Modernising the Public Sector through the Cloud

A report commissioned by the Microsoft Foundation

ACKOWLEDGEMENTS

With a considerable amount of technical awareness around the benefits of the adoption of cloud services and applications to enterprise development generally, this report was commission by the Microsoft Foundation and the South African Microsoft Office specifically to support decision-making for the development of a cloud policy, strategy and implementation in South Africa.The research and interviews were conducted during 2016 and the authors, Dr Alison Gillwald and Mpho Moyo, thank those interviewed from the public and private sector who contributed their time and knowledge to the paper, and hopefully to enhancing public service delivery in South Africa. We also thank Heba Ramzy and Siyabonga Madyibi, from Microsoft for enabling research access to Microsoft workshops, research and expertise on the cloud.

Enquiries:

Research ICT Africa

409 Old Castle Brewery

6 Beach Road

Woodstock 7925

South Africa

Tel: 021-4476332

Fax:021 4479529

www.researchICTafrica.net

EXECUTIVE SUMMARY

Information Communication Technology (ICT) is recognised as a key enabler of economic growth and development in South Africa. Progress towards modernising ICT in the public sector has been slow and the government lags the private sector in terms of ICT adoption, including cloud computing. The ICT policy environment remains fragmented and ICT adoption in the public sector has been hampered by protracted policy processes and stalled decision-making and generally there is a gap between what is stipulated in policy documents and implementation of these policies and guidelines in practice.

Negative macro-economic conditions have necessitated the need for the public sector to look for ways to meet the increasing demands for service delivery within a limited budget. Cloud computing, which falls under the domain of ICT is viewed as having the potential to promote greater efficiencies, integration, coordination and cost savings within the public sector. Cloud computing is also expected to enable the government to meet the objectives set out in the National Development Plan and SA Connect, including achieving better coordination between government departments and enabling the delivery of e-government services, yet the use these services have been limited within the public sector.

The absence of policy guidelines and a champion for cloud computing services is limiting the use of cloud computing services within the public sector. Other barriers include issues around data classification, data protection, security and residency, availability and cost of underlying broadband infrastructure, and lack of implementation of uniform open standards.

Generally, there is a “siloed” and fragmented approach to ICT usage, including cloud computing, within the public sector. As a result, many government departments remain disparate and are not interoperable. Most cloud computing deployments are ad hoc and uneven across different government departments as there is no centralised and coordinated approach to ICT deployment across all spheres of government, which could be addressed by developing a national centrally coordinated cloud strategy.

There are wider policies, regulation and legislation that affect the implementation of cloud computing services in government, including e-government legislation, information protection regimes, information storage and classification measures and privacy protection that can be expanded to cover cloud computing services.

Table of contents

ACKOWLEDGEMENTS 2

EXECUTIVE SUMMARY 3

ABBREVIATIONS 6

1. Background 8

2. South Africa's Macro-Economic Environment 9

3. Cloud Computing 9

3.1. Definitions 9

3.2. Types of cloud computing 10

3.3. Cloud services 10

3.3.1. Infrastructure as a Service (IaaS) 10

3.3.2. Software as a Service (SaaS) 11

3.3.3. Platform as a Service (PaaS) 11

4. Cloud in the ICT ecosystem 11

5. Significance of the Cloud 12

5.1. Value of cloud computing for the public sector 13

5.1.1. The United Kingdom 14

5.1.2. New Zealand 15

5.1.3. South Korea 17

5.2 Institutional arrangements and leadership 18

5.3 Fragmentation of mandate in government 19

5.4 Synthesis 20

6. The Benefits of Cloud Computing 22

7. The South African Case 23

7.1. Cloud market in South Africa 23

7.1.1. Drivers 23

7.1.2. Barriers 25

7.1.3. Private sector view of public sector cloud readiness 25

7.2. Status of cloud use by public sector in South Africa 26

7.2.1. Skills shortages in public sector 29

7.2.2. Absence of cloud computing policy for the public sector 29

7.2.3. Inconsistencies in the approach to cloud computing 29

7.3. Cloud mainly for noncritical processes 29

7.4. Assessment of public sector cloud computing awareness and deployment 30

7.4.1. City of Johannesburg (CoJ) 30

7.4.2. Government Pension Administration Agency (GPAA) 30

7.5. Identification of barriers to adoption of cloud computing for the public sector 31

7.5.1. Technical barriers 31

7.5.2. Managerial and organisational barriers 32

7.5.3. Policy challenges 33

8. SA Cloud readiness 34

8.1. Vision, policy framework and institutional arrangements 34

8.2. National Development Plan and Presidential Infrastructure Coordinating Council *34*
8.2.1. SA Connect implementation 35
8.2.2. ICT policy review 36
8.3. Applicable policy, regulation and legislation to regulate activities in the cloud in the South African government *37*
8.3.1. State Information Technology Agency (SITA) 38
8.3.2. Storage and management of records by South African governments 38
8.4. Information Protection Regime *38*
8.4.1. The Electronic Communications and Transactions Act 39
8.4.2. Electronic Communications Act 36 as amended by Act 1 2014 40
8.5. Protection of Personal Information Act 4 *41*

9. Cloud First Policy for South African Public Sector **42**
9.1. Open data policy *42*

10. E-gov, interoperability and standards **44**
10.1. Minimum Interoperability Standards for government information systems *45*
10.1.1 Capacity 46
10.1.2 Aims 46
10.1.3 Interoperability 46

11. Findings/Conclusions **47**
11.1. Institutional arrangements and leadership *47*
11.2. Fragmentation of mandate in government *47*
11.3. Lack of a coherent public policy *48*

12. Recommendations **48**
12.1. Position cloud as a solution to skills shortages *48*
12.2. Improve availability and quality of broadband infrastructure *48*
12.3. Develop a cloud computing policy framework *48*
12.4. Establish a designated champion for cloud computing services *49*
12.5. Implement and enforce open and interoperable standards to public sector procurement *49*
12.6. Adopt best practices to develop security framework for cloud services *49*
12.7. Expand data classification guidelines to include cloud computing *50*
12.8. Provide guidance for cloud vendor certification and compliance *50*

13. SUMMARY TABLE OF RECOMMENDATIONS/ACTIONS **51**

14. List of interviewees **53**

ABBREVIATIONS

BBBEE	Broad-Based Black Economic Empowerment
BRICS	Brazil, Russia, India, China and South Africa (five major national emerging countries).
CAPEX	Capital Expenditure
CIO	Chief Information Officer
CoJ	City of Johannesburg
DCS	Department of Correctional Services
DHA	Department of Home Affairs
DHS	Department of Human Settlements
DOJ	Department of Justice
DPSA	Department of Public Service and Administration
DSD	Department of Social Development
DTPS	Department of Telecommunications and Postal Services
ECA	Electronic Communication Act
ECTA	Electronic Communications and Transactions Act
E-GOV	Electronic government
FSB	Financial Services Board
G-Cloud	Government Cloud Computing
GCIO	Government Chief Information Officer
GDP	Gross Domestic Product
GDS	Government Digital Service
GITOC	Government Information Technology Council
GPAA	Government Pension Administration Agency
IaaS	Infrastructure as a Service
ICT	nformation and Communications Technology

IoT	Internet of Things
IT	Information Technology
ITU	International Telecommunications Union
KCC	Korean Cloud Computing
LTE	Long Term Evolution
MIOS	Minimum Interoperability Standards
MISS	Minimum Information Security Standards
NDP	National Development Plan
NPA	National Prosecuting Authority
NT	National Treasury
OPEX	Operational Expenditure
PaaS	Platform as a Service
PICC	Presidential Infrastructure Coordinating Council
POPI	Protection of Personal Information Act
PPP	Public-Private Partnership
SADC	Southern African Development Community
SADF	South African Defence Forces
SAPS	South African Police Services
SARS	South African Revenue Service
SIP	Strategic Integrated Project
SMES	Small and Medium Enterprises
SITA	State Information Technology Agency

1. BACKGROUND

Information Communication Technology (ICT) is viewed as a key enabler for the achievement of government policies for economic growth and development. The ICT policy environment in South Africa remains fragmented and unconducive to creating affordable and good quality high speed broadband access – a necessary, though not sufficient condition for cloud services to be optimised. Furthermore, the effective deployment of cloud computing within the largest and most disparate, collective user of ICTs in the country requires a policy to direct the strategic deployment of the cloud across the public sector.

In South Africa, the lack of affordable always-on, high-speed and high-quality bandwidth required by business, public institutions and citizens has impacted negatively on the country's development and global competitiveness. The World Economic Forum Network Readiness Index measures countries' propensity for the exploration of the opportunities offered by ICT, and the impact of ICT on the competitiveness of nations. Countries are ranked out of 143 countries globally. South Africa is an early adopter of advanced technology (individuals and corporations), on par with other developed nations, and the country ranked 65th in 2016 – up from 75th position in 2015. South Africa's Business use of ICT ranking improved from 34 in 2015 to 32 in 2016.

However, the government has lagged behind the private sector in strategic deployment of ICT. South Africa ranking in the government use index remained constant at 105 in 2016[1], far behind its comparator nations. This is confirmed by other e-government indices such as the United Nations E-Government Survey 2016 in which South Africa ranks 76th out of 192 countries[2].

While the private sector has cautiously adopted the cloud to optimise business, the response from the public sector as a whole has been sluggish and uneven. Some independent government agencies, such as the Financial Services Board (FSB) and also the big metros, not bound by national standards or procurement rules of the State IT Agency (SITA), have successfully embraced cloud services to meet their public mandates – specifically citizen engagement and service delivery.

Interviews with Chief Information Officers (CIOs) at national and provincial level and members of the Government Information Technology Council (GITOC) indicated high levels of frustration with their inability to deploy cloud services. The primary reason cited was the absence of standards being set by SITA, and consequently the explicit exclusion of cloud services in government ICT tenders. Another factor that inhibits the readiness of government – especially with departments outside of the economically more powerful provinces – is absence of the high-speed broadband networks needed for the effective operation of integrated enterprise cloud services. Even where these are available, the prohibitively high cost of broadband was cited as a major inhibitor of cloud service uptake.

In March 2015, the government concluded an ICT Policy Review (Green Paper) which aimed to develop an integrated e-strategy aligned to the National Development Plan, whereby ICT is expected to underpin the development of an inclusive, dynamic information society and knowledge economy. The review states that cloud computing has the potential to "promote growth, increase efficiencies and reduce costs for small and medium enterprises (SMEs)"[3]. The paper also identifies cloud computing's potential to lower barriers to entry for new players and support government IT development, e-government services and development initiatives. Despite

---

1 World Economic Forum (2016). "Global Information Technology Report". Available at: www.reports.weforum.org/gobal-information-technology-report-2016/.
2 United Nations (2016). "United Nations E-government Survey 2016: E-government in support of sustainable development". Available at: http://workspace.unpan.org/sites/Internet/Documents/UNPAN96407.pdf.
3 RSA (2015). "National Integrated ICT Policy Review Report". Available at: www.dtps.gov.za/.../102-ict-policy-review-reports-2015.html.

the fact that the ICT Green Paper states that there is a need to develop a cloud computing policy, none exists to date. This discussion paper contributes to filling this lacuna by identifying the bottlenecks that inhibit cloud deployment and the opportunities that would arise from the development of an enabling policy for cloud computing in the public sector.

2. SOUTH AFRICA'S MACRO-ECONOMIC ENVIRONMENT

South Africa is the second largest economy in Sub-Saharan Africa. GDP stood at USD312.8 billion at the end of 2015, down from USD349.9 billion at the end of 20144. The prevailing negative macro-economic conditions in South Africa – including the weakening of the rand against major currencies, rising inflation at 4.6 percent and unemployment at 24.5 percent at the end of 2015 – in the context of near stagnant economic growth of 1.3 percent at the end of 20155 and government's commitment to reduce state expenditure, have amplified the need for the public sector to streamline costs while delivering services. Reduced public sector expenditure is also an attempt to avert the downgrade of South Africa's economy to junk status by international rating agencies, which would have adverse effects and likely push South Africa into a recession (Treasury, personal interview, 21 July 2016).

With South Africa's economy projected to grow by less than one percent in 2016, the government has been utilising the impending crisis as an opportunity to examine areas of significant expenditure in the public sector, such as ICT, and to identify ways of reducing inefficiencies and costs (Treasury, personal interview, 21 July 2016). The current evidence from early adopter countries of the potential of cloud computing to streamline costs and improve information flows makes it an obvious mechanism to achieve such ends. This would require addressing bottlenecks in the current ICT policy environment that are inhibiting the ubiquitous and affordable broadband, enabling public information on open data policy and formulating a clear policy that would enable the widespread adoption of cloud computing in the public sector.

3. CLOUD COMPUTING

3.1. Definitions

Generally, there is a lack of clarity on what "the cloud" is or how it should be defined. This is due, in part, to the phrase "cloud computing" being misused to refer to a broad collection of services, delivered at different layers (e.g. infrastructure, application platform, software and business process), and implemented in different ways (public, private, hybrid and community), for a broad range of reasons.

For the purposes of this paper the cloud is understood as:[6]

"… 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."

---

4 World Bank (2016). "World Development Indicators World Data Bank". Available at: \
http://databank.worldbank.org/data/reports.aspx?
Code=NY.GDP.MKTP .CD&id=af3ce82b&report_name=Popular_indicators&populartype=series&ispopular=y.
5 Statistics South Africa (2016). "The economy: Winners and losers of 2015". Available at: http://www.statssa.gov.za/?p=6233.
6 Gillwald, A. et al. (2015). "The Cloud over Africa". Available at:
https://www.google.co.za/url?sa=t&source=web&rct=j&url=https://www.researchictafrica.net/publications/Evidence_for_ICT_Policy_Action/Policy_Paper_20_-_The_cloud_over_Africa.pdf&ved=0ahUKEwik-L7tjZ7SAhVJJMAKHbYFBhoQFggYMAA&usg=AFQjCNHnyYFZy-hLLr_D0VSnN7OCzITtVA.

Cloud computing services "provide organisations with convenient on-demand access to a common pool of configurable computing resources, networks, servers, security, storage, applications and services"[7]. In addition, cloud computing changes an organisation's infrastructure and the way it conducts business.

There is a need to distinguish between "cloud services" and "cloud-based services". Cloud services are utilised "…on demand at any time, through any access network, using any connected devices [that use] cloud computing technologies"[6]. Further, cloud services utilise software and applications that are located on the cloud and not on users' own devices. Cloud-based services include mass market applications i.e. social media and webmail offered over the internet, whereby the data does not sit on individuals' devices but is stored remotely in a data centre. Examples include Facebook, YouTube and Gmail.

3.2. Types of cloud computing

There are two broad types of cloud services, private cloud and public cloud, and various hybrid versions of these[6].

Private cloud: A private cloud refers to "a dedicated resource provided by a cloud service provider for a single client/user (for example a government or large business user)"[6].

Public cloud: Unlike private cloud, which is typically for a dedicated user/entity, a public cloud "is an open resource open to the public"[6]. Examples include mass market services like webmail, Gmail for example, which is often defaulted to when organisational systems are down, or Dropbox to store and send large documents to a colleague or client, and more integrated systems, like Apple's iCloud or Facebook.

Hybrid cloud: A hybrid cloud is a mixture of the deployment models described above, for example a mix of public and private cloud provision[6].

Cloud providers offer both public and private cloud services, which are often located in the same data centres. Governments and private companies may use multiple cloud services or cloud providers or hybrid models, where some part of their business is migrated to the cloud but not all. In this regard, interoperability in cloud provision becomes a critical factor, as this allows flexibility and enables users to switch between one cloud provider and the other[8].

3.3. Cloud services

3.3.1. Infrastructure as a Service (IaaS)

IaaS is a virtual, cloud-based replacement for physical hardware, such as processors and hard drives. Users make use of the storage, networks and other computing resources that allow them to deploy their own software, applications and operating systems. The underlying cloud infrastructure is managed and controlled by a third party. The user has control over the storage, operating systems and deployed applications, but may have limited control over networking components, such as host firewalls[9].

---

7 Macias, F. and Thomas, G. (2011). "Cloud Computing Advantages in the Public Sector. How Today's Government, Education and Healthcare Organizations Are Benefiting from Cloud Computing Environments. Cisco White Paper". Available at: www.cisco.com/c/dam/en_us/solutions/industries/docs/c11-687784_cloud_omputing_wp.pdf.
8 UNCTAD (2013). "Information Economy Report 2013. The cloud economy and developing countries." Available at: www.unctad.org.
9 Kushida, K. E., Murray, J. and Zysman, J. (2012). "The gathering storm: Analysing the cloud computing ecosystem and implications for public policy" in Communications & Strategies. No 85, 1st quarter 2012.

3.3.2. Software as a Service (SaaS)

Cloud applications are usually delivered in the form of SaaS. Under this model, users are able to remove complexities and costs involved in the installation, maintenance and upgrading of complex IT systems in their own environment[10]. In addition, users take advantage of providers running cloud infrastructure. Users can access the cloud through either a thin client interface, such as a web browser (e.g. web-based e-mail) or a programme interface and have no control over underlying cloud infrastructure.

3.3.3. Platform as a Service (PaaS)

PaaS involves the deployment of a user's own applications on platform tools, including programming tools that are on infrastructure owned and managed by the cloud provider. For example, application developers working on mobile applications usually use cloud-based platforms to develop and launch their services. The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application hosting environment9.The PaaS platform enables them to access a full repertoire of features, which make up the platform. For example, a developer working on Android applications can use PaaS to ensure that an application can automatically take advantage of changes implemented in, and follow the look and feel of, new releases of the Android operating system as they appear[11].

4. CLOUD IN THE ICT ECOSYSTEM

The cloud is therefore best understood as the latest technology to enhance the efficiency or health of the wider broadband ecosystem. According to Kim, Kelly and Raja (2010)[12] the networks, services, applications and content are conceptualised as the broadband ecosystem.

The cloud can be understood as cutting across the broadband ecosystem, with infrastructure, software, applications and content offered as cloud services. Its linkages to other elements in the ICT ecosystem can be conceptualised as illustrated in Figure 1 below. According to Kaplan (2005) "An ICT ecosystem encompasses the policies, strategies, processes, information, technologies, applications and stakeholders that together make up a technology environment for a country, government or an enterprise. An ICT ecosystem includes people – diverse individuals – who create, buy, sell, regulate, manage and use technology"[13].

Access to and affordability of these services are outcomes of the market structure, institutional arrangements and effectiveness of regulation, which in turn are outcomes of the policy and legal framework. Users that include citizens and consumers are at the centre of this ecosystem. Factors such as price and quality of service are used to measure the access and affordability of services that are provided. The policies and regulations are products of the state as well as of global/regional governance institutions, including the International Telecommunication Union (ITU), the Internet Corporation for Assigned Names and Numbers (ICANN) and World Trade Organization (WTO). The ability of the policy and legal framework to provide a favourable

---

10 Gillwald, A., Moyo, M. and Altman, M. (2012). "Cloud computing in South Africa: Prospects and challenges". Chapter in Cowhey, P., Kleeman, M. and San Diego, U.C. Unlocking the benefits of cloud computing for emerging economies. Available at: www2.itif.org.

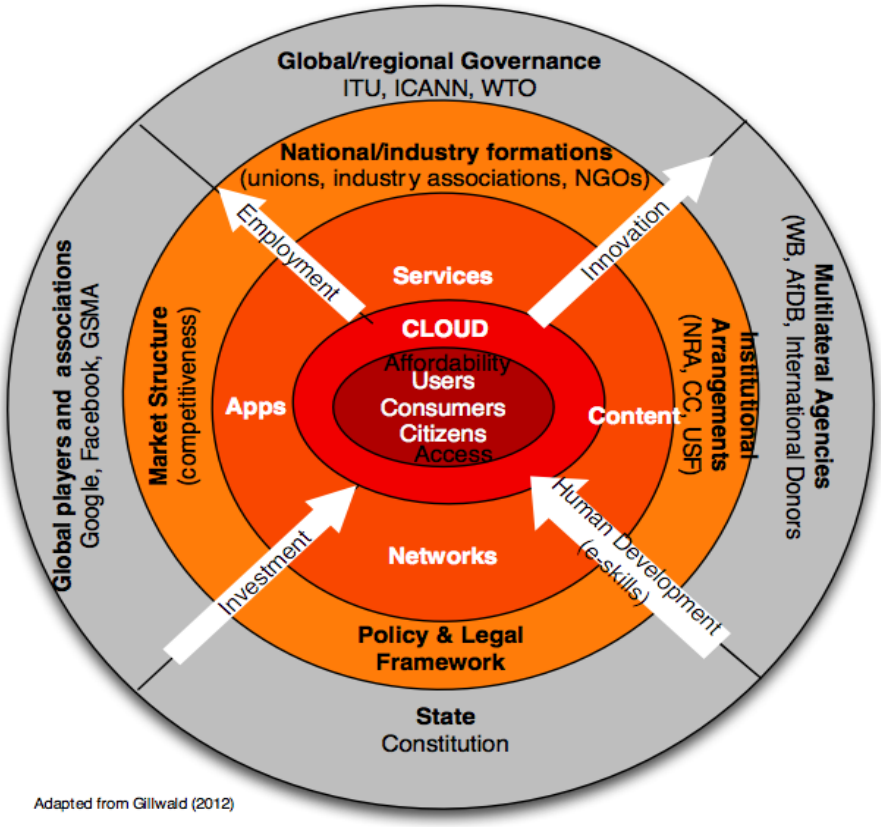
11 UNCTAD, (2013). "Information Economy Report 2013". The cloud economy and developing countries. Available at: www.unctad.org

12 Kim, Y., Kelly, T. and Raja, S. (2010). Building broadband: strategies and policies for the developing world. Available at: https://openknowledge.worldbank.org/handle/10986/2469.

13 Kaplan, J. (2005). "Roadmap for open ICT Ecosystems". Berkman Center, Harvard Law. Available at: http://cyber.law.harvard.edu/epolicy/roadmap.pdf.

environment is a major determinant of investment in order to drive growth of the sector and economy[14].

FIGURE 1: ICT ECOSYSTEM



From this we can see that cloud computing delivered via an internet connection is dependent on the availability of broadband infrastructure, which is critical to the availability and reliability of cloud computing services. These conditions are determined by the market structure, how competitive the services that arise from it are, or how effectively regulated they are, if not. The capacity of the regulator to be effective is determined, at least to some degree by the institutional arrangements and the autonomy of the regulator to implement policy.

5. SIGNIFICANCE OF THE CLOUD

Cloud computing has become a standard bearer in relation to the provision of IT services. With the global network traffic soaring for the Internet of Things (IoT), big data collection and analysis, and more mobile services than before, cloud computing is expected to account for 76 percent of the global data centre traffic in 2018. Likewise, the size of the global cloud computing market is estimated to grow from USD83.6 billion to USD188.2 billion between 2014 and 2019[15].

Cloud computing is viewed as the vehicle for the future of IT as organisations embark on digital transformation: IoT. Despite this, there is still significant anxiety and concern around relative cost

14 Gillwald, A. (2012). "Review of the Department of Communication's Colloqium on an integrated National ICT Policy. Available at: http://www.researchictafrica.net/docs/ICT_colloquium_SA.pdf.
15Jin-young (2016). "Korean government accelerates growth". Available at: http://www.businesskorea.co.kr/english/news/ict/14251-promotion-cloud-market-korean-government-accelerate-growth-cloud-computing.

and security/trust that are counteracting the growing interest in cloud computing. As a result, cloud strategies are increasingly focused on balancing the value of cloud against these concerns.

Some of the hesitancy to deploy cloud services results from technical concerns such as security, cost and governance. Largely this arises from a lack of familiarity or awareness of the evolution of cloud services and the hyper-connectivity, hyper-security, massive economies of scale and risk-managed services now available. Yet, even in cases where cloud is still treated as novel or risky for enterprises, one finds that it is already widely used by individuals in government and very often informally by organisations.

5.1. Value of cloud computing for the public sector

Governments around the world are looking for ways to deliver more efficient public services with reduced public resources[16]. In Europe and Asia, some countries have benefitted from the use of cloud computing and adoption is increasing.

The main benefit offered by cloud computing services within the public sector is cost savings through enhanced systems efficiency. Governments can reduce CAPEX spending on IT equipment, including internal servers, networking equipment, storage resources and software by shifting to a utility-based model. Instead of requiring a significant upfront investment to replace depreciating legacy equipment, expenditure becomes OPEX, whereby the public sector only pays for what it uses. Other benefits of cloud computing include reduced spending on energy consumption, as well as lower demand for systems management and maintenance, by shifting the management of IT resources to third parties. As a result, funds can be shifted to customer-facing activities and service delivery.

Cloud-computing is also viewed as having the ability to stimulate e-government[17] initiatives and has the potential to make government more efficient and the deployment of information systems for service delivery more cost effective[18].

Globally, cloud computing is a new way of thinking – and operating – for government IT departments. Global evidence from public sectors with cloud computing services supports the expected benefits of improved efficiency and cost savings, as well as solutions for mobile devices, sensor-based data collection and real-time analytics19.

The following international case studies will assist in establishing the best practices employed in cloud computing in international markets, as well as the approach of other public sectors to the adoption of cloud computing. The case studies will focus on how cloud computing can be applied in the context of the South African telecommunications market and political economy. This analysis of international case studies will also reveal the perceived benefits of cloud computing in the public sector, as well as other implications of cloud computing adoption on public policy. Lastly, the information presented will address obstacles to cloud computing adoption by the public sector.

---

16 Sallehudin, H., Che Razak, R. and Ismail, M. (2015). "Factors influencing cloud computing adoption in the public sector: An empirical analysis". Journal of Entrepreneurship and Business. Available at: www.researchgate.net/publication/281336943.
17 E-governance is defined as "the application of Information Communication Technologies (ICT) in Smitha, K. K., Thomas, T. and Chitharanjan, K. (2012). "Cloud-based E-governance system: A survey". Available at: www/sciencedirect.com.
18 Seddon, J. (2012). "India and the "Cloud"". Chapter in Cowhwey, P., Kleeman, M. and San Diego, U.C. Unlocking the benefits of cloud computing for emerging economies: A policy overview. Available at: http://irps.ucsd.edu/faculty/faculty-directory/peter-f-cowhey.htm.
19 Olsen (2015). "3 examples". Available at: https://enterprise.microsoft.com/en-us/industries/ government/3-examples-of-government-success-in-the-cloud/.

5.1.1. The United Kingdom

A UK government programme called Government Cloud Computing ("G-Cloud") promotes government-wide adoption of cloud computing. The initiative focuses on cloud computing's ability to scale up and down, save costs and create a more efficient, accessible means of delivering public services.

The G-Cloud framework includes:

- CloudStore – an online marketplace for ICT services, including Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS) and consulting services from programme vendors. Government agencies can purchase these cloud services on prepaid or annual contract bases. It is run on Microsoft's Windows Azure and also includes services from large cloud vendors.
- The G-Cloud authority – oversees and enforces standards and certifications for commodity services, including cloud computing. It also provides support for the public sector and resolves any cross-organisational issues.
- Data centre consolidation – an ongoing effort to close unused or underused data centres across UK government agencies to reach an optimal number of data centres. This part of the G-Cloud initiative moves government services to common cloud architecture, consisting of public, private and hybrid cloud environments[20].

Hence, the G-Cloud service is an initiative to ease procurement of cloud services by government departments and promote government-wide adoption of cloud computing. It is comprised of a series of framework agreements with cloud services suppliers and a listing of their services in the online store. This enables public sector organisations to compare and procure those services without having to do their own full review process. Inclusion in the CloudStore requires a self-attestation of compliance, followed by verification performed by the Government Digital Service (GDS) branch at its discretion[21].

The G-Cloud appointment process was streamlined in 2014 to improve efficiency[22] in the UK government, and the government's security classification scheme was simplified from six to three levels: official, secret, and top secret.

Instead of a centralised compliance assessment of cloud services, as previously pertained, the new process requires cloud service providers to self-certify and supply evidence in support of the 14 Cloud Security Principles of G-Cloud (currently at version 6).

The Crown Commercial Service (an agency that works to improve commercial and procurement activity by the government) renewed the classification of cloud services to G-Cloud v6, covering all of their offerings at the official level:

- Software as a Service (SaaS) – using the cloud to deliver applications;
- Platform as a Service (PaaS) – using the cloud to host, develop, and test applications;

---

20 TechTarget (n.d.). "G-cloud". Available at: http://searchcloudcomputing.techtarget.com/definition/G-cloud-government-cloud (accessed 10 August 2016).

21 Microsoft (n.d.). "G-Cloud". Available at: https://www.microsoft.com/en-us/TrustCenter/Compliance/UK-G-Cloud (accessed 10 August 2016).

22 The Wiltshire Council, which serves nearly a half-million citizens in southwest England, was the first in the UK to complete an rganization-wide implementation of Microsoft Office 365 as part of a cloud-based IT transformation strategy designed to adjust to tighter public sector budgets while improving service delivery to citizens. The efficiencies and savings from this implementation have cut the Council's IT spending by £5 million a yearabout 25 percent.ica.net

- Infrastructure as a Service (IaaS) – using the cloud in place of servers and other hardware; and
- Cloud consulting services – helping customers get the most from the cloud.

Every year, these vendors prepare documentation and submit evidence to attest that their in-scope enterprise cloud services comply with the principles, giving potential G-Cloud customers an overview of the vendors' risk environment. A GDS accreditor then performs a number of random checks on the vendors' assertion statements, samples the evidence, and makes a determination of compliance[22].

Key lessons and implications for South Africa

The UK's commitment to transferring all of the relevant government activities to cloud computing with its G-Cloud programme shows an all-encompassing approach that might be necessary for South Africa to realise the full range of benefits and improve service delivery rapidly. However, South Africa's institutional endowments do not lend themselves to such a commitment. Within the constraints of capacity, leadership, mandate and policy direction, the public sector in South Africa, and particularly SITA, does not appear to be in a position to implement an online marketplace for ICT services, an enforcement agency and consolidated data centre.

Efficiently procuring goods and services is a key enabler in this process. Borrowing from the UK, South Africa could gain certain comparative, review and compliance efficiencies beneficial to rapid public procurement, especially as it pertains to those ICT services government requires and SITA's ability to deliver. The latter would not be able to implement the constituent G-Cloud elements, with its inability to generate revenue and respond to ICT sectoral developments. More responsibility and accountability is needed to decentralise power while enforcing an autonomous and reactive mandate. The Department of Telecommunications and Postal Services (DTPS) would need to supply the necessary norms and standards to strengthen these institutional operations and leadership roles.

Another key lesson from the UK case is that the South African government would be required to develop, embrace and implement a technically advanced cloud policy: one that would challenge its capabilities and skills, which have fared quite well historically in the "development" stage of ICT policymaking, but fallen short on implementation (Senior government official, personal interview, 19 July 2016). An integrated national policy would be the first step in setting up an enabling environment for efficient means of delivery and management, such as G-Cloud. Without it, such initiatives would be restricted, at best, to a superficial role of instrumentalising ICT efficiencies, without the holistic and cross-cutting benefits of cloud computing.

At the national level, several officials raised the National Intelligence Agency as resistant to cloud computing, and several said the "closed security mindset" was unlikely to change, even in the face of evidence. With scepticism surrounding the security of online public sector data, fears of both national and personal information falling into the wrong hands – in addition to the belief that (despite evidence to the contrary) if government built, ran and operationalised systems they would be more secure – could thwart the efforts of forward-looking departments of government to modernise the public sector.

5.1.2. New Zealand

The NZ Government Chief Information Officer (GCIO) is based within the NZ Department of Internal Affairs and is responsible for providing guidance on how NZ government agencies should adopt cloud computing via a framework called "Requirements for Cloud Computing". This framework outlines what government agencies must do when adopting cloud services and the

22 Ibid.

government expects all New Zealand State Service agencies to work within it when assessing and adopting cloud services.

In 2014, the GCIO published a due diligence framework known as the ICT System Assurance[23], which is aimed at evaluating the risks of cloud service providers and establishing responsibilities between the cloud provider and the agency. Organisations that fall under the scope of the GCIO's mandate for providing ministers with government ICT System Assurance must apply this framework when they are deciding on the use of a cloud service. Other NZ state sector agencies are encouraged to use this framework as good practice guidance[24].

In October 2015, the New Zealand government endorsed a revised all-government ICT strategy that reaffirmed its "cloud first" policy on using information technology across the public sector. The revised strategy retains the "Cloud Computing Risk and Assurance Framework" that was developed and implemented under the authority of the GCIO.

As part of this effort, the GCIO has published a document entitled "NZ government Cloud Computing: Security and Privacy Considerations", which comprises 105 questions focused on security and privacy aspects of cloud services that are fundamentally related to data sovereignty. Vendor's responses to the 105-question framework gave government ministries more upfront information on how the vendors' cloud platforms can fit into their organisation, and how other agencies could meet official government mandates for the safe assessment of cloud services.

New Zealand's public and private sectors have historically lagged behind Australia in cloud computing adoption, partly due to data sovereignty regulations and the fact that there are few large data centres on the New Zealand archipelago. Cloud services located outside of New Zealand's jurisdiction, or owned by foreign companies, can introduce data sovereignty risks, but the cost-benefits of using cloud services has forced many to rethink their reservations about data leaving the country, especially since these jurisdictions have similar privacy laws and protections to New Zealand.[25]

However, government sees this as a reasonable risk to take. Last year, a report from the New Zealand Productivity Commission recommended that the country rethink the data sovereignty, security and privacy risks of offshore cloud computing, primarily with Australia. The devaluation of data sovereignty and reduced suspicion came after an acknowledgement of the high costs of retaining local data centres and their services, as well as that of the psychological, rather than technological, perception of risk in offshore data storage[26].

One of the key outcomes for adoption of cloud computing in the public sector is evident from New Zealand's Ministry of Health. After confirming its requirements for storage of personal health information were satisfied by one vendor's core cloud services, the ministry has been able to build upon a scalable foundation that enables its employees to take advantage of new technologies and faster data response times when providing healthcare.

---

23 See the ICT system assurance: https://www.ict.govt.nz/ict-system-assurance/about-ict-system-assurance/.
24 See requirements for cloud computing: https://www.ict.govt.nz/guidance-and-resources/information-management/requirements-for-cloud-computing/.
25 Henderson, N. (2012). "Study finds New Zealand cloud adoption slow as enterprises cite data sovereignty, latency issues", available at: http://www.thewhir.com/web-hosting-news/study-finds-new-zealand-cloud-adoption-slow-as-enterprises-cite-data-sovereignty-latency-issues (accessed 14 September 2016).
26 Smellie, P. (2014). "Government urged to cut costs with offshore cloud computing", available at: http://www.nbr.co.nz/article/govt-urged-cut-costs-offshore-cloud-computing-bd-157270 (accessed 14 September 2016).

Key lessons and implications for South Africa

In addition to a CIO, South Africa could also consider a due diligence framework, such as New Zealand's ICT System Assurance is necessary for coordinating assessments of cloud providers and services, as well as possibly centralising responsibilities in a particular agency for efficiency. The last policy point to learn from New Zealand is how the importance of recognising the cloud as the preferred hosting platform for the public sector is captured and stipulated in New Zealand's national ICT strategy.

South Africa should more formally, however, and more in line with its current institutional arrangements, consider the extensive benefits of having a formal cloud computing framework prescribing the actions and direction of government agencies when adopting cloud computing services.

A good start in South Africa would be to establish such a framework. To oversee this process in the South African context, GITOC could partner with DTPS in the policymaking phase in order to address cloud computing needs. A coherent public policy could originate out of this framework and stimulate sectoral change, without the necessity of a CIO.

Such coherence is a necessity to allow for certainty and flexibility. The balancing of these two is delicate since the latter is needed to react to global and industrial trends while clear targets and objectives ensure success in rapid reaction. These features of a policy and framework would reduce the cost of delays in regulation and enhance efficiency.

Government's concerns for data security and sovereignty could also be addressed through formal consultation avenues, such as the 105-question document submitted to vendors addressing such issues. The simplification of security standards and classification measures also helped the UK government in this regard. Relying on a discursive process between the public sector, as client, and cloud service provider enables both to follow through on a commitment to cloud computing and efficient service delivery. The DTPS should be in charge of leading such discussions to use feedback for the construction and implementation of standards and norms during adoption.

In addition to learning the public policy practices that have made cloud computing a success in New Zealand, South Africa would have to investigate data hosting centres that could alleviate the burden of having to self-provide such resource-heavy services.

Institutional initiative and creativity would be required by South Africa's bureaucratic departments to implement this unprecedented technology. Since implementation can be a finite, albeit complex and even drawn-out, procedure; the availability and ability of a champion to lead the change in management and operational procedures could be sufficient to set up the policy and maintenance requirements for cloud computing to successfully enhance government's capacity. The carrying out of upkeep and maintenance, however, as well as the continued investigation of opportunities for growing government's cloud computing capacities would demand extensive human resource development to accompany cloud initiatives.

The payoffs seen in New Zealand's health sector nevertheless incentivise the need for such growing pains in South Africa's public, service and economic sectors.

5.1.3. South Korea

South Korea's Communication Commission has allocated about USD500 million for the development of Korean Cloud Computing (KCC) facilities, and has partnered with the Ministry of Knowledge Economy and the Ministry of Public Administration and Security for the creation of cloud-based IT infrastructure to support the government and ICT industry.

The initiative is expected to boost cloud computing services in the South Korean market and, in turn, promote local participants to enter the market. As these participants gain expertise, they are expected to play an increasing role in the export of cloud services to the global market. Moreover, government agencies, which have been cautious in adopting cloud services, can currently leverage local service providers. This is aimed at garnering 10 percent of the global cloud computing market and reducing the public sector's ICT spending by 50 percent[27].

The success of all cloud initiatives stems from the success of the government in engaging Korean enterprise and building the appetite for cloud computing, which was at a low adoption rate in comparison to other nations[28].

The Ministry of Science, ICT & Future Planning developed the world's first (Korean) Cloud Computing Act in 2015, aimed at increasing the rate of cloud computing adoption in Korea from 6.4 percent to 13 percent between 2015 and 2016, as well as increasing the number of Korean cloud computing firms from 353 to at least 500 during the same period. In addition, it is planning to increase the use of private cloud computing tools by public institutions by at least 3 percent, so that the size of the domestic cloud computing market can reach 1.1 trillion won[15].

In line with this, the ministry is setting up a cloud computing support centre in Daegu City for public institutions to make better use of cloud computing tools provided by entities in the private sector. At the same time, it is going to allow enterprises in need of cloud computing in various industries to join the public-private deregulation task force currently led by IT firms in the private sector, so that industrial players are afforded the opportunity to identify regulatory bottlenecks in cloud computing uptake.

The ministry is also focusing on the enhancement of the productivity of start-ups and small and medium enterprises (SMEs) by means of cloud computing. To this end, it is to provide cloud computing software development tools and infrastructure required for ICT start-ups in cooperation with the Centres for Creative Economy and Innovation across the country.

More measures are scheduled to become available to assist in South Korean cloud computing firms' overseas business expansion, too. The measures are to cover Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). According to the Ministry, South Korean firms stand a chance in the field of SaaS, which is the largest of the three in terms of market size, but is still not a dominant player – unlike in the area of packaged software, led by a handful of companies, such as Microsoft and Oracle. When it comes to IaaS, leading South Korean enterprises are capable of exporting their infrastructure.

5.2 Institutional arrangements and leadership

Institutional arrangements and leadership play a role in driving adoption of cloud-based services in countries where this has been successful. It is recognised that the state, as one of the largest consumers of ICT has a key role to play in creating awareness and building trust (in cloud computing) by serving as a role model and leader in cloud-based services. Further, internal adoption of novel ICT services and new technologies that drive efficiencies and information flows has been most successful when there is a champion, or champions, formally or informally, within the organisation. SITA, which is responsible for identifying technologies that will improve government efficiency, has an important role to play in championing the benefits of cloud computing and DTPS is responsible for developing policy that will guide the adoption of these services within the public sector.

---

27 Chandrasekaran, A and Kapoor, M (2011). State of Cloud Computing in the Public Sector – A Strategic analysis of the business case and overview of initiatives across Asia Pacific. Available at www.frost.com/prod/servlet/cio/232651119

28 Davies (2016). "Korean government prioritises cloud". Available at: http://www.businesscloudnews.com/ 2016/03/30/korean-government-prioritizes-growth-of-cloud-computing/.

5.3 Fragmentation of mandate in government

The failed institutional arrangements that pertained until the last administration, which saw SITA as an implementation agency with the Department of Public Services and Administration (DPSA), were a well-documented failure and resulted in the relocation of SITA under the DTPS. However, the challenges faced by the DTPS as it attempts to recover from the results of its disruptive split from the Department of Communications, means that it has not been in a position to prioritise policies required to provide direction to SITA for implementation. Further, the legacy policy department, the DPSA, still appears to be responsible for setting norms and standards essential to procurement and operationalising the public sector. The dysfunctionality in the institutional arrangements may not lie in the location of SITA in a particular department, but in the nature of the procurement agency; its intention to be a revenue centre, not simply a cost centre; its lack of autonomy, on the one hand, to respond to changing business needs, new technologies and skills requirements, and, on the other, the concentration of power in it, the potential conflict of interests and the lack of accountability and responsiveness to its "clients". This could be enabled by allowing departments and agency to procure products and services in compliance with specified norms and standards, if they can secure them at a better price or quality level. SITA would still have the advantages of economies of scale and scope, but SITA would need to ensure efficiencies in its own sourcing of products and services.

Lack of a coherent public policy

ICT policy in South Africa is still treated as a narrow sector policy, that fails to reflect the cross cutting nature of ICTs in a modern economy and state. ICT is not only a growing services sector with the potential to add greater value to the economy, but cuts across the entire public sector and indeed the private sector. Policy can no longer focus on telecommunications, broadcasting, IT or the internet, but needs to be seen as an integrated national policy, Digital SA, that is not only focused on infrastructures and services but also on national human resource deficits in a knowledge economy, input costs of communications that may inhibit private and public sector enterprise, and citizen services across government. It requires certainty in vision and objectives and agreed strategies and targets, yet flexibility to respond to the dynamic global environment in which national development take place. It requires anticipation of national needs on the basis of global trends and national agencies that can fast-track policy and implement swiftly, to create an enabling environment of economic growth development, innovation and social coherence. Under such conditions market barriers would be reduced, costs and cost of delays – such as unified rights of way regimes, high-demand spectrum and cloud policies – would be reduced.

Key lessons and implications for South Africa

A noticeable necessity in the Korean case is the need for government's demand-stimulating investment and policy planning. By recognising both the need for cloud computing in the public sector as well as its potential for the private sector, the Korean government was able to dangle a carrot for investors and partners to buy in. In this way, the government's desire and ability steered industry towards supporting the adoption of cloud computing. This created a pool of local resources to draw on, and enabled a domestic market to develop for the improvement of its own cloud services, as well as those of foreign economies.

This ideology is strongly institutionalised and supported by a capable state; a large differential factor when compared to South Africa. That said, the benefits expected in South Korea from its cloud computing and data centre investments are admirable and should be kept in mind during the policymaking process. The government expects to compile SaaS, PaaS and IaaS gains in the market with those in the cloud market, while stimulating local and foreign demand and gaining returns on public investment.

While creating unattainable objectives would be detrimental, the cloud computing implementation process presents an opportunity for arranging the leadership and institutional structures in government, unifying the public mandate and constructing an effective and coherent policy – outcomes desperately needed for the South African economy and public sector.

The Korean government gave its Ministry the resources, mandate and authority to co-create a cloud adoption procedure with private actors. The leadership was championed from within the organisation with authoritative direction and investment, the mandate was carried out in tune with the private sector so as to incentivise supplemental investment and take up, and a policy was drawn up with specific investment targets and clear mandates for ministerial support of smaller investors.

In similar ways, South Africa would need to champion cloud computing adoption and engage the private actors, such as Microsoft in order to inform market interest and react to industry dynamics. Additionally, SITA's role would need to become more functional in the institutional arrangements as a procurement agency. SITA requires more autonomy when responding to business needs, new technologies and skills requirements, as well as a decentralisation of power to avoid conflicts of interest and a lack of accountability (CIO (a), personal interview, 24 June 2016).

The national policy requires strategic certainty and targets in addition to flexibility for responding to global dynamics. Anticipation of national development is needed to fast-track policy implementation and prioritise economic growth.

5.4 Synthesis

Table 1 below summarises the key global best practices and benefits thereof that can be drawn from public sector cloud adoption strategies in the UK, New Zealand and South Korea.

TABLE 1: GLOBAL BEST PRACTISE FOR CLOUD ADOPTION IN PUBLIC SECTOR

Key best practice	***United Kingdom***	***New Zealand***	***South Korea***
Designated champion for cloud computing	*"G-Cloud" authority*	*New Zealand Government Chief Information Officer (GCIO)*	*South Korea Communication Commission*
Succinct policy for cloud computing	*"G-Cloud" framework*	*Requirements for cloud computing framework*	*Government Integrated Computing Centre Cloud (G-Cloud)*
Demand side stimulation			*Allocated USD500 million to the development of a Korean cloud computing facility*

Development of cloud computing skills		*Using foreign data centres to cover their skills shortfall*	*The Ministry of ICT is providing cloud computing software development tools and infrastructure to support ICT start-ups in cooperation with the Centres for Creative Economy and Innovation across the country*
Vendor compliance and certifications	*G-Cloud authority – oversees and enforces standards and certifications using a 14- point compliance check list provided*	*ICT System Assurance used in the selection process of cloud computing service providers*	

Decentralised certification of vendors	*Providers self-certify and supply evidence in support of the 14 Cloud Security Principles of G-Cloud* *Verification is performed by the Government Digital Service (GDS) branch at its discretion*	*The "New Zealand Government Cloud Computing: Security and Privacy Considerations" framework is used for self-verification and to select a cloud service provider*	
Cloud computing's role in national ICT agendas is clearly articulated	*UK has adopted a cloud-first policy for procurement of ICT within the public sector*	*Cloud computing is identified as the preferred hosting platform for the public sector in New Zealand's national ICT strategy*	*Cloud computing recognised as important industry tool for development and is actively promoted by cloud computing legislation.*

Centralised cloud procurement ("marketplace")	*Referred to as the CloudStore, where government agencies purchase cloud services on a pay-as-you-go or yearly contract basis*		
National security entities' buy in	*The national security classification scheme is applied to cloud*		*Ministry of Public Administration and Security is part of the cluster driving cloud computing*
Government data classifications and security framework	*The UK government's security classification scheme was simplified from six to three levels: official, secret, and top secret.*		

6. THE BENEFITS OF CLOUD COMPUTING

Table 2 below summarises the significant benefits of cloud computing highlighted above. These will be use to inform the South African Public Sector Case Study:

TABLE 2: BENEFITS OF CLOUD COMPUTING

Benefit	***Comment***
Cost savings	By paying only for the services they use through cloud computing, organisations can reduce or eliminate ICT capital expenditure. Furthermore, further cost reductions can be achieved by reducing or redeploying their IT staff. Cloud computing allows for facilities consolidation i.e. resources can be pooled, including storage, computing, memory and network bandwidth, driving infrastructure cost savings. Cloud computing is location independent, i.e. users can access services remotely and therefore organisations could save on real estate and energy costs.
Ease of implementation	Cloud computing removes the need to purchase hardware, software licenses, or implementation services, enabling companies to deploy cloud computing rapidly.

Flexibility	Cloud computing offers more flexibility in matching ICT resources to business functions than past computing methods. It also increases staff mobility by enabling access to business information and applications from a wider range of locations and/or devices.
Scalability	Cloud computing enables businesses to meet growing or fluctuating bandwidth demands, without having to scramble for additional hardware/software. They can add or subtract capacity as the network load dictates.
Access to top-end IT capabilities	In markets like South Africa, with IT skills shortages and high labour costs, cloud computing helps alleviate the issue by allowing organisations greater access to high-calibre hardware, software and staff than they can attract or afford themselves.
Redeployment of IT staff	Organisations can make better use of valuable IT staff by moving them from routine operational and maintenance tasks to higher value tasks because cloud computing does not require as much provisioning and maintenance as past computing methods.
Focusing on core competencies	The ability to run cloud computing infrastructure, such as data centres is not the core competency of most organisations. Cloud computing removes this burden and allows organisations to focus on core and critical issues, such as public service delivery in government.
Better services and collaboration	Cloud computing allows organisations to better engage with customers/citizens, as cloud platforms enable access to a wide range of services on a single platform. Cloud computing also allows better collaboration between organisations' departments and organisations' employees.
Security	Cloud computing stores data in the cloud and not the local hardware. This provides greater security in the event that something happens to the hardware. It also allows for remote wiping of devices in the event they fall into the wrong hands. Furthermore, data centres that store the cloud infrastructure housing information typically adhere to global security standards.

7. THE SOUTH AFRICAN CASE

7.1. Cloud market in South Africa

Cloud computing in South Africa has been largely supplier-driven, with most organisations opting for private cloud deployment models – as opposed to the public cloud – due to data and security concerns[6].

The private sector is undergoing digital transformation and therefore realising the benefits of using technology to transform the way they conduct business. To this end the firms are evolving their technology ecosystems to support digital services, in order to improve service delivery to customers and achieve internal efficiencies and cost savings through their IT infrastructure.

The public sector is also starting to realise the benefits of going digital to better engage with its citizens and has earmarked ICT development as central to achieving economic growth and advanced service delivery through e-government services.

7.1.1. Drivers

Part of this transformation involves the use of cloud computing services, as cost pressures are increasing due to the challenging economic environment. The corporate segment in South Africa

is driving demand for cloud computing services, in order to take advantage of the cost-efficiencies, scalability, agility and other benefits (discussed above) offered by cloud computing. IT innovation is earmarked to achieve cost savings and better collaboration between government departments, efficiently use scarce skilled personnel and simplify the implementation of new technologies within the public sector. Although there is general awareness of the benefits offered by cloud computing services in the public sector, the use of the services has been limited.

Global vendors, including Amazon, Google, Microsoft, Sales Force and T-Systems, have significant presence in the cloud computing market in South Africa. Local players include Business Connexion Telkom, Dimension Data and its subsidiary Internet Solutions, MTN Business Solution, Neotel and Vodacom Business. Some local service providers identified SITA as a local competitor. These service providers say that the cloud has introduced flexibility, a strong value proposition, speeded-up time to market and the nature of new functionality.

“Basically using cloud is a lot faster as it reduces complexity of skills set required for extended functionality. This is particularly relevant for the setup of services. The workload associated with getting a server ready, before software can be deployed on it, before you can even start using a system in any non-cloud computer infrastructure is massive – the complexity of importing computing hard equipment, and then when it has arrived, the delay associated with preparing hardware for use.

“The whole workload associated with just getting the server ready can take months if coming offshore: ensuring the associated skills sets are available; installing operating systems; maintaining data bases, underlying computing infrastructure – server, op system – maintaining database; maintaining server data; and then, when that is all done, actually what have you got? Nothing…. Then you only have the potential to do something, but you are not yet adding value. The application CRM, mail applications, etc. still need to be added – it is then that it delivers value to the business. Fundamentally what the cloud does is avoid the extra time delays. You go online, buy computing, and it is available to you in business. This computing infrastructure is available equally to anyone, any time. This is the value proposition, whether you are a private company or a large public sector enterprise.” (Andrew Aitken, Internet Solutions, personal interview, 2 September 2016)

However, the trend towards migration with legacy networks was not a switch-on scenario, Aitken said, but a journey of transformation, trends plotting, analysed outcomes. Referring to an Internet Solution study of 6 000 migrations, Aitken said migration to the cloud starts off with non-core business applications, as organisations move to e-mail, hosted exchange and other mature offerings that have existed for over a decade but just were not referred to as cloud services.

Unlike half a decade ago, where local providers appeared to be threatened by the global cloud operators, the larger service providers recognised that different cloud platforms were required for use in different scenarios[29].

Aitken said the nature of the workload, together with the location of users determined the use of platform in the solution they offered. If applications were only accessed by users in a Johannesburg office on desktop, customers were advised to keep the application at data centre on its own premises. If the business required all branches in South African connected via VPN to WAN then that would be hosted more appropriately in a data centre, albeit on a private cloud solution.

On the other hand, the Department of Foreign Affairs, with embassies around the world would obviously be optimally operated on an international platform, such as Amazon or Azure, because the end users are from around the world. “You get economies of scale, speed to market. The

reduction in skills set required operate the underlying infrastructure that is not adding value." (Aitken, IS, personal interview, 2016)

Although the global hyper-connected platforms offered significant economies of scale, if the users were all local then the cost-benefit analysis would probably be in favour of a local provider.

"Besides the POPI[29] Act, which means that some customers demand that their data is stored locally, there may still be price parity between local providers and international platforms, because of the rand dollar exchange rate.

"Public and private cloud solutions are not competitors, it depends on the case and there is acceptance of the need for hybrid solutions. Cloud extends to local and hyper-scale cloud computing platforms, anywhere in world.

"IS believes customers, public or private sector, should make the choice of platform based on use case scenario, so strategically we have embraced international and local platforms, and we have built them into one single view, where organisations can spin up platforms via Azure or Amazon on the same interface. Encourage customers to select the right platform and deploy a local or international platform as required and which can all be managed through a single 'plane of glass'." (Aitken, IS, personal interview, 2016)

7.1.2. Barriers

Resistance to cloud migration comes primarily from two areas: security concerns, and redundancy in human resources and the need for reskilling – both in the public and private sector. The efficiencies offered by the cloud are often accompanied by resistance from IT and HR managers around what to do with those employees without the skills set and who are not trained up for the cloud.

A number of cloud providers indicated that, while they can offer very high levels of data security, cloud platforms were only as secure as the application users make it. Cloud service providers could secure their platforms and systems, but they were unable to guarantee security in the user's environment, over which they had not control.

"Both in the private sector and public sector, there is a tension that exists between the business users who know they can get close to getting the computing capability to accelerate business, and IT departments holding back on the grounds that cloud solutions would breach risk and compliance requirements and costs would spin out of control. But, because it has become so easy to access cloud, IT departments are being forced to accommodate cloud computing into their overall architectures. This is the same tension between government departments wanting to move ahead to improve efficiencies, and SITA holding back" (Aitken, IS, Persona Interview, 2 September 2016.

7.1.3. Private sector view of public sector cloud readiness

Several of the private and public sector interviewees believe that to modernise the public sector, government will require a cloud policy put in place first, such as in the UK. This would entail a shared model that would require, in the first instance, using applications available on the cloud. If applications were not available for the use required, then it would require sourcing infrastructure in the cloud, in order to load applications. Then, if these were not available, consideration could be given to deploying it locally.

---

29 Protection of Personal Information Act 4 of 1982

There are several successful cloud deployments in the public sector but these tend to be isolated. One of the globally renowned cases, in terms of successful e-government applications, is the SARS e-filing which is an internet solution platform. Many state organisations already have non-core services on the cloud, such as IP-based voice infrastructure, carrier grade voice infrastructure and hosted PABX- and IP-based contact centres. The Reserve Bank website provides another example, in the monetary policy committee press briefings, which are conducted through live video stream on cloud services.

One of the best examples of the power of cloud services is that of the IEC during the last local government elections, when, for a period of a week, the organisation leveraged the full breadth of cloud services off data centre to deal with the exponential hit rate: dedicated hardware infrastructure, virtualised infrastructure, multiple layers of security and the service provider backbone throughputs.

"It would take about three years to recover the investment, were it not scalable according to need, and had to be built to maximum need and then lie fallow and become redundant between elections. What the cloud was able to provide through the IEC website, was security technology to protect their website constantly, scanning technology to mitigate against identified threats, security capabilities to a far greater degree than their core business, to deliver a highly sophisticated and responsive system to meet their business needs, that they themselves would never have the breadth of expertise to undertake." (Aitken, personal interview, IS, 2016).

7.2. Status of cloud use by public sector in South Africa

South Africa has been an early adopter of e-commerce and e-government, and was one of the leaders with electronic transaction policy at the turn of the millennium. Despite this early commitment to exploiting ICT to enhance public sector delivery progress, modernising ICT within the public sector has been slow. Hampered by protracted policy processes and stalled decision-making generally, there is a gap between what is stipulated on paper and the implementation of policy prescriptions and standards within the public sector (Government official, personal interview, 17 August 2016). As a result, the South African public sector lags behind the private sector as well as behind African and global counterparts in terms of ICT adoption of advanced technologies, including cloud computing.

SITA's performance has been suboptimal by its own account, with customer satisfaction as low as 35 percent in the 2014/2015 financial year, particularly regarding challenges related to the turnaround time for procurement of IT resources[30]. This has fortunately been acknowledged by the current leadership, weaknesses identified, and strategies developed to overcome this serious barrier to effective government.

SITA identified the following as their strategic priorities for 2016:

- value-added procurement to lower the cost of goods and services;
- providing the core IT services of networking, hosting and data infrastructure;
- driving the e-government agenda of the public sector (with a focus on achieving integration);
- being the lead agency for cyber security;

30 SITA (2014/2015). State Information Technology Agency (SITA) Annual Report.

- being a customer-centric organisation with motivated employees; and
- developing transparency of costs and reducing costs[31].

As the case studies above show, the most cost-effective way of meeting these objectives in the public sector is through the deployment of cloud solutions. Chief Technical Officer (CTO) of the SITA, Pandelani Munyai, explains the conditions that give rise to this:

"It is critical for CIOs to understand the business of government and how technologies can be used to provide government services … At the same time, we can also look at disruptiveness as a powerful engine for innovation, inspiration and efficiency. Game-changing technologies are not only transforming every business process, but they also give us the ability to create new products and services that were impossible just a few years ago.

"Thus, the role of government CIOs has shifted from protecting and defending the status quo to embracing and extending new innovative capabilities … In today's era, government CIOs should focus more on information intelligence, platforms that enable new value chains and integrated ecosystems, as well as driving business transformation and accelerating growth"[32].

Although the value of ICTS is increasing among the top tiers of management within government, the tough financial situation in the country and accompanying general fiscal responsibility has chilled ICT investment. Currently, budgets are split more or less equally between software, hardware and services, though most is spent on hardware, then services and finally (not far behind) software. The biggest concern of public sector CIOs is data and system security, followed by skills shortages and talent management.

Significantly, public sector CIOs on average give their departments less than 50 percent for progress on the "digitalisation journey", as little progress has been made by SITA and government to implement emerging "disruptive technologies", including cloud computing. Given that the South African government is facing challenges to meet growing demand for enhanced service delivery with a limited budget, disruptive technologies, like cloud computing have the potential to enable government to meet its mandate and policy objectives of a collaborative government, greater internal efficiencies and better service delivery. CIOs believe that SITA is turning itself around but they acknowledge this will take time.

In addition, the government's legacy equipment is depreciating but there is limited budget to invest in upgrading the existing systems. Government IT departments also lack integration, due to a fragmented IT procurement process[33].

Cloud computing is expected to enable better interaction between government and citizens and enable the provision of e-government services (including e-health and e-education) for enhanced service delivery. Progress towards development of e-government services has been slow, as the use of cloud computing is limited within the public sector.

---

31 Parliamentary Monitoring Group (2016). "SITA on its 2016 Strategic and Annual Performance Plans". Available at: https://pmg.org.za/committee-meeting/22302/?utm_medium=meeting-card&utm_source=homepage.
32 Brainstorm (2016). CIO Directory. Available at: www.brainstormmag.co.za/shopx/cio-directory.
33 Mvelase, P. S., Dlamini, I. Z., Sithole, H. M. and Dlodlo, N. (2013). "Towards an E-government public cloud model: The case of South Africa". Available at: www.researchspace.csir.co.za.

As one of the largest single users of ICT and services, the public sector in South Africa is potentially amongst the greatest beneficiaries of the cost savings, flexibility, scalability and greater collaboration offered by cloud computing services.[34]

Well after this study was concluded, the SITA CEO, Dr Setumo Mohapi announced that a cloud strategy had been developed. Speaking at a workshop to discuss this paper Dr Mohapi said the cloud strategy tried to address the lack of value Government was getting from its vast IT expenditure that was increasing year on year.[35]

This was a key strategy, he said, to address South Africa's poor performance on e-government and other global indices that measure Government's role in IT ,or IT's role in Government. He said although as indicated in this report, there were several foundations played for IT-enhanced public services, there was "a gap been what was stated on paper and implementation in practice". However, there had been "major changes in the department which have resulted in the SITA achieving more in the past six months than it has in the last 15 years"[36].

Dr Mohapi announced that the department had developed an internal strategic document which was being used as a basis for implementing a cloud strategy for the public sector. He stated that there is an increased acknowledgment of the cost savings, flexibility and agility provided by cloud services within government. He emphasised that unlike other policy and plans, "..the strategic document was followed by implementation the following day".

Dr Mohapi stated that the major success of the internal strategy document was that the government was implementing what had been stated on paper which was addressing the challenges that SITA had in the past. Dr Mohapi advised that a similar strategic approach to that of cloud was being used to facilitate the implementation of the new e-government and e-services programmes being developed by the the Department of Telecommunications and Posts in collaboration with other government departments.

In February 2017, SITA awarded a contract to a cloud provider to provide cloud services for government. Dr Mohapi noted that it was one biggest contracts that SITA had ever entered into and that "…the capacity of the contract has been used up quickly due to high demand within government". Therefore, SITA is planning to go back to market to get more (capacity)".

Some examples where SITA has implemented cloud services, include the provision of a core disaster recovery system for the South African National Space Agency (SANSA). SITA is also implementing an Integrated Financial Management System on behalf of Treasury via the cloud. In March 2017, SITA switched on a disaster recovery system for the entire Free State province.

Cloud is also envisioned to enable integration in the education system. Dr Mohapi stated that the cloud system could be used to track a child from elementary school to tertiary school through the public school system and SITA could use CV verification software to analyse information provided on CVs by people looking for prospective employment to verify if the information is true. In this context information would be used to create value within government.

---

34 Gillwald, A., Moyo, M. and Altman, M. (2012). "Cloud computing in South Africa: Prospects and challenges". Chapter in Cowhey, P., Kleeman, M. and San Diego, U.C. Unlocking the benefits of cloud computing for emerging economies. Available at: www2.itif.org.

35Research ICT Africa was not able to interview the SITA CEO or CTO during the course of the study that was completed in December 2016, despite dozens of attempts and cancelled appointments.

36 Modernising the public sector through the cloud workshop. 24 March 2017, Johannesburg, hosted by Microsoft.

Dr Mohapi also stated that SITA has succeeded in automating and centralising the procurement system in government jointly with Treasury, which has led to reduced response times and increased efficiencies.

7.2.1. Skills shortages in public sector

ICT skills shortages in SA are arguably a bigger challenge than some of the other barriers to ICT diffusion, requiring as they do, very long term and catalysing investments to yield returns. In addition, the public sector is competing with the private sector for a limited pool of skilled resources and there is also variation in the salaries offered, which makes it challenging for the public sector to attract the right level of talent.

7.2.2. Absence of cloud computing policy for the public sector

The national and provincial levels of government are subject to the SITA Act, which sets the norms and standards regarding IT procurement in the public sector. SITA, in its past tender documents has prohibited the use of cloud computing services, which has constrained these at national and provincial government level. Various CIOs indicated that the norms and standards framework would need to be adapted to include cloud services as a standard, in order to drive their use within the public sector.

7.2.3. Inconsistencies in the approach to cloud computing

The local government level is not subject to the SITA Act, and therefore has been driving the use of cloud computing within the public sector. Most of the metros are deploying cloud services and in Ekhuruleni the integrated government communications system across the seven sub-municipalities are cloud based, offering a high level of delivery and efficiency. Generally, however, cloud computing deployments are ad hoc and uneven across different municipalities and local departments, with smaller and poorer municipalities, and generally without the expertise and resources to initiate cloud deployment. As a result, there is still a “siloed” and fragmented approach to ICT, including cloud computing, with many government systems disparate and not interoperable.

Several e-government services have been implemented by various government departments but they are not integrated, despite the benefits of doing so. Examples are: the Department of Home Affairs (DHA), Department of Correctional Services (DCS), Department of Social Development (DSD), South African Revenue Service (SARS), South African Defence Forces (SADF), Department of Human Settlements, South African Police Services (SAPS) and Department of Justice and National Prosecuting Authority (NPA). This has resulted in inefficient replication of effort and some systems that could benefit from talking to each other do not do so, such as, DHA and SAPS systems. The synergies that could be achieved through interconnected systems have been missed.

There is widespread acknowledgement in government on the benefits of cloud computing. There was consensus amongst those interviewed that cloud computing services could be leveraged to assist government rationalise its expenditure on IT services across all spheres. Cloud computing would also enable government to streamline the number of IT licenses, which are currently underutilised (Treasury, personal interview 21 July 2016).

7.3. Cloud mainly for noncritical processes

In cases where cloud computing has been adopted in the public sector, most respondents emphasised that government’s position is that no private or “sensitive” information is being put into the cloud. However, despite these concerns, according to several respondents there is widespread use of cloud-based services like Gmail – which sits in the cloud – to transmit official communications.

Due to the lack of sound guidelines on "acceptable" use of cloud in government, most departments using cloud computing are using it for noncritical processes, such as customer care and citizen engagement. As one GITOC member put it: "Nobody is explicitly saying what are the things that can or cannot go onto the cloud." (Personal interview, 12 July 2016)

7.4. Assessment of public sector cloud computing awareness and deployment

CIOs across various government departments acknowledge the benefits pertaining to the adoption of cloud computing solutions. However, the extent of their use varies significantly between departments. Below are examples of the use of cloud computing in the South African public sector:

7.4.1. City of Johannesburg (CoJ)

The CoJ has embarked on a three-phase approach to adopting cloud computing. In the first phase, CoJ piloted a cloud-based customer engagement application. Residents in the City are able to report road problems and service requests that are channelled through a call centre to the Johannesburg Road Agency. These include issues such as potholes, faulty traffic lights, damaged manholes or blocked storm drains. The application allows residents to record GPS coordinates and take photographic evidence, which is filtered through to a call centre that logs a ticket and dispatches the Johannesburg Road Agency to address the problem. The system also has a customer feedback loop, where it informs the resident once the problem has been resolved. Residents are also able to provide feedback to the City through the application.

In the second phase, CoJ also plans to introduce a transportation application that includes bus schedules, routes, etc.

Under phase three, CoJ plans to adopt a hybrid cloud model, where some of the data is stored internally and some on the cloud. The City emphasised that no private data will be put on the cloud, so as not to contravene Protection of Personal Information (POPI) Act.

The CoJ has embarked on a public Wi-Fi project. The economic benefits of the overall programme include a number of ICT-promoting elements, including SMME incubation in partnership with the University of Witwatersrand and a "Joburg Hackathon". The city spends R410m on ICT services annually, so that the saving of 30 percent already constitutes over R123m per annum. The City has used as part of its rationale the World Bank study that claims that a 10 percent increase in broadband penetration drives a 1.38 percent increase in GDP in developing economies. Given that CoJ has a "domestic product" of R313bn per year, that growth is more than 4bn per year. Most of the wards in Johannesburg (constituting 80 percent of the population) had poor or limited access to the internet. In the view of the City's Head of Broadband, Zolani Matbese, there was a strong shift to cloud-based applications, which meant that one had to live "in the cloud" in order to develop relevant applications[37].

7.4.2. Government Pension Administration Agency (GPAA)

GPAA stated that one of the main challenges it faced as a department were archaic systems that could not be backed up and/or lacked disaster recovery capabilities. GPAA's motivation to adopt cloud was to build resilience in its existing systems. One of the first things that GPAA addressed strategically in their migration to the cloud was introducing self-service and going paperless as a

37 Mybroadband. Zolani Matebese (the City of Jo'burg's Head of Broadband) delivered at a conference of the South Africa's Wi-Fi Alliance, outlined "Free Wi-Fi for Johannesburg". April 15, 2014. Available at: http://mybroadband.co.za/news/internet/100684-free-wi-fi-comes-to-joburg.htm.

means to address fraud and corruption issues in their department and build in more controls into their processes.

GPAA initially moved its call centre to the cloud. The initial key success was that within three days the new call centre was up and running seamlessly. The second success was the decentralisation of the call centre located in Tshwane, which was able to switch over into the regional call centres through the cloud. Furthermore, on average the GPAA is now utilising about 87 percent of its call centre capacity, using cloud.

The GPAA noted that it was difficult to move all its documents into the cloud. Given that it works with sensitive pension benefits data, GPAA requires a data classification policy to determine what can be put on the cloud and how to manage data that is on the cloud. It envisages adopting a "hybrid approach" to cloud computing in the future, whereby some documents are moved to the cloud, while other data is housed internally.

The GPAA has further plans to move its HR system and field service to the cloud. It noted that there needs to be a cloud policy in place before it can take that step. one benefit cited for moving to the cloud were the tangible cost savings of outsourcing the management of their call centre compared to building internal systems. Another benefit was business elasticity and the pay-as-you-use model offered by cloud computing, which results in further cost savings.

7.5. Identification of barriers to adoption of cloud computing for the public sector

7.5.1. Technical barriers

Availability and quality of broadband infrastructure to support widespread adoption

The availability and quality of broadband infrastructure in South Africa is uneven. The government has attempted to address this challenge by embarking on a national broadband plan, SA Connect, to expand access to rural and under-served areas. Generally, there is better access in larger cities, such as Johannesburg and Cape Town, while smaller cities and provinces (e.g. Limpopo) remain underserviced.

This results in inconsistencies in the adoption of cloud computing by public sector entities across the country, as some regions currently do not have adequate underlying communications infrastructure to fully deploy/adopt cloud computing (CIO(b), personal interview, 24 June 2016).

Vendor selection and quality of services

Uniform and transparent guidelines on vendor certification and compliance to determine the degree of service performance that can be expected/demanded for cloud computing is currently not available. In the absence of such guidelines, there is reluctance to engage any cloud service providers for fear of vendor non-compliance with national laws and standards for IT. As one CIO stated:

"…how then do I vet the cloud provider? Government must have standards or mechanisms of saying 'you need to go through these processes for you to be able to be a certified cloud provider for government". It's a question in every CIO's mind. But if you have that kind of vetting or mechanism, then it might deal with the issues of trust. (Personal interview, 19 July 2016)

Privacy and security

Maintaining the privacy and security of information held by public sector authorities is a key concern related to the adoption of cloud computing by the public sector, as well as ensuring compliance of cloud computing platforms with data protection and security laws. In terms of security, this entails preventing unauthorised access to sensitive personal data and government data[38].

There are also significant concerns around privacy of data stored in the cloud. While there is no real evidence that placing sensitive public information into a cloud environment, either on- or offshore, will risk breaches of privacy and security, this is a major concern within South Africa's public sector.

While the Protection of Personal Information Act (POPI) provides guidelines on the transfer of data outside the borders of South Africa, it does not state explicitly how to handle data stored on the cloud, which creates uncertainty around the use of cloud computing services in the public sector. One CIO noted: "When we discuss issues of POPI and cloud, people mention POPI [as the guideline] but there are no specifics in terms of what POPI says and whether cloud initiatives can have a negative impact on the intentions of POPI" (personal interview, 12 July 2016).

Security of government data is a key strategic focus for SITA. SITA is investing in upgrading its data centres and building up capacity for a government owned cloud computing facility for the public sector. It is also in the process of upgrading its ICT security standards and tackling cybercrime. This is because government is experiencing security breaches[31]. One CIO noted: "We are attacked almost every other day" (personal interview, 12 July 2016). Ironically, some CIOs noted that government personnel were using Gmail, which sits on the cloud as a backup to transmit messages, some of which were confidential (personal interviews, 23 June 2016).

Significant investment is required for government to build up its security capabilities to be on par with the high levels of security offered in a hyper scale environment by global cloud providers.

Lack of implementation of standards and interoperability

The lack of uniform standards in terms of procurement of government services has led to a fragmented approach to infrastructure management within the public sector, including cloud computing. As a result, many of the public sector IT systems are not interoperable.

One of the major concerns regarding the lack of uniform standards is the risk of vendor lock-in, due to the use of legacy systems. This creates challenges in terms of rationalisation of resources or consolidation under cloud computing and has therefore constrained widespread adoption of cloud services.

7.5.2. Managerial and organisational barriers

Lack of coherent approach to ICT infrastructure management

The management of ICT infrastructure is fragmented. Despite an undertaking by government to adopt open source, the actual implementation is yet to materialise and therefore results in "siloed" systems that make it difficult to interconnect related systems to provide seamless experiences for citizens (government official, personal interview, 17 August 2016). Furthermore, current IT systems and data are owned by different departments (e.g. national government, provincial government,

38 Paquette, S., Jaeger, P. T. and Wilson, S. C. (NBED). Identifying the security risks associated with governmental use of cloud computing. Available at: http://cloud.report/Resources/Whitepapers/8a35dc58-ebc9-4e62-bddf-4493debe0817_12.pdf.

municipal authorities) with varying access requirements and platforms. This makes it a challenge for government to undertake large scale migration to a uniform cloud solution.

Data residency and trust concerns

According to Nolan and Tobin (2011)[39] "concern over loss of control is arguably one of the biggest obstacles when moving to the cloud". Some of the government respondents stated that there were concerns over the management of private citizen data by third parties. Others stated that there is a preference to adopt a "hybrid model" in their cloud migration strategy, where some of the non-critical data is put on the cloud and private, highly sensitive data is kept on-premise.

There is a perception of loss of control if sensitive data is housed off-premise. Several officials stated that there were concerns about data being located outside South African borders, as most of the cloud computing providers are global players, with data centres located mainly in Europe and the United States.

There is generally mistrust of the security of data located in other locations, despite cloud service providers maintaining that data is highly secure in a hyper scale environment. The POPI ACT states that data can be located outside the borders of South Africa, as long as it stored in an environment where there is equivalency of data protection laws or greater. Therefore, the objection of data being stored outside South Africa's border is political in nature. There is general consensus among some respondents that the government prefers for data to be kept within the country or within the African continent (CIOs, personal interviews, 24 June 2016).

Cost of data as an input cost

Although the landing of undersea cables in the last few years has driven down data communication prices, national transmission costs in South Africa remain high. Bandwidth costs are a major input within the public sector and are viewed as being prohibitively high. Since cloud computing runs over the internet, the high cost of data is limiting the uptake of cloud computing services, despite the IT cost savings by adopting such services (senior government official, personal interviews, 19 July 2016).

7.5.3. Policy challenges

Inadequate policy, legal and regulatory frameworks to deal with emerging technological issues

There is no provision made for cloud computing services in the current public sector ICT policy frameworks in South Africa, which predate the era of cloud computing. Although many of the respondents acknowledged the perceived benefits of cloud computing, the most cited reason for its limited use in the public sector is the lack of a national policy and adequate guidelines.

The lack of policy direction with regards to the adoption of cloud computing, combined with the fear of job losses by CIOs across the spheres of government, should they decide to adopt cloud solutions in the absence of guidelines, has limited the uptake of cloud computing services within South African public sector.

"Without policy direction it becomes difficult for one to say let's go to the cloud. We do acknowledge the benefits that comes with cloud computing…."(CIO, personal interview, 12 July 2016).

---

39 Nolan, P. and Tobin, O. (2011). Cloud computing in the public sector: Risks and reward. Public Affairs, Ireland. Available at: https://www.pitb.gov.pk/sites/pitb.gov.pk/files/Government_Cloud_SaleemRafik_0.pdf

"What we first have to know [before using cloud] is what is allowed on the cloud and what is not allowed on the cloud and by when…"(CIO(b), personal interview, 23 June 2016).

"I see the benefits of the cloud but I am afraid I will lose my job. We are government employees and we work within frameworks…" (CIO, personal interview, 19 July 2016).

8. SA CLOUD READINESS

8.1. Vision, policy framework and institutional arrangements

The deployment of cloud services by enterprises, both private and public, is dependent on an enabling policy and regulatory environment. This includes not only ubiquitous high-speed infrastructure, available at cost-based prices but also a secure and trusted online environment. This requires legal frameworks that safeguard users' rights and data online through protecting users' privacy, allowing access to non-confidential or classified public information and national response systems to respond to cyber threats.

Several of the foundations for an enabling environment for cloud services are available. This includes a constitution that guarantees fundamental human rights, freedom of information and expression, requires administrative justice within the public service and regulatory bodies; legal frameworks that acknowledge the importance of communications systems to the modernisation of the economy and society through the establishment of dedicated Ministries and regulatory bodies to develop the ICT sector, and specific agencies and frameworks for the deployment of ICTs in the public sector.

While the foundational legal frameworks in South Africa are strong, the sector specific laws, institutional arrangements and capacity are weaker. South Africa has gone some way to meeting some of these conditions, but the progress to fulfilling several of these necessary conditions for cloud services has been uneven.

8.2. National Development Plan and Presidential Infrastructure Coordinating Council

The national broadband plan, SA Connect, identifies a central role for "a seamless information infrastructure by 2030 that will underpin a dynamic and connected vibrant information society and a knowledge economy that is more inclusive, equitable and prosperous". As envisaged in the National Development Plan (NDP), at the core of this will be: "a widespread communication system that will be universally accessible across the country at a cost and quality that meets the communication [needs] of citizens, business and the public sector, and provides access to the creation and consumption of a wide range of converged applications and services required for effective economic and social participation."[40]

"This ecosystem of digital networks, services, applications, content and devices, will be firmly integrated into the economic and social fabric of the country. Together, these broadband elements provide an enabling platform for economic enterprise, active citizenship and social engagement and innovation. It will connect public administration to the active citizen; promote economic growth; development and competitiveness; drive the creation of decent work; underpin nation-building and strengthen social cohesion; and support local, national and regional integration."[41]

---

40 National Development Plan (2012). National Planning Commission. Available at: https://nationalplanningcommission.files.wordpress.com/2015/02/ndp-2030-our-future-make-it-work_0.pdf.
41 National Development Plan 2012:170. National Planning Commission. Available at: https://nationalplanningcommission.files.wordpress.com/2015/02/ndp-2030-our-future-make-it-work_0.pdf.

Further, SA Connect operationalises the NDP and the New Growth Path, which both identify the knowledge economy as one of the drivers of job creation. In 2012, the Presidential Infrastructure Coordinating Commission (PICC) launched Strategic Integrated Project (SIP) 15: Expanding Access to Communication Technology. It aims "to ensure universal service and access to reliable, affordable and secure broadband services by all South Africans, prioritising rural and under-serviced areas and stimulating economic growth"[42].

Further, this broadband policy gives effect to the Constitution of South Africa by creating the conditions in a modern electronic world "to improve the quality of life of all citizens and free the potential of each person". In doing so, it enables equality in the rights, privileges and benefits of citizenship, including the guarantees of freedom of expression and association in the Bill of Rights. This aligns with the declaration by the Human Rights Council of the United Nations General Assembly that access to the internet is a basic human right which enables individuals to "exercise their right to freedom of opinion and expression".[43]

8.2.1. SA Connect implementation

Although, there are significant programmes underway under the National Development Plan's vision for 2030, key infrastructure projects are expected to be impacted by the current high fiscal deficits, especially with available resources needing to be directed to power shortages. In December 2013, the Cabinet approved an ambitious national broadband policy, strategy and plan referred to as "South Africa Connect" (SA Connect), which is an expression of the vision stipulated in the National Development Plan. The plan aims to position South Africa as a broadband leader and to ensure that all South Africans have basic broadband access by 2030 and that 50 percent have access to 100mbps broadband speeds by 2020.

In acknowledgement of extensive investments required to meet these targets and the limitations on state funding, SA Connect proposes the leveraging of the extensive public and private broadband networks already rolled out across the country to deploy broadband to under-served areas. It proposes as an immediately executable programme the pooling of public sector demand for broadband in order to facilitate the smart procurement of high-quality broadband connectivity and services to address public sector broadband needs. "This will simultaneously serve the communication needs in critical domains (such as education, health and safety and security) and enable network extension to areas that might not ordinarily be reached by operators by reducing the associated investment risk as well as by ensuring demand"[44] This will also reduce government's ongoing operational expenditure on communications through upfront capital expenditure. Ultimately, this aggregated public demand could serve as an anchor tenant to guarantee significant demand for investors and thereby enhancing the viability of networks in "uneconomic" areas.

As both supply- and demand-side measures to improve access to the internet and further stimulate demand for broadband connectivity, the connection of schools and clinics was to be prioritised, together with the deployment of free public Wi-Fi networks at these points of connection for citizens to access e-government and other services. Although it has taken nearly three years for this to happen, in July 2016 SITA put out a tender to connect 8 000 clinics as part of the National Health Services plan, which should get the implementation of SA Connect underway.

---

42 National Broadband Policy and Plan: SA Connect (2013:2). Government Gazette no 37119. Available at: www.gov.za>files>37119_gon953.

43 National Broadband Policy and Plan: SA Connect (2013:2). Government Gazette no 37119. Available at: www.gov.za>files>37119_gon953.

44 National Broadband Policy and Plan: SA Connect (2013:5). Government Gazette no 37119. Available at: www.gov.za>files>37119_gon953.

In the meantime, competing and complementary investments in both intercity transmission routes, backhaul and access networks have continued. The SA Connect plan has suffered from a lack of agreement over some issues, such as the lead agency in the project. In addition, government has insufficient funds to meet the ambitious rollout targets. The successful implementation of the SA Connect plan is key to the adoption of cloud computing services in South Africa.

8.2.2. ICT policy review

In 2012, an ICT policy review panel was appointed to start the ICT policy review process. In April 2014, the ICT Review Framing Paper was released to stimulate public discussions on the relevance of existing policy objectives and principles and to develop new policies for the sector. In 2014, a National Integrated ICT Green Paper for public discussion was published to discuss the status quo of the communications sector and what needs to be done to ensure its development. The Green Paper outlined different options in addressing the convergence of technologies and a policy and regulatory structure that will be used to extend services to all and provide for the opening of the sector to new innovative services. In 2016 formal policy position on key issues relating to ICT was set out in the National Integrated ICT Policy White Paper, which provides the framework for new ICT legislation.

The 2014 Green Paper considers e-government as a demand-stimulation service. For instance, the Green Paper recognises that e-government services enable an increase in ownership of devices for end-users and are key enablers for government modernisation.

Section 7.5 of the Green Paper discusses innovation and applications, including cloud computing. It acknowledges that "Cloud computing is expected to drive future growth in the IT sub-services market"[45]. The very short section on cloud computing offers nothing more than a definition, with no further discussion on how these services should be implemented. Nevertheless, the Green Paper has advanced and explicit references to innovation.

The discussion paper makes reference to cloud computing in Section 4.6. It acknowledges the potential cost savings, and the possibility that national government should act, through policy design and other measures, to promote the benefits and common cloud standards across the public services. It recognises that the potential of cloud computing is in the collaboration with neighbouring countries and the international community "to ensure that the benefits of this platform can be realised while protecting privacy, security and consumer rights. The impact of cloud services on taxation and cross-border controls will also have to be carefully considered".[46]

The Discussion Paper simply argues for further exploration of cloud computing for example in "education, health care and promotion of open government"*[44]*.. It cites the OECD study on cloud computing impacts and the role of government policy listing specific issues for clarification. These include:

- raising awareness of cloud computing;
- developing intra-government policies;
- research and development on cloud computing solutions and open standards;
- open and appropriate standards to limit vendor lock-in;

45 ICT Integrated Green Paper, (2014:54). Available at: http://www.gov.za/sites/www.gov.za/files/37261_gon44.pdf.
46 ICT Integrated Green Paper, (2014: 123). Available at: http://www.gov.za/sites/www.gov.za/files/37261_gon44.pdf.

- evaluation of cloud computing and analysing data on revenues, supply and demand, cross-border flows of data and the location of data;
- building cloud computing infrastructure in South Africa, and seeking SADC and BRICS partners;
- competition and trade issues;
- issues pertaining to taxation; and
- consumer protection, privacy and security[44].

While existing policy does not prohibit parts of government from adopting cloud computing, and while some parts of government may already use cloud computing (for example the e-toll panel in Gauteng placed selected documents on Dropbox and the Gauteng Education Department will use Moodle to host some of its educational materials), the discussion paper raises the point that more comprehensive policy and other guidance is required.

Some jurisdictions abroad have done extensive work to adapt legal frameworks or prepare the necessary legal frameworks, to address key issues in cloud computing with respect to electronic government and electronic transactions, such as laws dealing with confidentiality, security, risk, contracts, ownership of information, and regulation of personal data, international data transfers, and other important matters.

8.3. Applicable policy, regulation and legislation to regulate activities in the cloud in the South African government

Policy, regulation and legislation affecting the implementation of cloud computing services in government relate to e-government legislation, information protection regime, information storage and classification measures and privacy protection.

South African legislation on e-government is articulated in many acts, regulatory frameworks and initiatives that all together govern the implementation of these services in local and national governments. From an institutional arrangement perspective, the Department of Public Service and Administration (DPSA) is responsible for the development and coordination of government's overall e-government strategy. In addition, DPSA sets norms and standards for the public sector, which ensures that service-delivery mechanisms, integrated systems and access, human resources, institutional development, and governance initiatives are responsive to the needs of the citizens. At an implementation level, SITA and GITO are the bodies in charge of coordinating the deployment of e-government projects. While SITA is responsible for the acquisition, installation, implementation, and maintenance of IT in the public sector, the GITO Council, which consists of national and provincial IT officers, is responsible for consolidating and coordinating IT initiatives in government, including e-government, to facilitate service delivery.

The following acts and policies affect, to some degree, the implementation of IT services and e-government initiates in the public sector: The White Paper on Transforming Public Service Delivery, Promotion of Access to Information Act, Protection of Personal Information Act, Electronic Communication and Transaction Act, Electronic Government Policy Framework, Minimum Information Security Standards, Minimum Interoperability Standards and Policy on Free and Open Software. Collectively, this body of legislation aims to promote transparency accountability, good governance, information security, and openness in the acquisition and use of IT services. The legislation also affects cloud computing services, and creates a complex legal architecture dealing with data security, personal data protection, and electronic transactions.

8.3.1. State Information Technology Agency (SITA)

The implementing organ of IT systems in government is SITA. The SITA Act (1988) established an agency to provide centralised ICT services to government departments, particularly at the national level. The Agency is in charge of providing information technology, information systems and related services in a maintained information systems security environment according to approved policy and standards. SITA was initially located in the DPSA between 1999 and 2014, but is now located in the Department of Telecommunications and Posts (DTPS) following the restructuring of various communication portfolio organisations across different departments.

Despite the many criticisms of SITA concerning its suboptimal performance in relation to its mandate in servicing the public sector, it is the largest consumer and user of IT products and services in South Africa.

Although SITA was moved from the DPSA to DTPS, it still adheres to the government's "IT House of Values", aiming to achieve reduced costs, increased productivity and increased services to our citizens. SITA operates within Treasury procurement rules and meets public sector needs with Treasury budgets.

The South African Treasury is coordinating austerity measures to curb public sector expenditure, and to aggregate procurement and licenses to create efficiencies and benefits from economies of scale. This imperative is likely to affect SITA's procurement process and aligns closely with the inevitable shift from licensed products to cloud services in the industry.

8.3.2. Storage and management of records by South African governments

The National Archives of South Africa Act (No 43 of 1996) establishes national archives and governs the storage and management of the records held by government bodies. The Act gives significant importance to records management. It addresses issues related to the introduction of electronic records and it attempts to contribute to administrative efficiency and to accountable and transparent governance through meticulous management and care of the records of governmental bodies.

The Act established a National Archives Commission linked to the former Minister of Arts, Culture, Science and Technology, which was divided into two separate Departments in August 2002: The Department of Arts & Culture; and the Department of Science & Technology. The Commission promotes the coordination of archival policy formulation and planning at both national and provincial levels and therefore it acts as society's watchdog by ensuring that the National Archives carries out its statutory mandate.

The National Archives Act defines citizens' constitutional rights, such as the access to any information held by the state and, concomitant to that right, the right to privacy. The Act additionally ensures that no records that protect the rights of citizens are destroyed. Overall, no government records may be destroyed without the consent of the National Archivist, who is closely monitored by the National Archives Commission, which in turn has to act in accordance with the final authority vested in the formal Minister of Arts, Culture, Science and Technology.

The Act however, does not provide explicit guidelines or processes on managing data stored in the cloud.

8.4. Information Protection Regime

A body of national laws and regulations governs the disclosure of certain information retained by public administrations. Such laws include the Protection of Information Act 4 of 1982, as amended, the South African Police Services Act 68 of 1995, the Intelligence Services Act 65 of

2002, the Intelligence Services Oversight Act 40 of 1994, the Defence Act 42 of 2002 and the Public Service Regulations, 2001.

The current information protection regime consists of the Minimum Information Security Standards (MISS, 1996) which is an official national information security policy of government. MISS replaced the former 1988 Guidelines for the Protection of Classified Information and applies to all departments of state subject to the Public Service Act 103 of 1994.

MISS sets out security measures to protect classified information, including physical security, access control, computer security and communication security. The measures to protect classified information include the classification and reclassification of documents, handling of classified documents, access to classified information, storage of classified documents and removal of classified documents from premises.

Classified information is considered "sensitive information … which must … be exempted from disclosure and must enjoy protection against compromise".[47]here are four types of classified information, namely top secret, secret, confidential, and restricted. The relevant structures responsible for such data and its classification approve authorised disclosure.

Key concerns with respect to computer security include confidentiality of data, integrity of data and the availability of information systems[48]. Only classified data is considered as sensitive. The author of a document is responsible for classification and must guard against the under-classification, over-classification or unnecessary classification of documents. The head of an institution or his/her delegate must on a regular basis test classifications of documents generated in his/her institution against the criteria applicable to the relevant classification. The MISS policy requires the formulation of a department-specific information security policy, and the establishment of an information security function and staff. Although MISS is mainly concerned with the physical security of documents, it is envisaged that policy and standards for communications security and computer security will be updated separately to keep abreast of technology adoption, including cloud computing.

The current system on information protection is burdensome on government resources, resulting in overprotection of information that does not actually require protection. A lack of clarity and direction on what actuallyrequires protection has resulted in a state of affairs characterised by an unstable and inconsistent classification and declassification system, excessive costs and inadequate implementation.

8.4.1. The Electronic Communications and Transactions Act

The Electronic Communications and Transactions Act (ECTA) 25 of 2002 was established to define, regulate and govern e-commerce in South Africa. Its impact on electronic communications and transactions is substantial. The Act applies to any form of electronic communication, including e-mail, internet and SMS. The Act is very wide and deals with a broad spectrum of issues, including cyber inspectors, liability of service providers and domain names.

ECTA provides the legal interpretation of data messages, which it defines as data "generated, sent, received or stored by electronic means…" Several sections of ECTA may require interpretation from the perspective of data stored in a cloud environment, including what constitutes "information in its original form" (section 14) and information retention (section 16). In the section on e-government services, it states that:

---

47 Minimum Information Security Standards (1996). Definition 4. Available at: http://right2info.org/resources/publications/laws-1/SA_Minimum%20Information%20Security%20Standards.pdf.
48 Minimum Information Security Standards (1996). Definition 6. Available at: http://right2info.org/resources/publications/laws-1/SA_Minimum%20Information%20Security%20Standards.pdf

"Any public body that, pursuant to any law – (a) accepts the filing of documents, or requires that documents be created or retained; … may, notwithstanding anything to the contrary in such law – (i) accept the filing of such documents, or the creation or retention of such documents in the form of data messages…"[49]

Nothing in this section prevents the storage of data messages in the cloud. Section 28 of ECTA requires the relevant public body to publish in the Government Gazette, amongst other things, "the appropriate control processes and procedures to ensure adequate integrity, security and confidentiality of data messages…" [50]

It is not known to what extent the sections of the legislation referred to above have been interpreted as being applicable to the utilisation of cloud computing for e-government, whether in terms of government-to-government administration or in terms of government-to-citizen or government-to-business information sharing and transactions.

Chapter VIII of ECTA, sections 50 and 51 deal with protection of personal information obtained through electronic transactions. The important section here is section 51(6), which states, "a data controller may not disclose any of the personal information held by it to a third party, unless required or permitted by law or specifically authorised to do so in writing by the data subject". This section could be interpreted to apply directly to hosting personal information obtained by government in a cloud environment that is hosted outside government.

The section of the ECTA dealing with hosting (section 75) is not relevant to government utilisation of cloud computing. The remaining sections of the Act deal with, amongst other things, a limited set of matters pertaining to cybercrime, including unauthorised access to, interception of or interference with data, penalties and the jurisdiction of the courts.

In observing the transitioning to a cloud computing environment, whether for e-government or for e-commerce, the ECTA and the POPI Act should be assessed in terms of their applicability and relevance to cloud computing; as well as their alignment with international cloud computing law.

Cybercrime is a pertinent matter with respect to the provision and use of cloud services, due to the risks associated with data access in the cloud. South Africa is a signatory to the Council of Europe Convention on Cybercrime, 2001. While it had not yet ratified the Convention in 2013, ECTA provides a framework for addressing issues in cybercrime. As mentioned earlier, ECTA covers a range of issues that would be pertinent to cloud computing, including consumer protection, protection of personal information, protection of critical databases, appointment and powers of cyber inspectors, and provisions pertaining to cybercrime. However, many of these provisions do not specifically refer to the instance of cloud computing and may therefore have limited application in law, with respect to activities in the cloud environment. Most importantly, while the legislation required the presentation to Cabinet of a national e-strategy within three years of promulgation of the Act (RSA, 2002, sections 5(1)–5(11)), intended to encourage widespread supply of e-government services, no e-strategy emerged.

8.4.2. Electronic Communications Act 36 as amended by Act 1 2014

The provisions contained in ECA are open to wide interpretation and can be argued to include innovations, such as various forms of cloud computing. Cloud services could be interpreted to fall under the legal definition of "electronic communications service", namely "any service provided to the public, sections of the public, the state, or the subscribers to such service, which consists

---

49 The Electronic Communications and Transactions Act 25 of 2002, Section 27. Government Gazette 23708. Available at: http://www.gov.za/sites/www.gov.za/files/a25-02.pdf.

50 The Electronic Communications and Transactions Act 25 of 2002 Section 28(e). Government Gazette 23708. Available at: http://www.gov.za/sites/www.gov.za/files/a25-02.pdf.

wholly or mainly of the conveyance by any means of electronic communications over an electronic communications network, but excludes broadcasting services".

However, the ECA does not explicitly seek to regulate matters pertaining to cloud computing as an electronic communications service. Specifically, provisions for the required levels of connectivity for widespread and effective use of cloud service innovations were added in the 2014 amendment legislation, which includes a heightened level of attention to diffusion of broadband infrastructure and services across South Africa.

8.5. Protection of Personal Information Act 4

The Protection of Personal Information Act 4 (POPI) is one of the most important pieces of legislation with respect to cloud computing, due to its creating the framework for the protection of personal data. This legislation was signed into law on 27 November 2013 but only comes into force in mid-2017 at the earliest. Key issues applicable to cloud computing include regulation of personal data, anonymisation of personal data and fragmentation of personal data. The legislation seeks to promote the constitutional right to privacy contained in section 14 of the Constitution of the Republic of South Africa Act of 1996. In terms of the Constitution, "the right to privacy includes a right to protection against the unlawful collection, retention, dissemination and use of personal information".

The Act applies to the processing of personal information with respect to identifiable, living natural persons and identifiable, existing juristic persons, including processing by automated means. The definition of processing includes data storage. The provisions of the Act are extensive and studies need to be conducted to assess the level of readiness of cloud services for compliance with the POPI Act.

Potential users of cloud services in government will need to develop a readiness plan and profile, as a means to advancing the opportunities for innovative uses of internet and other electronic communications resources, where personal data is concerned.

A key section of the legislation pertains to transfer of personal information outside the Republic of South Africa, providing that (RSA, 2013, section 72): "A responsible party in the Republic may not transfer personal information about a data subject to a third party who is in a foreign country unless various legal provisions are met". Specifically, the third party recipient in a foreign country needs to be subject to a law, binding corporate rules or binding agreement that provides an adequate level of protection that is substantially similar to that provided for in South Africa's POPI Act. This and other provisions of section 72 would limit the utilisation of cloud-based services, where this would require the hosting of personal information in a foreign country that does not comply with this threshold requirement.

Regarding future government utilisation of hosted resources and services for government-held data that is effectively personal data of either natural or juristic persons, while not prohibited, Section 72 of the POPI Act requires that government departments using public cloud services would need to know where their off-shore data is being hosted.

9. CLOUD FIRST POLICY FOR SOUTH AFRICAN PUBLIC SECTOR

Cloud policy needs to be business and not technology driven, and as such the problems and requirement of the public sector have been articulated in several policies and frameworks over the years. Although many of the fundamental challenges remain, their nature may have shifted.

Good policies have not been operationalised with clear strategies, budgets and timelines. Standards, norms and frameworks have not been updated in years. This section seeks to identify existing frameworks, gaps within them, or need for updating.[51]

9.1. Open data policy

As indicated above, cloud policy for the public sector needs to be understood as part of a wider information and data policy, which, to be optimal, should be open. Data capability is underpinned by the ability of the public and private sector to access and share data appropriately.

This open data revolution will change the way in which the public and private sector engage with citizens, develop policy, deliver services, and the way they are held accountable. "Open data is data that can be freely used, shared and built on by anyone, anywhere, for any purpose"[52].

Although no formal open data policy has been adopted at national government level, there are such initiatives within other levels of government. Here again local government has led the way with the City of Cape Town having adopted an open data policy in September 2014 for the online portal it uses for citizen engagement. The policy states: "The open data portal will assist citizen engagement with the City by making it easier for members of the public to access data. Enhancing transparency will empower citizens to hold the City to account"[53].

The policy further states that the data available on the portal will exclude the following:

a) Third party data that is copyrighted or where the third-party owner has prohibited the City from publishing the data;

b) Information that discloses private information or in any way infringes on the privacy of the individual citizens;

c) Information that exposes the City to unacceptable risk;

d) Information that the City is not legally permitted to disclose;

e) Confidential information; and

f) Any other content deemed to be inappropriate by the Open Data Steering Committee.

Again, although it is not formal policy, in the last year, SITA has espoused an open data approach on several public platforms. It has pointed out that South Africa, like any other developing country is embarking on the concept of doing more with less. The challenge is to improve the quality of service using ICT while at the same time reducing the cost.

---

[51] Despite public references and frameworks to open data that Acting-DG Joe Mjwara of the Department of Telecommunications and Post, the department under which SITA now falls, and which are found in presentations made in conferences, SITA remains as opaque as ever. Despite having the statutorily required notices on the Access to Information Act on its website even getting copies of public presentations for research purposes (even with the endorsement of the research for public policy purposes by the Acting -DG) was impossible.

52 SITA (2016). "Open data and open partnerships to facilitate open government", World IP Day, April 2016. Available at: http://www.cipc.co.za/files/8614/6435/1332/SITA_Open_Government_Presentation_2016_04.pdf.

53 City of Cape Town (2014). "Open Data Policy". Available at: http//web1,capetown.gov.za/ web1/OpenDataPortal/.

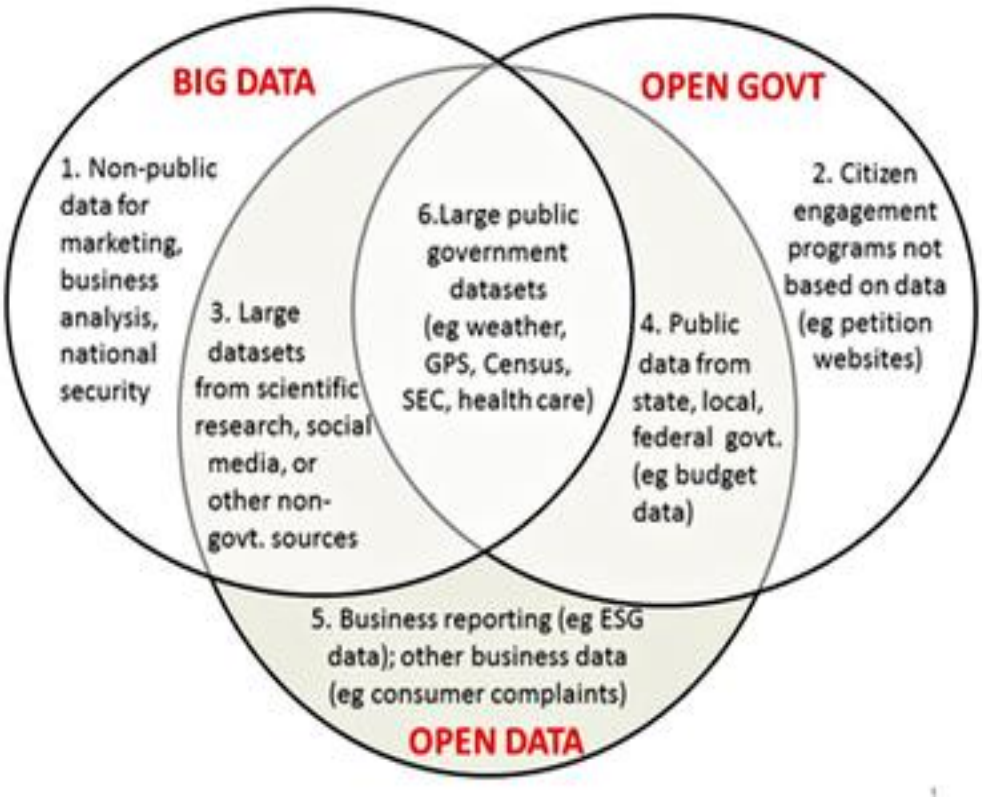
Data and Information Management practices are often the best "unrealised" or "untapped" opportunities to directly address these high level challenges, especially when it comes to common and shared services. One of the greatest opportunities and challenges facing policymakers today is the ever-increasing significance of data. Data underpins businesses and the economy, providing new insights into citizen needs and enabling new products and services to be developed.

According to SITA: "Government is committed to develop an open data community involving the public and private sector, communities, academia, and the citizen. The establishment of the Open Data ecosystem will benefit citizens by providing access to cradle to grave information irrespective of data ownership or origin"[54].

The success of open data hinges on the insight of government and the private sector to make information transparent and available to citizens.

"There must be a drive for public-private partnership towards reuse of data and information. In light of the lack of a current open data policy for government, and to unleash the potential of open data, one of our next steps could be to come up with an open data policy that sticks within South Africa much deeper and makes this fundamental change permanent… we can demonstrate the value of open governance to economic growth, inclusive development and improved citizen engagement and empowerment"[55].

FIGURE 2: SITA PROPOSED OPEN DATA MODEL



Source: SITA, presentation World IP Day, 2016

[54] 54 National Development Plan (2012). National Planning Commission. Available at: https://nationalplanningcommission.files.wordpress.com/2015/02/ndp-2030-our-future-make-it-work_0.pdf.
[55] Ibid.

An open data policy provides an excellent framework for the development and management of public data, not only public sector data. It creates an information policy environment that needs to be integrated with the national statistical framework, which ensures data remains a public good, in the national statistical sense.

As the enabler of ICT for government, SITA needs to lead the implementation of the open data policy to foster greater openness and accountability in government.

SITA has identified a number of principles to underpin an open data policy:

- establish a strong commitment to opening data;
- Ensure commitment to open partnerships and open data;
- Develop a government-wide framework on open data, through an inclusive process – open information, open data and open dialogue;
- Review and evolve enabling legislations and practices with regards to open data;
- Identify and publish some information sets as open data, in line with current government and private sector legislative frameworks and guiding principles;
- Manage the availability of the data sets through data governance structures; and
- Actively promote the use of open data inside government, so that government becomes both a primary provider and a primary user of open data[40].

This is fundamental to making sure government is truly committed and also impacts the point made earlier about internal skills. As government uses its own open data (inside and across agencies) as well as open data published by a private company, openness becomes business as usual instead of being seen as a parallel, independent initiative. In order to stick, open data must go to the core of how government operates.

10. E-GOV, INTEROPERABILITY AND STANDARDS

In 1994, the new government was facing a few challenges, among which were lack of coordination between departments, incompatibility of systems and architecture, waste of resources, and IT not driven by business processes.

Although there has been progress, which would facilitate cloud computing implementation, such as the e-government strategy that produced the Minimum Interoperability Standards (MIOS), several initiatives addressing these challenges have stalled or not been updated, and there is a sense in which many of these challenges face the government again 15 years on. Government has become even more complex and interlinked in a fast-changing world, with even greater local demands on it, yet technologies and standards have not been deployed to make government more efficient and connected.

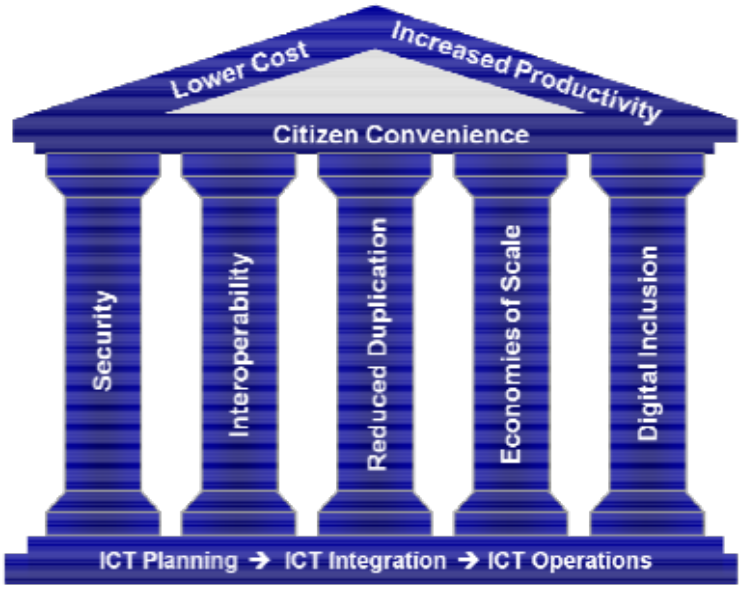
The main challenges identified by GITOC are:

- Diverse and fragmented ICT planning methods (frameworks and processes)
- Inconsistent Enterprise Architecture (EA) plans and reporting;

- Incomplete ICT system inventories in government;
- Departmental EA capability maturity;
- Unclear ICT governance (responsibilities and guidance);
- Moving from "techno-centric" to "information centric" to "business centric" (exchanging data efficiently and integrating service delivery);
- Collaboration and cooperation – national priorities are poorly coordinated and contracted;
- The priority of performance over conformance result in low levels of interoperability; and
- Regulation and security complexities often default to isolation of systems.

10.1. Minimum Interoperability Standards for government information systems

FIGURE 3: GOVERNMENT ICT HOUSE OF VALUE



Source: SITA (2015)[56]

To operationalise the values and the commitment of the South African government to the continuous improvement of public service, as represented by its national, provincial and local departments and associated agencies, the government embarked on an e-government programme in 2001.

SITA's Standards and Certification Unit, in consultation with GITOC: Standing Committee on Architecture developed the Minimum Interoperability Standards (MIOS) for Government Information Systems. It provides "a framework for effective, efficient and economic management and utilisation of Information and ICT Resources in government" as illustrated in Figure 3 above.

56 SITA presentation to Government CIO Summit, March 2015, Magaliesburg, available at http://govciosummit.co.za/documents/2015-03.../GCIO%20Summit%20ICT_Strategy.pptx

While the values of delivery espoused then still pertain, the MIOS is desperately in need of updating. The expressed value (pillars) include:

(i) security;

(ii) interoperability;

(iii) reduced duplication;

(iv) economies of scale; and

(v) digital inclusion.

10.1.1 Capacity

The House of Values importantly acknowledges the need for strong foundations: the capabilities required to ensure the realisation of the expressed values in the outcomes. These include:

- ICT planning, which requires the capabilities that set the direction and standard for ICT, enterprise architecture and to validate/certify compliance and performance.

- ICT integration, which requires the capabilities that develop ICT system and technology infrastructure into integrated ICT solutions.

- ICT operations, which require the capabilities to ensure that ICT systems and technology infrastructure are maintained in a reliable, available and secure environment[57].

10.1.2 Aims

The aims of the e-government programme are to:

- Lower the costs of government service delivery operations, by reducing time, complexity, repetition and duplication of tasks;

- Increase productivity of government operations, by improving the quality and quantity of public sector outputs or introducing new processes to produce outputs and render services that were previously not possible; and

- Enhance citizen convenience when interacting with government by offering equal access to government information systems and services, providing better information, improving information service quality and privacy, providing remedies and offering best value for money.

10.1.3 Interoperability

MIOS document highlights: “The advancement of interoperability in government is an ongoing process and should be managed as a long-term programme. It is, therefore incumbent upon the members of the Government Information Technology Officers Council to promote the objectives of interoperability and to observe the principles and comply with the standards as set out in MIOS during the life-cycle management of IS/ICT in government. It is also essential that MIOS remains updated and that it aligns to stakeholder requirements, changes in legislative environment, so that

57 Minimum Interoperability Standards v5.0 (2011). Available at: gissa.org.za/special-interest-groups/open-source/foss-documents/.

government can embrace the potential of technological advancement in the market and address the archival issues inherent to the digital age"[58]

Several CIOs spoke about their inability to implement cloud services as inhibiting their ability to fulfil their mandates. They contended that MIOS needs to encourage cloud services, which, they believe, are essential to the modernisation of the public service (Personal interviews, 23 June 2016).

11. FINDINGS/CONCLUSIONS

Cloud services are indisputably best able to address many of the business challenges in the public sector, primarily the modernisation of the public sector through enabling greater efficiencies, integration and coordination, cost savings and, more particularly, payment to scale for only what is used. Cloud computing has the potential to enable government to meet its objectives set out in the National Development Plan and SA Connect of achieving a connected government and achieving internal efficiencies by enabling better coordination between public sector departments. Secondly, cloud computing is expected to enable better interaction between government and citizens and enable the provision of e-government services (including e-health and e-education) for enhanced service delivery.

11.1. Institutional arrangements and leadership

Institutional arrangements and leadership play a role in driving adoption of cloud-based services, in countries where this has been successful. It is recognised that the state, as being one of the largest consumers of ICT has a key role to play in creating awareness and building trust (in cloud computing) by serving as a role model and leader in cloud-based services. Further, internal adoption of novel ICT services and new technologies that drive efficiencies and information flows has been most successful when there is a champion, or champions, formally or informally, within the organisation. SITA, which is responsible for identifying technologies that will improve government efficiency, has an important role to play in championing the benefits of cloud computing, and DTPS is responsible for developing policy that will guide the adoption of these services within the public sector.

11.2. Fragmentation of mandate in government

The failed institutional arrangements that pertained until the last democratic administration, which saw SITA as an implementation agency with the DPSA, were a well-documented failure and resulted in the relocation of SITA under the DTPS. However, the challenges faced by the DTPS as it attempts to recover from the results of its disruptive split from the Department of Communications, means that it has not been in a position to prioritise policies required to provide direction to SITA for implementation. Further the legacy policy department DPSA still appears to be responsible for setting norms and standards essential to procurement and operationalising the public sector. The dysfunctionality in the institutional arrangements may not lie in the location of SITA in a particular department but in the nature of the procurement agency, its intention to be a revenue centre, not simply a cost centre, its lack of autonomy, on the one hand, to respond to changing business needs, new technologies and skills requirements, and on the other, the concentration of power in it, the potential conflict of interests and the lack of accountability and responsiveness to its "clients". This could be enabled by allowing departments and agency to

58 Minimum Interoperability Standards v5.0 (2011: 7). Available at: gissa.org.za/special-interest-groups/open-source/foss-documents/.

procure products and services in compliance with specified norms and standards, if they can secure them at a better price or quality level. SITA would still have the advantages of economies of scale and scope, but it would need to ensure efficiencies in its own sourcing of products and services.

11.3. Lack of a coherent public policy

ICT policy in South Africa is still treated as a narrow sector policy that fails to reflect the cross cutting nature of ICTs in a modern economy and state. ICT is not only a growing services sector with the potential to add greater value to the economy but cuts across the entire public sector and indeed the private sector. Policy can no longer focus on telecommunications, broadcasting, IT or the internet, but needs to be seen as an integrated national policy, Digital SA, that is not only focused on infrastructures and services but on national human resource deficits in a knowledge economy, input costs of communications that may inhibit private and public sector enterprise, and citizen services across government. It requires certainty of vision and objectives and agreed strategies and targets, yet flexibility to respond to the dynamic global environment in which national development take place. It requires anticipation of national needs on the basis of global trends and national agencies that can fast-track policy and implement swiftly to create an enabling environment of economic growth development, innovation and social coherence. Under such conditions market barriers, costs and cost of delays – such as unified rights of way regimes, high-demand spectrum, and cloud policies – would be reduced.

12. RECOMMENDATIONS

12.1. Position cloud as a solution to skills shortages

Government needs to address the issue regarding ICT skills shortages at two levels. The first is in the terrain of national education policy, the mainstreaming of ICT into the education curricula, in specialist training, education and research at a tertiary level. The second is within the public sector itself: on-the-job training is required to enable public servants to effectively utilise new technologies and services, as well as the commitment of significant budgets to further training and professional development in those areas. In the short-to-medium term, cloud services have the potential to bridge some of the skills shortages by providing user-friendly, cost–effective solutions to the current skills deficit.

12.2. Improve availability and quality of broadband infrastructure

Ubiquitous broadband infrastructure is key to the success of the adoption of cloud computing within the public sector. The government has a role to play in fast tracking the rollout of broadband infrastructure to under-served areas through public-private partnerships (PPP's). In addition, government needs to finalise the allocation of spectrum from the digital dividend (800MHz and 2.6GHz) in order to facilitate the expansion of advanced Long Term Evolution (LTE) mobile broadband services.

12.3. Develop a cloud computing policy framework

Cloud computing is not covered in the current public sector ICT framework in South Africa. Although several regulations and policies, such as the White Paper on Transforming Public Service Delivery, Promotion of Access to Information Act, Protection of Personal Information Act, Electronic Communication and Transaction Act and Minimum Information Security Standards Act affect cloud computing services, there is a need for a dedicated cloud policy.

This cloud policy must take into account issues, such as public information classification for cloud, security standards for provisioning of cloud computing, vendor compliance requirements, prioritising cloud in the national ICT agenda (e.g. NDP, SIP 15, National Integrated ICT Framework, etc.) and recognising cloud as a preferred hosting platform for the public sector. Furthermore, the policy must include demand side stimulation strategies, as seen in the South Korean cloud strategy for public sector.

The South African government will be required to develop, embrace and implement a technically advanced cloud policy: one that would challenge its capabilities and skills, and a solid implementation plan based on global based practice.

12.4. Establish a designated champion for cloud computing services

Global best practice shows a designated entity that spearheads all cloud related policy developments, so that implementation of cloud and integration of cloud agenda should be in place. This can be a special entity like G-Cloud in the UK or a collaborative effort between relevant entities, which in the case of South Africa can include DTPS, DPSA, state security and SITA.

It is, however, important to recognise and clearly define the mandate of this entity.

12.5. Implement and enforce open and interoperable standards to public sector procurement

In order to achieve the interoperability guidelines of MIOS, South Africa's government can establish a centralised cloud computing marketplace, as seen in the case of UK G-Cloud initiative's CloudStore. This marketplace would ensure that cloud vendors adhere to uniform and/or interoperable standards for cloud provisioning and configuration.

Furthermore, the centralised system for procurement by government agencies could address the current status quo of fragmented, poorly administered and bureaucratic IT procurement processes.

Centralised procurement can provide economies of scale and, in this case, it can be a viable tool to achieve Treasury's efforts to rationalise ICT spend in the public sector.

The open and interoperable standards through the marketplace can potentially avoid vendor lock-in and non-interoperable solutions.

12.6. Adopt best practices to develop security framework for cloud services

The MISS policy, which covers security of physical government documents and information will need to be updated separately to keep abreast of technology adoption, including cloud computing.

Furthermore, the following best practices in the approach to developing a security framework for cloud can be considered:

- Government develops a central security framework that is applied across all departments to ensure consistency of approach to cloud and avoid fragmentation caused by custom requirements and implementation.

- Government establishes and communicates a robust classification of data handled by and under the care of government. This classification should reflect the different levels of sensitive information and provide guidelines to handle each level accordingly.
- This data classification should be transferred effectively to cloud computing.
- The data security requirements should be mapped to the published data classification for cloud to ensure adequate protective measures are in for each category of data in the cloud[59].

12.7. Expand data classification guidelines to include cloud computing

Although guidelines exist for the classification of data under the Archiving Act on how to manage, protect and store confidential data, government needs to customise this legislation to also address the context of using cloud computing.

The UK G-Cloud's Short Guide to Business Impact Levels CESG's IS1/IS2 Technical Risk Assessment Method [60]provides a reliable way of establishing a given impact and the risk to information assets. The most important thing to remember is that impact levels are assessed against three different criteria:

- Confidentiality – the risk of an information asset getting into the hands of someone it should not.
- Integrity – the risk of somebody having the ability to modify an information asset that they should not.
- Availability – the risk of someone, or something, preventing access to an information asset by legitimate users.

12.8. Provide guidance for cloud vendor certification and compliance

Government should develop uniform and transparent guidelines for vendor certification and compliance for the provision of cloud computing services in the public sector. It proposes a "de-centralised" approach whereby government develops compliance guidelines, cloud vendors self-certify and a designated standards board verifies that vendors are compliant.

59 Kemp, R. Seeding the global public cloud: Part II – The UK's approach as pathfinder for other countries. Kemp IT Law, London. Available at: http://www.kempitlaw.com/wp-content/uploads/2015/10/Part-I-Seeding-the-Global-Public-Sector-Cloud.pdf.

60 http://www.channelpro.co.uk/advice/8256/g-cloud-a-quick-guide-2

13. SUMMARY TABLE OF RECOMMENDATIONS/ACTIONS

Table 3 below is a summary of the recommendations and action points to be pursued by government in establishing a cloud computing policy:

TABLE 3: RECOMMENDATIONS AND ACTION POINTS

Recommended focus areas	***Government/Public sector action***
Broadband policy	Finalise the implementation of the SA Connect Policy in order to drive the successful adoption within the public sector. This will entail: ▪ Rationalising state resources to avoid duplication; ▪ Clarifying issues around the lead telecommunications agency and funding in order to meet the ambitious targets; and ▪ Cooperating with the private sector and leveraging existing infrastructure to expand broadband access.
National integrated ICT policy framework	▪ Finalise the ICT policy framework and provide future roadmap. ▪ Invest in ICT development to establish a vehicle to promote economic growth. ▪ Fast track the rollout of broadband infrastructure to under-served areas, through PPPs. ▪ Finalise the allocation of spectrum from the digital dividend (800MHz and 2.6GHz). ▪ Adapt ICT framework to include disruptive technologies like cloud computing (including developing a dedicated cloud computing policy).
Cloud computing policy framework	▪ Develop a technically advanced cloud computing policy framework, which is currently not existent.
Data classification, management and storage	▪ Revise the classification of systems and processes and expand current classification framework (e.g. Archiving Act) to include cloud computing.
Data protection and security	▪ Implement and adapt POPI legislation to cover cloud computing services. ▪ The cloud computing framework needs to make provision for data security and protection in line with international standards. ▪ Update MISS framework to cover cloud computing services. ▪ Develop a central security framework that is applied across all departments to ensure consistency of approach to cloud and avoid fragmentation. ▪ Establish and communicate a robust classification of data handled by and under the care of government and transfer the data classification effectively to cloud computing.

Interoperability	▪ Expand MIOS interoperability framework to cover cloud computing. ▪ Implement and enforce interoperability among government departments. ▪ Centralise the definition of interoperability standards. ▪ Propagate open standards for procurement and data.
Cloud computing compliance	▪ Consider centralising cloud procurement. ▪ Define compliance parameters and procedures. ▪ Appoint dedicated compliance overseer for cloud computing.
Skills	▪ Position cloud as a solution to skills shortages. ▪ Policy to include demand side stimulation for private sector as a means to develop skills. ▪ Partnerships with private sector to grow specialist skills.
Prioritisation of cloud computing	▪ Identify and appoint a champion for cloud computing. ▪ Incorporate cloud computing into existing policy and legislation. ▪ Adopt and communicate an official position of cloud in the public sector. ▪ Government acts as an “anchor tenant” of cloud computing services.

- *Source: Prepared by Authors, 2016*

14. LIST OF INTERVIEWEES

Andrew Aitken, CEO Cloud Services, Internet Solutions

Constance Gadzikwa, Education Department SETA

Joe Mjwara, Director General, Department of Posts and Telecommunications

Kiruben Pillay, Ekurhuleni Municipality

Lungi Ngaingwana, Department of Social Development

Mmamathe Makhekhe-Mokhuane, Chairperson, GITO Council, Department of Water and Sanitation

Moritz Botha, Pumezo Gulwa and Tumelo Ntlaba, Procurement Department, National Treasury

Patrick Mokwena, Northern Cape Department of Education

Schalk Human, Chief Director, SCM ICT, National Treasury

Tumelo Kganane, CIO, City of Johannesburg

SITA CEO and CTO were not available to be interviewed over the six-month period research period, which compelled the authors to rely heavily on the website and literature, and on the input from the departments they service.