# GOVERNMENT ICT STANDARDS

## Cloud Computing Standard

ICTA 7:002:2019

Second Edition 2019

The ICT Authority is a State Corporation under the State Corporations Act 446
www.icta.go.ke

## REVISION OF ICT STANDARDS

In order to keep abreast of progress in industry, ICTA Standards shall be regularly reviewed. Suggestions for improvements to published standards, addressed to the Chief Executive Officer, ICT Authority, are welcome.

## ICT AUTHORITY (ICTA)

Head Office: P.O. Box 27150, Nairobi-00100, Tel.: (+254 202) 211 960/61
E-Mail: standards@ict.go.ke, Web:http://standards.icta.go.ke

## DOCUMENT CONTROL

| | |
|---|---|
| Document Name: | Cloud Computing Standard |
| Prepared by: | ICTA Cloud Computing Standard Technical Committee |
| Edition: | Second Edition |
| Approved by: | Board of Directors |
| Date Approved: | 13th January 2020 |
| Effective Date: | 1st February 2020 |
| Next Review Date: | After 3 years |

# CONTENTS

# FOREWORD

The ICT Authority has the mandate to set and enforce ICT standards and guidelines across all aspects of information and communication technology including Systems, Infrastructure, Processes, Human Resources and Technology for the public service. The overall purpose of this mandate is to ensure coherent and unified approach to acquisition, deployment, management and operation of ICTs across the public service in order to achieve secure, efficient, flexible, integrated and cost effective deployment and use of ICTs.

To achieve this mandate, the Authority established a standards committee to identify the relevant standard domains and oversee the standards development process. The committee consulted and researched broadly among subject matter experts to ensure conformity to acceptable international and national industry best practices as well as relevance to the Kenyan public service. The committee eventually adopted the Kenya Bureau of Standards (KEBS) format and procedure for standards development. In an engagement founded on a memorandum of understanding KEBS, participated in the development of these Standards and gave invaluable advice and guidance.

For example, the Cloud Computing Standard, which falls under the overall Government Enterprise Architecture (GEA), has therefore been prepared in accordance with KEBS standards development guidelines which are, in turn, based on the international best practices by standards development organizations including ISO.

The Authority's Directorate of Programmes and Standards has the oversight role and responsibility for management, enforcement and review of this standard. The Directorate shall carry out quarterly audits in all the Ministries, Counties, and Agencies (MCA) to determine compliance to this Standard.

The Authority shall issue a certificate for compliance to agencies upon inspection and assessment of the level of compliance to the standard. For non-compliant agencies, a report detailing the extent of the deviation and the prevailing circumstances shall be tabled before the Standards Review Board who shall advise and make recommendations to remedy the shortfall.

The ICT Authority management, conscious of the central and core role that standards play in public service integration, fostering shared services and increasing value in ICT investments, shall prioritize the adoption of this standard by all Government agencies. The Authority therefore encourages agencies to adhere to this standard in order to obtain value from their ICT investments.

**Dr. Katherine W. Getao, EBS**

**Chief Executive Officer**

**ICT Authority**

# 1.0 INTRODUCTION

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.
NIST specify five characteristics of cloud computing:

a. **On-demand self-service** involves customers using a web site or similar control panel interface to provision computing resources such as additional computers, network bandwidth or user email accounts, without requiring human interaction between customers and the vendor.

b. **Broad network access** enables customers to access computing resources over networks such as the Internet from a broad range of computing devices such as laptops and smart-phones.

c. **Resource pooling** involves vendors using shared computing resources to provide cloud services to multiple customers. Virtualization and multi-tenancy mechanisms are typically used to both segregate and protect each customer and their data from other customers, and to make it appear to customers that they are the only user of a shared computer or software application.

d. **Rapid elasticity** enables the fast and automatic increase and decrease to the amount of available computer processing, storage and network bandwidth as required by customer demand.

e. **Pay-per-use measured service** involves customers only paying for the computing resources that they actually use, and being able to monitor their usage. This is analogous to household use of utilities such as electricity.

Cloud computing is a new concept in the market and its adoption has been slow but steady due to slow pace in standardisation, security concerns, continous evolution and compliance concerns. Despite this setbacks, cloud computing offers a number of benefits such as:

- ❖ Cloud computing solutions are scalable: agencies can purchase as much or as little resource as they need at any particular time. They pay for what they use.
- ❖ Agencies do not have to make large capital outlays on computing hardware, or pay for the upkeep of that hardware.
- ❖ Cloud computing provides economies of scale through all-of-government volume discounts. This is particularly beneficial for smaller ICT users.
- ❖ Agencies can easily access the latest versions of common software, which deliver improved and robust functionality, and eliminating significant costs associated with version upgrades.
- ❖ If agencies are able to access the same programmes, and up-to-date versions of those programmes, this will improve resiliency and reduce productivity losses caused when applications are incompatible across agencies

This ICT standard outlines the various considerations for Ministries, counties and agencies in the selection of cloud computing services and models such as IaaS, SaaS, Paas and public cloud, private cloud, community cloud and hybrid cloud.

## 2.0 SCOPE

This standard shall provide guidelines on acquisition and deployment of cloud based computing products and services. The standard guides the MCDAs as consumers and also guide providers of cloud services. Areas covered include:

i. General requirements
ii. User context of cloud computing: This entails the parties, the roles, the sub-roles and the cloud computing activities

- Cloud service customer
- Cloud service provider

iii. Cross cutting aspects

## 3.0 NORMATIVE REFERENCES

The following standards contain provisions, which, through reference in this text, constitute provisions of this standard. All standards are subject to revision and, since any reference to a standard is deemed to be a reference to the latest edition of that standard, parties to agreements based on this standard are encouraged to take steps to ensure the use of the most recent editions of the standards indicated below. Information on currently valid national and international standards can be obtained from Kenya Bureau of Standards.

**ISO/IEC 17788:2014, Cloud computing**
Overview and vocabulary, provides definitions of common cloud computing terms, including those for cloud service categories such as Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). It also specifies the terminology for cloud deployment models such as "public" and "private" cloud. ISO/IEC 17788 draws on definitions developed by the National Institute of Standards and Technology, including SP 800-145: The NIST Definition of Cloud Computing, SP 800-146: Cloud Computing Synopsis and Recommendations and SP 500-292: NIST Cloud Computing Reference Architecture.

**ISO/IEC 17789:2014, Cloud computing**
Reference architecture, contains diagrams and descriptions of how the various aspects of cloud computing relate to one another.

**ISO/IEC 27017:2015 / ITU-T X.1631**
— Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services
- Guidelines on security and privacy in public cloud computing. NIST Special publication 800-144

- Cloud computing Synopsis and recommendations. NIST Special publication 800-146
- Cloud computing management audit/assurance (Aug.2010)-ISACA
- Article 31 of the Kenya Constitution. Existing laws, legislations and policies.

## 4.0 TERMS AND DEFINITIONS

For the purposes of this ICTA Standard the following definitions, abbreviations and symbols apply:

### 4.1.1 Cloud computing

Cloud computing is a concept that refers to services, applications, and data storage delivered online through powerful file servers interconnected through the internet infrastructure.

### 4.1.2 Interoperability

Interoperability typically refers to the ability to easily move workloads and data from one cloud provider to another or between private and public clouds

### 4.1.3 Privacy

Information privacy is the assured, proper, and consistent collection, processing, communication, use and disposition of disposition of personal information (PI) and personally-identifiable information (PII) throughout its life cycle. (Source: adapted from OASIS)

### 4.1.4 Software as a Service (SaaS)

The capability provided to the consumer is to use the providers applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings. Popular SaaS offerings include e-mail and collaboration and customer relations management
(Source: NIST CC Definition)

### 4.1.5 Platform as a Service (PaaS)

The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations. (Source: NIST CC Definition)

### 4.1.6 Infrastructure as a Service (IaaS)

The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls). (Source: NIST CC Definition)

### 4.1.7 Private Cloud

The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise. (Source: NIST CC Definition)

### 4.1.8 Community Cloud

The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise. (Source: NIST CC Definition)

### 4.1.9 Public Cloud

The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services. (Source: NIST CC Definition).

### 4.1.10 Hybrid Cloud

The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds). (Source: NIST CC Definition]

**A role** is a set of cloud computing activities that serve a common purpose.

**A sub-role** is a subset of the cloud computing activities for a given role

**Cloud service customer (CSC)**: A party which is in a business relationship for the purpose of using cloud services.

**Cloud service provider (CSP)**: A party which makes cloud services available.

**Cloud service partner (CSN)**: A party which is engaged in support of, or auxiliary to, activities of either the cloud service provider or the cloud service customer, or both.

**A party** is a natural person or legal person, whether or not incorporated, or a group of either. Parties in a cloud computing system are its stakeholders.

A party can assume more than one role at any given point in time and can engage in a specific subset of activities of that role. Examples of parties include, but are not limited to, large corporations, small and medium sized enterprises, government departments, academic institutions and private citizens.

**Architecture**: Fundamental concepts or properties of a system in its environment embodied in its elements,relationships and in the principles of its design and evolution.

**Personally identifiable information (PII)**: Any information that (a) can be used to identify the PII principal to whom such information relates, or (b) is or might be directly or indirectly linked to a PII principal.

**Activity**: A specified pursuit or set of tasks.

### Abbreviations

IaaS-Infrastructure as a service
PaaS- Platform as a service
SaaS- Software as a service
NIST-National institute of science and technology
SLA-Service level agreement
PI – Personal information
PII- personal identifiable information
MCDA- Ministry, county, Department, Agency
TCO- Total cost of ownership
GoK- Government of kenya
CSC - cloud service customer
CSP - cloud service provider
CSN - cloud service partner

## 5.0 GENERAL REQUIREMENTS

5.1 Use of Cloud Computing services must comply with all current laws, Information security standard, and risk management policies.

5.2 MCDAs shall not host critical applications in the public cloud [Refer to Systems and Applications Standard]

5.3 To mitigate against risks associated with vendor lock-in, MCDAs shall prepare an exit strategy as part of contracting with the Cloud Service Provider.

5.4 MCDAs shall obtain copies of potential cloud service providers' most recent standards-based security assessment/assurance as early in the procurement cycle as possible.

5.5 Cloud solutions that store personally identifiable citizen data shall be within the boundaries of Kenya.

5.6 MCDAs shall determine their licensing needs projected over a period and ensure the cloud provider meets the needs.

5.7 MCDAs handling data on foreigners shall ensure compliance to applicable laws of their countries of origin.

5.8 If data stored with a cloud service provider is to be encrypted this shall be done using cryptographic keys owned and managed by the Government of Kenya (See information security Standard)

5.9 Mobile apps are cloud services if "they store, process or transport MCDA information outside the network boundary".

5.10 In all cases, a cloud computing solution shall only be considered after a thorough risk evaluation (as per GoK Information Security Standard) has been completed, reviewed and accepted by the MCDAs Chief Information Security Officer or delegate.

5.11 Cloud computing solutions must be supported by facilities that meet Uptime Institute Tier-3 or higher rating. Anything less than this needs extra resiliency capabilities.

5.12 MCDA shall ensure that adequate safeguards are in place to secure authentication, authorization, and other identity and access management functions, and are suitable for the organization.

5.13 MCDAs shall acquire cloud solutions in reference to the list of accredited cloud providers provided by ICT Authority.

5.14 MCDAs shall ensure that negotiated SLA requirements supersede Master Service agreements.

5.15 Contracts with cloud service providers shall include:

5.15.1 An exit plan especially requiring the cloud provider to provide a way for MCDAs to extract data easily and economically.

5.15.2 Requirement for data sanitization from storage media, electronic and physical access rights be revoked from the cloud provider, and assets provided to the provider returned or, if not possible, be securely purged.

5.15.3 Non-Disclosure Agreement (recommended before provisioning any service)

5.15.4 Full disclosure in case of breaches to regulated information.

5.15.5 Data ownership (the Government of Kenya retains exclusive ownership of ALL data held in a cloud provider's solution which was entered by MCDA, systems or affiliates in all media forms e.g. online, backup and archive etc.)

5.15.6 Any other standard intellectual property clauses (as are relevant to the service)

5.15.7 Data location (It should be explicitly stated in contracts that it should be in Kenya)

5.15.8 Privacy legislation compliance
5.15.9 Service Level Agreements (to meet availability, performance, and disaster recovery requirements)
5.15.10 Service management processes
5.15.11 Procedures for incident response and ensure that they meet the requirements of the organization
5.15.12 Audit mechanisms and tools to ensure organizational practices are followed throughout the system lifecycle
5.15.13 The application of appropriate retention policies to stored data based on its classification - this means the cloud service provider's solution must not hinder compliance with the Public Records Act
5.15.14A clear process documenting the responsibilities of each party with respect to extracting MCDA data and destroying data at the end of the contract
5.15.15Provision for a cloud service provider being taken over/bought-out by another organisation (this should include ensuring the ownership, access rights and protection of any data the MCDA owns cannot be lost when there is a change of cloud service provider ownership)

# 6.0 USER CONTEXT OF CLOUD COMPUTING

## 6.1 Cloud service customer

Cloud service customers are MCDAs that have a business relationship with a cloud service provider for the purpose of using cloud services. These MCDAs shall establish the following roles and responsibilities

### 6.1.1 Cloud service user

MCDAs acquring cloud services shall identify cloud service users to consume the cloud services. The use cloud service activities shall involve

- The provision of user credentials to enable the cloud service provider to authenticate the user and grant access to the cloud service;
- The invocation of the cloud service, which then operates and delivers its specified outcomes.

### 6.1.2 Cloud service administrator

MCDAs shall appoint a cloud service administrator;
The cloud service administrator shall ensure the smooth operation of the customer's use of cloud services, and that those cloud services are running well with the customer's existing ICT systems and applications. The cloud service administrator shall oversee all the operational processes relating to the use of cloud services and acts as the focal point for technical communications between the cloud service customer and the cloud service provider.
The cloud service administrator's cloud computing activities include:

- perform service trial;
- monitor service;
- administer service security;
- provide billing and usage report;
- handle problem reports;
- administer tenancies .

### 6.1.3 Cloud service business manager

MCDAs shall appoint a cloud service business manager;
The Cloud service business manager shall ensure that business goals are met through the acquisition and use of cloud services in a cost efficient way. The main responsibilities of the cloud service business manager concern financial and legal aspects of the use of cloud services, including approval, on-going ownership and accountability.
The cloud service business manager's cloud computing activities shall include:

- Adjusting business plan to accommodate the use of cloud services;
- Tracking the use of the services and dealing with accounting and financial management;
- Handling billing/invoices received from the cloud service provider for the use made of cloud services;
- Ensuring that billing matches the actual usage of cloud services made by the cloud service customer;
- Making payments to the cloud service provider;
- Keeping accounts in relation to the use of cloud services
- Request audit report

### 6.1.4 Cloud service integrator

MCDAs shall appoint a cloud service integrator rensonsible for the integration of cloud services with existing ICT systems, including application function and data.
The cloud service integrator's cloud computing activities includes connecting ICT systems to cloud services.

## 6.2 Cloud service provider

A cloud service provider is party that makes cloud services available to cloud service customers. The cloud service provider is responsible for dealing with the business relationship with cloud service customers. A cloud service provider may be a government agency or a private entity. The cloud service provider shall establish the following roles and responsibilities:

### 6.2.1 Cloud service operations manager

A cloud service provider shall appoint a cloud service operations manager responsible for performing all operational processes and procedures of the cloud service provider, ensuring that all services and associated infrastructure meet operational targets.
The cloud operations manager's cloud computing activities shall include:

- preparing systems;
- monitoring and administering services;
- managing assets and inventory;
- providing audit data.

### 6.2.2 Cloud service deployment manager

A cloud service provider shall appoint a service deployment manager responsible for the planning of the deployment of cloud service into production.
The cloud service deployment manager's activities shall include:

- defining environment and processes;
- defining and gathering metrics;
- defining deployment steps.

### 6.2.3 Cloud service manager

The cloud service provider shall appoint cloud service manager responsible for ensuring that the cloud service provider's services are available for use by cloud service customers, and that they function correctly and comply with targets specified in the service level agreement. The cloud service manager's activities shall include:

- providing cloud services;
- deploying and provisioning of cloud services;
- performing service level management.

### 6.2.4 Cloud service business manager

The cloud service provider shall appoint a cloud service business manager responsible for the business aspects of offering cloud services to cloud service customers. The cloud service business manager's cloud computing activities shall include:

- managing business plan to provide cloud services;
- managing customer relationships;
- managing financial processing

### 6.2.5 Customer support and care representative

The customer support and care representative shall be responsible for reacting to customer issues and queries in a timely and cost efficient way, with the goal of maintaining customer satisfaction with the cloud service provider and the cloud services offered.

The customer support and care representative's cloud computing activities includes handling customer requests.

### 6.2.6 Inter-cloud provider

The inter-cloud provider relies on one or more peer cloud service providers to provide part or all of the cloud services offered to cloud service customers by that inter-cloud provider. The inter-cloud provider's cloud computing activities shall include:

- managing peer cloud services;
- performing peering, federation, intermediation, aggregation and arbitrage.

### 6.2.7 Cloud service security and risk manager

The cloud service security and risk manager shall be responsible for ensuring that the cloud service provider appropriately manages the risks associated with the development, delivery, use and support of cloud services. The cloud service security and risk manager's cloud computing activities shall include:

- managing security and risks;
- designing and implementing service continuity ;
- ensuring compliance.

### 6.2.8 Network provider

The network provider is responsible for providing network connectivity and network services for the cloud service customer, cloud service partner and cloud service provider. The network provider's cloud computing activities shall include:

- providing network connectivity;
- delivering network services;
- offering dynamic control of network connectivity as an NaaS.

# 7.0 CROSS-CUTTING ASPECTS

## 7.1 Auditability

7.1.1 MCDAs shall ensure that cloud services are independently audited for assurance that those services are provided and used in consistency with the associated service agreements between them, cloud service providers and cloud service partners.

7.1.2 The MCDA shall ensure that governing agreements guarantee availability and security of data and evidence including records and logs of activities and conditions of the operational environments of all parties. This is necessary for the audit of the usage, environment, availability and performance of cloud services and associated resources.

## 7.2 Availability

MCDAs shall put in place measures to guarantee that cloud services are accessible and usable upon demand.

## 7.3 Governance

It is the responsibility of the MCDA to implement governance to rationalize SLAs and other contractual elements of the MCDA to cloud service provider relationship.

## 7.4 Interoperability

7.4.1 MCDAs shall ensure that they are able to interact with the cloud service and exchange information according to a prescribed method and obtain predictable results as per the agreed specification, one that is possibly standardized.

7.4.2 The MCDA shall be able to use widely available ICT facilities in-house when interacting with cloud services, avoiding the need to use proprietary or highly specialized software.

7.4.3 The MCDA shall have a consistent and interoperable interface to the cloud service management functionality and be able to interact with two or more cloud service providers without needing to deal with each provider in a specialized way.

7.4.4 The cloud service implementations shall support the evolution of the standards used, both from an earlier version of a standard to a later version, or from one standard to a different one, while minimizing disruptive changes.

## 7.5 Maintenance and versioning

7.5.1 Maintenance of cloud services shall be subject to governance practices that are transparent to the MCDA,

7.5.2 Maintenance shall be documented in the SLA for the cloud services and shall include the capability for the customer to report problems and request fixes and also a mechanism for the cloud service provider to notify the customer of pending maintenance changes and their schedule.

7.5.3 MCDAs shall ensure that appropriate labelling of a service is done to identify the version (or of components of a service, such as the operating system level used in an IaaS service), so that it is clear to the customer that a particular version is in use. The service shall be given a new version label when maintenance of a cloud service occurs.

7.5.4 Where significant changes are made to a service between two versions, the older version of the service shall be available in parallel with the new versions for an agreed period of time.

### 7.6 Performance

MCDAs shall ensure that metrics for performance are defined in the SLA for each performance condition identified and these metrics shall be monitored during operation of the cloud service to ensure that the service meets the performance terms of the SLA. The metrics shall include:
a. Availability of the service;
b. Response time to complete service requests;
c. Transaction rate at which service requests are executed;
d. Latency for service requests;
e. Data throughput rate (input and output);
f. Number of concurrent service requests (scalability);
g. Capacity of data storage;
h. for IaaS and PaaS) the number of concurrent execution threads available to an application;
i. (for IaaS and PaaS) the amount of memory (RAM) available to the running program;
j. Data centre network IP address pool and/or VLAN range capacity

### 7.7 Portability

a. MCDAs shall ensure that they avoid lock-in when they choose to use cloud services. They shall ensure that they can move cloud service customer data or their applications between multiple cloud service providers at low cost and with minimal disruption.

b. Cloud data portability:-MCDAs shall be able to copy their data into or out of a cloud service through network access or by physical transfer of storage devices.

c. Cloud application portability:- Cloud services shall allow the migration of items such as a fully-stopped virtual machine instance or a machine image (IaaS service) from one cloud service provider to another cloud service provider, or the migration of application components (PaaS service) from one cloud service provider to another. In both cases, there is a related aspect of the support of portability of metadata relating to the application components, providing information about the relationships of program components and about the required infrastructure for the program components (e.g., load balancing configuration, firewall settings).

### 7.8 Protection of personally identifiable information (PII)

a. MCDAs shall ensure the protection, assurance, proper and consistent collection, processing, communication, use and disposition of personally identifiable information (PII) in relation to cloud services.

b. MCDAs shall ensure adherence of cloud services to Kenya statutory, regulatory and legal requirements rules and regulations applied to the handling of PII

### 7.9 Resiliency

a. MCDAs shall implement a set of monitoring, preventive and responsive processes to enable a cloud service to provide continuous operations, or predictable and verifiable outages, through failure and recovery actions. These can include hardware, communication and/or software failures, and can occur as isolated incidents or in combination, including serial failure. These processes can include both automated and manual actions, usually spanning multiple systems, and thus their description and realization are part of the overall cloud infrastructure, not an independent function.

### 7.10 Reversibility

a. MCDAs shall put in place measures to retrieve their data and application artefacts and for the cloud service provider to delete all their data, as well as contractually specified cloud service derived data after an agreed period.

b. They shall ensure the "right to be forgotten" is implemented, in that the that once they indicate to the cloud service provider that their use of the service(s) will cease, there will be an orderly process for the cloud service customer to retrieve their data and their application artefacts and that the cloud service provider will delete all copies and not retain any materials belonging to them after an agreed period.

### 7.11 Security

Cloud security is fully described in the information security standard and stipulates the following;

a. MCDAs shall implement security capabilities for cloud services including those for access control, confidentiality, integrity and availability.

b. MCDAs shall implement facilities to enable early detection, diagnosis and fixing of cloud service and resource related problems; secure logging of access records, activity reports, session monitoring and packet inspections on the network; provision of firewalling, and malicious attack detection and prevention for the cloud service providers' systems. One user should not be able to disrupt other users' use of cloud services.

c. Intranet level security shall be provided on the network connecting the MCDA to the cloud service provider (for example, through the use of VPN capabilities).

### 7.8 Protection of personally identifiable information (PII)

d. MCDAs shall ensure a clear definition of the information security responsibilities between them and the provider to ensure that all aspects of security are covered, to avoid responsibility ambiguity.

e. MCDAs shall implement security measures that address the threats affecting the specific cloud service category i.e IaaS, PaaS, SaaS.

f. MCDAs shall implement security measures that address the threats affecting  the specific cloud deployment models

g. MCDAs shall properly catalogue their data and identify its sensitivity and the risk to the business of its leakage, loss or corruption. (See Information Security Standard on how to identify the sensitivity of data).

h. In case of encryption, MCDAs shall ensure the responsibility for key management is clearly defined and the logical and physical control of the keys, as well as the data are implemented

### 7.12 Service levels and service level agreements

a. MCDAs shall ensure service level agreements are in place to assure an agreed upon quality of service with cloud service provider.

b. The cloud computing service level agreement (cloud SLA) is a service level agreement b. The SLA shall cover terms regarding

- The quality of service
- Security
- Performance and remedies for failures to meet the terms of the SLA.

c. The SLA shall list a set of promises explicitly not made to MCDAs, i.e., limitations and obligations that cloud service customers need to accept.

d. The cloud SLA shall define the classification of data objects (i.e., cloud service customer data, cloud service provider data, and cloud service derived data), who has access and control of data objects in these data classifications and how they will be used.

e. The service level agreement shall specify information relating to the availability of the services, the confidentiality and integrity of the services and the access controls which apply to the services. The service level agreement shall specify how any personally identifiable information will be handled in relation to the cloud services.

f. MCDAs shall review he service agreement – alternatively known as the master service agreement (MSA), terms of service (ToS), terms and conditions (T&C), or simply “the contract” – (which is the higher order document in agreements between parties and the service level agreement (SLA) is subservient) to ensure they are aligned.

# APPENDIX 1: CLOUD COMPUTING DEPLOYMENT MODELS

The rapid transition towards cloud computing has increased the demands for more deployment models. MCDAs shall select cloud computing deployment models depending on their data sensitivity and management requirements

### 1.1 Private Cloud

Private cloud (internal cloud) infrastructure is dedicated to a single particular organization or group.
A private cloud is not shared with other organizations and can be privately owned or leased. It may be managed by the organization or a third party and can exist at on-premises or off-premises. A Private cloud is more expensive and secure when compared to public cloud. A Private cloud is hosted inside the organization's firewall and can be accessed by users within the organization via intranet.
Private clouds are flexible and service-based. Processes, services and data are managed within the organization. In private cloud there are no additional security regulations, legal requirements or bandwidth limitations that can be present in a public cloud environment, by using a private cloud, the cloud service providers and the clients have optimized control of the infrastructure and improved security, since user's access and the networks used are restricted. Private clouds are classified into on premise private cloud and externally hosted private cloud. The key characteristics of private cloud include enhanced security measure, dedicated resources and better customization.

### 1.2 Public Cloud

A public cloud (external cloud) infrastructure is offered via web applications as well as web services over the internet to the public or a large industry group and is owned by an organization selling cloud services. A public cloud provides an elastic, cost-effective way to deploy IT solutions. The term public does not mean that users' data is publicly visible as the public cloud dealers always deliver an authorized and authentication access control for the clients. This type of cloud is known for its availability to the public or bigger of the institution from the third party that is based on providing services to its client through the internet. It is considered as the easiest to be setup since it liberates the user from burdens of equipment, application or transfer speed costs. This cloud provides a cost-effective and elastics meaning to solutions deployed Organization pays for only those services and resources they have used. Public cloud involves applications such as customer relationship management (CRM), messaging and office productivity. The key characteristics of public cloud include availability and reliability, freedom of self-service, pay as you use flexibility and elasticity.

### 1.3 Hybrid Cloud

This cloud deployment model exists due to mixed needs of an organization. It is combination of two or more cloud service deployment models (Private, Public, and Community).
Organizations may host critical applications on private clouds and applications with relatively less security concerns on the public cloud.

A combination of a public and a private cloud is joined together for the purpose of keeping business-critical data and services in their control on private cloud and outsourcing less-critical processing to the public cloud. Hybrid cloud enables organizations to maintain their cost and security at a reasonable level; but at the same time, issues regarding standardization and interoperability of clouds should be considered. Some key characteristics of hybrid cloud include optimal use of resources, data center consolidation, high availability and risk transfer.

### 1.4 Community Cloud

A community cloud is a shared infrastructure by several organizations and supports a specific community that has shared concerns e.g., mission, security requirements, policy, and compliance considerations.

The community cloud infrastructure is supervised, then utilized by a different number of institutions that have the same core business, projects or shareable demands infrastructures such as software and hardware so that the running costs of IT can be reduced It may be managed by the organizations or a third party and may exist at on-premises or off-premises. Community cloud offers higher level of privacy, security and policy compliances. Examples of community clouds include Google's Government Cloud, academic clouds, etc.

### The Comparative Analysis of the Types of Cloud Deployment Models

To facilitate the choice of the appropriate deployment models of cloud computing by opting for the ones with the most business-critical features, MCDAs shall be guided by the following matrix

The comparative analysis of the best cloud deployment models

| | Public | Private | Community | Hybrid |
|---|---|---|---|---|
| **Ease of setup and use** | Easy | Requires IT proficiency | Requires IT proficiency | Requires IT proficiency |
| **Data security and privacy** | Low | High | Comparatively high | High |
| **Data control** | Little to none | High | Comparatively high | Comparatively high |
| **Reliability** | Vulnerable | High | Comparatively high | High |
| **Scalability and flexibility** | High | High | Fixed capacity | High |
| **Cost-effectiveness** | The cheapest one | Cost-intensive, the most expensive one | Cost is shared among community members | Cheaper than a private model but more costly than a public one |
| **Demand for in-house hardware** | No | Depends | Depends | Depends |

# APPENDIX 2 CLOUD COMPUTING SERVICE DELIVERY MODELS

Cloud computing consists of various types of services that are delivered to the users as on-demand. MCDAs shall select cloud computing service delivery models depending on their computing requirements. The cloud service delivery models include:

## 2.1 Software as a Service (SaaS)

In this model, the provider facilitates the clients with licensed applications running on a cloud infrastructure through a thin client interface such as a web browser over the internet on pay-per-use pricing pattern. Clients are not required to manage or control the underlying cloud infrastructure including network, servers, operating systems or storage. Currently, SaaS is a perfect model to access the light weight applications such as word processor, media player etc. However when it comes to heavy weight applications such as playing online 3D games, the performance of SaaS may go down due to buffering time. Several provide SaaS Vendors such as Zoho Suite, Apple's MobileMe and Google Docs. Normally the provider resides and maintains client hired applications on a specific virtual machine in a virtualized cloud environment.

## 2.2 Platform as a Service (PaaS)

In this model, provider facilitates the clients with the programming language platforms and software such as but not limited to Java, Python or .Net, to deploy their created or acquired applications on the cloud infrastructure over the internet with Application Program Interfaces (APIs) or website portals. PaaS providers facilitate several services for application developers such as virtual development environment, application standards based on the developers' requirements, configured toolkits for the virtual development environment and ready-made distribution channel for public application developers. Clients have control over the deployed applications and possibly application hosting environment configurations. However, clients do not have control over the underlying cloud infrastructure including network, servers, operating systems or storage. In PaaS model, it's the cloud provider's responsibility to secure the computing platform and development environment, while the clients must secure their applications themselves. Example of PaaS providers are Google App Engine, Force.com, and Microsoft Azure.

## 2.3 Infrastructure as a Service (IaaS)

In this cloud service delivery model the provider facilitates the capability to clients for provision processing, storage, networks and other fundamental computing resources where the clients are able to deploy and run arbitrary software that includes operating systems and applications. IaaS delivers a platform virtualization environment as a service. Clients have control over memory, CPU, IP addresses, operating systems; storage, deployed applications and possibly limited control of selected networking components e.g., host firewalls. Clients do not manage or control the underlying cloud infrastructure. In IaaS model, cloud providers must provide a trusted host and Virtual Machine Monitoring (VMM) environment for the clients. Example of IaaS providers are Amazon EC2 and S3, Sun Microsystems and Dropbox.
Others service models include:-
Integration as a Service (IgaaS), Business Process as a Service (BPaaS), Business Process as a Service (BPaaS), Management as a Service (MaaS, Security as a Service (SecaaS)

# APPENDIX 3: GOVERNANCE OF CLOUD COMPUTING SERVICES

| Requirement | Checklist | Comments |
|---|---|---|
| **Governance of Cloud Computing Services** | 1. Determine if the IT, information security and key business functions have defined integrated governance framework and monitoring processes.<br>2. Determine if the IT and information security functions and key business units are actively involved in the establishment of SLAs and contractual obligations.<br>3. Determine if the information security function has performed a gap analysis of the service provider's information security capabilities against the organization's information security policies and threat and vulnerabilities/IT risk emanating from the transition to cloud computing.<br>4. Determine if the cloud provider has identified control objectives for the provided services.<br>5. Determine if the organization maintains an inventory of all services provided via the cloud.<br>6. Determine that the business cannot procure cloud services without the involvement of information technology and information security | |
| | 1. Determine if the responsibilities for governance are documented and approved by the service provider and customer.<br>2. Determine if reporting relationships between the service provider and customer are clearly defined, identifying the responsibilities of both organizations' governance processes. | |
| | 1. Obtain the SLAs; determine if the SLAs reflect the business requirements.<br>2. Determine that the SLAs can be monitored using measurable metrics and that the metrics provide appropriate oversight and early warning of unacceptable performance.<br>3. Determine if the SLA contains clauses that ensure services in case of vendor acquisition or changes in management. | |

| Requirement | Checklist | Comments |
|---|---|---|
| Enterprise Risk Management | 1. Determine if the organization has an ERM model.<br>2. If an ERM model has been implemented, determine if the cloud computing risk assessment is in alignment with the enterprise ERM.<br>3. Determine if the services provided by the service provider and the processing model selected will limit the availability or execution of required information security activities, such as:<br>- Restrictions on vulnerability assessments and penetration testing<br>- Availability of audit logs<br>- Access to activity monitoring reports<br>- Segregation of duties<br>4. Determine if the risk management approach includes the following:<br>- Identification and valuation of assets and services<br>- Identification and analysis of threats and vulnerabilities with their potential impact on assets<br>- Analysis of the likelihood of events using a scenario approach<br>- Documented management approval of risk acceptance levels and criteria<br>- Risk action plans (control, avoid, transfer, accept)<br>5. Determine if, during the risk assessment, the identified assets include both service-provider- and customer-owned assets and if the information security classifications used in the risk assessments are aligned.<br>6. Determine if the risk assessment includes the service model and the service provider's capabilities and financial condition. | |

| Requirement | Checklist | Comments |
|---|---|---|
| | 1. Determine if the results of the risk action plans are incorporated into the SLAs.<br>2. Determine if a joint service provider/customer risk assessment was conducted to verify if all reasonable risk has been identified and if risk remediation alternatives were identified and documented.<br>3. Where the risk assessment of the service provider has identified risk management that is either ineffective or not comprehensive, determine if the organization has performed an analysis of their compensating controls and if such controls will address the service provider's control shortcomings. | |
| | 1. Determine if management has performed an analysis of their quantification and acceptance of residual risk prior to implementing a cloud solution.<br>2. Determine if the individual accepting such risk has the authority to make this decision. | |
| Information Risk Management | 1. Determine if a risk framework has been identified and approved.<br>2. Determine if a maturity model is used to assess the effectiveness.<br>3. Review the results of the maturity model results, and determine if the lack of maturity materially affects the audit objectives.<br>- Documented management approval of risk acceptance levels and criteria<br>- Risk action plans (control, avoid, transfer, accept) | |

| | | |
|---|---|---|
| | 1. Identify the technology controls and contractual requirements necessary to make fact-based information risk decisions. Consider:<br>- Information usage<br>- Access controls<br>- Security controls<br>- Location management<br>- Privacy controls<br>2. For SaaS, determine that the organization has identified analytical information required from the service provider to support contractual obligations relating to performance, security and attainment of SLAs.<br>3. Obtain the analytical data requirements, and determine if the organization routinely monitors and evaluates the attainment of SLAs.<br>4. For PaaS, determine that the organization has identified the information available and the control practices necessary to manage the application and development processes effectively that address availability, confidentiality, data ownership, concerns around e-discovery, privacy and legal issues.<br>5. Determine if the organization has established monitoring practices to identify risk issues.<br>6. For IaaS, determine that the organization has identified and monitors the control and security processes necessary to provide a secure operating environment.<br>7. Determine if the service provider makes available metrics and controls to assist customers in implementing their information risk management requirements. | |
| **Third-party Management** | 1. Determine if the service provider routinely has independent third-party assessments performed and issued.<br>2. Determine if the scope of the third-party assessment includes descriptions of the following service provider processes:<br>- Incident management<br>- Business continuity and disaster recovery<br>- Backup and co-location facilities<br>3. Determine if the service provider routinely performs internal assessments of conformance to its own policies, procedures and availability of control metrics. | |

| Requirement | Checklist | Comments |
|---|---|---|
| | 1. Determine if the service provider's information security governance, risk management and compliance processes are routinely assessed and include:<br>- Risk assessments and reviews of facilities and services for control weaknesses<br>- Definition of critical service and information security success factors and key performance indicators<br>- Frequency of assessments<br>- Mitigation procedures to ensure timely completion of identified issues<br>- Review of legal, regulatory, industry and contractual requirements for comprehensiveness<br>- Cloud service provider's oversight of risk from its own critical vendors<br>- Terms of use due diligence to identify roles, responsibilities and accountability of the service provider<br>- Legal review for local contract provisions, enforceability and laws pertaining to jurisdictional issues that are the responsibility of their service provider | |
| | 1. Determine if the customer has performed due diligence with respect to the service provider's information security governance, risk management and compliance processes (see section Operations\Compliance CO3 Control 6 testing)<br>2. Determine if the customer has prepared for the loss of service provider services including:<br>- A business continuity and disaster recovery plan for various processing interruption scenarios<br>- Tests of the business continuity and disaster plan<br>- Inclusion of the business users and their business impact analysis in the continuity plan | |

| Requirement | Checklist | Comments |
|---|---|---|
| **Legal and Electronic Discovery** | 1. Determine if the contractual agreement defines both parties' responsibilities related to discovery searches, litigation holds, preservation of evidence and expert testimony.<br>2. Determine that the service provider contract requires assurance to the customer that their data are preserved as recorded, including the primary data and secondary information ( metadata and logs).<br>3. Determine that service providers understand their contractual obligations to provide guardianship of the customer's data. Review contracts to determine this is specifically addressed.<br>4. Determine that the customer's duty of care includes full scope of contract monitoring, including:<br>- Precontract due diligence<br>- Contract term negotiation<br>- Transfer of data custodianship<br>- Contract termination or renegotiation<br>- Transition from processing<br>5. Determine that the contract stipulates and both parties understand their obligations for both expected and unexpected termination of the relationship during and after negotiations and that the contract and/or pre-contract agreement provides for the orderly and timely return or secure disposal of assets.<br>6. Determine that the contractual obligations specifically identify suspected data breach responsibilities of both parties and cooperative processes to be implemented during the investigation and any follow-up actions.<br>7. Determine that the agreement provides for the customer to have access to the service provider's performance and tests for vulnerabilities on a regular basis.<br>8. Determine that the contract establishes rights and obligations for both parties during transition at the conclusion of the relationship and after the contract terminates. | |

| | | |
|---|---|---|
| | 9. Determine if the contract establishes the following data protection processes:<br>- Full disclosure of the service provider's internal security practices and procedures<br>- Data retention policies in conformance with local jurisdiction requirements<br>- Reporting on geographical location of customer data<br>- Circumstances in which data can be seized and notification of any such events<br>- Notification of subpoena or discovery concerning any customer data or processes<br>- Penalties for data breaches<br>- Protection against data contamination between customers (compartmentalization)<br>10. Encryption requirements for data in transit, at rest and for backup are clearly identified in the cloud contractual agreement. | |
| | 1. Determine that the customer has considered and established controls within the contractual obligations to ensure retention of data and intellectual property ownership.<br>2. Determine that the customer has considered and established controls within the contractual obligations to protect personal data that must remain private.<br>3. Determine that the customer has developed appropriate issue monitoring processes to oversee the service provider's performance of contract requirements.<br>4. Determine that the customer has established internal issue monitoring to identify customer contractual compliance deficiencies. | |
| **Legal Compliance** | 1. Determine if cross-border and local laws are defined and considered in the contract.<br>2. Determine if the service provider and customer have an agreed-upon unified process for responding to subpoenas, service of process and other legal requests. | |

| | | |
|---|---|---|
| **Right to Audit** | 1. Review the audit rights in the contract, and determine if audit activities can be restricted or curtailed by the service provider.<br>2. If audit rights issues are identified, prepare an appropriate summary of the findings and escalate to service provider relationship management. If necessary and appropriate, escalate to the audit committee. | |
| | 1. Obtain the third-party report.<br>2. Determine that the report addresses the control environment utilized by the customer.<br>3. Determine that the descriptions and processes are relevant to the service provider's customers.<br>4. Determine that the report has described the key controls necessary for the reviewer to assess compliance with appropriate control objectives.<br>5. Determine that the report and testing will satisfy the customer's assurance charter and compliance requirements of all regulators having jurisdiction over the customer.<br>6. Using the approved customer audit universe, compare the scope of the audit universe to the scope of the third-party report; identify gaps in the latter requiring additional assurance coverage.<br>7. Determine if the service provider relationship crosses international boundaries and if this affects the ability to rely upon the third-party report. | |
| **Auditability** | 1. Determine if supplementary assurance assessments (if a third-party review has been provided) or primary assurance assessments are required.<br>2. Generate appropriate requests to the service provider, and schedule reviews. Note: Utilize appropriate audit/assurance programs for these reviews. | |

| | | |
|---|---|---|
| **Compliance Scope** | 1. Determine if the customer has identified the legal and regulatory requirements of which it must comply.<br>2. Determine if the customer has aggregated requirements to minimize duplication.<br>3. Using the documentation assembled in the Governance and Enterprise Risk Management, Legal and Electronic Discovery, and Right to Audit sections, perform a gap analysis against the data regulations to determine if there are any regulatory requirements that cannot be satisfied by the cloud computing model. | |
| | 1. Determine that the responsibilities for data protection are based on the risk for the deployment scenario.<br>2. Review the contract to determine the assignment of responsibilities.<br>3. Based on the contract, determine if the customer and service provider each have established appropriate data protection measures within the scope of their responsibilities. | |
| **Certifications** | 1. Determine if the service provider has received ISO 27001 certification. If so, adjust the scope of the audit/assurance program to reflect this certification. | |
| **Service Transition Planning** | **All cloud solutions**<br>1. Determine that the hardware and software requirements and feasibility for moving from the existing service provider (legacy provider) to another provider (new provider) have been documented for each cloud computing initiative.<br>2. Determine that an alternate service provider for each legacy service provider has been identified and that the feasibility for transferring processes has been evaluated.<br>3. Determine if the feasibility analysis includes procedures and time estimates to move large volumes of data, if applicable.<br>4. Determine if the portability process has been tested. | |

| | | |
|---|---|---|
| | **IaaS cloud solutions**<br>1. Determine if the feasibility analysis of transferring from the IaaS legacy service provider involves any proprietary functions or processes that would preclude or delay the transferring of operations.<br>2. Determine if the portability analysis includes processes to protect the intellectual property and data from the legacy service provider once the transfer has been completed.<br>PaaS cloud solutions<br>1. Determine if the feasibility analysis includes identification of application components and modules that are proprietary and would require special programming during transfer.<br>2. Determine if the portability analysis includes:<br>- Translation functions to a new service provider<br>- Interim processing until a new service provider is operational<br>- Testing of new processes before promotion to a production environment at the new service provider<br>SaaS cloud solutions<br>1. Determine if the portability analysis includes:<br>- A plan to back up the data in a format that is usable by other applications<br>- Routine backup of data<br>- Identification of custom tools required to process the data and plans to redevelop<br>- Testing of the new service provider's application and due diligence before conversions. | |

# APPENDIX 4: RISK ASSESSMENT CHECKLIST

- My data or functionality to be moved to the cloud is not business critical
- The provider was audited by a third party to determine their compliance with GoK information security standards?
- I have reviewed the vendor's business continuity and disaster recovery plan
- I will maintain an up-to-date backup copy of my data
- My data or business functionality will be replicated with a second vendor
- The network connection between me and the vendor's network is adequate
- The Service Level Agreement (SLA) guarantees adequate system availability
- Scheduled outages are acceptable both in duration and time of day
- Scheduled outages affect the guaranteed percentage of system availability
- I would receive adequate compensation for a breach of the SLA or contract
- Redundancy mechanisms and offsite backups prevent data corruption or loss
- If I accidentally delete a file or other data, the vendor can quickly restore it
- I can increase my use of the vendor's computing resources at short notice
- I can easily move my data to another vendor or in-house
- I can easily move my standardised application to another vendor or in-house
- My choice of cloud-sharing model aligns with my risk tolerance
- My data is not too sensitive to store or process in the cloud
- I can meet the legislative obligations to protect and manage my data
- I know and accept the privacy laws of countries that have access to my data
- Strong encryption approved by ASD protects my sensitive data at all times
- The vendor suitably sanitises storage media storing my data at its end of life
- The vendor securely monitors the computers that store or process my data
- I can use my existing tools to monitor my use of the vendor's services
- I retain legal ownership of my data
- The vendor has a secure gateway environment
- The vendor's gateway is certified by an authoritative third party
- The vendor provides a suitable email content filtering capability
- The vendor's security posture is supported by policies and processes
- The vendor's security posture is supported by direct technical controls
- I can audit the vendor's security or access reputable third-party audit reports
- The vendor supports the identity and access management system that I use
- Users access and store sensitive data only via trusted operating environments
- The vendor uses endorsed physical security products and devices
- The vendor's procurement process for software and hardware is trustworthy
- The vendor adequately separates me and my data from other customers
- Using the vendor's cloud does not weaken my network security posture
- I have the option of using computers that are dedicated to my exclusive use
- When I delete my data, the storage media is sanitised before being reused
- The vendor does not know the password or key used to decrypt my data
- The vendor performs appropriate personnel vetting and employment checks
- Actions performed by the vendor's employees are logged and reviewed
- Visitors to the vendor's data centres are positively identified and escorted
- Vendor data centres have cable management practices to identify tampering
- Vendor security considerations apply equally to the vendor's subcontractors
- The vendor is contactable and provides timely responses and support
- I have reviewed the vendor's security incident response plan

- The vendor's employees are trained to detect and handle security incidents
- The vendor will notify me of security incidents
- The vendor will assist me with security investigations and legal discovery
- I can access audit logs and other evidence to perform a forensic investigation
- I receive adequate compensation for a security breach caused by the vendor
- Storage media storing sensitive data can be adequately sanitised

# APPENDIX 5: CLOUD SERVICE PARTNER

A cloud service partner (CSN) is a party which is engaged in support of, or auxiliary to, activities of either the cloud service provider or the cloud service customer, or both.
A cloud service partner's cloud computing activities vary depending on the type of partner and their relationship with the cloud service provider and the cloud service customer. The roles associted with the cloud service partner shall include:

## 5.1 Cloud service developer

The cloud service developer is responsible for designing, developing, testing and maintaining the implementation of a cloud service. This can involve composing the service implementation from existing service implementations.
The cloud service developer's cloud computing activities shall include:

- design, create and maintain service components ;
- composing services;
- testing services.

## 5.2 Cloud auditor

The cloud auditor is responsible for conducting audit of the provisions and use of cloud services. A cloud audit typically covers operations, performance and security, and examines whether a specified set of audit criteria are met.
The cloud auditor's cloud computing activities shall include:

- performing audit;
- reporting audit results.

## 5.3 Cloud service broker

The cloud service broker is responsible for negotiating relationships between cloud service customers and cloud service providers. The cloud computing activities of a cloud service broker include:

- acquiring and assessing customers;
- assessing marketplace;
- seting up legal agreements;

# APPENDIX 6: CHECKLISTS

| CRITERIA | RATING | |
|---|---|---|
| | Y | N |
| 5.1 Use of Cloud Computing services complies with all current laws, Information security standard, and risk management policies. | | |
| 5.16 MCDA hosts critical applications in the public cloud [Refer to Systems and Applications Standard] | | |
| 5.19 To mitigate against risks associated with vendor lock-in, MCDA has prepared an exit strategy as part of contracting with the Cloud Service Provider. | | |
| 5.22 MCDA has obtained copies of potential cloud service providers' most recent standards-based security assessment/assurance as early in the procurement cycle as possible. | | |
| 5.25 Cloud solutions that store personally identifiable citizen data are within the boundaries of Kenya. | | |
| 5.28 MCDA has determined their licensing needs projected over a period and ensure the cloud provider meets the needs. | | |
| 5.31 MCDA handling data on foreigners has ensured compliance to applicable laws of their countries of origin. | | |
| 5.34 If data stored with a cloud service provider is to be encrypted this has been done using cryptographic keys owned and managed by the Government of Kenya (See information security Standard) | | |
| 5.37 Mobile apps are cloud services if "they store, process or transport MCDA information outside the network boundary". | | |
| 5.40 The cloud computing solution has been considered after a thorough risk evaluation (as per GoK Information Security Standard) has been completed, reviewed and accepted by the MCDAs Chief Information Security Officer or delegate. | | |
| 5.43 Cloud computing solutions are supported by facilities that meet Uptime Institute Tier-3 or higher rating. Anything less than this needs extra resiliency capabilities. | | |
| 5.46 MCDA has ensured that adequate safeguards are in place to secure authentication, authorization, and other identity and access management functions, and are suitable for the organization. | | |
| 5.49 MCDA has acquired cloud solutions in reference to the list of accredited cloud providers provided by ICT Authority. | | |
| 5.52 MCDA has ensured that negotiated SLA requirements supersede Master Service agreements. | | |

| CRITERIA | RATING | | |
|---|---|---|---|
| | Y | N | % |
| 5.55 Contracts with cloud service providers include: | | | |
| 5.57.1 An exit plan especially requiring the cloud provider to provide a way for the MCDA to extract data easily and economically. | | | |
| 5.57.4 Requirement for data sanitization from storage media, electronic and physical access rights be revoked from the cloud provider, and assets provided to the provider returned or, if not possible, be securely purged. | | | |
| 5.57.7 Non-Disclosure Agreement (recommended before provisioning any service) | | | |
| 5.57.10 Full disclosure in case of breaches to regulated information. | | | |
| 5.57.13 Data ownership (the Government of Kenya retains exclusive ownership of ALL data held in a cloud provider's solution which was entered by MCDA, systems or affiliates in all media forms e.g. online, backup and archive etc.) | | | |
| 5.57.16 Any other standard intellectual property clauses (as are relevant to the service) | | | |
| 5.34 If data stored with a cloud service provider is to be encrypted this has been done using cryptographic keys owned and managed by the Government of Kenya (See information security Standard) | | | |
| 5.37 Mobile apps are cloud services if "they store, process or transport MCDA information outside the network boundary". | | | |
| 5.40 The cloud computing solution has been considered after a thorough risk evaluation (as per GoK Information Security Standard) has been completed, reviewed and accepted by the MCDAs Chief Information Security Officer or delegate. | | | |
| 5.43 Cloud computing solutions are supported by facilities that meet Uptime Institute Tier-3 or higher rating. Anything less than this needs extra resiliency capabilities. | | | |
| 5.46 MCDA has ensured that adequate safeguards are in place to secure authentication, authorization, and other identity and access management functions, and are suitable for the organization. | | | |
| 5.49 MCDA has acquired cloud solutions in reference to the list of accredited cloud providers provided by ICT Authority. | | | |
| 5.52 MCDA has ensured that negotiated SLA requirements supersede Master Service agreements. | | | |

| CRITERIA | RATING | | |
|---|---|---|---|
| | Y | N | % |
| 5.2.1 Data location (It should be explicitly stated in contracts that it should be in Kenya) | | | |
| 5.57.22 Privacy legislation compliance | | | |
| 5.57.25 Service Level Agreements (to meet availability, performance, and disaster recovery requirements | | | |
| 5.57.28 Service management processes | | | |
| 5.57.31 Procedures for incident response and ensure that they meet the requirements of the organization | | | |
| 5.57.34 Audit mechanisms and tools to ensure organizational practices are followed throughout the system lifecycle | | | |
| 5.57.40 The application of appropriate retention policies to stored data based on its classification - this means the cloud service provider's solution must not hinder compliance with the Public Records Act | | | |
| 5.57.43 A clear process documenting the responsibilities of each party with respect to extracting MCDA data and destroying data at the end of the contract | | | |
| 5.37 Provision for a cloud service provider being taken over/bought-out by another organisation(this should include ensuring the ownership, access rights and protection of any data the MCDA owns cannot be lost when there is a change of cloud service provider ownership. | | | |

# 6.0 USER CONTEXT OF CLOUD COMPUTING

| CRITERIA | RATING | | |
|---|---|---|---|
| | Y | N | % |
| **6.1 Cloud service customer** | | | |
| Cloud service customers are MCDAs that have a business relationship with a cloud service provider for the purpose of using cloud services. These MCDA has established the following roles and responsibilities | | | |
| **6.2.9 Cloud Service User** | | | |
| MCDA acquring cloud services has identified cloud service users to consume the cloud services.<br>The use of cloud service activities involves<br>• The provision of user credentials to enable the cloud service provider to authenticate the user and grant access to the cloud service;<br>• The invocation of the cloud service, which then operates and delivers its specified outcomes. | | | |
| | | | |
| | | | |
| | | | |
| **6.2.10 Cloud service administrator** | | | |
| MCDA has appointed a cloud service administrator; | | | |
| The cloud service administrator has ensured the smooth operation of the customer's use of cloud services, and that those cloud services are running well with the customer's existing ICT systems and applications. The cloud service administrator has overseen all the operational processes relating to the use of cloud services and acts as the focal point for technical communications between the cloud service customer and the cloud service provider. | | | |
| The cloud service administrator's cloud computing activities include: | | | |
| • perform service trial; | | | |
| • monitor service; | | | |
| • administer service security; | | | |
| • provide billing and usage report; | | | |
| • handle problem reports; | | | |
| • administer tenancies . | | | |
| **6.2.11 Cloud service business manager** | | | |
| MCDAs shall appoint a cloud service business manager; | | | |
| The Cloud service business manager has ensured that business goals are met through the acquisition and use of cloud services in a cost efficient way. The main responsibilities of the cloud service business manager concern financial and legal aspects of the use of cloud services, including approval, on-going ownership and accountability. | | | |

| | | | |
|---|---|---|---|
| The cloud service business manager's cloud computing activities include: | | | |
| • adjusting business plan to accommodate the use of cloud services; | | | |
| • tracking the use of the services and dealing with accounting and financial management; | | | |
| • handling billing/invoices received from the cloud service provider for the use made of cloud services; | | | |
| • ensuring that billing matches the actual usage of cloud services made by the cloud service customer; | | | |
| • making payments to the cloud service provider; | | | |
| • keeping accounts in relation to the use of cloud services | | | |
| • request audit report | | | |
| **6.2.12 Cloud service integrator** | | | |
| MCDA has appointed a cloud service integrator rensonsible for the integration of cloud services with existing ICT systems, including application function and data. | | | |
| The cloud service integrator's cloud computing activities includes connecting ICT systems to cloud services. | | | |
| **6.3 Cloud service provider** | | | |
| A cloud service provider is party that makes cloud services available to cloud service customers. The cloud service provider is responsible for dealing with the business relationship with cloud service customers. A cloud service provider may be a government agency or a private entity. The cloud service provider shall establish the following roles and responsibilities: | | | |
| **6.3.1 Cloud service operations manager** | | | |
| A cloud service provider has appointed a cloud service operations manager responsible for performing all operational processes and procedures of the cloud service provider, ensuring that all services and associated infrastructure meet operational targets. | | | |
| The cloud operations manager's cloud computing activities include: | | | |
| • preparing systems; | | | |
| • monitoring and administering services; | | | |
| • managing assets and inventory; | | | |
| • providing audit data. | | | |

| **6.3.2 Cloud Service Deployment Manager** | | | |
|---|---|---|---|
| A cloud service provider has appointed a service deployment manager responsible for the planning of the deployment of cloud service into production. | | | |
| The cloud service deployment manager's activities include: | | | |
| • defining environment and processes; | | | |
| • defining and gathering metrics; | | | |
| • defining deployment steps. | | | |
| **6.3.3 Cloud service manager**<br>The cloud service provider has appointed cloud service manager responsible for ensuring that the cloud service provider's services are available for use by cloud service customers, and that they function correctly and comply with targets specified in the service level agreement. The cloud service manager's activities shall include:<br>• providing cloud services;<br>• deploying and provisioning of cloud services;<br>• performing service level management. | | | |
| **6.3.4 Cloud service business manager**<br>The cloud service provider has appointed a cloud service business manager responsible for the business aspects of offering cloud services to cloud service customers. The cloud service business manager's cloud computing activities shall include:<br>• managing business plan to provide cloud services;<br>• managing customer relationships;<br>• managing financial processing | | | |
| **6.3.5 Inter-cloud provider**<br>The inter-cloud provider relies on one or more peer cloud service providers to provide part or all of the cloud services offered to cloud service customers by that inter-cloud provider. The inter-cloud provider's cloud computing activities include:<br>• managing peer cloud services;<br>• performing peering, federation, intermediation, aggregation and arbitrage. | | | |
| **6.3.6 Customer support and care representative**<br>The customer support and care representative is responsible for reacting to customer issues and queries in a timely and cost efficient way, with the goal of maintaining customer satisfaction with the cloud service provider and the cloud services offered.<br>The customer support and care representative's cloud computing activities includes handling customer requests. | | | |

| | | | |
|---|---|---|---|
| **6.3.7 Cloud service security and risk manager** | | | |
| The cloud service security and risk manager is responsible for ensuring that the cloud service provider appropriately manages the risks associated with the development, delivery, use and support of cloud services. The cloud service security and risk manager's cloud computing activities include: | | | |
| • managing security and risks; | | | |
| • designing and implementing service continuity ; | | | |
| • ensuring compliance. | | | |
| | | | |
| **6.3.8 Network provider** | | | |
| The network provider is responsible for providing network connectivity and network services for the cloud service customer, cloud service partner and cloud service provider. The network provider's cloud computing activities shall include: | | | |
| • providing network connectivity;<br>• delivering network services;<br>• offering dynamic control of network connectivity as an NaaS. | | | |

# 7.0 CROSS-CUTTING ASPECTS

| | | | |
|---|---|---|---|
| **7.1 Auditability** | | | |
| | | | |
| 7.1.1 MCDAs ensures that cloud services are independently audited for assurance that those services are provided and used in consistency with the associated service agreements between them, cloud service providers and cloud service partners | | | |
| 7.1.2 The MCDA ensures that governing agreements guarantee availability and security of data and evidence including records and logs of activities and conditions of the operational environments of all parties. This is necessary for the audit of the usage, environment, availability and performance of cloud services and associated resources. | | | |
| | | | |
| | | | |
| **7.2 Availability**<br>MCDA has put in place measures to guarantee that cloud services are accessible and usable upon demand. | | | |
| **7.3 Governance**<br>It is the responsibility of the MCDA to implement governance to rationalize SLAs and other contractual elements of the MCDA to cloud service provider relationship. | | | |
| **7.4 Interoperability**<br>7.4.1 MCDAs has ensured that they are able to interact with the cloud service and exchange information according to a prescribed method and obtain predictable results as per the agreed specification, one that is possibly standardized.<br>7.4.2 The MCDA is able to use widely available ICT facilities in-house when interacting with cloud services, avoiding the need to use proprietary or highly specialized software.<br>7.4.3 The MCDA has a consistent and interoperable interface to the cloud service management functionality and be able to interact with two or more cloud service providers without needing to deal with each provider in a specialized way.<br>7.4.4 The cloud service implementations supports the evolution of the standards used, both from an earlier version of a standard to a later version, or from one standard to a different one, while minimizing disruptive changes. | | | |

| | | | |
|---|---|---|---|
| **7.5 Maintenance and versioning**<br>7.5.1 Maintenance of cloud services is subject to governance practices that are transparent to the MCDA,<br>7.5.2 Maintenance is documented in the SLA for the cloud services and shall include the capability for the customer to report problems and request fixes and also a mechanism for the cloud service provider to notify the customer of pending maintenance changes and their schedule.<br>7.5.3 MCDA ensures that appropriate labelling of a service is done to identify the version (or of components of a service, such as the operating system level used in an IaaS service), so that it is clear to the customer that a particular version is in use. The service shall be given a new version label when maintenance of a cloud service occurs.<br>7.5.4 Where significant changes are made to a service between two versions, the older version of the service is made available in parallel with the new versions for an agreed period of time. | | | |
| **7.6 Performance**<br>MCDA ensures that metrics for performance are defined in the SLA for each performance condition identified and these metrics shall be monitored during operation of the cloud service to ensure that the service meets the performance terms of the SLA. The metrics shall include:<br>a. Availability of the service;<br>b. Response time to complete service requests;<br>c. Transaction rate at which service requests are executed;<br>d. Latency for service requests;<br>e. Data throughput rate (input and output);<br>f. Number of concurrent service requests (scalability);<br>g. Capacity of data storage;<br>h. (for IaaS and PaaS) the number of concurrent execution threads available to an application;<br>i. (for IaaS and PaaS) the amount of memory (RAM) available to the running program;<br>j. Data centre network IP address pool and/or VLAN range capacity | | | |

| | | | |
|---|---|---|---|
| **7.7 Portability**<br>a. MCDA ensures that they avoid lock-in when they choose to use cloud services. They ensure that they can move cloud service customer data or their applications between multiple cloud service providers at low cost and with minimal disruption.<br>b. Cloud data portability:-MCDA is able to copy their data into or out of a cloud service through network access or by physical transfer of storage devices.<br>c. Cloud application portability:- Could services allow the migration of items such as a fully-stopped virtual machine instance or a machine image (IaaS service) from one cloud service provider to another cloud service provider, or the migration of application components (PaaS service) from one cloud service provider to another. In both cases, there is a related aspect of the support of portability of metadata relating to the application components, providing information about the relationships of program components and about the required infrastructure for the program components (e.g., load balancing configuration, firewall settings). | | | |
| **7.8 Protection of personally identifiable information (PII)**<br>a. MCDA ensures the protection, assurance, proper and consistent collection, processing, communication, use and disposition of personally identifiable information (PII) in relation to cloud services.<br>b. MCDAs ensures adherence of cloud services to Kenya statutory, regulatory and legal requirements rules and regulations applied to the handling of PII | | | |
| **7.9 Resiliency**<br>a. MCDA implements a set of monitoring, preventive and responsive processes to enable a cloud service to provide continuous operations, or predictable and verifiable outages, through failure and recovery actions. These can include hardware, communication and/or software failures, and can occur as isolated incidents or in combination, including serial failure. These processes can include both automated and manual actions, usually spanning multiple systems, and thus their description and realization are part of the overall cloud infrastructure, not an independent function. | | | |

| | | | |
|---|---|---|---|
| **7.10 Reversibility**<br>a. MCDA has put in place measures to retrieve their data and application artefacts and for the cloud service provider to delete all their data, as well as contractually specified cloud service derived data after an agreed period.<br>b. They ensure the "right to be forgotten" is implemented, in that the that once they indicate to the cloud service provider that their use of the service(s) will cease, there will be an orderly process for the cloud service customer to retrieve their data and their application artefacts and that the cloud service provider will delete all copies and not retain any materials belonging to them after an agreed period. | | | |
| **7.11 Security**<br>Cloud security is fully described in the information security standard and stipulates the following;<br>a. MCDAs has implemented security capabilities for cloud services including those for access control, confidentiality, integrity and availability.<br>b. MCDAs has implemented facilities to enable early detection, diagnosis and fixing of cloud service and resource related problems; secure logging of access records, activity reports, session monitoring and packet inspections on the network; provision of firewalling, and malicious attack detection and prevention for the cloud service providers' systems. One user should not be able to disrupt other users' use of cloud services.<br>c. Intranet level security has been provided on the network connecting the MCDA to the cloud service provider (for example, through the use of VPN capabilities).<br>d. MCDA has ensured a clear definition of the information security responsibilities between them and the provider to ensure that all aspects of security are covered, to avoid responsibility ambiguity.<br>e. MCDA has implemented security measures that address the threats affecting the specific cloud service category i.e IaaS, PaaS, SaaS.<br>f. MCDAs has implemented security measures that address the threats affecting the specific cloud deployment models<br>g. MCDA has properly catalogued their data and identify its sensitivity and the risk to the business of its leakage, loss or corruption. (See Information Security Standard on how to identify the sensitivity of data).<br>h. In case of encryption, MCDAs has ensured the responsibility for key management is clearly defined and the logical and physical control of the keys, as well as the data are implemented | | | |

| | | | |
|---|---|---|---|
| **7.12 Service levels and service level agreements**<br>a. MCDAs has ensured service level agreements are in place to assure an agreed upon quality of service with cloud service provider.<br>b. The cloud computing service level agreement (cloud SLA) is a service level agreement b. The SLA covers terms regarding<br>• The quality of service<br>• Security<br>• Performance and remedies for failures to meet the terms of the SLA.<br>c. The SLA lists a set of promises explicitly not made to MCDAs, i.e., limitations and obligations that cloud service customers need to accept.<br>d. The cloud SLA defines the classification of data objects (i.e., cloud service customer data, cloud service provider data, and cloud service derived data), who has access and control of data objects in these data classifications and how they will be used.<br>e. The service level agreement specifies information relating to the availability of the services, the confidentiality and integrity of the services and the access controls which apply to the services. The service level agreement shall specify how any personally identifiable information will be handled in relation to the cloud services.<br>f. MCDA reviews service agreement – alternatively known as the master service agreement (MSA), terms of service (ToS), terms and conditions (T&C), or simply “the contract” – (which is the higher order document in agreements between parties and the service level agreement (SLA) is subservient) to ensure they are aligned. | | | |

| CLOUD COMPUTING STANDARD WORKING GROUP |
|---|
| JUSTINE MBOGO- MOICT |
| JAMES WAFULA- ICTA |

ICT Authority
Telposta Towers, 12th Floor, Kenyatta Ave
P.O. Box 27150 - 00100 Nairobi, Kenya
t: + 254-020-2211960/62
Email: info@ict.go.ke or communications@ict.go.ke or standards@ict.go.ke
Visit: www.icta.go.ke
Become a fan: www.facebook.com/ICTAuthorityKE
Follow us on twitter: @ICTAuthorityKE

ICT Authority