Towards a National Cloud Strategy for Kenya

Focus on Public Sector

**RANICTP workshop
May 2017**

**Tonny K. Omwansa, PhD
@tomwansa**

Overview

- Two Cloud Adoption Surveys

- Draft Cloud Strategy

- Way forward

2013 Cloud Study

2013 Cloud Survey – Design

- **Determinants of cloud computing:**
  - Factors that affect cloud related performance and its outcomes/impacts
  - Characteristics: Reliability. Agility. Usability. Sustainability etc
  - Policy and legal frameworks. Market. Standards etc.

- **Strategies or actions of Cloud Computing actors:**
  - Instrumental in delivering the outcomes/impacts of the cloud
  - Costing. Promotion. Training etc.

- **Outcomes/Impacts of Cloud Computing**
  - Improved operational efficiency
  - Enhanced market reach
  - **etc**
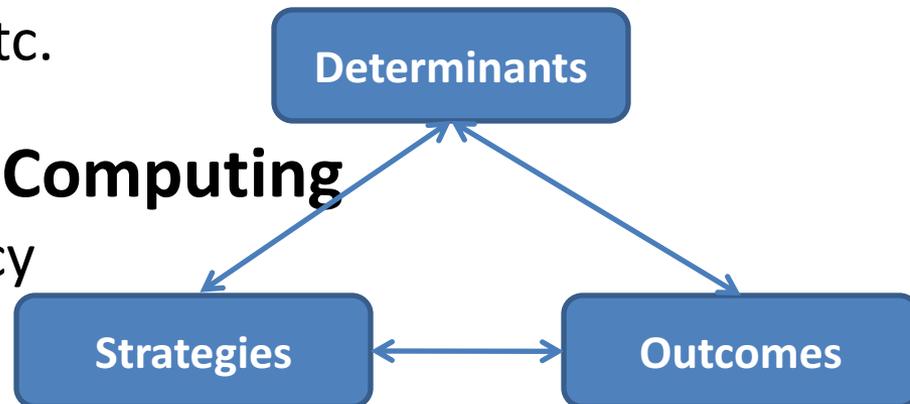
2013 Cloud Survey – Output

- Timelines: June 2013 - April 2014

- Quantitative (60 institutions) and Qualitative (12 in depth interviews)

- Baseline report available at http://www.c4dlab.ac.ke/wp-content/uploads/2014/04/CC-study-report-April-2014.pdf

2013 Cloud Survey – Emerging topics

- Governance, Legal and regulatory frameworks
- Standards
- Conflict resolution
- Safe/Fair Contract Terms/Conditions
- Licensing
- Location of Data
- Cross border and territorial issues
- Skills & Awareness
- Encouraging adoption
- Vendor locking
- Market Characteristics (competitive landscape/ maturity)
- Network infrastructure, application and data readiness
- Government readiness and role
- Service Level Agreements

- Portability of applications
- Integration with legacy environment
- Public Cloud Procurement Guidance
- Culture change
- Alignment to government strategies
- What services should go to the public/community cloud (Decision Framework for Cloud Migration)
- Security requirements (Statutory compliance to laws, regulations, agency requirements; Data characteristics; Privacy and confidentiality; Integrity - authorized, complete, and accurate; Data controls and access policies)
- Protecting security yet maximize value
- Selecting a cloud solution
- Ensuring competitiveness

2013 Cloud Survey - Key Findings

1. Adoption of cloud computing in Kenya is fairly recent. Most organizations adopted a form of cloud service either 2010/11.

2. More organizations utilized pure private cloud (39%) compared to utilizing a public cloud (22%).

3. The key barrier:
   – Additional cost of investment
   – Technical skills (security, architecture and design, storage and virtualization)
   – Perceived reliability of service, security and privacy of data
   – Geographical location

4. Lack of knowledge of policy/legal frameworks for cloud (80%)
   – Those aware: "its not flexible, comprehensive and effective"

5. Majority of the respondents (75%) not aware of any standards

2013 Cloud Survey - Key Findings

6. Cloud services market was ready (90%).
   - Leading consumers: financial sector, telecommunications

7. Benefits of cloud were consistent with literature:
   - cost savings in hardware, software and personnel,
   - improved system performance and management,
   - flexibility in access to processing and storage capacity
   - higher elasticity degree
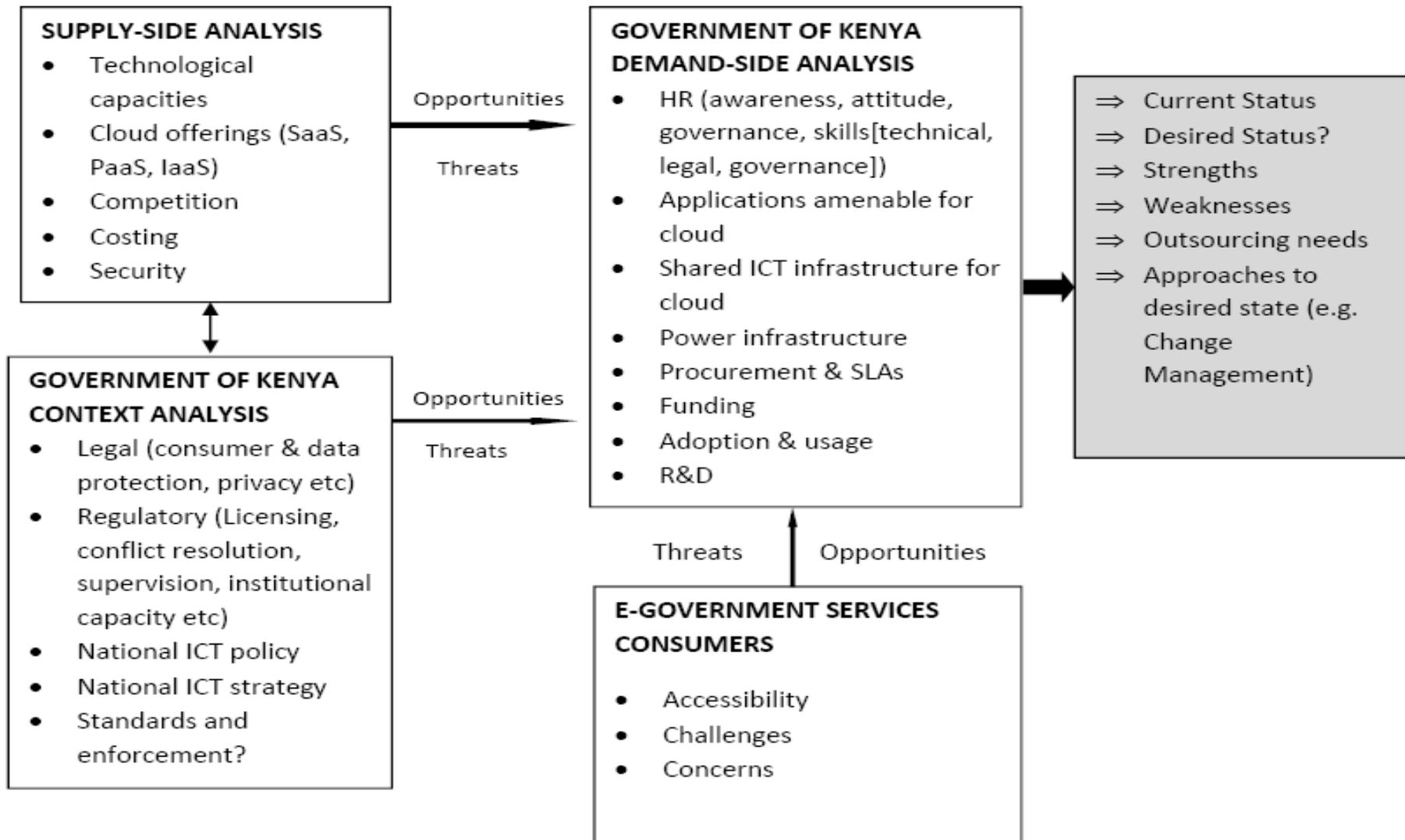   - etc

2013 Cloud Survey - Recommendations

1. A national cloud readiness survey to inform cloud strategy

2. Developing a national cloud strategy

3. Government to champion utilization of cloud services

4. Enhancement of relevant legal/regulatory frameworks
   - protection of cloud service users
   - cyber security challenges
   - guaranteeing secure online payments
   - privacy and data security
   - etc

5. Development of the human resource capacity
   - technical skills, legal and business processes

6. Enhance awareness of cloud technologies
   - demystify and circulate accurate information

2014/15 Cloud Study

2014/5 Cloud Survey - Background

1. An in-depth study, focused on public sector

2. Target consumer: ICT Authority

3. Anchored on ICT Masterplan

4. Objective: developing a Cloud strategy

5. Based on a SWOT analysis

6. Data collected: June 2014 to February 2015

7. 45 in-depth interviews (suppliers, MDACs, public, opinion shapers)

2014/5 Cloud Survey - Framework

SUPPLY-SIDE ANALYSIS
- Technological capacities
- Cloud offerings (SaaS, PaaS, IaaS)
- Competition
- Costing
- Security

Opportunities

Threats

GOVERNMENT OF KENYA CONTEXT ANALYSIS
- Legal (consumer & data protection, privacy etc)
- Regulatory (Licensing, conflict resolution, supervision, institutional capacity etc)
- National ICT policy
- National ICT strategy
- Standards and enforcement?

Opportunities

Threats

GOVERNMENT OF KENYA DEMAND-SIDE ANALYSIS
- HR (awareness, attitude, governance, skills[technical, legal, governance])
- Applications amenable for cloud
- Shared ICT infrastructure for cloud
- Power infrastructure
- Procurement & SLAs
- Funding
- Adoption & usage
- R&D

Threats   Opportunities

E-GOVERNMENT SERVICES CONSUMERS
- Accessibility
- Challenges
- Concerns

⇒ Current Status
⇒ Desired Status?
⇒ Strengths
⇒ Weaknesses
⇒ Outsourcing needs
⇒ Approaches to desired state (e.g. Change Management)

Findings - Situational analysis

Strengths

- **Leadership** - National leadership understands and champions technology

- **Launched projects** – Several e-gov services amenable for the cloud

- **Legal/regulatory environment** – Progressive (various policy documents)

- **Local Infrastructure capabilities** - High quality networks, Some good DCs

- **Institutional establishments** – Regulatory and supervisory exist

- **Policy documents** - A number of policies have been developed e.g. ICT policy, National cybersecurity plan, ICT Masterplan etc

- **Institutional readiness** - Most institutions interviewed have LANs, connectivity & other infrastructural developments needed for cloud.

Findings - Situational analysis

Weaknesses

- **Governance and change management** - Weak human capital, traditional mindset, resistance to change

- **Service acquisition & funding** – SLAs, funding mechanism and procurement laws aren't all aligned to acquisition and management of cloud

- **Availability and reliability** - Network Dependence at Critical Hours - Provision of reliable access, round-the-clock support, security levels, high internet speeds are paramount issues that need to be addressed.

- **Information assurance and data security** - Assurance of privacy and confidentiality of data and information in the cloud are key issues that the Government must consider during cloud offering, as they are very sensitive.

- **Legal and regulatory issues** - There are perceived gaps in the legal and policy frameworks surrounding cloud computing, as well as inadequate enforcement and political interferences

Findings - Situational analysis

Opportunities

- **Governance** - Reduced costs, improved access and service delivery.

- **Accessibility & reliability** - Ease of use of access, improved productivity

- **Higher flexibility & scalability** - Dynamic and rapid scale of capacity.

- **Laws & policies** - Providers adherence to national & international laws /policies

- **Variety** - Improved bargaining power of Gov (ability to procure from wide variety of providers, local providers and international)

- **Pricing** - Favorable pricing models depending on client needs.

- **Technical and human capital** – Providers have invested in competent staff to support clients with access to updated technology.

Findings - Situational analysis

Threats

- **Governance** - Possible IT staff reduction, internal resistance to change and working practice, long bureaucratic procurement process, trust, funding.

- **Lack of control** - Control is transferred to the cloud provider.

- **Security and privacy concerns** - Data privacy, data protection, loss of control over data, target to external attacks, potential malicious insider activity.

- **Interoperability** - Integration with in house systems.

- **Legal and regulatory environment** - Lack of specific standard regulation on data protection, user privacy issues, SLAs etc

- **Technology/Infrastructure, skills and awareness** - Unpredictable performance, lack of sensitization and awareness of cloud services being offered, lack of technological and human capability, reliability of power supply, lack of high speed internet connection in certain parts of the country.

- **Vendor lock-in** – Potential challenge to easy migration among providers.

Draft Cloud Strategy

Vision

- The vision of the ICT Master Plan is:
  - *Kenya as a regional ICT hub and a globally competitive digital economy*

  - This vision can be taken as the Government's vision with respect to ICT.

- Cloud Strategy Vision
  - ***Delivering value of e-government services to stakeholders by exploiting cloud computing services***

  - Value to Government agency that outsources
    - e.g. reduced total costs of ownership and better service delivery etc

  - Value to businesses and citizens that the Government agencies serve
    - e.g. increased flexibility, convenience, ease of use of government services, better quality of services etc

Strategic Objective

- The strategic objective of the Shared Services theme of the **ICT Authority Strategic Plan 2013-2017** is:

  To facilitate efficient and effective delivery of government online services using a suitable combination of private and public cloud computing offerings

- One of the means of achieving this objective is '*to develop and implement a public service cloud computing strategy*'.

    – The objective of this cloud strategy is **"to expound the above Shared Services strategic objective and guide its implementation."**

Desired State

- **Many more shared commodity services and solutions**

  A range of shared ICT services and solutions available on the cloud so the government, its agencies and related bodies can use what they need, when they need it, and not create duplicate services that cannot be shared.

- **Scalability and flexibility**

  The ability, if required, for departments and agencies to change infrastructure to fit to their needs.

Desired State

- **Competitive marketplace**

  A range of service providers constantly improving the quality and value of the solutions they offer which the government can take advantage of.

- **Ready and easy to use**

  Complete solutions that are already assured for security, performance and service management

Desired State

- **Cost effectiveness**

    Cloud computing will bring down the unit per cost of consumed IT service because it reduces cost of electricity consumption, lower Infrastructural labor cost of distribution, and provides reliability in the event of disaster and Business continuity- high availability and reliability

- **High scalability of IT investment**

    The cloud provides on-demand access to shared resources that reduced upfront cost of IT investments through turning the fixed capital expenditure in IT into operative costs depending based upon size of demand

Desired State

- **Mobility**

  Increased capacity to work from anywhere and from any device.

- **Improved governance**

  Greater traceability of government transactions and services

Guiding Principals

- **Increase the speed** with which ICT services are deployed

- Use of **global standards and best practices** to provide high quality and consistency

- **Reducing waste** by avoiding duplication, breaking down silos and promoting sharing of idle resources

- **Increase project success rates** by sharing of information and inter-agency collaboration

- Use of **open standards** for data and architecture to facilitate greater interoperability, openness and re-use of ICT solutions

Guiding Principals

- **Cost consciousness** by reducing price government pays for assets by increasing sharing & re-use of ICT services/solutions

- **Promote flexibility, convenience and ease of use** of government services by citizens

- **Agility** to help improve way government delivers business change

- **Enhancing accountability and trust** by clearly defining internal and provider responsibilities while building trust into business processes

Strategy Specifics - SaaS

- ICT Authority to design, implement and manage ICT infrastructure to deliver software application services to Ministries, Departments, Agencies and the Counties regardless of their location.

- Backend activities will be managed from central locations in a one-to-many model.

- SaaS to have elements of Public and Private

Strategy Specifics – SaaS (public)

- Applications, data or processes which are public-facing, non-sensitive, non-confidential, non-mission critical or needing significant future scalability to be considered for public cloud.

- Respective implementing agencies should also consider compliance and budgetary requirements.

- Examples:
  - open data, public information repositories, analysis of non-sensitive or non-confidential data and front-end elements of online services or apps that do not store sensitive data.

Strategy Specifics – SaaS (private)

- Applications, data or processes with characteristics like: sensitive, confidential and mission critical should be considered for private cloud.

- The implementing agency should also consider compliance requirements.

- Examples:
  - financial systems, procurement platforms, HR systems, identity details, medical records and financial details.

Strategy Specifics - IaaS

- Government to establish infrastructure that can be shared and provided to other stakeholders as a service.

  - This infrastructure to be accessible to other organizations within gov on need basis

- The Government Core Connectivity Network (GCCN), the National Optic Fibre Backbone Infrastructure (NOFBI) and County Connectivity Infrastructure (CCI) represents the basic infrastructure on which e-government services run.

  - This infrastructure cannot be outsourced given the privacy and confidentiality of some of the Government data sets.
  - The government will therefore have to ensure that this infrastructure is reliable and recruit highly skilled persons to support it.

Strategy Specifics – IaaS strategies

General

- **Consolidation of the various connectivity projects** into one integrated network that provides seamless connectivity

- **Review the design of the network elements** and improve their scalability, reliability, security and cost

- **Outsource certain elements** of the network infrastructure in order to manage scalability, effectiveness and cost. e.g., construction of infrastructure, maintenance and redundancy

- **Consolidate the procurement and maintenance of ICT infrastructure** across the national government Ministries, Departments and Agencies.

Strategy Specifics – IaaS strategies

General

- **Review the operation of NOFBI** by Orange given its unacceptably low quality of service, intertwining with Orange infrastructure, open access to ducts and termination points.

- Consider providing **infrastructure as a service to the County Governments** and provide **last mile connectivity** with appropriate technologies, e.g. white spaces, Wimax,

- Develop and retain a **core ICT infrastructure team** that has the requisite skills to design, implement and maintain the core Government infrastructure.

Strategy Specifics – IaaS strategies

Computing and storage

- **Build a network of distributed Government Data Centers** based on global standards and best practice to ensure high availability.

- **Migrate all existing critical applications** that are currently in gov offices to Government owned and managed data centers

- **Consolidate all Government budgets for DCs** in the short to medium term in order to consolidate and reduce costs.
  - begin with a survey to identify who in Government has DC plans in the short to medium term and build case for consolidation and transfer to a distributed GDCs approach.

Strategy Specifics – IaaS strategies

Computing and storage

- **Introduce a commercialization model** (e.g. sharing space and services) in GDCs to guarantee sustainability

- Market to **critical anchor tenants** who can use the government cloud infrastructure as a service e.g. KRA, CBK, KPLC

- For all GDCs, **outsource all non-core elements**, especially power and backup systems, cooling and HVAC to local qualified companies.

- **Build capacity** in Government for data centre personnel
  - Introduce a **DC career path** that ensures that DC professionals can grow to the top in a technical career

Strategy Specifics – IaaS strategies

Disaster recovery and business continuity

- For **mission critical** applications high availability must be guaranteed. It is therefore necessary to run the applications in active-active mode in two data centres

- For **non-mission critical** applications, an active-passive approach across two data centres but with clear restore targets is recommended

- For **disaster recovery**, primary and secondary sites should be separated by a minimum distance as per global best practice

Strategy Specifics - PaaS

- PaaS enables government to provide tools on demand that enable subscribers to develop new applications or services. The cloud based application development tools also enable testing, deployment, collaboration, hosting and maintenance of developed solutions.

- Examples of platforms that can be deployed as a service include Content Management Systems (CMS), Spatial Data Infrastructure (SDI), Data Warehouses and Open Data platforms.

//More work to be done on PaaS

Strategy Implementation – Key issues

1. Policy Recommendations

2. Strategic Projects

3. Funding

4. Standards

5. Governance Structure

6. Change Management

7. Critical Success Factors

8. Risks and Mitigation Strategies

9. Monitoring and Evaluation

Strategy Implementation – Key issues

Policy Recommendations

- Consolidation of network infrastructure and DC budgets in MDAs

- Consolidation of mission critical applications hosted in high availability environment and in DCs designed to global standards

- No development and deployment of silo systems - The systems developed or procured by MDAs should:

  - be generic

  - be standards-based

  - share infrastructure, including storage, network links and information without duplication

  - be integrated with other systems according to a guideline (operation manual) to be developed by ICTA

Strategy Implementation – Key issues

Strategic Projects

Category	Project	Timeframe
GDCs	Upgrade GDC Ruaraka	6 months
	Implement a containerized DC	12 months
	Complete Naivasha DC	18 months
	Build a Tier 4 DC	2-3 years
	Build other DCs to achieve distributed network of DCs	> 3 years
Network Infrst	Complete NOC to manage infrastructure	6 months
	Re-design GCCN and on-board key clients	6 months
	Fast-track NOFBI phase 2 implementation	24 months
	Fast-track CCP phase 2 and ensure all key county offices are connected	15 months
Applications	Implement Government Enterprise Architecture to facilitate integration	6 months
	Migrate applications designated for public cloud	12 months
Legal/Regulatory fwrk	Review legal frameworks for procuring cloud services	12 months
	Review regulatory framework (consumer privacy, confidentiality, etc.)	12 months
	Review data protection legislation	12 months

Strategy Implementation – Key issues

Funding Sources

- **Government**

  The National Government will consolidate all ICT budgets in MDs in the line Ministry (MoICT).

- **Agencies and County Governments**

  ACs to fund specific aspects of cloud computing in consultation with the ICT Authority and pay for some of the shared services that they need and are available in a Government private cloud.

Strategy Implementation – Key issues

Funding Sources

- **Private Sector**

  Development of suitable incentives and tax breaks to private sector both within and outside the ICT sector to fund some of the cloud computing projects.

  – Incentives may include: Development of Special Purpose Vehicles/Private Sector Consortiums and waivers on certain levies, licensing fees, tax incentives and tax breaks.

- **Development Partners**

  Kenya will ;leverage on her funding priorities when approaching development partners (bi-lateral, multi-lateral or other development partners) who have ICT at the top of their support priority lists to fund some of the cloud computing projects.

Strategy Implementation – Key issues

Standards

Global standards exist such as

- ISO/IEC JTC 1/SC 38 (standardization of Cloud Computing and Distributed Platforms)
- ISO 27018:2014 (code of practice revolving around the protection of Personally Identifiable Information (PII) in public clouds)
- COBIT (governance and management by bridging the gap between control requirements, technical issues and business risks)
- ICTA has been working on a set of guiding standards

- The Kenyan Government should therefore ensure that it adopts global practices prior to the adoption and development of cloud services.

Strategy Implementation – Key issues

Governance Structure

- Governance structure in National ICT Master Plan shall be used
- Strengthening needed particularly on:
  - Who makes decision on adding cloud services and how will it be funded;
  - How IT resources are allocated and scheduled;
  - Who will be responsible for managing the cloud service provider and how cloud services be managed and controlled.
- Cloud governance structures for consideration and customization:
  - The US Federal Cloud Computing Initiative Governance Structure
  - Government of Canada IT Services Governance Structure
  - Scheper's Cloud Governance Model
  - Guo's Cloud Governance Model
  - Microsoft Cloud Governance Model

Strategy Implementation – Key issues

Change Management

- Some areas needing management:

- **Changes to organizational processes:**
  - Staff should be prepared. Changes in the processes affecting many aspects like daily operations, roles and responsibilities.

- **Stakeholder engagement:**
  - A stakeholder engagement plan. Actively keep stakeholders updated.

- **Training:**
  - Including but not limited to legal, technical, business analysis, systems architecture, change management, vendor management and governance.

- **Awareness:**
  - All be made aware of new approach, challenges and anticipated benefits.

Strategy Implementation – Key issues

Critical Success Factors – Seven key

1. Developing a competent support team in Gov for CC

2. Operationalization of the Governance Structure in the National ICT Master Plan (Cabinet Steering Committee Chaired by HE the President)

3. Managing change within gov and general public

4. Legal/regulatory frameworks to encourage & support CC adoption

5. Available and reliable Government ICT infrastructure

6. Funding, especially for scaling and recurrent expenditure

7. Active engagement and participation of County Governments

Strategy Implementation – Key issues

Risks and Mitigation Strategies

	Risks	Mitigation Strategies
1	Resistance to change	Implement a change management program with key elements mentioned above
2	Inappropriate procurement legislation	Amendment of the procurement legislation to allow for procurement and scaling of cloud services
3	Insufficient or inadequate legal and regulatory environment	Strengthen the legal and regulatory environment to support the new paradigm
4	Lack of funding to support new set ups and additional costs of utilizing public cloud	Consolidation of cloud focused budgets by different MDAs

Strategy Implementation – Key issues

Risks and Mitigation Strategies

	Risks	Mitigation Strategies
5	Poor quality services, including unavailability of services due to threats like cyber attacks, distributed denial of service attacks and system failures, loss of data security and protection because of the off-premise characteristics of third party providers, etc.	- Professional due diligence of service providers - Establishment and enforcement of comprehensive contractual agreements with relevant consequences of liabilities - Enforce strict SLAs and monitor them closely - Clustering, replication and disaster recovery solutions to achieve the necessary reliability.

Strategy Implementation – Key issues

Risks and Mitigation Strategies

	Risks	Mitigation Strategies
6	Loss of privacy and data assurance due to aspects like breaches, access, ownership and storage location	- Establishment and enforcement of comprehensive contractual agreements with relevant consequences of liabilities - Standards enforcement and audit controls measures - Privacy and security laws enforcement - For public cloud, ensure understanding of applicable laws. - Appropriate exit strategies
7	Lack of pricing clarity in variety of costs	Transparent contractual agreements drafted and managed by qualified persons.
8	Unavailability of relevant skills	Develop appropriate capacity building and career progression programs

Strategy Implementation – Key issues

Monitoring and Evaluation

- M&E of performance shall be the responsibility the Shared Services Director at ICT Authority.

- This Director will monitor the implementation of the strategy on a quarterly basis and report to the ICT Authority CEO, the ICTA Board and other relevant units in Government.

Next steps…

Stakeholder engagements

Revisions

Adoption

@tomwansa