implementation of the Kenya Cloud Policy.

S/No	Item	Responsible Organ	Roles
1	Policy Body	Ministry of Information, Communications and the Digital Economy.	• Defining the objectives and scope of the Kenya Cloud Policy. • Setting the guidelines for the policy and publishing. • Defining the roles and responsibilities of the different involved entities, in the context of the Cloud Policy. • Updating and adjusting the Kenya Cloud Policy when required.
2	Cloud Adoption Committee	Multi-agency committee to be constituted by the PS responsible for ICT	• Oversee cloud adoption across the different entities through pilots and supporting Entities during the migration process with technical and commercial expertise. • Checking the cybersecurity, technical and commercial requirements.

			• Handling accreditation of Cloud services offered to entities. • Administrating the Marketplace that will connect Cloud suppliers with the buyers. • Ensuring standards and interoperability compliance.
3	Security Body	Governing Body for Cybersecurity	• Issuing the cloud cybersecurity controls and guidelines based on existing regulations while checking the compliance with these controls.
4	Cloud Service Providers (CSPs)	CSP	• Providing the Cloud computing services in its different forms: public, Gov-Cloud and private. Includes international as well as local players
5	National Data Management Office	This will include ODPC and other bodies dealing with data	• Mange, govern, digitize and grow the national data to empower the national assets and capabilities. • Also, protect the personal and sensitive data by setting strategies, policies, regulations and the required controls, implement it and

			monitor the compliance against it. • Establish data classification policy, enable its application and ensure compliance with it.
6	Entities	All entities as defined in 'Scope of the policy' section. These entities are buyers of Cloud services.	• All the entities mentioned above will ensure continuous and transparent collaboration to drive the Cloud adoption.

5 CHAPTER FIVE: MONITORING, EVALUATION AND REVIEW

5.1 Monitoring and Evaluation

Monitoring and evaluation of cloud-based applications and systems will adhere to internal audit standards equivalent to those for on-premises systems. Oversight committees, such as the IT Steering Committee or Internal Audit Committee appointed by the ministry will be responsible for reviewing the ongoing effectiveness and efficiency of cloud arrangements, ensuring compliance with vendor terms, and considering necessary amendments. Adoption of common and open standards, wherever feasible, aims to uphold overall integrity and facilitate seamless integration with core systems.

5.1.1 Risk Management

Entities will be required to undertake comprehensive annual risk assessments concerning network access, storage, and maintenance of public sector information and records held by CSP.

As entities evaluate ICT delivery options, risk profile assessments will be necessary for each option. Having a full understanding of the risks and opportunities associated with cloud-based solutions will be critical, both from an end-user and delivery capability perspective.

Evaluation of cloud options will involve addressing all identified risks and taking into account:

i. Data Protection Act (DPA) 2019
ii. Computer misuse and cyber-crimes Act 2018
iii. National Cyber Security Strategy (NCSS) 2022
iv. Minimum Information Security Standards (MISS)
v. ISO 31000 Risk management – Principles and guidelines

5.1.2 Risks Mitigation

Depending on the service type, business need, and delivery model adopted, entities will need to understand and mitigate various risks, including but not limited to:

i. **Disaster Recovery:** Disaster recovery plans must be well-documented and tested, as with all ICT delivery options.

ii. **Data Location and Retrieval:** Understanding data residence and sovereignty requirements and managing implications will be necessary.

iii. **Legal and Regulatory:** Monitoring legal precedent and evolving case law will be essential, given the lack of precedence and many untested areas in emerging technologies.

iv. **Information Governance and Management:** Ensuring compliance of cloud service providers and their offerings with all applicable Kenyan information management frameworks will be imperative.

v. **Privacy:** Ensuring compliance of cloud service providers and their offerings with all applicable Kenyan legislative requirements regarding the privacy of information will be necessary.

vi. **Security:** Ensuring compliance of cloud service providers and their offerings with all applicable Kenyan legislative requirements regarding the security of information will be crucial.

vii. **Licensing:** Existing software licensing models, which may be less flexible than a cloud deployment solution, may need to be re-evaluated and adapted accordingly.

5.2 Review

The policy will undergo periodic review as necessary to ensure its continued relevance and effectiveness in addressing evolving technological and regulatory landscapes. Any updates or revisions required will be carried out based on the identified needs and emerging requirements within the organization.