2017

Towards a Cloud Readiness Assessment Framework and Index for Africa

Dr. Tonny Omwansa,
Associate Professor, University of Nairobi
(tomwansa@uonbi.ac.ke)
Mr. Rizwan Tufail,
Founder, Innovonomics – The Center for Innovation Economics (rizwan.tufail@innovonomics.com)

Executive Summary:

Technology has had a profound impact on business, government and society in the past few years, and the transformative role of technology has now been universally accepted. Cloud computing has fundamentally altered the technical landscape, accelerating technology-driven change and making large-scale even society-wide technology solutions not only possible but also practical. Therefore, governments across the world are trying to accelerate deployment and adoption of information and communication technologies. However, to make effective use of cloud computing technologies, countries have to be 'ready' to adopt these technologies and make full of them; this readiness is not only in technical terms but covers all aspects of regulation, human capacity, organizational and technical infrastructures. Therefore, measuring cloud computing e-readiness is vital. Although several e-readiness assessment models have been developed in the past but few have evolved to account for the complex requirements for cloud computing adoption, and none has effectively addressed the vastly different requirements for cloud computing adoption in developing countries. This report introduces the concept of cloud computing, revisits existing readiness indices, highlights the constraints of these indices and then proposes and presents a μpreliminary application to selected countries of an assessment framework and index that overcomes the limitations highlighted above.

Keywords: cloud computing; e-readiness assessment; cloud computing readiness index

Table of Contents

Introduction

Background

Cloud computing uptake is in the early stages in many of the African countries, with large corporations being the early adopters. Most cloud computing providers are global vendors/suppliers, with very few local cloud providers. In general, the cloud market is largely supply-side driven.

Usage of cloud services in the public sector is limited in many countries, with some effort by certain governments to promote development of cloud strategies. Countries like South Africa, Nigeria, Kenya and Ghana have reported lead the pack in shaping the cloud ecosystem. Policy environment, governance, broadband infrastructure, skill sets and other critical elements that promote uptake and diffusion of cloud services are rapidly improving in a number of African countries.

The need for cloud technology in many African countries is not in question, particularly given that many of these economies are dominated by the informal sector, and have a large small business sector that could benefit from cloud computing. Additionally, the uptake of mobile devices creates an opportunity for providing cloud services over mobile devices. In terms of economic development impacts, cloud computing opens great opportunities for African countries to engage global markets and in essence leapfrog the lack of traditional infrastructure that has traditionally been used elsewhere to facilitate global trade. There are numerous opportunities for innovators to rapidly create market relevant solutions.

Despite the progressive trends and obvious demand, many of the African countries experience significant challenges. African countries ranks low in the global e-readiness index and various barriers affect market growth, including lack of affordable backbone infrastructure, high cost of communication, ineffective regulation, insufficient relevant skills and inaccurate perceptions.

A number of countries have conducted national cloud readiness surveys, while organizational like Research ICT Africa, ITU and UNCTAD have conducted cross country surveys that provide snapshots of the regional cloud computing development. Organizing regional initiatives and benchmarking against one another helps countries in regions to progress, especially when considering new

technologies like cloud computing. Worldwide, organizations such as the Asia Cloud Computing Association whose mission is to accelerate the growth and development of cloud computing in Asia Pacific, have helped the regional develop the cloud computing agenda through dialogue, training and public education.

With this background in mind, this study proposes to develop a cloud readiness index for Africa that will not only provide an indication of the status, but also provide a platform for monitoring progress over time and help identify bottlenecks that slow uptake of cloud technology and by extension the digital future of Africa.

Problem Definition

Though several countries in Africa have made specific strides towards national cloud adoption, there is no clear way to rank all the countries using a standard tool.

Though reports published by a number of organizations indicate to a reasonably degree the status of cloud computing adoption in Africa, there currently lacks a coherent and consistent index that interrelates various critical elements of cloud technology development. The lack of such an index implies that countries do not have a yardstick to help prioritize areas where they need to develop.

The cloud readiness index proposed will provide an opportunity for stakeholders, led by the governments in the various countries, to engage internally and regionally on what needs to be done to position the countries to exploit the opportunities and benefits of cloud computing.

Aim

The aim of this study is to develop a cloud readiness index for Africa. Additionally, the contribution to the research and state-of-the-art knowledge that this project builds is to understand how a cloud index in an emerging market geography would differ from a more developed world perspective. Finally, we believe that the index will over time become a critical component into policy-making by governments in Africa, by identifying and highlighting thematic areas where more development work and focus is required.

Objectives

1. Develop a conceptual model that identifies the key constructs and their relationships for cloud adoption and diffusion in the region
2. Using the model in objective 1, engagement with industry stakeholders and existing literature identify key elements that would constitute the index framework
3. Populate the framework in objective 2 using primary and secondary data to generate an index
4. Validate the index using relevant and available avenues

Scope

During this study, the index will focus on 5 progressive countries in Africa. This is due to resource constraints and the fact that Africa has over 50 countries which is a very large region. This study will help cement the methodology and approach for the index, and subsequent studies can be used to expand the index to other countries.

Motivations for Proposed Assessment Framework and Ranking Tool:

We submit that there are three key motivations for creating the proposed assessment framework and ranking tool:

1. Assessment frameworks and tools need to be updated frequently to reflect advances in technology, and to account for increased technology deployments.
2. Based on our investigation of related literature, there is no published works related to Cloud Computing and national readiness, or markedly, an attempt to understand Cloud Computing Readiness, i.e. the state of readiness of a nation or geography to benefit fully from cloud computing. In this article, we present a framework to do so. Shifting landscape of new technologies and consumer preferences means that e-readiness is a rapidly developing construct, and static measures may therefore fail to capture its impact, if not updated regularly [35
3. The current readiness assessment tools and ranking have been developed primarily from a developed world perspective. A readiness index for developing countries needs to take into account the peculiar environment and

challenges that may be unique to the region. Huang [36] acknowledges there are differences between developed and developing economies with respect to e-readiness assessment models for e-business implementation. To illustrate, availability of technical skills required to run a modern technology infrastructure may be easily available, affordable and accessible in some parts of the developed world, but can be a challenge in some developing countries.

4. Some of the values or range of values for the indicators appropriate for a developing country like Kenya are very different from those in a developed country like Finland. For example, the most optimal for the sub-indicator Internet bandwidth per 1000 citizens used in Kenya may be much smaller than what it would be for developed countries (e.g. Finland). Using a range of values that results in an entire continent being scored 1 on a scale of 1-4, as an example, does not yield any practical insights or actionable guidance for policy-makers and business leaders.

Concept of e-Readiness

In its broadest sense, e-readiness can be defined as the level of preparedness and keenness of a nation or community to participate in the information and knowledge society [1,2] e-readiness assessments are important because their output can be a predictor of how well a country can perform in the new, global digital economy. It provides policy makers with details of their economy's competitiveness relative to its international counterparts and allows them to pinpoint areas of strengths and weaknesses [3].

Experts pointed out that in order for countries to put ICT to effective use, they must first be "e-ready" in terms of Information Technology (IT) infrastructure including applications and services, accessibility of IT to the population, and the appropriate legal and regulatory frameworks [4]. Therefore, many development agencies, research organizations, universities and world organizations have created instruments for assessing e-readiness either in the form of self-assessment tools or surveys. In addition, many initiatives by individual researchers attempt to improve or develop general frameworks.

E-Readiness is often assessed by understanding, assessing, measuring and possibly benchmarking progress in the most important areas for the adoption of information and communication technologies, including their application to industry, commerce and society at large. As an example, researchers at the Center International Development (CID) [1], housed at the Harvard Kenney School described an 'e-ready' society as:

> "One that has the necessary physical infrastructure (high bandwidth, reliability, and affordable prices), has integrated current ICTs throughout businesses (commerce, local ICT sector), communities (local content, organizations online, ICTs used in everyday life, ICTs taught in schools), and the government (e-government)".

On the other hand, the World Bank Information for Development Program [5} defined e-readiness for a state as:

> “The preparedness of states to provide governance equitably and cost effectively and the capacity to reflect in the degree of integration the deprived segments of society attain application of ICT as an e-governance tool. Apart from this the ability of the state to provide business, the capacity to participate in the provincial level digital economy and further networking with national level digital economy”.

Using these concepts of e-readiness, a number of organizations have created assessment frameworks and indices to measure and benchmark e-readiness. As an example, the World Economic Forum’s Networked Readiness Index is a globally recognized benchmark of nations’ e-readiness, and is based on the CID definition of e-readiness [6].

The challenge, however, is that these assessment frameworks, tools and indices do not accurately account for the developments of technology in the past decade, in particular with the development of cloud computing technologies. These methodologies and tools were developed in an era of mainframe computing and then updated to reflect the change towards a PC/desktop centric evolution of technology, and then to a lesser extent the mobile computing platform. In an era when computing power has become commoditized, readiness is less about technology access, and much more about the policy infrastructure that allows this computing power to be used effectively, and with trust.

Before we discuss how the readiness concept has to evolve in the age of cloud computing, and what impact it has on assessment frameworks and tools, it is worthwhile to understand cloud computing in greater detail.

Concept of Cloud Computing:

Cloud Computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [8].

This cloud model is composed of five essential characteristics:

- **On-demand self-service**: computer services such as email, applications, network or server service can be provided as needed. It means that organizations can request and manage their own computing resources with minimal 'friction'
- **Broad network access**: Capabilities are available over the network and accessed through thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations). This way, the cloud makes it easier for organizations to bring their application closer to users.
- **Resource pooling**: Computing resources are pooled to serve multiple consumers, with different physical and virtual resources dynamically assigned and reassigned according to consumers demand. This results in increased application density on single hardware, much higher resource utilization, and as a consequence, the price for resource usage continues to fall and resources can easily be shifted to match the point of demand.
- **Rapid elasticity**: Computing capabilities can be elastically provisioned and released to scale rapidly in proportion to demand. Resources appear to be unlimited and can be appropriated in any quantity at any time, allowing organizations to expand and contract the amount of resources, thus saving money when the application is under light load and needs limited computing resources. This essentially reduces the requirement for meticulous capacity planning, as organizations will be able to add resources as and when required.
- **Measured service**: Computing services are available to users on a metered capability basis – in a pay-per-use model - which enables resource use optimization. This allows organizations to optimize their applications for lower resource utilization, anticipate financial needs better and budget more effectively for future growth.

In essence, these characteristics mean that organizations (public-sector, business or civil society organizations) in a country can easily deploy cloud computing without the need to purchase hardware, software licenses, or implementation services (Ease

of Implementation). They can reduce or eliminate ICT capital expenditures and decrease ongoing operating expenditures by paying only for the services they use and by reducing or redeploying their ICT staffs (Cost Savings). When user loads increase, organizations need not to secure additional hardware and software, but can instead add and subtract network load capacity (Scalability). Cloud Computing can increase staff mobility by enabling access to business information and applications from a wider range of locations and/or devices (Flexibility). It allows smaller organizations to access higher-caliber hardware, software, and ICT staff than they can attract and/or afford themselves (Access to IT Capabilities). Organizations can focus ICT staff on higher-value tasks by reducing or eliminating constant server updates and other computing issues (Redeployment of IT Staff). In short, Cloud Computing can make it much easier to reduce or shed functionalities like running data centres as well as developing and managing software applications, allowing organizations to concentrate on critical issues such as the development of policy and the design and delivery of services (Focusing on Core Competencies) [9], [10], [11], [12], [13].

However, Cloud Computing like any new technology has challenges. Many challenges of Cloud Computing relate to a developing understanding of the technologies, service models as well as benefits; these challenges are compounded by the relative underdevelopment of the marketplace for cloud services [11].

To illustrate, one area of challenge pertains to open standards and interoperability because of a lack of standards when using and implementing Cloud Computing, not only within one country but even more markedly, when cloud computing services cross national boundaries. To take advantage of all the benefits and possibilities of cloud computing, governments will need to promote open, internationally comparable standards for the cloud, thereby enabling a greater level of confidence in the reliability and continuity of these services, and enabling users to switch cloud service providers with a minimum of cost and risk [14].

Another area of concern is the security and privacy of information held in Cloud Computing environments. Serious considerations must be given to using Cloud Computing to handle information that is vital to a business, to the security of citizens,

or in the case of public sector use, to maintaining public trust and confidence in government. Issues of privacy and security are complicated by the fact that cloud computing providers may locate and back-up data in a number of different jurisdictions with differing levels of protection. This means that users of Cloud Computing enabled applications and services need to assure themselves that the security surrounding cloud environments complies with laws, policies, and protocols [15]. One way of mitigating these uncertainties is for organizations to ensure that appropriate service-level agreements (SLAs) are in place, and equally importantly, that they have adequate mechanisms and skills for assessing performance against those SLAs.

A related challenge is assuring business continuity; risk of data loss due to improper backups or system failures can seriously derail operations for a business or a public sector organization. That means that organizations need to understand these business continuity risks and be assured that effective remedies for those risks (such as strong contracts, effective SLAs, disaster recovery, and business continuity plans) are in place–especially if using offshore cloud services [10].

Conversely, since Cloud Computing services rely fully on the availability, speed, quality and performance of the internet as the underlying mechanism to connect consumers of these services and the service provider, Internet dependency–performance and availability becomes even more important [16]. In fact it can be argued that the focus shifts from pure access to the internet (irrespective of the quality), to a question of quality of internet access with issues like intermittency and uptime becoming more critical.

Measuring e-Readiness

There are two primary objectives of measuring e-readiness. The first is a diagnostic mechanism as part of ICT strategic planning for a country, community or institution. An example of this approach is the CID assessment methodologies. The second is purposes of ranking e-readiness; comparing countries, communities or institutions. An example of this is the Networked Readiness Index (NRI) by the World Economic Forum (WEF) used to compare, benchmark and rank countries.

In the following section, we briefly review the main e-readiness diagnostic assessment models that motivated the development of our framework, namely, the CID assessment tool [1].

CID e-readiness tool

The CID e-readiness tool was titled, “Readiness for the Networked World – A Guide for developing countries”. It was developed by the Information Technology Group at the Center for International Development (CID), at the Harvard Kennedy School of Government.

The CID e-readiness tool defines 19 indicators of the degree of e-readiness of a community or country. The 19 indicators are split into five main categories as follows:

i) **Network access category** – measures the readiness of the ICT infrastructure. It defines six indicators, namely – Information infrastructure, Internet availability, Internet affordability, network speed and quality, hardware and software, and service and support. These indicators were designed to measure the availability, cost, and quality of ICT networks and services

ii) **Networked economy category** – was measures the use of ICT by businesses and the government for commerce (B2C or B2B) and the availability of the human capital used to support the services. It has four indicators, namely, ICT employment opportunities, B2C electronic commerce, B2B electronic commerce and e-government. These indicators accomplish the objective of measuring how businesses and governments use ICTs to interact with the public and with each other.

iii) **Networked learning category** – was designed to measure the level of access to ICT by educational institutions, and the utilization of ICT in teaching and learning, and availability of ICT training programs. It has three indicators, namely, schools access to ICTs, enhancing education with ICTs, and developing the ICT workforce. These indicators collectively address the question of how educational systems integrated ICTs into their processes, and their attempts to prepare the ICT workforce.

iv) **Networked society category** – was designed to measure the degree to which people and organizations use ICT. It has four indicators, namely, people and organizations online, locally relevant content, ICT in everyday life, and ICTs in the workplace. The indicators in combination answer the question of how effectively and to what extent individuals in the community use ICT at work and in their personal lives.

v) **Network policy category** – was designed to assess the ICT policies and/or legislation and the success or failure of the regulatory environment in a particular community. It has two indicators, namely, telecommunications regulation, and ICT trade policy. These indicators measure the extent to which the policy environment promotes or hinders the growth of ICT adaptation and use.

In e-readiness assessment of using the CID tool, each of the 19 indicators are staged on a scale of 1 to 4, where 1 represents unprepared and 4 represents the highest state of readiness. The final results are then presented as a radar diagram for the 19 indicators.

E-Readiness Ranking Methodologies

Some of the organizations involved in developing e-readiness rankings are (1) the International Telecommunication Union (ITU) developed the ICT Development Index (IDI), (2) World Economic Forum (WEF) developed the Network Readiness Index (NRI)), (3) Economist Intelligence Unit (EIU) developed the e-Readiness rankings), and (4) the United Nations Department of Economic and Social Affairs (UN-DESA) developed the e-Readiness Index.

These tools use different sets of indicators and weightage of these indicators (depending on their own assessment of the importance of that indicator) to create these rankings. It is possible to identify four major thematic areas from the e-readiness literature [18]:

- ICT infrastructure mainly relates to the elements of ICT infrastructure that need to be available to citizens if they are to use e-government services.
- Human capital relates to citizens' education and knowledge on how to use computers and the internet.

- ICT usage reflects how citizens use computers and the internet in their daily lives.
- ICT regulations relate to legislative provisions that affect the use of e-government.

Next, we take a deeper look at the four ranking methodologies identified earlier.

ICT Development Index (IDI)

In 2003, International Telecommunication Union (ITU) introduced a readiness index, namely, the Digital Access Index (DAI), which it claimed as an important step forward in measuring technology adoption. DAI distinguished itself from other indices by including a number of new variables, such as education and affordability. In 2005, the ITU created the Digital Opportunity Index (DOI), a framework based on internationally agreed indicators. Finally, in early 2009, the ITU launched the new "ICT Development Index" (IDI), which combines two existing ITU indices: the "Digital Opportunity Index" (DOI) and the "ICT Opportunity Index" (ICT-OI) [19]. The ITU eGovernment Quick-check Tool uses three sub-indices of the IDI: The ICT access sub-index (40%), the ICT use sub-index (40%) and ICT skills (20%).

Each sub-index comprises indicators with the same weight; (1) the ICT access sub-index includes indicators on fixed telephone lines and mobile cellular subscribers per 100 inhabitants; (2) international Internet bandwidth per Internet user; and (3) proportion of households with a computer and with Internet access.

Meanwhile, the IDI's ICT use sub-index is composed of (1) indicators on Internet users, (2) fixed broadband Internet subscribers and (3) mobile broadband subscribers per 100 inhabitants. Finally, the ICT skills index encompasses three indicators: (1) adult literacy rate, (2) secondary gross enrolment ratio and (3) tertiary gross enrolment ratio. [20], [21]

Network Readiness Index (NRI)

The Networked Readiness Index is defined as "the degree of preparedness of a nation or community to participate in and benefit from ICT developments" [6]. The

Index is a composite of three sub-indexes, namely, the environment for ICT offered by a given country or community; the readiness of the community's key stakeholders (individuals, businesses, and governments) to use ICT; and finally, the usage of ICT amongst these stakeholders.

The NRI has been designed as a macro-level tool for policymakers and global leaders. The index signals broad trends, flags opportunities and deficits, and makes a unique contribution to the understanding of how nations are performing relative to one another with regard to their participation in the Networked World [17]. It influences a broad range of decisions by policy makers and businesses, such as investors' choice of a destination, effective Internet regulation or stimulation, as well as identification of investment opportunities.

The NRI was derived from the CID tool but uses a modified set of 48 indicators to measure the nine categories of indicators. The indicators were derived from both hard facts data and perceptions data obtained by surveying senior government and business executives. The values of the indicators were mapped into a scale of 1 to 7 and then statistically used to derive the index.

The World Economic Forum (WEF), in their Global Information Technology Report 2016, features the latest results of the Network Readiness Index (NRI), offering an overview of the current state of ICT readiness in the world.

E-Readiness Rankings

The Economist Intelligence Unit (EIU) has been publishing an annual e-readiness ranking of 69 countries since 2000. Its model is a weighted collection of nearly 100 quantitative and qualitative criteria, organized into six distinct categories measuring the various components of a country's social, political, economic and technological development. These, in turn, are weighted according to their assumed importance as influencing factors and each of them has a number of sub-indicators (variable) scored on a scale of one to ten. According to its report on 2010, EIU changed the name "e-readiness ranking" to be "digital economy rankings" and made some changes to weights at the indicators and sub-indicators (variables) levels [22].

Unfortunately, the EIU has since then discontinued the development of the e-readiness ranking/digital economy rankings.

e-Readiness Index

The UNDESA e-readiness survey considers a relatively comprehensive assessment of e-government including both general and specific indicators [23]. Its readiness Index is a comprehensive scoring of the preparedness and capacity of national administrations to use information communication technology in the execution of government functions. It is comprised of four indices [24] briefly described below:

1. Online service index: based on a comprehensive survey of 192 countries' national websites the survey evaluates countries based on the four-stage of e-government development: emerging online presence, enhanced presence, transactional presence and connected presence.
2. Telecommunication infrastructure index: it is a composite of five indicators: number of personal computers per 100 persons, number of Internet users per 100 persons, number of telephone lines per 100 persons, number of mobile cellular subscriptions per 100 persons and number of fixed broadband subscribers per 100 persons, all weighted equally.
3. Human capital index: It is a composite of two indicators, adult literacy rate and the combined primary, secondary, and tertiary gross enrolment ratio, with two thirds weights assigned to adult literacy rate and one third to the gross enrolment.
4. E-participation index: It is a supplementary index which focuses on the use of the Internet to facilitate "e-information", "e-consultation", and "e-decision making." The overall index is calculated by the first three indexes with the same weight for each ((⅓*online service index) + (⅓*telecommunication index) + (⅓*human capital index)).

Evolution of e-Readiness Ranking Models Over Time – EIU Example

To understand the differences and identify the deriver of changes over the various versions of an e-readiness index, we reference the review of the EIU e-readiness rankings series, undertaken by Fathy and Ibrahim [25].

As Fathy and Ibrahim point out, since launching the rankings in 2000, EIU has repeatedly upgraded and refined their methodology. The 2000 e-readiness survey was based on only two measures: business environment and connectivity. The rankings for subsequent years (2001 to 2006), however, were based on six basic measures: connectivity and technology infrastructure (25%), business environment (20%), consumer and business adoption (20%), legal and regulatory environment (15%), social and cultural infrastructure (15%) and supporting e-services (5%) [26], [27], [28], [29], [30], [31].

The primary categories changed were changed in 2007. The ranking criteria of the two categories – connectivity and technology infrastructure (20%), and consumer and business adoption (25%) – was adjusted to reflect the growing importance of high-speed internet affordability and the availability of digital public services for both individuals and enterprises. In parallel, the legal environment category (10%) was refined to reflect a more focused look at the specific government frameworks that influence e-adoption. Additionally, a new category, government policy and vision (15%), was added to better highlight the impact that policy has on determining a country's overall e-readiness. Social and cultural environment (15%) remained unchanged and business environment (15%) lost some weight to make way for the new category (government policy and vision). Finally, supporting e-services indicator was eliminated in this version [32].

Another effect is worth highlighting. EIU regularly reviews the criteria for measuring e-readiness and refines the methodology on a periodic basis, at the level of the individual variable in each category. Therefore, in 2004, the EIU made a small but significant change, adding broadband penetration as a criterion to measure connectivity [29]. In 2005, the methodology underwent significant modification with many criteria being assigned revised weights to reflect their changed importance in determining e-readiness. New and more precise means of assessing performance in some criteria were developed and added, including those in the areas of internet

security and connectivity (internet affordability, internet security and the penetration of public-access wireless “hotspots”) and in ICT spending and education (degree of entrepreneurship and innovation). Connectivity was weighted more heavily towards broadband penetration (20%) that year to reflect its growing importance in ICT development. On the other hand criteria that no longer accurately reflect the key drivers or determinants of the digital economy were removed [30].

No major changes were introduced in 2006. However, several new ranking variables were introduced and some individual measures were removed or their weightage was reassessed in the e-readiness model in 2007. With reference to connectivity, the 2007 index recognized that broadband internet access was a more critical factor—not only its penetration levels, but also its affordability to households. EIU 2007 also eliminated fixed-line phones as an indicator and increased weightage of mobile penetration, as mobile phones became cheaper and, with text messaging and mobile commerce applications, increasingly powerful digital devices. EIU 2007 re-evaluated the consumer and business adoption category to evaluate the utilization of digital channels by individuals and businesses. It also slightly increased its weight relative to connectivity and other categories [32].

The EIU’s e-readiness rankings methodology remained largely unchanged in 2008 [33], but in 2009 several changes were made to the methodology. Three new “usage” indicators were added to the “consumer and business adoption” category: (1) use of the internet by consumers, (2) the use of online public services by citizens and (3) the use of online public services by businesses. Two existing indicators assessing the availability of online public services for citizens and businesses was moved to the “government policy and vision” category. Additionally, the e-participation indicator was added to the government policy and vision category. An indicator of international internet bandwidth per head also was added to the “connectivity and technology infrastructure” category. Elsewhere in this category, some measures were removed (personal computers and WiFi hotspots). The “educational level” indicator in the “social and cultural environment” category were broadened to include data on gross enrolment in education, in addition to the existing measure of school life expectancy. The “electronic ID” indicator previously was in “connectivity and technology infrastructure”, moved to the “legal environment”

category. Also in this category, the indicator “laws covering the internet” was revaluated to focus exclusively on cybercrime, data privacy and anti-spam legislation. Lastly, in EIU 2009 the 1-5 scoring scale changed to a 1_0 scoring scale for all indicators [34].

In 2010, a large number of modifications to EIU model were made. Four changes were in the “connectivity” category of indicators, and one was in “social and cultural environment”. For connectivity, broadband quality and mobile quality were added. In measuring “broadband affordability”, the lowest connection speed was updated to 256 kilobytes per second (kbps) (previously this was 128 kbps) to reflect the technology changes that has taken place, and also to account for the increased bandwidth requirements of newer applications and services. The scoring scale for “internet user penetration” was adjusted, with 100% of the population representing the highest penetration achievable in a country (this previously was 75%); this was done to reflect the great strides in internet access penetration that had taken place in the intervening years. Finally, in the social and cultural environment category, the “educational level” indicator was expanded to encompass a third sub-indicator, “gross enrolment in tertiary education” [22].

It can be concluded from the analysis above that changes had to be made to the index on a regular basis to ensure that the index and its methodology remained relevant in the face of technological developments, including the advances in technology like the high-speed internet, the availability of digital public services and the penetration and advancing of mobile technologies. Please see Table 1.

Methodology

In this section, we provide a description of how we went about designing, developing and testing the index.

We started the process with a desktop review of the literature and background materials. Various existing frameworks and indices were studied. As many indicators and sub-indicators were identified and their application on national cloud computing analysed. While analysing the various indices, indicators and sub-indicators, an assessment of their relevance in the African context was considered. This helped in deciding if to include the indicators and sub-indicators in the proposed model.

We realized that not all indicators and sub-indicators were of equal significance in determining the readiness of a country. We therefore proposed a weighting mechanism which would guide in allocating the significance level for each indicator or sub-indicator. The actual data to be captured for each sub-indicator was decided upon, including the data type as well as the potential source.

The indicators were group into categories thus shaping the index that we named Africa Cloud Index (ACI). Once the cloud assessment framework had been developed, we tested it by applying the data of shortlisted African countries.

Introducing the Africa Cloud Readiness Index (ACRI)

The model described in this paper has been derived from the CID assessment models and is therefore diagnostic in nature. It utilizes a staging framework with quantifiable targets for each indicator, which is useful for developing roadmaps for accession to higher stages of readiness. This approach has previously been used to create an assessment framework for Higher Education [37]. The framework borrows from CID and the NRI methodologies but has additional different variables and indicators.

Although the 19 indicators by the CID [1] could have been adopted for use in the model proposed in this paper, many of the indicators needed to be reconsidered in a world where the delivery model for technology has changed dramatically. We have, therefore, drawn inspiration from the CID tool, but expanded upon it by eliminating indicators that were not relevant and added indicators that are more relevant.

Additionally, we have developed quantitatively measurable sub-indicators that could be staged on a linear scale of 1 to 3. Apart from eliminating some of the 19 indicators, we introduced new indicators and defined new categories.

The final model contains 38 indicators classified into nine categories, namely:

i. Standards
ii. Policy
iii. Infrastructure
iv. Access
v. Training and Skills
vi. Networked Business
vii. Networked Government
viii. Operations
ix. Freedom, Expression and Lifestyle

Each of the indicators has been derived from sub-indicators. 101 sub-indicators have been defined in this model. Each of the indicators is staged on a scale of 1 to 3, with 1 being unprepared and 3 the highest state of readiness. The indicators were then weighted, relative to their importance.

Below, we provide a brief indication as to why some indicators had to be weighted.
To make effective use of the cloud, governments has to ensure that the standards which respond to high priority security, interoperability, and portability requirements are in place for a Cloud Computing environment. For example, in USA, as part of the Federal Cloud Computing Initiative, the National Institute of Standards and Technology (NIST) is leading and facilitating the development of Cloud Computing standards (SAJACC and FedRAMP) which support interoperability, portability, and security to enable important usage scenarios [38]. Many of Cloud Computing challenges related to the need for policies and regulations (open standards and interoperability, business continuity, strategy, privacy, rules and policies). Therefore, the weight for this component is considered to be relatively high.

ICT infrastructure has historically been considered as one of the main indicators to preparedness of a country to adopt technologies. However, as infrastructure is

hosted on cloud, nations do not have to spend on hardware, software, skills resources and maintenance. Therefore, ICT infrastructure as a component of readiness index gets less weight. In addition, its variables may be confined to the factors affect the connectivity and affordability like electricity production, mobile network coverage and secure Internet servers.

Cloud computing, however, makes it even more critical that nations have high-speed, always-on internet, with adequate security and privacy considerations that Cloud Computing demands. Therefore, connectivity as an indicator gets more attention. On the other hand, taking into account the high penetration of mobile devices, ease of use by the public and the possibility of provision Cloud Computing services through these devices, it is nevertheless critical that measures for device access are included, and weighted appropriately.

Skills present a very interesting challenge. On the one hand, researchers have pointed out that stated that Cloud Computing is considered as an attractive option when skilled IT staff or equipment is difficult and expensive to come by [39] (Nearly two-thirds of executives asserted they pursued cloud services at least partly for this reason). Therefore human capital as a component of an e-government readiness index may take less weight. However, by the same token, if a government or nation wants to develop its own cloud infrastructure, availability of skills can become a key challenge. This highlights that a contextually aware usage of the assessment tool will be critical.

Pillars, indicators and the sub-indicators

Table 1 shows the pillars, indicators and the sub-indicators of our proposed framework. The full table, with data sources, weights etc is included in the appendix.

Table 1: Pillars, Indicators and sub-indicators of proposed Index

Pillars	Indicator	Sub-Indicator
Standards	S1 Standards-Making Institutions	S1.1 Is there a regulatory body responsible for standards development for the country?
	S2 Alignment to International Standards	S2.1 Does the government participate in international standards-setting process?
		S2.2 Are international standards favoured over domestic

		standards?
	S3 Open Standards	S3.1 Are there any laws or policies in place that implement technology neutrality in government?
		S3.2 Are cloud computing services able to operate free from laws or policies that mandate the use of certain products (including, but not limited to types of software), services, standards or technologies?
		S3.3 Are cloud computing services able to operate free from laws or policies that establish preferences for certain products (including, but not limited to types of software), services, standards or technologies?
		S3.4 Are cloud computing services able to operate free from laws that discriminate based on the nationality of the vendor, developer or service provider?
	S4 Standards Framework	S4.1 Are there laws, regulations or policies that establish a standards setting framework for interoperability and portability of data?
	S5 Trade Standards	S5.1 Is the downloading of applications or digital data from foreign cloud based service providers free from tariff or other trade barriers?
Policy	P1 Privacy Policy	P1.1 Are there laws or regulations governing the collection, use or other processing of personal information?
		P1.2 Is there an effective agency (or regulator) tasked with the enforcement of privacy laws?
		P1.3 Is there a strict consent requirement for the collection, storage and dissemination of personal data?
		P1.4 Does the law provide users with the right to review their stored information?
		P1.5 Does the law provide users with the right to be forgotten or deleted?
		P1.6 Are there administrative sanctions for non-compliance? How much? (None, Medium, Severe)
		P1.7 Is notification of breaches towards the government and/or users obligatory (None, Govt or User, Both)
	P2 Intellectual Property Protection Policy and Effectiveness	P2.1 Is the country a member of TRIPS agreement?
		P2.2 Have IP laws been enacted to implement TRIPS
		P2.3 Is the country party to the WIPO Copyright Treaty?
		P2.4 Are criminal sanctions available for unauthorized making available of copyright materials digitally?
		P2.5 Are there laws governing ISPs liability for content that infringes copyright?
		P2.6 Software piracy rate, % software installed
		P2.7 Perception of Effectiveness: Intellectual property protection, 1-7 (best)
	P3 Data Protection Policy	P3.1 Is there a Data Protection Policy in place?
		P3.2 Are data protection impact assessments obligatory?
		P3.3 Is a data protection officer required?
		P3.4 Are firms required to retain data for a fixed period of time?
	P4 Cyber Security Policy	P4.1 Is there a law or regulation that gives electronic signatures clear legal weight?
		P4.2 Are ISPs and content service providers free from mandatory filtering or censoring

		P4.3 Global Cybersecurity Index
	P5 Cyber Crime Policy	P5.1 Are cybercrime laws in place?
		P5.2 Are cybercrime laws consistent with the Budapest Convention on Cybercrime?
		P5.3 Laws relating to ICTs, 1-7 (best)
	P6 Data Sovereignty and Portability	P6.1 Are there rules for differentiated treatment of data based on data classification, i.e. different treatment for data of different levels of sensitivity?
		P6.2 Is there a data localization requirement (i.e. is the transfer of data outside of country borders disallowed) (No, Limited, Both)
Infrastructure	I1. Fixed Network Performance	I1.1 Fixed Internet - upload (UL) speeds in kilobits per second (kbps)
		I1.2 Fixed Internet - download (DL) Speed in kilobits per second (kbps)
		I1.3 Fixed Internet - latency in milliseconds (ms)
		I1.4 Fixed Broadband Quality: Avg. Page Load Time (ms)
	I2. Mobile Network Performance	I2.1 Mobile Internet - upload (UL) speeds in kilobits per second (kbps)
		I2.2 Mobile Internet - download (DL) Speed in kilobits per second (kbps)
		I2.3 Mobile Internet - latency in milliseconds (ms)
		I2.4 Mobile Broadband Quality: Avg. Page Load Time (ms)
	I3 International Connectivity: Bandwidth Per Capita	I3.1 Bandwidth Per Capita (Int'l Internet bandwidth, kb/s per user)
	I4 Internet Server Infrastructure	I4.1 Secure Internet servers/million pop.
Access	N1 Mobile Penetration	N1.1 Mobile phone subscriptions/100 pop.
	N2 PC Penetration	N2.1 Households w/ personal computer, %
		N2.2 Availability of latest technologies, 1-7 (best)
	N3 Internet Penetration	N3.1 Households w/ Internet access, %
		N3.2 Mobile network coverage, % pop.
		N3.3 Individuals using Internet, %
	N4 Broadband Subscriptions	N4.1 Fixed broadband Internet subs/100 pop.
		N4.2 Mobile broadband subs/100 pop.
	N5 Affordable Access	N5.1 Prepaid mobile cellular tariffs, PPP $/min.
		N5.2 Fixed broadband Internet tariffs, PPP $/month
		N5.3 Mobile-broadband as % of GNI per capita
	N6 Industry Structure	N6.1 Internet & telephony competition, 0–2 (best)
Training, Skills and Awareness	T1 Quality of education	T1.1 Quality of educational system, 1-7 (best)
		T1.2 Quality of primary education, 1-7 (best)
		T1.3 Quality of management schools, 1-7 (best)
		T1.4 Quality of math & science education, 1-7 (best)
	T2 Educational Enrolment	T2.1 Primary education enrollment rate (net), %
		T2.2 Secondary education gross enrollment rate, %
		T2.3 Tertiary education gross enrollment rate, %
		T2.4 Expected years of schooling
		T2.5 Mean years of schooling

	T3 Trained Workforce	T3.1 Adult literacy rate, %
		T3.2 % of workforce with tertiary degree
		T3.3 Graduates in science & engineering, %
Networked Business	B1 Technology adoption by business	B1.1 Firm-level technology absorption, 1-7 (best)
		B1.2 ICT use for business-to-business transactions, 1-7 (best)
		B1.3 Business-to-consumer Internet use, 1-7 (best)
	B2 ICT, Business and Skills	B2.1 Extent of staff training, 1-7 (best)
		B2.2 Knowledge-intensive jobs, % workforce
	B3 ICT and Business Innovation	B2.1 Impact of ICTs on business models, 1-7 (best)
		B2.2 Impact of ICTs on new organizational models, 1-7 (best)
Networked Governme nt	G1 ICT Vision and Leadership	G1.1 Importance of ICTs to gov't vision, 1-7 (best)
		G1.2 Gov't success in ICT promotion, 1-7 (best)
		G1.3 Impact of ICTs on access to basic services, 1-7 (best)
		G.1.4 Internet access in schools, 1-7 (best)
	G2.1 Government ICT Services	G2.1 Government Online Service Index, 0–1 (best)
		G2.2 ICT use & gov't efficiency, 1-7 (best)
		G2.3 E-Participation Index, 0–1 (best)
	G3.1 Gov't Procurement Leadership	G3.1 Gov't procurement of advanced tech, 1-7 (best)
Operations	O1 Labor Cost and Availability	O1.1 Ranking on labor cost (Pay and productivity, 1-7 (best))
		O1.2 Availability of Scientists and engineers
		O1.3 Availability of research and training services
	02 Political Risks	O2.1 Ranking on political stability
	O3 Energy Availability	O3.1 Electricity production, kWh/capita
		O3.2 % of population with access to electricity
		O3.3 Electricity Consumption (MWh /Capita)
	O4 Energy Reliability	O4.1 Quality of Electricity Supply
		O4.2 Energy Architecture: Economic Development and Growth
		O4.3 Energy Architecture: Access and Security
	O5 Energy Affordability	O5.1 Cost of getting electricity (% of income per capita)
	06 Operational Complexity	061 No. procedures to enforce a contract
		06.2 No. days to enforce a contract
Freedom, Expression and Lifestyles	F1 Lifestyle and Expression	F1.1.1 Use of virtual social networks, 1-7 (best)
		F1.1.2 Wikipedia edits/mn pop. 15–69.
		F1.1.3 Video uploads on YouTube/pop. 15–69.
	F2 Freedom of Expression & Lack of Censorship	F2.1.1 Freedom on the Net Status (Freedom Score 0 = Best, 100 = Worst)

Background on the selected countries

Next step in the process was to identify a shortlist of countries that we could use as test-cases for this methodology. It was deemed important that these countries have a relatively developed absorption capacity for cloud services. Secondly, it was deemed desirable to have a broad geographical mix, to take into account the diversity of economic, social and governmental situations. The countries chosen for our analysis are:

1. Egypt
2. Kenya
3. Mauritius
4. Morocco
5. South Africa

The next section has a detailed overview of these countries from the perspective of Internet and digital technologies.

Egypt:

When the government in Egypt blocked all Internet services to the country, at the height of anti-government protests in early 2011, it came as a shock to many. Although there have been instances worldwide of autocratic regimes limiting internet and radio access, this seemed the first time that a country with a modernizing economy blocked access to the Internet, resulting in a 90 percent drop in Internet traffic to and from Egypt.[1][2] This action, aside from their political and social outcomes, resulted in short-term and long-term impacts on the economy, with immediate loss of nearly $90m to the telecommunication sector, in terms of revenues lost from services it could not deliver[3], and a much longer-term impact on the economy, particularly through the impact of communication services on sectors like tourism, manufacturing and others. Beyond that, this action by the government also undermined the confidence of international investors in terms of business continuity, no doubt casting a longer term shadow on the economy.

---

[1] http://www.nytimes.com/2011/01/29/technology/internet/29cutoff.html?_r=0

2 http://www.telegraph.co.uk/news/worldnews/africaandindianocean/egypt/8288163/HowEgypt-shut-down-the-internet.html

[3] http://www.oecd.org/countries/egypt/theeconomicimpactofshuttingdowninternetandmobilephoneservicesinegypt.htm

Much has changed across the world, and in Egypt, since then, both politically as well as technologically. The growing adoption of cloud computing services for personal, government and business across the world, has made telecommunication services an even more integral and foundational part of life. The Snowden episode has brought the issues of privacy and national security, to the front, and countries across the world are assessing how to balance these and other conflicting goals. Like many other countries across the world, the government of Egypt is keeping a close eye on these developments.

It is interesting to observe that on paper, at least, there are no laws in Egypt that specifically govern life in a digital world awash with data. As an example, Egyptian law does not have any specific provisions which regulate online privacy, and it does not have any specific provisions which regulate electronic marketing, and the conduct of such marketing services.

There is no general data protection law in Egypt, and there is no national authority responsible for data protection in Egypt, even if certain types of data and information are protected by specific laws and the constitution. Article 57 of the Egyptian Constitution promulgated in January 2014 provides for the protection of privacy and secrecy of, inter alia, mails, phone conversations and other methods of communication. It was mandated that these could not be monitored, inspected or confiscated without a prior court order and even then, for a limited period of time as regulated by the law. he Egyptian Constitution has not defined data protection. However, it referred to the legislative authority to regulate the communication of data in a manner that does not encroach upon the privacy of citizens, their rights and National Security.

However, there has been little progress in translating these articles in the constitution into laws that would operationalize these intentions. Media reports [4]disclosed discussions in Parliament about a new Cyber Crime Bill, but there was widespread concern that its focus seems to be more on regulating speech and expression, rather

[4] http://www.al-monitor.com/pulse/originals/2016/06/egypt-enacts-cyber-crime-law-preserve-national-security.html

than protecting individual rights; the creation of a High Council for Cyber Security[5], before the legislative framework that would govern its operations was highlighted as a risk by many. Additionally, a leaked tender document from the Ministry of Interior revealed plans to conduct mass surveillance of social media by systematically monitoring Facebook, Twitter and YouTube and possibly mobile phone applications such as WhatsApp, Viber and Instagram; the move was characterized by civil society organizations as an attack on internet privacy and freedom of expression[6], and highlighted once again the urgent need for legislation – and enforcement - that protects individuals freedoms and privacy online, not only from criminals but also from their own administration.

At the current time, Egypt does not have a law governing protection, and the use of, personal data. There are indeed piecemeal provisions related to data protection in different laws and regulations in Egypt. As an example, constitutional principles concerning individuals' right to privacy under the Egyptian Constitution as well as general principles on compensation for unlawful acts under the Egyptian Civil Code govern the collection, use and processing of personal data. Additionally, the Egyptian Penal Code no. 58/1937 imposes criminal punishment for unlawful collection of images or recordings for individuals in private places. Other laws that provide for protection and confidentiality on certain data and within define contexts, include:

- Egyptian Labour Law no. 12/2003 (confidentiality of the employee's file information including punishment and assessment)
- Egyptian Banking Law no. 88/2003 (confidentiality of client and account information).
- Egyptian Civil Status Law no. 143/1994 provides for the confidentiality of citizens' civil status data.
- The Executive Regulations of Mortgage Finance Law no. 148/2001 issued by virtue of Cabinet Decree no. 1/2001 as amended by Prime Minister Decree no. 465/2005 has clauses that ensure confidentiality of the data of the clients of mortgage finance companies.

[5] http://www.al-monitor.com/pulse/en/originals/2015/01/egypt-cyber-security-council-privacy.html
[6] https://www.amnesty.org/en/latest/news/2014/06/egypt-s-attack-internet-privacy-tightens-noose-freedom-expression/

- The Egyptian Telecommunications Law no. 10/2003 safeguards the privacy of telecommunications and imposes penalties which account to imprisonment in some cases on the unauthorized violation of such privacy.
- The Mentally Disordered Care Law no. 71/2009 has clauses that ensure confidentiality of the patient's data.

One of the problems of not having a predominant data protection law is that there is no definition of personal data, private life or sensitive personal data under Egyptian law, the Constitutional Declaration or the New Constitution. Egyptian law does indeed provide examples, on a case-by-case basis, of the personal data that are protected under that particular law. Article 77 of the Labour Law, for example, provides that the employees' files that must be kept by the employer (as mentioned below) includes the employee's personal data such as his name, job, professional skills when he joined the workplace, domicile, marital status, salary, starting date of his work, the holiday leave he takes, punishments imposed on him and the reports of his superiors on his work. There is however, no universal definition of sensitive personal data under Egyptian law. This lack of an agreed-upon definition makes it difficult to legislate to protect it, and, with relevance to online data flows, makes it difficult to argue for different classification, and treatment or protection, of different type of data.

Similarly, there is lack of clarity around the appropriate use of the data, and the penalties for an infringement. According to the Egyptian Civil Code, the collection, use or processing of personal data is prohibited in case it violates the individual right to privacy and provided that such collection, use or processing constitutes a fault pursuant to the Egyptian Civil Code. A fault is defined by the judiciary, and is based on an act or omission that violates an obligation imposed by the law or runs contrary to assumed caution and care of the average man.

Finally, there is ambiguity around how the data can be collected. Currently, only data which is considered relevant to the subject's private life requires his/her consent for collection. Only a competent court will determine whether specific data is considered pertinent to the private life of the subject or not and whether the collection or

processing of such data violates an obligation imposed by the law or is evidence of a lack of caution and care that can be assumed of the average man. This means that ex-ante, it is difficult for a data processor to know what level of care to taken when collecting which element of personal data.

Note that the collection of data about the employee is required by law (Article 77 of the Egyptian Labour Law) which stipulates that that each employer must keep a file for each employee which includes their personal data. Only certain persons are authorised by the law to have access to such data.

The same general principles applicable to data collection and processing indicated above apply to the transfer of data; the data controller may not transfer data pertinent to the private life of the data subject except after obtaining the consent of the data subject, unless otherwise permitted by the law. Once again, the implication for a data processor is clear. It is difficult, if not impossible, to know ex-ante what data related to an individual can be moved offshore for processing, without exposing the firm to the vagaries of the interpretation of ‘private life’ and ‘private data’ by a court at some later date. As is clear, this does much to reduce business confidence, and introduces unnecessary ambiguity and concerns.

Kenya:

In Kenya, like in many other African countries, legislation and regulations covering the digital sphere have been helped if not driven by economic interests. A Data Protection Bill was drafted in 2012, circulated widely for feedback, and a subsequent draft forwarded to the Attorney General for publication. Over the past years, there have been numerous reports that the Bill is ready to be tabled to Parliament, but that has not yet happened. As of the writing of this report, the Data Protection Bill 2013 still awaits presentation in front of parliament, debate and then adoption.

As hinted above, the Data Protection Bill is being discussed as part of wider strategy by the Kenyan government called the 'Connected Kenya Master Plan (2012-2017)', which 'envisions the country as a globally competitive and respected knowledge-based economy [with] strengthen[ed] ICT business development.' The bill has been prepared alongside legislation on access to information which, if passed, would give

effect to Article 35 of the Kenyan Constitution which provides for citizens' right to access to information held by the country.'

The Data Protection Bill recognizes that 'data protection in relation to personal information is a corollary to the expectation of privacy, a human right that is in keeping with best international practices', reads the Bill's Memorandum. 'The Bill is borne out of the realization that data protection is crucial for the promotion of e-transactions in the global digital economy where a lot of information is processed automatically.'[7]

In the absence of the data protection bill, principles of privacy are protected by other more general, but broadly applicable legal instruments, including (1) Constitution (Article 31 specifically protects the right to privacy), (2) the 2009 Kenya Information and Communications Act which, under (a) its Article 31 penalises the unlawful interception of communications by service providers), (b) Article 83 which criminalizes wilful interception and provides guidelines for retention of data, and (c) Article 93 which provides guidance on data disclosure, and (4) the Kenya Information And Communications (Consumer Protection) Regulations, 2010, which makes it a criminal offense to monitor communication. However, these protections, particularly against surveillance, have eroded somewhat through recent developments, including (1) 2012 National Intelligence Service (NIS) Act, article 36 of which allows the rights to privacy set out in Article 31 of the Constitution, to be "limited in respect of a person suspected to have committed an offence to the extent that subject to section 42, the privacy of a person's communications may be investigated, monitored or otherwise interfered with", and also by (2) The Prevention of Terrorism Act 2012 which grants extensive powers to state authorities to limit fundamental freedoms and encroach on the right to privacy through surveillance. In light of the challenges highlighted above, the data Protection Bill when passed, would enshrine data protection further, and define clearer boundaries.

Once law, the Data Protection Bill will give effect to Article 31(c) of the Constitution, which outlines the right of every person not to have "information relating to their

[7] http://www.dataguidance.com/dataguidance_privacy_this_week.asp?id=2306

family or private affairs unnecessarily required or revealed" and Article 31(d), the right not to have " the privacy of their communications infringed". It will also regulate the collection, retrieval, processing, storing, use and disclosure of personal data. Yet the proposed legislation does not explicitly address the protection of data stored in the "cloud" (synchronised storage centres for digital data). Nevertheless, the enactment of the Data Protection Bill is crucial in that it will provide a clear legal framework on how personal information — from medical records, identification, banking information, educational records — being held by private and public institutions is stored, retrieved and disclosed to ensure that constitutional safeguards are clear, and subsequently enforced to protect the rights of individuals.

The proposed Bill will also provide clarity around exceptions. As an example, 31 of the Kenya Information and Communication Act clearly states that licensed telecommunication operators are legally prohibited from implementing technical requirements necessary to enable lawful interception, and section 15(1) of the Kenya Information and Communications (Consumer Protection) Regulations 2010, states that a licensee "shall not monitor, disclose or allow any person to monitor or disclose, the content of any information of any subscriber transmitted through the licensed systems by listening, tapping, storage, or other kinds of interception or surveillance of communications and related data".

However, the recently adopted Kenya Information and Communications (Registration of Subscribers of Telecommunication Services) Regulations 2014 permit access to private or confidential information on consumers without a court order.

One concern is contradicting legislations and guidelines that could come in, due to the prolonged delay in passing the Data Protection Bill. As an example, in December 2015 Kenya's Communications Authority invited the public to comment on the draft Kenya Information and Communications Regulations 2016. Clause 10 (1) of the Cybersecurity Regulations introduced requirements on data localisation which,

irrespective of their merits and demerits, could be more stringent, or at odds with the Data Protection Bill once it is finally approved[8].

Mauritius:

Mauritius has a strong legal framework and executive processes in place to ensure protection of personal data. It not only has a long history of involvement in these issues, but also is only the second non-European state, after Uruguay, to ratify the *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, also known as "Convention 108"[9].

Convention 108 is the first binding international instrument which protects the individual against abuses which may accompany the collection and processing of personal data, and which at the same time seeks to regulate the trans-frontier flow of personal data. In addition to providing guarantees with reference to the collection and processing of personal data, it outlaws the processing of "sensitive" data on a person's race, politics, health, religion, sexual life, criminal record, etc., in the absence of proper legal safeguards. The Convention also enshrines the individual's right to know that information is stored on him or her and, if necessary, to have it corrected. The Convention also imposes some restrictions on trans-border flows of personal data to States where legal regulation does not provide equivalent protection. Mauritius has already ratified the treaty, and it will enter into force on 1 October 2016.[10]. Being a signatory to the convention not only assures its own citizens of the highest standards of protection available to their data, but it also gives confidence to investors looking to start data processing business in Mauritius, and ensures that data processors operating in Mauritius can provide these services to other signatory countries.

The legislative instrument that guides data protection in Mauritius is the Data Protection Act that was enacted by the National Assembly in 2004 with the aim of protecting the fundamental privacy rights of individuals against the use of data

[8] https://www.article19.org/data/files/medialibrary/38413/Kenya-Cyber-Security-and-Electronic-Transactions-Legal-Analysis-21-April-2016.pdf

[9] http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=g57Ca9ut

[10] http://www.i-policy.org/2016/06/mauritius-joins-the-data-protection-convention-convention-108.html

concerning them without their informed consent. The Act came into operation in February 2009. The Data Protection Office, a public office under the aegis of the Ministry of Technology, Communication and Innovation, is the primary data protection authority in the country. The Data Protection Commissioner, who heads the Data Protection Office, is responsible for the enforcement of the Act.

Within the context of the Data Protection Act, 'Personal data' means (1) data which relate to an individual who can be identified from those data, and (2) data or other information, including an opinion forming part of a database, whether or not recorded in a material form, about an individual whose identity is apparent or can reasonably be ascertained from the data, information or opinion. Sensitive personal data is defined under the Act as personal information concerning a data subject and consisting of information pertaining to (1) racial or ethnic origin, (2) political opinion or adherence, (3) religious belief or other belief of a similar nature, (4) membership of a trade union, (5) physical or mental health, (6) sexual preferences or practices, (7) the commission or alleged commission of an offence, and (8) any proceedings for an offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

The Data Protection Act requires that all data controller and data processor must register in writing with the Data Protection Commissioner, including amongst other things, (1) a description of the personal data being, or to be processed by or on behalf of the data controller, and of the category of data, (2) subjects, to which the personal data relates, (3) a description of the purpose for which the personal data is or will be processed, (4) a description of any recipient to whom the data controller intends or may wish to disclose the personal data, (5) the names, or a description of, any country to which the data controller directly or indirectly transfers, or intends or may wish, directly or indirectly, to transfer the data, (6) the class of data subjects, or where practicable the names of data subjects, in respect of whom the data controller holds personal data.

A data controller must not collect personal data unless it is collected for a lawful purpose connected with the function or activity of the data controller, and the collection of the data is necessary for that purpose. If the data controller collects

personal data directly from the data subject, the data controller must at the time of collecting personal data ensure that the data subject concerned is informed of the fact that the data is being collected, the purpose or purposes for which the data is being collected, the intended recipients of the data, the consequences for that data subject if all or any part of the requested data is not provided, whether or not the data collected shall be processed and whether or not the consent of the data subject shall be required for such processing, and his right of access to, the possibility of correction of and destruction of, the personal data to be provided. Sensitive personal data cannot be processed unless the data subject has given his express consent to the processing of the personal data, or made the data public.

The above requirements will not apply to the processing of sensitive personal data if such processing is (1) necessary to (a) protect the vital interests of the data subject or another person, (b) for the performance of a contract to which the data subject is a party, (c) for compliance with a legal obligation to which the data controller is subject, (2) is required by any investigatory authority under the Financial Intelligence and Anti-Money Laundering Act, or (3) is required by law.

The Act provides that, personal data shall not be transferred to another country, unless that country ensures an adequate level of protection for the rights of data subjects in relation to the processing of personal data. The adequacy and the level of protection of a country shall be assessed in the light of all the circumstances surrounding the data transfer, having regard in particular to (1) the nature of the data, (2) the purpose and duration of the proposed processing, (3) the country of origin and the country of final destination, (4) the rules of law, both general and sectoral, in force in the country in question, and (5) any relevant codes of conduct or other rules and security measures which are complied with in that country. The above data protection principle shall not apply where (1) the data subject has given his consent to the transfer, or (2) the transfer is necessary (a) for the performance of a contract between the data subject and the data controller, or for the taking of steps at the request of the data subject with a view to his entering into a contract with the data controller, (b) for the conclusion of a contract between the data controller and a person, other than the data subject, which is entered into at the request of the data subject, or is in the interest of the data subject, or for the performance of such a

contract, or (c) in the public interest, to safeguard public security or national security. Finally, transfer is also allowed if it is made on 'such terms as may be approved by the Data Protection Commissioner as ensuring the adequate safeguards for the protection of the rights of the data subject.'

Morocco:

Morocco has a robust data protection framework in place to protect the privacy, security and integrity of data in the country. Personal data protection is governed in Morocco by the Law n° 09-08 (passed 220) relating to the protection of individuals with respect to the processing of personal data and by its implementation Decree n° 2-09-165 passed in 2009.

Law n° 09-08 was important because its article 1.1 provided a clear definition of personal data in Morocco, as "any information of any nature and independently of its format, including the sound and images relating to an identified or identifiable individual, referred to in the Law as a 'concerned individual.' A person is deemed identifiable when he or she can be identified directly or indirectly, especially by reference to an identification number or one or several specific elements of his or her physical, physiological, genetic, psychological, economic, cultural or social identity." Additionally, article 1.3 defined sensitive data as 'any information pertaining to a 'concerned individual' that reveals racial and ethnic origin, political, philosophical, religious opinions or trade union affiliation, or that concern sex life or health, including the genetic data.'

The primary data protection authority in the country is the Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel ('CNDP') (in English 'National Control Commission for the Protection of Personal Data'), which is responsible for enforcing the Law.

As per the law, the processing of any personal data requires a prior notification to the CNPD. In contrast, the processing of sensitive data or of personal data that includes ID card numbers requires a prior authorization from the CNDP. All applications – notification and authorization – require providing amongst other things, (1) the purpose(s) of processing the data, (2) the identity and the address of the data controller, (3) the personal data processed and the categories of persons about whom personal data are processed, (4) the time period for which the data will be

retained, (5) the recipients or categories of recipients of the personal data, and (6) the measures taken to ensure the security of the processing. Additional specific security measures are required when processing sensitive data.

Similarly, the law also provides guidance to processors. Any personal data must be collected for specific, explicit and legitimate purposes and be subsequently processed in accordance with these purposes for which they are collected, and all personal data must be accurate, comprehensive and, when necessary, kept up to date. The processing of personal data shall have received the individual's consent unless it is required by the law, a contract, or a public service, or circumstances in which 'the processing relates to achieving a legitimate interest of the data controller, balanced against the interests and fundamental rights and liberties of the concerned individual.'

Critically for the purposes of our paper, the transfer of a data subject's personal data to another country is allowed only if the country provides a sufficient level of protection in relation to an individuals' private life and fundamental rights and liberties. The sufficient nature of the protection is evaluated with regards to national laws and applicable security measures. Data controllers may transfer personal data out of Morocco to countries that are not deemed to offer adequate protection if the transfer is necessary to (1) safeguarding the individual's life, (2) safeguarding the public interest, (3) comply with obligations relating to the recognition, exercise or defense of a legal right, (4) to the performance of a contract between the data controller and the individual, or pre-contractual measures undertaken at the individual's request, and (5) to the conclusion or the performance of a contract in the interest of the individual, between the data controller and a third party.

The entity processing the data must take all reasonable precautions with regard to the nature of the data and the risk presented by the processing, in order to preserve the security of the data and, among other things, to prevent third parties gaining unauthorized access to such data.

Violations of the obligations set forth in the Law are punishable as an administrative and/or criminal offence.

It is interesting to note that although the provision of the Law n° 09-08 will clearly protect the privacy and personal data of Moroccan citizens, its main driving objective is to facilitate the growth of the digital economy by encouraging foreign investment, including in the offshoring and business process outsourcing business. With 52,000 jobs and MAD 7.6 billion of turnover at the end of 2011, the Moroccan offshoring market is 5 times larger than South Africa's, and to 4 times the size of the Tunisian or Egyptian offshoring market11. The protection of personal data transfer was seen critical to creating trust in the legal framework and is therefore one of the conditions and drivers of the development of new technologies and of the digital economy in Morocco. Since 2009, when the law was passed, unsurprisingly, Morocco has been making efforts to have its level of data protections recognized by the EU in order to promote further international business and encourage foreign investment.

South Africa:

In August 2013, the South African National Assembly passed the Protection of Personal Information (POPI) Bill, after more than four years of discussions and deliberations. In passing this bill, South Africa is preparing to fundamentally change the data privacy and protection environment for its citizens and business. The President promulgated the bill into law in November, although implementation of a large number of provisions in the act has not commenced yet, with broad expectation that the notification to this effect would come by end-2016.

The POPI Act is wide in its application and will, subject to certain exclusions, impact all persons processing personal information. European data protection practitioners will note that many aspects of POPI are based broadly on similar European legislation, including (1) the establishment of an Information Regulator to manage, monitor and enforce compliance, (2) a similar definition of Personal Data (referred to in POPI as Personal Information), and (3) the concepts of Data Subject, Data Processor (referred to in POPI as Operator), Processing and Data Controller (referred to in POPI as Responsible Party).

[11] http://www.lexology.com/library/detail.aspx?g=9bd21a58-fe63-4f20-8788-3a0dee604c66

Additionally, the right data principles introduced in POPI are similar to the seven data protection principles referred to in European legislation. The right principles at the heart of POPI are:

1. Accountability – the Responsible Party is accountable for ensuring compliance
2. Processing Limitation – setting out the rules for how Personal Information will be processed lawfully, in a reasonable manner that does not infringe the privacy of the Data Subject and with either the Data Subject's consent or in fulfilling certain other requirements such as the legitimate interest of the Data Subject
3. Purpose Specification – Personal Information must be collected for a specified purpose of which the Data Subject is aware
4. Further Processing Limitation – Further processing of Personal Information must be compatible with the purpose for which it was collected
5. Information Quality – The Responsible Party must take reasonable practical steps to ensure that the Personal Information is complete, accurate, not misleading and updated where necessary
6. Openness – The Responsible Party is required to notify both the Information Regulator and the Data Subject before it may process Personal Information
7. Security Safeguards – The Responsible Party is required to ensure the integrity of the Personal Information in its possession or under its control by implementing appropriate, reasonable, technical and organisational measures to prevent loss, damage or destruction of Personal Information or unlawful processing
8. Data Subject Participation – the Data Subject has the right to access and request information about his/her Personal Information held by a Responsible Party and require the Responsible Party to correct or destroy Personal Information

What distinguishes the situation after POPI with the past, when the interpretation of personal data was largely left to interpretation, is the precise and broadly-scoped definition of "Personal Information". Under POPI, Personal Information includes

information relating to both an identifiable, living, natural person, and where applicable, an identifiable juristic person, and includes:

- information about a person's race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth;
- information relating to education, medical, financial, criminal or employment history;
- any identifying number, symbol, email address, physical address, telephone number or other particular assignment to the person;
- the blood type or any other biometric information of the person;
- the personal opinions, views or preferences of the person;
- correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
- the views or opinions of another individual about that person; and
- the name of the person, if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.

The POPI Act allows a data subject the right to request that a responsible party correct or delete personal information that is inaccurate, irrelevant and excessive, or which the responsible party is no longer authorized to retain.

The primary government institution responsible for overseeing the execution and implementation of POPI is the Information Regulator, which has already been established under the law. In the performance of its functions, the Regulator is obliged to have due regard to and take account of (1) the information protection conditions, (2) the protection of all human rights and social interests which compete with the right to privacy (including the desirability of the free flow of information), (3) international obligations accepted by South Africa, and (4) developing international guidelines relevant to the protection of individual privacy. On the other hand, the critical role of the Information Protection Officer in public and private bodies who will

be responsible for ensuring compliance of their organization, and will liaise with the Information Regulator to ensure the act is implemented.

Under the POPI Act, personal information may only be processed if the data subject (or a competent person where the data subject is a child) expressly consents to the processing of the personal information, unless the exclusions with regard to consent apply. The consent of the data subject is not required where the processing of personal information (1) is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is party, (2) complies with an obligation imposed by law on the responsible party, (3) protects a legitimate interest of the data subject, (4) is necessary for the proper performance of a public law duty by a public body; or (5)is necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied.

Finally, and is most relevant to this paper, the POPI Act makes the transfer of Personal Information outside of South Africa subject to certain exceptions -- broadly determined by whether the transfer is in the best interest of the Data Subject or whether the Data Subject has consented. Critically. It requires the data recipient (in a foreign country) to be subject to a law or contract which (1) upholds principles of reasonable processing of the information that are substantially similar to the principles contained in the POPI Act, and (2) includes provisions that are substantially similar to those contained in the PPI Act relating to the further transfer of personal information from the recipient to third parties.

While the actual stringency with which POPI is implemented still remains to be seen, given that it has not come into force yet, it is expected that POPI will significantly increase the safeguards available to ordinary citizens and business. At the same time, however, it will significantly increase the administrative burden of companies of all sizes. Companies will need to invest in a number of areas including upgraded technologies, enhanced managerial skills, tighter processes to ensure consent of data subjects. The economic costs of these measures, and how they impact the economy at large, are what we wish to aim to study in this report.

Discussion and Conclusion

We applied the proposed model to the five countries chosen. The model was populated with data. The staging framework was then used to score the indicators 1-3 and the resulting framework has been color-coded. The detailed results are shown in the appendix.

The summary results are shown in Table 2 below. South Africa and Mauritius are the two countries that have made the most progress in terms of their cloud-readiness, with Egypt worst-placed.

However, looking at the individual pillars shows that even the most well-placed countries have opportunities to make progress – and learn from the progress made by others - in specific pillars. This is reflected in Figure 1.

Table 2: Applying the pillars to the five Africa countries

Pillars	Egypt	Kenya	Mauritius	Morocco	South Africa
Standards	0.24	0.25	0.25	0.25	0.25
Policy	0.37	0.39	0.49	0.48	0.52
Infrastructure	0.12	0.24	0.15	0.20	0.22
Access	0.24	0.16	0.24	0.25	0.24
Training, Skills and Awareness	0.17	0.16	0.24	0.19	0.22
Networked Business	0.16	0.20	0.22	0.14	0.24
Networked Government	0.15	0.21	0.21	0.17	0.14
Operations	0.15	0.16	0.26	0.20	0.21
Freedom, Expression and Lifestyles	0.15	0.22	0.22	0.22	0.25
Overall Score	0.21	0.24	0.28	0.26	0.28

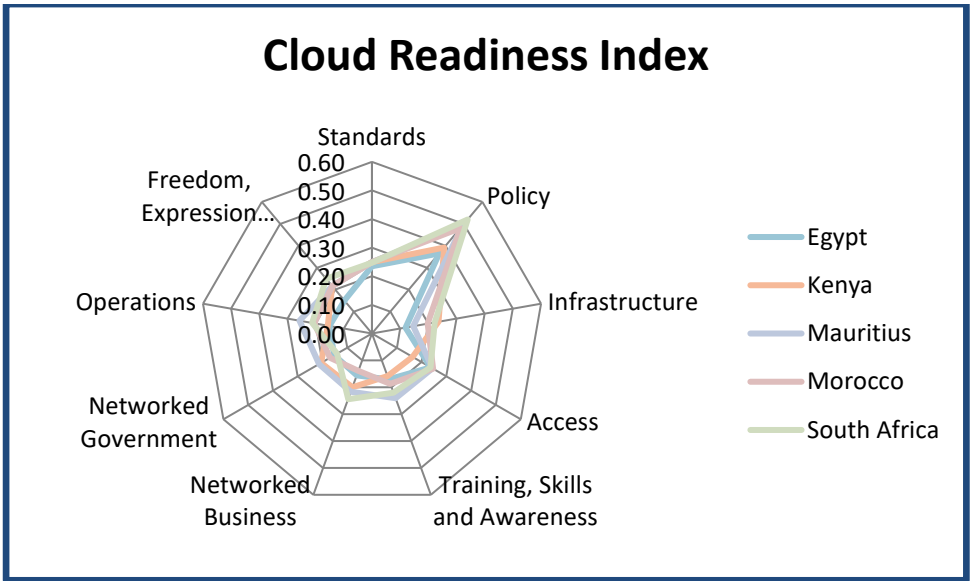

Figure 1: Cloud Readiness Index in the five countries

Finally, going one step further to look at the 38 indicators presents a rich amount of actionable data and insights that can be used to guide further action. As one example, see Open Standards, where South Africa, despite its overall lead, has huge opportunities to improve. This data is provided in Table 3.

Table 3: Indicators applied on the five countries

Pillars	Indicator	Egypt	Kenya	Mauritius	Morocco	South Africa
Standards	S1 Standards-Making Institutions	0.30	0.30	0.30	0.30	0.30
	S2 Alignment to International Standards	0.75	0.75	0.75	0.75	0.75
	S3 Open Standards	0.75	0.75	0.75	0.75	0.38
	S4 Standards Framework	0.25	0.25	0.25	0.25	0.75
	S5 Trade Standards	0.30	0.45	0.45	0.45	0.30
Policy	P1 Privacy Policy	0.20	0.41	0.52	0.53	0.57
	P2 Intellectual Property Protection Policy and Effectiveness	0.38	0.41	0.41	0.41	0.36
	P3 Data Protection Policy	0.15	0.15	0.30	0.23	0.38
	P4 Cyber Security Policy	0.45	0.40	0.45	0.45	0.35
	P5 Cyber Crime Policy	0.35	0.40	0.40	0.40	0.45
	P6 Data Sovereignty and Portability	0.30	0.20	0.40	0.40	0.50
Infrastructure	I1. Fixed Network Performance	0.38	0.50	0.56	0.44	0.56
	I2. Mobile Network Performance	0.31	0.56	0.00	0.44	0.56
	I3 International Connectivity: Bandwidth Per Capita	0.40	1.20	0.80	0.80	0.80
	I4 Internet Server Infrastructure	0.10	0.10	0.10	0.30	0.30
Access	N1 Mobile Penetration	0.20	0.10	0.30	0.30	0.30
	N2 PC Penetration	0.50	0.30	0.50	0.50	0.50
	N3 Internet Penetration	0.40	0.27	0.53	0.60	0.47
	N4 Broadband Subscriptions	0.50	0.40	0.40	0.30	0.50
	N5 Affordable Access	0.47	0.27	0.40	0.47	0.40

	N6 Industry Structure	0.30	0.30	0.30	0.30	0.20
Training, Skills and Awareness	T1 Quality of education	0.35	0.88	0.88	0.70	0.61
	T2 Educational Enrolment	0.78	0.36	0.84	0.48	0.78
	T3 Trained Workforce	0.58	0.35	0.69	0.69	0.81
Networked Business	B1 Technology adoption by business	0.56	0.67	0.67	0.56	0.78
	B2 ICT, Business and Skills	0.67	0.67	0.83	0.50	1.00
	B3 ICT and Business Innovation	0.33	0.67	0.67	0.33	0.67
Networked Government	G1 ICT Vision and Leadership	0.42	0.83	0.92	0.58	0.42
	G2.1 Government ICT Services	0.78	0.56	0.56	0.44	0.67
	G3.1 Gov't Procurement Leadership	0.33	0.67	0.67	0.67	0.33
Operations	O1 Labor Cost and Availability	0.20	0.35	0.30	0.30	0.20
	02 Political Risks	0.20	0.20	0.60	0.40	0.60
	O3 Energy Availability	0.40	0.15	0.40	0.30	0.40
	O4 Energy Reliability	0.27	0.27	0.60	0.60	0.40
	O5 Energy Affordability	0.15	0.15	0.45	0.15	0.30
	06 Operational Complexity	0.30	0.45	0.23	0.30	0.23
Freedom, Expression and Lifestyles	F1 Lifestyle and Expression	1.00	0.67	0.67	1.17	1.00
	F2 Freedom of Expression & Lack of Censorship	0.50	1.50	1.50	1.00	1.50

The proposed model achieves three core objectives

1. Presenting the intellectual foundation for a more robust, cloud readiness framework that speaks to the unique challenges of developing countries in general, and the African continent in particular.
2. It allows a very insightful and nuanced appreciation of the progress that countries are making towards cloud readiness. Most critically, it has shown that countries have uneven strengths (and catch-up areas) in making progress; South Africa which seems best prepared across the continent in terms of cloud readiness can use this framework to pinpoint areas of improvement, for example in the Networked Government indicator.
3. By highlighting the areas for concern, and pinpointing actionable areas, the model becomes a playbook that countries and national governments across the continent can use to plan their progress in terms of cloud readiness.

In conclusion, we believe that this proposed cloud readiness index can be a great generic resource for countries in emerging markets to evaluate their progress in cloud computing.

References

[1] CID (2000), “The Readiness for the Networked World: A guide for Developing Countries,” Information Technology Group, Center for International Development, Harvard University: Available on-line at (http://www.readinessguide.org)

[2] Bridges (2002), “Comparison of E-readiness Assessment Models” available at http://www.bridges.org/ereadiness/tools.html

[3] Bui, T. X., S. Sankaran & I. M. Sebastian. 2003. A Framework for Measuring National E-Readiness. International Journal of Electronic Business. 1: 3–22.

[4] Ghavamifar, A., L. Beig & G. Montazer. 2008. The Comparison of Different E-Readiness Assessment Tools. In Information and Communication Technologies: From Theory to Applications, 2008. ICTTA 2008. 3rd International Conference on, IEEE. 1–5.

[5] InfoDev, (2003). India: E-Readiness Assessment Report 2003 for States/Unions Territories and Central Ministries/Departments. Department of Information Technology. World Bank Group. On-line: http://www.mit.gov.in/ereadiness/index.asp

[6] S. Dutta and I Mia (2010), Global Information Technology Report 2010-2011, World Economic Forum, 2011

[7] Youssef, A. E. 2012. Exploring Cloud Computing Services and Applications. Journal of Emerging Trends in Computing and Information Sciences. 3.

[8] Mell, P. & T. Grance. 2011. The NIST Definition of Cloud Computing (draft). NIST Special Publication. 800: 145.

[9] Kurdi, R., A. Taleb-Bendiab, M. Randles & M. Taylor. 2011. EGovernment Information Systems and Cloud Computing (Readiness and Analysis). In Developments in E-systems Engineering (DeSE), IEEE. 404–409.

[10] Craig, R., J. Frazier, N. Jacknis, S. Murphy, C. Purcell, P. Spencer & J. Stanley. 2009. Cloud Computing in the Public Sector: Public Manager’s Guide to Evaluating and Adopting Cloud Computing. White Paper. Cisco Internet Business Solutions Group. Availble: www.cisco.com/web/about/ac79/docs/sp/Cloud_Computing.pdf.

[11] Rastogi, A. .2010. A model Based Approach to Implement Cloud Computing in e-Governance. International Journal of Computer Applications. 9: 15–18.

[12] Brian, H., T. Brunschwiler, H. Dill, H. Christ, B. Falsafi, M. Fischer, S. G. Grivas, C. Giovanoli, R. E. Gisi & R. Gutmann. 2008. Cloud Computing. Communications of the ACM. 51: 9–11.

[13] Bhardwaj, S., L. Jain & S. Jain. 2010. Cloud Computing: A Study of Infrastructure as aA Service (IAAS). International Journal of Engineering and Information Technology. 2: 60–63.

[14] Galal-edeen, A. a. 2012. Proposed Development Model of eGovernment to Appropriate Cloud Computing. International Journal of Reviews in Computing. 9: 7.

[15] ATSE. 2010. Cloud Computing: Opportunities and Challenges for Australia, report of a study by the Australian academy of Technological sciences and engineering (ATSE). Availble: http://www.egov.vic.gov.au/trends-and-issues/information-andcommunications-technology/cloud-computing/cloud-computingopportunities-and-challenges-for-australia-in-pdf-format-1367kb.html

[16] Sahu, B. L. & R. Tiwari. 2012. A Comprehensive Study on Cloud Computing. International Journal. 2.

[17] G.S. Kirkman, The Networked Readiness Index: Measuring the Preparedness of Nations for the Networked World, Global Information Technology Report 2003-2004, World Economic Forum, 2004

[18] Ismail, H. A. A. 2008. Citizens' Readiness for E-Government in Developing Countries. Middlesex University.

[19] ITU. 2012. Measuring the Information Society. Available: http://www.itu.int/en/publications/ITU-D/Pages/default.aspx.

[20] ITU. 2009. e-Government Implementation Toolkit, introduction: eGovernment Readiness Assessment Framework. Available: http://www.itu.int/ITU-D/ict/publications/idi/

[21] [22] E. I. Unit, 2010. Digital economy rankings 2010: Beyond e-readiness, A report from the Economist Intelligence Unit. Available: http://www.eiu.com/site_info.asp?info_name=digitaleconomy_2010.
[23] Ojo, A., T. Janowski & E. Estevez. 2005. Determining Progress Towards e-Government-What are the Core Indicators? 5th European Conference on e-Government, Antwerpen. 313–322.
[24] UNDESA. 2012. The United Nations e-Government Survey: EGovernment for the People. Available: http://www.unpan.org/egovkb/global_reports.
[25] Fathey, M & O. Ibrahim, 2013, Refining E-government Readiness Index by Cloud Computing, JurnalTeknologi 65:1 (2013) 23-34
[26] E. I. Unit, 2001. The Economist Intelligence Unit/Pyramid Research ereadiness Rankings. Retrieved June. 8.
[27] E. I. Unit, 2002. The Economist Intelligence Unit e-readiness Rankings, July 2002. Economist Intelligence Unit.
[28] E. I. Unit, 2003. The 2003 e-readiness Rankings. Economist Intelligence Unit.
[29] E. I. Unit, 2004. IBM Corporation. 2004. Scandinavia Consolidates Lead in Fifth Annual Economist Intelligence Unit e-readiness rankings.
[30] E. I. Unit, 2005. The 2005 e-readiness rankings, Economist Intelligence Unit.
[31] E. I. Unit, 2006. The 2006 E-readiness Rankings: Raising the Bar. Economist Intelligence Unit.
[32] E. I. Unit, 2007. The 2007 e-readiness Rankings: A White Paper. Economist Intelligence Unit.
[33] E. I. Unit, 2008. E-readiness Rankings 2008, Maintaining Momentum: A White Paper from the Economist Intelligence Unit. London, United Kingdom: Economist Intelligence Unit and The IBM Institute.
[34] E. I. Unit, 2009. E-readiness Rankings 2009: The Usage Imperative. The Economist. A report from the Economist Intelligence Unit written in cooperation with the IBM Institute for Business Value.
[35] EIU. 2007. The 2007 e-readiness rankings: Raising the bar, A white paper from the Economist Intelligence Unit. Available: http://www.eiu.com/site_info.asp?info_name=eiu_2007_e_readiness_r ankings.
[36] Huang, J. H. et. Al, ”An e-readiness Assessment Framework and Two Field Studies”, Communications of the Association for Information Systems, 14 (19), 364-386, 2004.
[37] KASHORDA, M and T. M WAEMA, ICT Indicators in Higher Education: Towards an E-readiness Assessment Model , Proceedings and reports of the 4th UbuntuNet Alliance annual conference, 2011, pp 57-76
[38] Kundra, V. 2010. State of Public Sector Cloud Computing. Washington. DC: CIO Council.
[39] Harris, J. G. & A. E. Alter. 2010. Cloudrise: Rewards and Risks at the Dawn of Cloud Computing.

Appendices

Appendix 1: Proposed Model with Weightage, Data Sources and Data Types

Pillars	Pillar Weightage		Indicator	Sub-Indicator
Standards	10 %	S1 Standards-Making Institutions	10%	S1.1 Is there a regulatory body responsible for standards development for the country?
		S2 Alignment to International Standards	25%	S2.1 Does the government participate in international standards-setting process?
				S2.2 Are international standards favored over domestic standards?
		S3 Open Standards	25%	S3.1 Are there any laws or policies in place that implement technology neutrality in government?
				S3.2 Are cloud computing services able to operate free from laws or policies that mandate the use of certain products (including, but not limited to types of software), services, standards or technologies?
				S3.3 Are cloud computing services able to operate free from laws or policies that establish preferences for certain products (including, but not limited to types of software), services, standards or technologies?
				S3.4 Are cloud computing services able to operate free from laws that discriminate based on the nationality of the vendor, developer or service provider?
		S4 Standards Framework	25%	S4.1 Are there laws, regulations or policies that establish a standards setting framework for interoperability and portability of data?
		S5 Trade Standards	15%	S5.1 Is the downloading of applications or digital data from foreign cloud based service providers free from tariff or other trade barriers?
Policy	20 %	P1 Privacy Policy	20%	P1.1 Are there laws or regulations governing the collection, use or other processing of personal information?
				P1.2 Is there an effective agency (or regulator) tasked with the enforcement of privacy laws?
				P1.3 Is there a strict consent requirement for the collection, storage and dissemination of personal data?
				P1.4 Does the law provide users with the right to review their stored information?
				P1.5 Does the law provide users with the right to be forgotten or deleted?
				P1.6 Are there administrative sanctions for non-compliance? How much? (None, Medium, Severe)
				P1.7 Is notification of breaches towards the government and/or users obligatory (None, Govt or User, Both)
		P2 Intellectual Property Protection Policy and Effectiveness	15%	P2.1 Is the country a member of TRIPS agreement?
				P2.2 Have IP laws been enacted to implement TRIPS
				P2.3 Is the country party to the WIPO Copyright Treaty?
				P2.4 Are criminal sanctions available for unauthorized making available of copyright materials digitally?
				P2.5 Are there laws governing ISPs liability for content that infringes copyright?
				P2.6 Software piracy rate, % software installed

				P2.7 Perception of Effectiveness: Intellectual property protection, 1-7 (best)
		P3 Data Protection Policy	**15%**	**P3.1 Is there a Data Protection Policy in place?**
				P3.2 Are data protection impact assessments obligatory?
				P3.3 Is a data protection officer required?
				P3.4 Are firms required to retain data for a fixed period of time?
		P4 Cyber Security Policy	**15%**	**P4.1 Is there a law or regulation that gives electronic signatures clear legal weight?**
				P4.2 Are ISPs and content service providers free from mandatory filtering or censoring
				P4.3 Global Cybersecurity Index
		P5 Cyber Crime Policy	**15%**	**P5.1 Are cybercrime laws in place?**
				P5.2 Are cybercrime laws consistent with the Budapest Convention on Cybercrime?
				P5.3 Laws relating to ICTs, 1-7 (best)
		P6 Data Sovereignty and Portability	**20%**	**P6.1 Are there rules for differentiated treatment of data based on data classification, i.e. different treatment for data of different levels of sensitivity?**
				P6.2 Is there a data localization requirement (i.e. is the transfer of data outside of country borders disallowed) (No, Limited, Both)
Infrastructure	**10 %**	**I1. Fixed Network Performance**	**25%**	**I1.1 Fixed Internet - upload (UL) speeds in kilobits per second (kbps)**
				I1.2 Fixed Internet - download (DL) Speed in kilobits per second (kbps)
				I1.3 Fixed Internet - latency in milliseconds (ms)
				I1.4 Fixed Broadband Quality: Avg. Page Load Time (ms)
		I2. Mobile Network Performance	**25%**	**I2.1 Mobile Internet - upload (UL) speeds in kilobits per second (kbps)**
				I2.2 Mobile Internet - download (DL) Speed in kilobits per second (kbps)
				I2.3 Mobile Internet - latency in milliseconds (ms)
				I2.4 Mobile Broadband Quality: Avg. Page Load Time (ms)

		I3 International Connectivity: Bandwidth Per Capita	40%	I3.1 Bandwidth Per Capita (Int'l Internet bandwidth, kb/s per user)
		I4 Internet Server Infrastructure	10%	I4.1 Secure Internet servers/million pop.
Access	10 %	N1 Mobile Penetration	10%	N1.1 Mobile phone subscriptions/100 pop.
		N2 PC Penetration	20%	N2.1 Households w/ personal computer, %
				N2.2 Availability of latest technologies, 1-7 (best)
		N3 Internet Penetration	20%	N3.1 Households w/ Internet access, %
				N3.2 Mobile network coverage, % pop.
				N3.3 Individuals using Internet, %
		N4 Broadband Subscriptions	20%	N4.1 Fixed broadband Internet subs/100 pop.
				N4.2 Mobile broadband subs/100 pop.
		N5 Affordable Access	20%	N5.1 Prepaid mobile cellular tariffs, PPP $/min.
				N5.2 Fixed broadband Internet tariffs, PPP $/month
				N5.3 Mobile-broadband as % of GNI per capita
		N6 Industry Structure	10%	N6.1 Internet & telephony competition, 0–2 (best)
Training, Skills and Awareness	10 %	T1 Quality of education	35%	T1.1 Quality of educational system, 1-7 (best)
				T1.2 Quality of primary education, 1-7 (best)
				T1.3 Quality of management schools, 1-7 (best)
				T1.4 Quality of math & science education, 1-7 (best)
		T2 Educational Enrolment	30%	T2.1 Primary education enrollment rate (net), %
				T2.2 Secondary education gross enrollment rate, %
				T2.3 Tertiary education gross enrollment rate, %
				T2.4 Expected years of schooling
				T2.5 Mean years of schooling
		T3 Trained Workforce	35%	T3.1 Adult literacy rate, %
				T3.2 % of workforce with tertiary degree
				T3.3 Graduates in science & engineering, %
Networked Business	10 %	B1 Technology adoption by business	33%	B1.1 Firm-level technology absorption, 1-7 (best)
				B1.2 ICT use for business-to-business transactions, 1-7 (best)
				B1.3 Business-to-consumer Internet use, 1-7 (best)
		B2 ICT, Business and Skills	33%	B2.1 Extent of staff training, 1-7 (best)
				B2.2 Knowledge-intensive jobs, % workforce
		B3 ICT and Business Innovation	33%	B2.1 Impact of ICTs on business models, 1-7 (best)
				B2.2 Impact of ICTs on new organizational models, 1-7 (best)
Networked	10	G1 ICT Vision	33%	G1.1 Importance of ICTs to gov't vision, 1-7 (best)

Govnt	**%**	**and Leadership**		
				G1.2 Gov't success in ICT promotion, 1-7 (best)
				G1.3 Impact of ICTs on access to basic services, 1-7 (best)
				G.1.4 Internet access in schools, 1-7 (best)
		G2.1 Government ICT Services	**33%**	**G2.1 Government Online Service Index, 0–1 (best)**
				G2.2 ICT use & gov't efficiency, 1-7 (best)
				G2.3 E-Participation Index, 0–1 (best)
		G3.1 Gov't Procurement Leadership	**33%**	**G3.1 Gov't procurement of advanced tech, 1-7 (best)**
Operations	**10 %**	**O1 Labor Cost and Availability**	**15%**	**O1.1 Ranking on labor cost (Pay and productivity, 1-7 (best))**
				O1.2 Availability of Scientists and engineers
				O1.3 Availability of research and training services
		02 Political Risks	**20%**	**O2.1 Ranking on political stability**
		O3 Energy Availability	**15%**	**O3.1 Electricity production, kWh/capita**
				O3.2 % of population with access to electricity
				O3.3 Electricity Consumption (MWh /Capita)
		O4 Energy Reliability	**20%**	**O4.1 Quality of Electricity Supply**
				O4.2 Energy Architecture: Economic Development and Growth
				O4.3 Energy Architecture: Access and Security
		O5 Energy Affordability	**15%**	**O5.1 Cost of getting electricity (% of income per capita)**
		06 Operational Complexity	**15%**	**061 No. procedures to enforce a contract**
				06.2 No. days to enforce a contract
Freedom, Expression and Lifestyles	**10 %**	**F1 Lifestyle and Expression**	**50%**	**F1.1.1 Use of virtual social networks, 1-7 (best)**
				F1.1.2 Wikipedia edits/mn pop. 15–69.
				F1.1.3 Video uploads on YouTube/pop. 15–69.
		F2 Freedom of Expression & Lack of Censorship	**50%**	**F2.1.1 Freedom on the Net Status (Freedom Score 0 = Best, 100 = Worst)**

Appendix 2: Proposed Model With Live Data

Sub-Indicator	Egypt	Kenya	Mauritius	Morocco	South Africa
S1.1 Is there a regulatory body responsible for standards development for the country?	Y	Y	Y	Y	Y
S2.1 Does the government participate in international standards-setting process?	Y	Y	Y	Y	Y
S2.2 Are international standards favored over domestic standards?	Yes	Yes	Yes	Yes	Yes
S3.1 Are there any laws or policies in place that implement technology neutrality in government?	Yes	Yes	Yes	Yes	No
S3.2 Are cloud computing services able to operate free from laws or policies that mandate the use of certain products (including, but not limited to types of software), services, standards or technologies?	Yes	Yes	Yes	Yes	Medium
S3.3 Are cloud computing services able to operate free from laws or policies that establish preferences for certain products (including, but not limited to types of software), services, standards or technologies?	Yes	Yes	Yes	Yes	Medium
S3.4 Are cloud computing services able to operate free from laws that discriminate based on the nationality of the vendor, developer or service provider?	Yes	Yes	Yes	Yes	No
S4.1 Are there laws, regulations or policies that establish a standards setting framework for interoperability and portability of data?	No	No	No	No	Yes
S5.1 Is the downloading of applications or digital data from foreign cloud based service providers free from tariff or other trade barriers?	Limited	Yes	Yes	Yes	Limited
P1.1 Are there laws or regulations governing the collection, use or other processing of personal information?	No	Yes	Yes	Yes	Y
P1.2 Is there an effective agency (or regulator) tasked with the enforcement of privacy laws?	No	No	Yes	Yes	Yes
P1.3 Is there a strict consent requirement for the collection, storage and dissemination of personal data?	n	y	y	y	y
P1.4 Does the law provide users with the right to review their stored information?	n	y	y	y	y
P1.5 Does the law provide users with the right to be forgotten or deleted?	n	n	y	y	y
P1.6 Are there administrative sanctions for non-compliance? How much? (None, Medium, Severe)	n	m	n	m	m
P1.7 Is notification of breaches towards the government and/or users obligatory (None, Govt or User, Both)	n	n	Govt or User	n	yes
P2.1 Is the country a member of TRIPS agreement?	Yes	Yes	Yes	Yes	Yes
P2.2 Have IP laws been enacted to implement TRIPS	Yes	Yes	Yes	Yes	Yes
P2.3 Is the country party to the WIPO Copyright Treaty?	No	Yes	Yes	Yes	No
P2.4 Are criminal sanctions available for unauthorized making available of copyright materials digitally?	Yes	Yes	Yes	Yes	Yes
P2.5 Are there laws governing ISPs liability for content that infringes copyright?	No	Yes	Yes	Yes	Yes
P2.6 Software piracy rate, % software installed	62	78	55	66	34
P2.7 Perception of Effectiveness: Intellectual property protection, 1-7 (best)	3.237102	3.692129	4.421032	4.029583	5.410273

P3.1 Is there a Data Protection Policy in place?	No	No	Yes	Yes	Yes
P3.2 Are data protection impact assessments obligatory?	n	n	n	n	y
P3.3 Is a data protection officer required?	n	n	y	n	y
P3.4 Are firms required to retain data for a fixed period of time?	n	n	n	n	n
P4.1 Is there a law or regulation that gives electronic signatures clear legal weight?	Yes	Yes	Yes	Yes	Yes
P4.2 Are ISPs and content service providers free from mandatory filtering or censoring	No	Yes	Yes	Yes	Yes
P4.3 Global Cybersecurity Index	0.588 (9)	0.412 (15)	0.588 (9)	0.559 (10)	0.382 (16)
P5.1 Are cybercrime laws in place?	Yes	Yes	Yes	Yes	Yes
P5.2 Are cybercrime laws consistent with the Budapest Convention on Cybercrime?	No	Yes	Yes	Yes	Yes
P5.3 Laws relating to ICTs, 1-7 (best)	3.051598	4.184687	4.436834	3.885928	4.568996
P6.1 Are there rules for differentiated treatment of data based on data classification, i.e. different treatment for data of different levels of sensitivity?	No	No	Yes	Yes	Yes
P6.2 Is there a data localization requirement (i.e. is the transfer of data outside of country borders disallowed) (No, Limited, Both)	limited	no	no	no	limited
I1.1 Fixed Internet - upload (UL) speeds in kilobits per second (kbps)	654	4462	7124	585	1436
I1.2 Fixed Internet - download (DL) Speed in kilobits per second (kbps)	1913	4879	12633	3800	3727
I1.3 Fixed Internet - latency in milliseconds (ms)	91	75	54	111	53
I1.4 Fixed Broadband Quality: Avg. Page Load Time (ms)	3530	5257	_	3772	3697
I2.1 Mobile Internet - upload (UL) speeds in kilobits per second (kbps)	716	2838	_	836	1649
I2.2 Mobile Internet - download (DL) Speed in kilobits per second (kbps)	1959	5257	_	3806	4158
I2.3 Mobile Internet - latency in milliseconds (ms)	162	136	_	148	109
I2.4 Mobile Broadband Quality: Avg. Page Load Time (ms)	3642	7006	_	4097	5666
I3.1 Bandwidth Per Capita (Int'l Internet bandwidth, kb/s per user)	4.2	23.7	16.1	14.9	18.1
I4.1 Secure Internet servers/million pop.	5.442142	9.142177	6.166822	175.827	129.9745
N1.1 Mobile phone subscriptions/100 pop.	114.306	73.84325	132.2498	131.7131	149.1935
N2.1 Households w/ personal computer, %	45.08	12.27	51.27	52.5	28.05
N2.2 Availability of latest technologies, 1-7 (best)	3.87596	5.053436	5.010247	5.051488	5.340807
N3.1 Households w/ Internet access, %	36.78	16.9	47.53	50.4	37.3
N3.2 Mobile network coverage, % pop.	99.8	89.08	99	99.2	99.9
N3.3 Individuals using Internet, %	31.7	43.4	41.44	56.8	49
N4.1 Fixed broadband Internet subs/100 pop.	34.88214	74.18518	42.35391	27.65251	30.59528
N4.2 Mobile broadband subs/100 pop.	43.49516	9.093004	31.74156	26.82478	46.69968
N5.1 Prepaid mobile cellular tariffs, PPP $/min.	0.065113	0.098947	0.178141	0.142173	0.222511
N5.2 Fixed broadband Internet tariffs, PPP $/month	34.88214	74.18518	42.35391	27.65251	30.59528
N5.3 Mobile-broadband as % of GNI per capita	2.7	5.89	1.43	4.73	1.48
N6.1 Internet & telephony competition, 0–2 (best)	1.6	2	2	2	1.066667
T1.1 Quality of educational system, 1-7 (best)	2.135099	4.328674	4.093514	2.774101	2.248946
T1.2 Quality of primary education, 1-7 (best)	2.128913	3.710753	4.371876	2.995655	2.544361

T1.3 Quality of management schools, 1-7 (best)	2.530363	4.350288	4.268504	4.07014	5.231128
T1.4 Quality of math & science education, 1-7 (best)	2.557214	3.948601	4.410402	4.003753	1.969974
T2.1 Primary education enrollment rate (net), %	95.10083	83.57701	98.12052	98.27114	89.55526
T2.2 Secondary education gross enrollment rate, %	86.04825	67.64039	97.93816	69.06295	98.22828
T2.3 Tertiary education gross enrollment rate, %	30.05602	4.04812	40.32104	16.15857	19.2
T2.4 Expected years of schooling	12.22	11.05	13.6	11.17	13.1
T2.5 Mean years of schooling	7.5	7	7.2	4.4	8.5
T3.1 Adult literacy rate, %	75.23647	77.96503	90.62253	72.37732	94.26664
T3.2 % of workforce with tertiary degree	18.7	3	11.2	9.2	17.1
T3.3 Graduates in science & engineering, %	11.8	n/a	22.9	34.9	19
B1.1 Firm-level technology absorption, 1-7 (best)	3.842309	4.839742	5.02873	4.528695	5.434675
B1.2 ICT use for business-to-business transactions, 1-7 (best)	4.704924	5.097343	4.595579	4.201857	5.291157
B1.3 Business-to-consumer Internet use, 1-7 (best)	4.047321	4.736793	3.764591	4.083482	4.568877
B2.1 Extent of staff training, 1-7 (best)	2.739614	4.229302	4.507137	3.351711	4.857138
B2.2 Knowledge-intensive jobs, % workforce	36.25113	n/a	20.37445	6.78555	24.77639
B2.1 Impact of ICTs on business models, 1-7 (best)	3.767109	4.835889	4.531895	4.080813	4.537622
B2.2 Impact of ICTs on new organizational models, 1-7 (best)	3.825423	4.379862	4.411389	3.673162	4.350339
G1.1 Importance of ICTs to gov't vision, 1-7 (best)	2.568976	4.711957	4.550813	4.305306	3.295684
G1.2 Gov't success in ICT promotion, 1-7 (best)	3.300611	4.929681	4.868032	4.487711	3.828671
G1.3 Impact of ICTs on access to basic services, 1-7 (best)	3.816415	4.345078	4.544787	3.616595	3.400331
G.1.4 Internet access in schools, 1-7 (best)	2.702613	3.975781	4.333058	3.13502	3.104099
G2.1 Government Online Service Index, 0–1 (best)	0.6013	0.4314	0.4314	0.2484	0.4575
G2.2 ICT use & gov't efficiency, 1-7 (best)	3.841006	4.415458	4.409158	4.101765	3.77423
G2.3 E-Participation Index, 0–1 (best)	0.6842	0.0526	0.0789	0	0.1579
G3.1 Gov't procurement of advanced tech, 1-7 (best)	3.250229	3.683667	3.688387	3.735673	3.255988
O1.1 Ranking on labor cost (Pay and productivity, 1-7 (best))	3.041286	4.116311	4.247679	3.977658	2.683268
O1.2 Availability of Scientists and engineers	4.300765	4.151894	3.680066	4.14028	3.399498
O1.3 Availability of research and training services	3.23855	4.803038	4.40615	4.095279	4.492867
O2.1 Ranking on political stability	23.5	31.3	81.2	53	61
O3.1 Electricity production, kWh/capita	1673.065	183.4592	1870.937	664.8478	5180.906
O3.2 % of population with access to electricity	100	23	100	100	85.4
O3.3 Electricity Consumption (MWh /Capita)	1.7	0.17	2.18	0.91	4.24
O4.1 Quality of Electricity Supply	3.358706	3.775316	5.143952	5.468322	3.768681
O4.2 Energy Architecture: Economic Development and Growth	0.33	0.39	0.49	0.49	0.59
O4.3 Energy Architecture: Access and Security	0.69	0.36	0.76	0.76	0.65
O5.1 Cost of getting electricity (% of income per capita)	304.6	1020.2	277	1974.5	729.5
061 No. procedures to enforce a contract	42	44	34	40	29
06.2 No. days to enforce a contract	1010	465	519	510	600
F1.1.1 Use of virtual social networks, 1-7 (best)	5.771155	5.703807	5.580406	5.503633	5.540504
F1.1.2 Wikipedia edits/mn pop. 15–69.	439	107	998.8	390.4	363.8
F1.1.3 Video uploads on YouTube/pop. 15–69.	7.7	0.9	N/A	12.3	3.0
F2.1.1 Freedom on the Net Status (Freedom Score 0 = Best, 100 = Worst)	60	28	26	44	26

Appendix 3: Staging framework used

Sub-Indicator	1	2	3
S1.1 Is there a regulatory body responsible for standards development for the country?	No	Limited/Medium	Yes
S2.1 Does the government participate in international standards-setting process?	No	Limited/Medium	Yes
S2.2 Are international standards favored over domestic standards?	No	Limited/Medium	Yes
S3.1 Are there any laws or policies in place that implement technology neutrality in government?	No	Limited/Medium	Yes
S3.2 Are cloud computing services able to operate free from laws or policies that mandate the use of certain products (including, but not limited to types of software), services, standards or technologies?	No	Limited/Medium	Yes
S3.3 Are cloud computing services able to operate free from laws or policies that establish preferences for certain products (including, but not limited to types of software), services, standards or technologies?	No	Limited/Medium	Yes
S3.4 Are cloud computing services able to operate free from laws that discriminate based on the nationality of the vendor, developer or service provider?	No	Limited/Medium	Yes
S4.1 Are there laws, regulations or policies that establish a standards setting framework for interoperability and portability of data?	No	Limited/Medium	Yes
S5.1 Is the downloading of applications or digital data from foreign cloud based service providers free from tariff or other trade barriers?	No	Limited/Medium	Yes
P1.1 Are there laws or regulations governing the collection, use or other processing of personal information?	No	Limited/Medium	Yes
P1.2 Is there an effective agency (or regulator) tasked with the enforcement of privacy laws?	No	Limited/Medium	Yes
P1.3 Is there a strict consent requirement for the collection, storage and dissemination of personal data?	No	Limited/Medium	Yes
P1.4 Does the law provide users with the right to review their stored information?	No	Limited/Medium	Yes
P1.5 Does the law provide users with the right to be forgotten or deleted?	No	Limited/Medium	Yes
P1.6 Are there administrative sanctions for non-compliance? How much? (None, Medium, Severe)	No	Limited/Medium	Yes
P1.7 Is notification of breaches towards the government and/or users obligatory (None, Govt or User, Both)	No	Govt or User	Yes
P2.1 Is the country a member of TRIPS agreement?	No	Limited/Medium	Yes
P2.2 Have IP laws been enacted to implement TRIPS	No	Limited/Medium	Yes
P2.3 Is the country party to the WIPO Copyright Treaty?	No	Limited/Medium	Yes
P2.4 Are criminal sanctions available for unauthorized making available of copyright materials digitally?	No	Limited/Medium	Yes
P2.5 Are there laws governing ISPs liability for content that infringes copyright?	No	Limited/Medium	Yes
P2.6 Software piracy rate, % software installed	<50%	<75%	<90%
P2.7 Perception of Effectiveness: Intellectual property protection, 1-7 (best)	<3.5	<5	>5
P3.1 Is there a Data Protection Policy in place?	No	Limited/Medium	Yes
P3.2 Are data protection impact assessments obligatory?	No	Limited/Medium	Yes
P3.3 Is a data protection officer required?	No	Limited/Medium	Yes
P3.4 Are firms required to retain data for a fixed period of time?	No	Limited/Medium	Yes
P4.1 Is there a law or regulation that gives electronic signatures clear legal weight?	No	Limited/Medium	Yes
P4.2 Are ISPs and content service providers free from mandatory filtering or censoring	No	Limited/Medium	Yes

P4.3 Global Cybersecurity Index	<0.40	<.50	>.50
P5.1 Are cybercrime laws in place?	No	Limited/Medium	Yes
P5.2 Are cybercrime laws consistent with the Budapest Convention on Cybercrime?	No	Limited/Medium	Yes
P5.3 Laws relating to ICTs, 1-7 (best)	<3.5	<4.5	>4.5
P6.1 Are there rules for differentiated treatment of data based on data classification, i.e. different treatment for data of different levels of sensitivity?	No	Limited/Medium	Yes
P6.2 Is there a data localization requirement (i.e. is the transfer of data outside of country borders disallowed) (No, Limited, Both)	No	Limited/Medium	Yes
I1.1 Fixed Internet - upload (UL) speeds in kilobits per second (kbps)	<1200	<2400	>2400
I1.2 Fixed Internet - download (DL) Speed in kilobits per second (kbps)	<2000	<5000	>5000
I1.3 Fixed Internet - latency in milliseconds (ms)	>120	<90	<60
I1.4 Fixed Broadband Quality: Avg. Page Load Time (ms)	>5000	<5000	<3000
I2.1 Mobile Internet - upload (UL) speeds in kilobits per second (kbps)	<1000	<2000	>2000
I2.2 Mobile Internet - download (DL) Speed in kilobits per second (kbps)	<2000	<4000	>4000
I2.3 Mobile Internet - latency in milliseconds (ms)	>150	>120	<120
I2.4 Mobile Broadband Quality: Avg. Page Load Time (ms)	>5000	<5000	<3000
I3.1 Bandwidth Per Capita (Int'l Internet bandwidth, kb/s per user)	<10	<20	>20
I4.1 Secure Internet servers/million pop.	<10	<100	>100
N1.1 Mobile phone subscriptions/100 pop.	<100	<125	>125
N2.1 Households w/ personal computer, %	<20	<40	>40
N2.2 Availability of latest technologies, 1-7 (best)	<3.5	<5.25	>5.25
N3.1 Households w/ Internet access, %	<20	<40	>40
N3.2 Mobile network coverage, % pop.	<90	<95	>95
N3.3 Individuals using Internet, %	<40	<50	>50
N4.1 Fixed broadband Internet subs/100 pop.	<30	<50	>50
N4.2 Mobile broadband subs/100 pop.	<20	<40	>40
N5.1 Prepaid mobile cellular tariffs, PPP $/min.	>0.15	<0.12	<0.08
N5.2 Fixed broadband Internet tariffs, PPP $/month	>45	<45	<30
N5.3 Mobile-broadband as % of GNI per capita	>5	<5	<2
N6.1 Internet & telephony competition, 0–2 (best)	0-.75	0.75-1.5	1.5-2
T1.1 Quality of educational system, 1-7 (best)	<2.5	<2.5	>4
T1.2 Quality of primary education, 1-7 (best)	<2.5	<3	>3
T1.3 Quality of management schools, 1-7 (best)	<3.5	<5	>5
T1.4 Quality of math & science education, 1-7 (best)	<3.5	<5	>5
T2.1 Primary education enrollment rate (net), %	<85	<95	>95
T2.2 Secondary education gross enrollment rate, %	<70	>70	>85
T2.3 Tertiary education gross enrollment rate, %	<10	>10	>20
T2.4 Expected years of schooling	<12	>12	>13
T2.5 Mean years of schooling	<5	>5	>7.5
T3.1 Adult literacy rate, %	<85	<90	>95
T3.2 % of workforce with tertiary degree	<10	>10	>15
T3.3 Graduates in science & engineering, %	<15	>15	>25
B1.1 Firm-level technology absorption, 1-7 (best)	<4	<5	>5
B1.2 ICT use for business-to-business transactions, 1-7 (best)	<4.5	<5.5	>5.5
B1.3 Business-to-consumer Internet use, 1-7 (best)	<4	<5	>5
B2.1 Extent of staff training, 1-7 (best)	<3.5	<4.5	>4.5
B2.2 Knowledge-intensive jobs, % workforce	<15	>15	>20

B2.1 Impact of ICTs on business models, 1-7 (best)	<4	<4.5	>4.5
B2.2 Impact of ICTs on new organizational models, 1-7 (best)	<4	<4.5	>4.5
G1.1 Importance of ICTs to gov't vision, 1-7 (best)	<3.5	<4.5	>4.5
G1.2 Gov't success in ICT promotion, 1-7 (best)	<3.5	<4.5	>4.5
G1.3 Impact of ICTs on access to basic services, 1-7 (best)	<3.5	<4.5	>4.5
G.1.4 Internet access in schools, 1-7 (best)	<3.5	<4.5	>4.5
G2.1 Government Online Service Index, 0–1 (best)	<0.40	<.50	>.50
G2.2 ICT use & gov't efficiency, 1-7 (best)	<4	<4.5	>5
G2.3 E-Participation Index, 0–1 (best)	<0.10	<.10	>.15
G3.1 Gov't procurement of advanced tech, 1-7 (best)	<3.5	<4.5	>4.5
O1.1 Ranking on labor cost (Pay and productivity, 1-7 (best))	<3.5	<4.5	>4.5
O1.2 Availability of Scientists and engineers	<3.5	<4.5	>4.5
O1.3 Availability of research and training services	<3.5	<4.5	>4.5
O2.1 Ranking on political stability	<35	<60	>60
O3.1 Electricity production, kWh/capita	<200	<1500	>1500
O3.2 % of population with access to electricity	<85	<90	>95
O3.3 Electricity Consumption (MWh /Capita)	<1.5	<3.5	>3.5
O4.1 Quality of Electricity Supply	<4	<5	>5
O4.2 Energy Architecture: Economic Development and Growth	<0.35	<.45	>.45
O4.3 Energy Architecture: Access and Security	<0.45	<.75	>.75
O5.1 Cost of getting electricity (% of income per capita)	>750	<750	<500
061 No. procedures to enforce a contract	<30	<40	>40
06.2 No. days to enforce a contract	>750	<750	<500
F1.1.1 Use of virtual social networks, 1-7 (best)	<5.5	<5.75	>5.75
F1.1.2 Wikipedia edits/mn pop. 15–69.	<200	<500	>500
F1.1.3 Video uploads on YouTube/pop. 15–69.	<3	<5	>5
F2.1.1 Freedom on the Net Status (Freedom Score 0 = Best, 100 = Worst)	>50	<50	<40

Appendix 4: Populating the sub-indicators

Sub-Indicator	Egypt	Kenya	Mauritius	Morocco	South Africa
S1.1 Is there a regulatory body responsible for standards development for the country?	3	3	3	3	3
S2.1 Does the government participate in international standards-setting process?	3	3	3	3	3
S2.2 Are international standards favored over domestic standards?	3	3	3	3	3
S3.1 Are there any laws or policies in place that implement technology neutrality in government?	3	3	3	3	1
S3.2 Are cloud computing services able to operate free from laws or policies that mandate the use of certain products (including, but not limited to types of software), services, standards or technologies?	3	3	3	3	2
S3.3 Are cloud computing services able to operate free from laws or policies that establish preferences for certain products (including, but not limited to types of software), services, standards or technologies?	3	3	3	3	2
S3.4 Are cloud computing services able to operate free from laws that discriminate based on the nationality of the vendor, developer or service provider?	3	3	3	3	1
S4.1 Are there laws, regulations or policies that establish a standards setting framework for interoperability and portability of data?	1	1	1	1	3
S5.1 Is the downloading of applications or digital data from foreign cloud based service providers free from tariff or other trade barriers?	2	3	3	3	2
P1.1 Are there laws or regulations governing the collection, use or other processing of personal information?	1	3	3	3	3
P1.2 Is there an effective agency (or regulator) tasked with the enforcement of privacy laws?	1	1	3	3	3
P1.3 Is there a strict consent requirement for the collection, storage and dissemination of personal data?	1	3	3	3	3
P1.4 Does the law provide users with the right to review their stored information?	1	3	3	3	3
P1.5 Does the law provide users with the right to be forgotten or deleted?	1	1	3	3	3
P1.6 Are there administrative sanctions for non-compliance? How much? (None, Medium, Severe)	1	2	1	2	2
P1.7 Is notification of breaches towards the government and/or users obligatory (None, Govt or User, Both)	1	1	2	1	3
P2.1 Is the country a member of TRIPS agreement?	3	3	3	3	3
P2.2 Have IP laws been enacted to implement TRIPS	3	3	3	3	3
P2.3 Is the country party to the WIPO Copyright Treaty?	3	3	3	3	1
P2.4 Are criminal sanctions available for unauthorized making available of copyright materials digitally?	3	3	3	3	3
P2.5 Are there laws governing ISPs liability for content that infringes copyright?	3	3	3	3	3
P2.6 Software piracy rate, % software installed	2	2	2	2	1
P2.7 Perception of Effectiveness: Intellectual property protection, 1-7 (best)	1	2	2	2	3
P3.1 Is there a Data Protection Policy in place?	1	1	3	3	3
P3.2 Are data protection impact assessments obligatory?	1	1	1	1	3

P3.3 Is a data protection officer required?	1	1	3	1	3
P3.4 Are firms required to retain data for a fixed period of time?	1	1	1	1	1
P4.1 Is there a law or regulation that gives electronic signatures clear legal weight?	3	3	3	3	3
P4.2 Are ISPs and content service providers free from mandatory filtering or censoring	3	3	3	3	3
P4.3 Global Cybersecurity Index	3	2	3	3	1
P5.1 Are cybercrime laws in place?	3	3	3	3	3
P5.2 Are cybercrime laws consistent with the Budapest Convention on Cybercrime?	3	3	3	3	3
P5.3 Laws relating to ICTs, 1-7 (best)	1	2	2	2	3
P6.1 Are there rules for differentiated treatment of data based on data classification, i.e. different treatment for data of different levels of sensitivity?	1	1	3	3	3
P6.2 Is there a data localization requirement (i.e. is the transfer of data outside of country borders disallowed) (No, Limited, Both)	2	1	1	1	2
I1.1 Fixed Internet - upload (UL) speeds in kilobits per second (kbps)	1	3	3	1	2
I1.2 Fixed Internet - download (DL) Speed in kilobits per second (kbps)	1	2	3	2	2
I1.3 Fixed Internet - latency in milliseconds (ms)	2	2	3	2	3
I1.4 Fixed Broadband Quality: Avg. Page Load Time (ms)	2	1		2	2
I2.1 Mobile Internet - upload (UL) speeds in kilobits per second (kbps)	1	3		1	2
I2.2 Mobile Internet - download (DL) Speed in kilobits per second (kbps)	1	3		2	3
I2.3 Mobile Internet - latency in milliseconds (ms)	1	2		2	3
I2.4 Mobile Broadband Quality: Avg. Page Load Time (ms)	2	1		2	1
I3.1 Bandwidth Per Capita (Int'l Internet bandwidth, kb/s per user)	1	3	2	2	2
I4.1 Secure Internet servers/million pop.	1	1	1	3	3
N1.1 Mobile phone subscriptions/100 pop.	2	1	3	3	3
N2.1 Households w/ personal computer, %	3	1	3	3	2
N2.2 Availability of latest technologies, 1-7 (best)	2	2	2	2	3
N3.1 Households w/ Internet access, %	2	1	3	3	2
N3.2 Mobile network coverage, % pop.	3	1	3	3	3
N3.3 Individuals using Internet, %	1	2	2	3	2
N4.1 Fixed broadband Internet subs/100 pop.	2	3	2	1	2
N4.2 Mobile broadband subs/100 pop.	3	1	2	2	3
N5.1 Prepaid mobile cellular tariffs, PPP $/min.	3	2	1	2	1
N5.2 Fixed broadband Internet tariffs, PPP $/month	2	1	2	3	2
N5.3 Mobile-broadband as % of GNI per capita	2	1	3	2	3
N6.1 Internet & telephony competition, 0–2 (best)	3	3	3	3	2
T1.1 Quality of educational system, 1-7 (best)	1	3	3	2	1
T1.2 Quality of primary education, 1-7 (best)	1	3	3	2	2
T1.3 Quality of management schools, 1-7 (best)	1	2	2	2	3
T1.4 Quality of math & science education, 1-7 (best)	1	2	2	2	1
T2.1 Primary education enrollment rate (net), %	3	1	3	3	2

T2.2 Secondary education gross enrollment rate, %	2	1	3	1	3
T2.3 Tertiary education gross enrollment rate, %	3	1	3	2	2
T2.4 Expected years of schooling	2	1	3	1	3
T2.5 Mean years of schooling	3	2	2	1	3
T3.1 Adult literacy rate, %	1	1	2	1	2
T3.2 % of workforce with tertiary degree	3	1	2	2	3
T3.3 Graduates in science & engineering, %	1	1	2	3	2
B1.1 Firm-level technology absorption, 1-7 (best)	1	2	3	2	3
B1.2 ICT use for business-to-business transactions, 1-7 (best)	2	2	2	1	2
B1.3 Business-to-consumer Internet use, 1-7 (best)	2	2	1	2	2
B2.1 Extent of staff training, 1-7 (best)	1	2	3	2	3
B2.2 Knowledge-intensive jobs, % workforce	3	2	2	1	3
B2.1 Impact of ICTs on business models, 1-7 (best)	1	2	2	1	2
B2.2 Impact of ICTs on new organizational models, 1-7 (best)	1	2	2	1	2
G1.1 Importance of ICTs to gov't vision, 1-7 (best)	1	3	3	2	1
G1.2 Gov't success in ICT promotion, 1-7 (best)	1	3	3	2	2
G1.3 Impact of ICTs on access to basic services, 1-7 (best)	2	2	3	2	1
G.1.4 Internet access in schools, 1-7 (best)	1	2	2	1	1
G2.1 Government Online Service Index, 0–1 (best)	3	2	2	1	2
G2.2 ICT use & gov't efficiency, 1-7 (best)	1	2	2	2	1
G2.3 E-Participation Index, 0–1 (best)	3	1	1	1	3
G3.1 Gov't procurement of advanced tech, 1-7 (best)	1	2	2	2	1
O1.1 Ranking on labor cost (Pay and productivity, 1-7 (best))	1	2	2	2	1
O1.2 Availability of Scientists and engineers	2	2	2	2	1
O1.3 Availability of research and training services	1	3	2	2	2
O2.1 Ranking on political stability	1	1	3	2	3
O3.1 Electricity production, kWh/capita	3	1	3	2	3
O3.2 % of population with access to electricity	3	1	3	3	2
O3.3 Electricity Consumption (MWh /Capita)	2	1	2	1	3
O4.1 Quality of Electricity Supply	1	1	3	3	1
O4.2 Energy Architecture: Economic Development and Growth	1	2	3	3	3
O4.3 Energy Architecture: Access and Security	2	1	3	3	2
O5.1 Cost of getting electricity (% of income per capita)	1	1	3	1	2
061 No. procedures to enforce a contract	3	3	1	2	1
06.2 No. days to enforce a contract	1	3	2	2	2
F1.1.1 Use of virtual social networks, 1-7 (best)	1	2	2	2	2
F1.1.2 Wikipedia edits/mn pop. 15–69.	2	1	2	2	2
F1.1.3 Video uploads on YouTube/pop. 15–69.	3	1		3	2
F2.1.1 Freedom on the Net Status (Freedom Score 0 = Best, 100 = Worst)	1	3	3	2	3