PROVINCE OF KWAZULU-NATAL

FOURTH INDUSTRIAL REVOLUTION

CLOUD FIRST POLICY

premier

Office Of The Premier
PROVINCE OF KWAZULU-NATAL

premier

Office Of The Premier
PROVINCE OF KWAZULU-NATAL

KZN CLOUD FIRST POLICY

Version 1.00

Date: 28 February 2020

Accreditation

This document is platformed, with credit, on the DPSA Cloud first policy that is awaiting ratification. It contains the basis of the required information from the policy with upliftment to address pertinent financial decision making pertinent to cloud within the province of Kwazulu Natal.

Document Version Control

Date	Author	Version
02 February 2020	KZN OTP ICT DEPT	Version 0.0.1
28 February 2020	KZN OTP ICT DEPT	Version 1.0.0

Approvals

The Cloud First Business Case Template is approved by the Director General of the Province.

Name	Signature	Date

Review Period

This template will be reviewed annually or subsequent to any significant issue arising that has not been considered

Name	Signature	Date

Contact Information

For more information on this policy or to inquire about a variation that is not covered, pls contact the KZN Office of The Premier ICT Governance Department.

TABLE OF CONTENTS

Definitions/Glossary

DPSA	Department of Public Service and Administration
GCIO	Government Chief Information Office
GITOC	Government Information Technology Officer Council
SITA	State Information Technology Agency
PSA	Public Service Act
ICT	Information and Communications Technology
SSA	State Security Agency
ISO	International Standards Organisation
ISACA	Information Systems Audit and Control Association
NIST	The National Institute of Standards and Technology
CSP	Cloud Service Provider
HIPAA	Health Insurance Portability and Accountability Act (USA)
GDPR	General Data Protection Regulation (European Union)
IaaS	Infrastructure as a Service
PaaS	Platform as a Service
SaaS	Software as a Service
ISO/IEC27001/ ISO17799	Information security management Standard

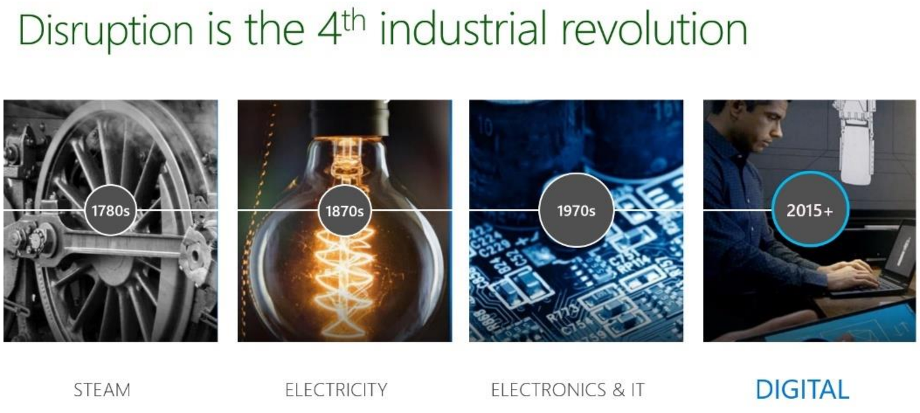
Legislative

Public Service Act 30 of 2007
Public Service Regulations of 2001 as amended 16 July 2004
Public Administration Management Act of 2014
Promotion of Access to Information Act, No 2 of 2000
State Information Technology Agency Act no 88 of 1998
Intelligence Services Act 65 of 2002 - SSA
National Archives of South Africa Act 43 of 1996
The Protection of Personal Information Act no 4 of 2013(POPI)

Foreword

The primary aim of the KwaZulu-Natal Cloud First Policy being signed into provincial policy is to help propagate the the momentum of the fourth industrial revolution (4IR) or digital transformation.

Digital transformation, also called digital disruption or digital business, is the integration of digital technology into all areas of execution - fundamentally changing how entities operate, engage their employees, citizens, stakeholders and how it delivers disruptive value to its customers.



The digital embrace is changing the capability of departments, and this change is growing faster than the pace of transformation in organizations.

Digital transformation is not a new concept, but the conversation has shifted to how rather than why.

DIGITAL SOCIETY SOUTH AFRICA:

South Africa's National e-Strategy

towards a thriving and inclusive digital future

The 2030 National e-Strategy states its problem statement on Digital Transformation as "

"The Digital Industrial Revolution will have an impact on three segments of society, namely business, government and individuals. The African Continent has an opportunity to make a significant contribution to the success of the revolution, as it is likely that some of its biggest challenges can become unique opportunities."

Digital business reached a tipping point since 2018 as organizations embrace and scale their digital capabilities. Enterprises around the world are making significant investments in the technologies and services that enable the digital transformation of their service delivery models, products, and services.

Strategic digital transformation started becoming more pervasive in 2019. Budgets are soaring in technology whilst over-all cost savings debunk the business case to invest in technology.

The list of disruptive technologies on the radar of stakeholders is expanding.

Ownership is now moving to the senior leadership and managed by cross-functional, collaborative groups.

Ramaphosa's remarkably tech-focused Sona: what he said about ICT

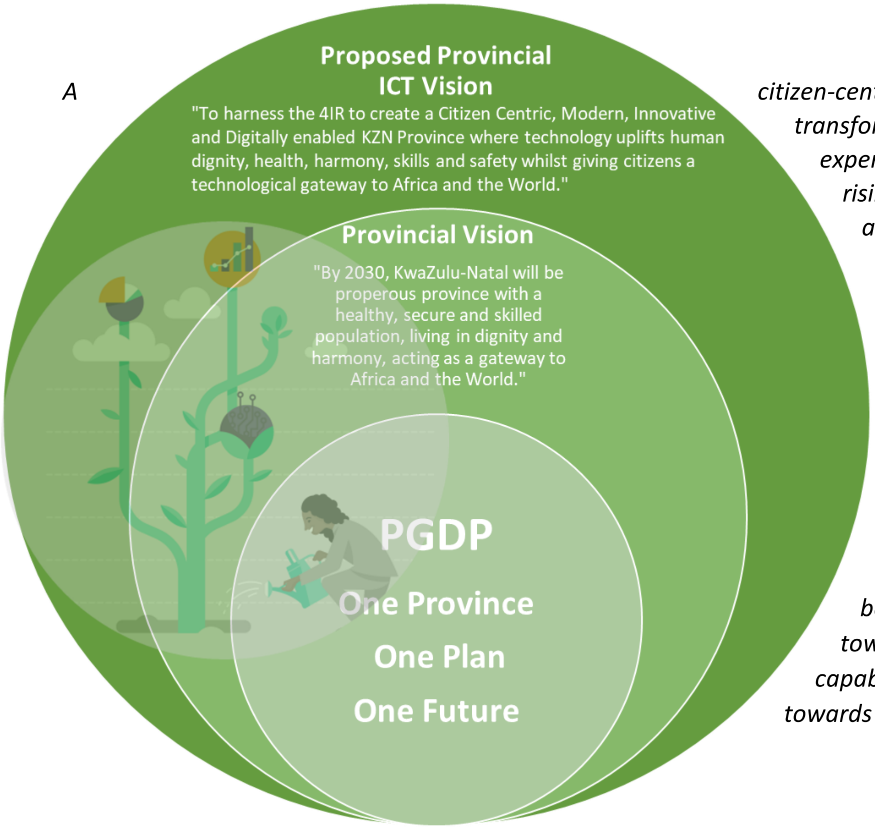
By DUNCAN MCLEOD — 7 February 2019 1 Comment

Cyril Ramaphosa (photo: GCIS)

Technohubs launch 2016

The 2020 State of the Nation Address by President Ramaphosa, made a plea to embrace digital transformation to expedite citizen delivery and grow the economy.

The Province of KwaZulu Natal, led by The Premier, is embarking on a number of technology investments that will contribute towards unlocking the province's potential via 4IR.



Proposed Provincial ICT Vision

"To harness the 4IR to create a Citizen Centric, Modern, Innovative and Digitally enabled KZN Province where technology uplifts human dignity, health, harmony, skills and safety whilst giving citizens a technological gateway to Africa and the World."

Provincial Vision

"By 2030, KwaZulu-Natal will be properous province with a healthy, secure and skilled population, living in dignity and harmony, acting as a gateway to Africa and the World."

PGDP

One Province

One Plan

One Future

A citizen-centric experience continues to lead digital transformation investment priorities, but employee experience and organizational culture are also rising in importance to empower and accelerate change, growth, and innovation.

Ethics in 4IR is a growing focus area as more conscience-driven decisions are made on how far technology pervasiveness is allowed into human daily existence.

Hence, A unified province acting strategically in the choice of 4IR impact will expedite the radical provincial transformation being anticipated. This strategy is aimed towards guiding, creating a 4IR delivery capability and further focusing the 4IR potential towards the anticipated 2030 results for this province.

1 INTRODUCTION

1.1 The Kwazulu Natal Province seeks to minimise its ownership of technical infrastructure and move towards a consumption-based model. Central to this new direction is the adoption of cloud services that enable Government to be more flexible, scalable and deliver better services to more people. Cloud computing is the building block in the digital transformation of the public services.

1.2 At the core of the cloud first policy (policy) is that provincial departments may adopt cloud-computing services as the first option when making investment decisions on obtaining new Information and Communication Technology (ICT) services or replacing existing services.

1.3 The benefits realised by governments that adopt a cloud environment are numerous, including but not limited to:

a) **Improved business engagement** across the organization by aligning Information Technology (IT) to programmes and business objectives;

b) **Support sustainability measures** by more efficiently aligning resource capacity with actual demand and consumption, minimising government waste by reducing excess computing capacity and power consumption;

c) **Enhanced end-to-end service delivery** by making information more easily accessible, allowing for nimbler response times to citizens, businesses and stakeholders;

d) **Realized cost savings** by paying for only what is consumed (purchased "as-a-service"), thereby ensuring taxpayers' Rands are well spent;

e) **Fuel an entrepreneurial culture** both inside and outside government, stimulating the economy and innovation ecosystem;

f) **Enhanced reputation** by promoting open government and fostering public engagement;

g) **Efficiency improvements** by using the cloud computing model for IT services, the government will be able to reduce data centre infrastructure expenditure;

h) **Better utilisation of ICT Assets** with cloud computing, IT infrastructure resources are pooled and shared across large numbers of applications and organisations. Cloud computing can complement data centre consolidation efforts by shifting workloads and applications to infrastructures owned and operated by third parties;

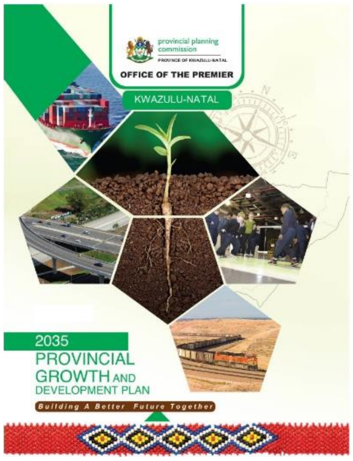
i) **Reduce duplication c**loud computing will help departments to mitigate the fragmented data, application, and infrastructure silo issues and funding models by focusing on IT services as a utility; and

j) **Data centre consolidation c**loud computing can accelerate data centre consolidation efforts by reducing the number of applications hosted within government-owned data centres. For those that continue to be owned and operated directly by departments (e.g., by implementing private IaaS clouds), environments will be more interoperable and portable, which will decrease data centre consolidation and integration costs because it reduces unnecessary heterogeneity and complexity in the IT environment.

1.4 The Province is putting into place policy and guidelines necessary to accelerate the adoption to cloud and to become less technology-centric and more outcome focused.

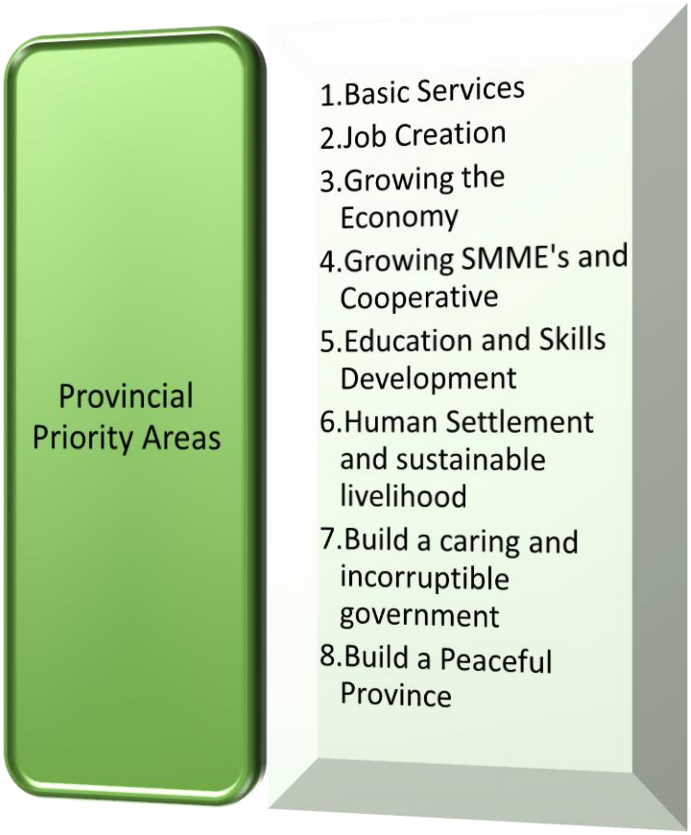
1.5 All Cloud based investments must be mobilised towards the provincial PGDP goals, strategic objectives and highest priority items.

PGDP and APP plan alignment


provincial planning commission
PROVINCE OF KWAZULU-NATAL
OFFICE OF THE PREMIER
KWAZULU-NATAL
2035
PROVINCIAL
GROWTH AND
DEVELOPMENT PLAN
Building A Better Future Together

Select which of the PGDP 2035 Goals are being targeted by this intervention. (Delete the tick not applicable)

1	**Inclusive Economic Growth**	✓
2	**Human Resource Development**	✓
3	**Human and Community Development**	✓
4	**Strategic Infrastructure**	✓
5	**Environmental Sustainability**	✓
6	**Governance and Policy**	✓
7	**Spatial Equity**	✓



Provincial Priority Areas

1.Basic Services
2.Job Creation
3.Growing the Economy
4.Growing SMME's and Cooperative
5.Education and Skills Development
6.Human Settlement and sustainable livelihood
7.Build a caring and incorruptible government
8.Build a Peaceful Province

These 7 PGDP 2035 goals are under-pinned by 31 strategic objectives and further driven by the province's highest priority areas.

This policy aims focus the 4IR effect towards the provincial plans and seek the highest impact on the province's plans.

2 PURPOSE

2.1 To give direction to Provincial departments on considerations before procuring cloud services. Departments can also use the considerations outlined in this policy as guidance in reviewing existing cloud solutions.

3 SCOPE AND OBJECTIVE

3.1 The Policy applies to all KwaZulu Natal provincial departments as per Public Service Act,1994.

3.2 This policy applies to the cloud-based variants of :

- Infrastructure as a Service (IaaS),
- Platform as a Service (PaaS), and
- Software as a Service (SaaS).

It applies to public cloud, private cloud, and community cloud implementations as well as any hybrid of cloud solutions or cloud and non-cloud hybrid solutions.

3.3 The objective of the policy is to promote the use of cloud computing in government and foster a structural approach to cloud adoption.

4 AUTHORITY AND RESPONSIBILITY

4.1 Section (3) (1) of the Public Service Amendment Act of 2007 (PSA) mandates the Minister to establish norms and standards for an effective administration of the public service and improve service delivery.

The National Cloud First Policy is intended to enhance information management in the public service as per PSA S (3) (1) (f).

Whilst this motion is in progress, this provincial policy uplifts all of national planning to guide provincial initiatives and mobilise on the president's call to 4IR momentum.

4.2 The Accounting Officers[1] of departments are responsible for ensuring that this policy is applied within their departments.

4.3 The Accounting Officers are responsible for ensuring that the cloud computing policy and Standard requirements are satisfied before approving an external cloud service.

4.4 It is also recommended that compliance is regularly reviewed by each department's Risk and Audit Committee.

[1] Public Administration Management Act, 2016, Chapter 5 Section (14) (a)(I,ii,iii.iv),(b),(c)(d)

5 SOUTH AFRICA REGULATORY/COMPLIANCE FRAMEWORK

5.1 South Africa Acts and Regulations

The primary instruments regulating the collection, storage, access, use and disclosure of data by the South African public service departments are:

a) Section 13(1) of the National Archives and Records Service of South Africa Act, 1996: regulates the creation, management and protection of the records of public offices and provides for public access to those records.
b) The Protection of Personal Information Act No. 4 of 2013: provides for the protection of personal information and contains obligations in relation to storage, access, use and disclosure.
c) The Consumer Protection Act No. 68 of 2008: spells out the rights of the Consumer and the responsibilities of the supplier.
d) Promotion of Access to Information Act 2 of 2000 (PAIA): all private bodies (entities mentioned above as defined in PAIA) and public bodies (mainly state departments and state administrations as defined in PAIA) must give access to their records if a party requests a record in terms of PAIA.

Many other legislative instruments regulate public service data. These include:
a) Electronic Communications and Transactions Act (ECT Act) 2002
b) The Financial Intelligence Centre Act (38 of 2001) (the FIC Act)
c) Public Service Act 2001
d) Public Service Regulation
e) Public Administration Act

Public service departments must also bear in mind Parliament's powers to compel production of records under the South Africa Constitution and Standing Orders

5.2 Compliance Requirements

5.2.1 Departments are required to comply with a range of legislative frameworks concerning the security[2], privacy[3], access, storage, management, retention and disposal of government data and information[4] .

5.2.2 The CSP is expected to comply with all specified security standards in line with security classification of the data[5]. Compliance with relevant or mandated third party standards such as ISO/IEC27001, HIPAA[6] and GDPR[7] are to be detailed within the business case for each application.

[2] National Cybersecurity Frameworks, Electronic Communication Transaction Act (ECTA)

[3] Promotion of Access to Access to Information Act 2 of 2000 (PAIA), South African National Health Act (SANHA) and the Protection of Personal Information Act (POPI)

[4] National Archives of South Africa Act 43 of 1996

[5] Minimum Information Security Standards (MISS)

[6] Health Insurance Portability and Accountability Act (HIPAA) USA

[7] General Data Protection Regulation (GDPR) European Union.

5.2.3 The CSP must be obligated to notify contracting department within 72 hours (best practice – see EU GDPR definition of any security breach via the contractually agreed procedure. Failure to do so may result in penalties being levied in line with contractual terms and conditions.

5.2.4 The CSP must prohibit unauthorized access to, use or alteration of, the data stored. The method and procedures for this must be detailed in the contractual terms.

5.2.5 The Protection of Personal Information Act no 4 of 2013(POPI), cover the provisions for the use and storage of personal and private data within the state/territory.

5.2.6 Under POPI Act no 4 of 2013, where records are being transferred outside of South Africa for storage with or maintenance by CSP based outside South Africa, public sector departments must:

a. ensure that a responsible party may not transfer personal information about a data subject to a third party who is in a foreign country unless the recipient is subject to a binding agreement which effectively upholds the principles of reasonable processing of the information. Alternatively, that there are adequate laws in place (substantially similar to the provisions contained in the Act) which afford this protection.

b. assess and address the risks involved in taking and sending records out of the Government for storage with or maintenance by CSP based outside of South Africa

c. ensure the CSP facilities and services conform to requirements in standards on electronic records issued by National Archives of South Africa

d. ensure contractual arrangements and controls are in place for the safe custody and proper preservation of records

e. ensure that the ownership of the records remains with the contracting department

f. monitor the arrangement to ensure the CSP is meeting relevant requirements as defined in the in the SLA (see section 8.10, contract terms)

g. as with all emerging technologies there is legal precedent and many untested areas. This needs to be monitored as case law evolves.

6 POLICY

6.1 Goal

The Provincial Government will reduce the cost of ICT by eliminating duplication and fragmentation and will lead by example in using cloud services to reduce costs, lift productivity and develop better agile services.

6.2 Policy Statement

6.2.1 The Provincial departments, local departments and municipal departments are required to use cloud services for new ICT services and when replacing any existing ICT services, whenever the cloud services:

a) are fit for purpose;
b) offer the best value for money; and
c) provide adequate management of risk to information and ICT assets.

6.2.2 The decision on the appropriate ICT delivery model will be based on an assessment of the business case, including the cost benefit analysis and achieving value for money over the life of the investment.

6.2.3 The Fourth Industrial Revolution requires that government adapt on how citizen access public services, that is, services delivery should be citizen centric. The South African Government is committed to modernising its operations through numerous approaches and the usage and, or adoption of cloud computing based services is among those. By deploying cloud computing services, government will reduce costs, increase security, increase productivity, and develop excellent agile citizen services.

6.2.4 To achieve Cloud-First policy, all national and provincial departments must develop business case before re-investing on ICT products and services (data centre/technology refresh). The decision on the appropriate ICT delivery model will be based on an assessment of each application, incorporating fit for the purpose, cost benefit analysis and achieving value for money over the life of the investment.

6.2.5 The province of KwaZulu Natal will adopt a Cloud-First policy with the aim for:

a) Reducing the Total Cost of Ownership of specific or selected ICT products and services in line with the ICT House of Value by eliminating duplication of solutions and fragmentation in the technology environment, and leveraging the efficiencies of on-demand provisioning of ICT services;
b) Increasing productivity and agility, and thus improving citizen services;
c) Promoting green ICT by reducing government data centres thus reducing carbon emission;
d) Developing ICT skills sets required for Fourth Industrial Revolution; and
e) Agility in the deployment of Services.

6.3 Policy Principles

This policy is based on the following driving principles:

6.3.1 Cloud should be the first option before any on-premises investment is done. The option should be fit for the purpose.

6.3.2 Data classification, Information Security and Privacy policy should be developed, see section 10 below.

6.3.3 Total cost of ownership should cost effective in the medium to long term.

6.3.4 Government departments are recommended to consider software as a service (SaaS) as the first cloud-first strategic option.

6.3.5 Government departments should utilise the Government Cloud developed and maintained by the State Information Technology Agency (SITA), and where possible, engage SITA on the process to accredit Cloud Service Provider (CSP).

6.3.6 Government departments must plan for cloud computing as a strategic enabler, rather than as an outsourcing arrangement or technical platform.

6.3. 7 Government departments must evaluate the benefits of cloud acquisition based on a full understanding of the costs of cloud compared with the costs of other technology platform business solutions.

6.3.8 Government departments must take an enterprise risk management perspective to manage the adoption and use of cloud.

6.3.9 Government departments must integrate the full extent of capabilities that cloud providers offer with internal resources to provide a comprehensive technical support and delivery solution.

6.3.10 Government departments must manage accountabilities by clearly defining internal and provider responsibilities.

6.3.11 Government departments must make trust an essential part of cloud solutions, building trust into all business processes that depend on cloud computing.

6.4 Procurement and Sourcing

In using cloud services to reduce costs, lift productivity and develop better services, departments are to:

6.4.1 use ICT refresh points as a trigger for evaluating cloud services;

6.4.2 adopt public cloud services for testing and development needs and for hosting public facing websites;

6.4.3 evaluate private, public or hybrid cloud services for operational systems as defined by information requirements;

6.4.4 consider opportunities to develop/adopt cross entity or portfolio cloud services and/or build on initiatives established by other entities;

6.4.5 comply with relevant legislative and regulatory requirements and to select cloud services commensurate with the requirements of the information.

6.4.6 This policy requires that an adoption of cloud-based services is initially and routinely explored whenever a system is being considered for replacement. Application end-of-life planning must plan for the adoption, wherever practicable, of cloud-based replacements. Where possible, the use of government-sourced buying frameworks should be used.

6.5 Value for Money and Business Case

For each application moved to the cloud, a full business case must be developed to demonstrate compliance with this policy, and a full cost-benefit analysis must be developed, as well.

The business case is expected to cover:

- □ PGDP and APP plan alignment
- □ Tangible Financial Benefits
- □ Total Cost of Ownership
- □ Important Financial Benchmarks
- □ Financial Metric Assumptions and Implications
- □ Anticipated Savings Areas
- □ Intangible Benefits
- □ Recommended Solution
- □ Expected Discounted Cash Flow of the investment
- □ TCO Comparison
- □ Highest Savings areas expected
- □ Financial Savings Realisation Timeline
- □ Current Situation Contextualisation
- □ Proposed Current Situation Response Plan
- □ Implementation Approach
- □ Culture and Change Management
- □ Department Capability
- □ ICT Asset Depreciation Horizon
- □ Re-Sale / Re-Deployment of Existing Assets
- □ International Benchmarks (Optional)

6.6 Oversight

6.6.1 Cloud-based applications and systems are subject to the same internal audit standards as systems and applications hosted on-premises. Oversight committees (IT Steering Committee / Internal Audit Committee will review, the continuing effectiveness and efficiency of cloud arrangements and what may need amendment to comply with vendor terms and conditions.

6.6.2 To this end, the adoption of common and open standards, where possible, is expected to ensure that the overall integrity and ease of integration with core systems is maintained.

7 RISK MANAGEMENT

7.1 Departments must undertake comprehensive risk assessments annually in relation to network access, storage and maintenance of public sector information and records held by CSP.

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

7.3 Evaluation of cloud options will address all identified risks and take account of:

a) *Minimum Information Security Standards (MISS)*
b) *National Cyber Security Policy Framework (NCPF) 2015*
c) *The Internal Audit Guidelines and the Risk Management Framework (Framework) for the Public Sector*[7]
d) *ISO 31000 Risk management – Principles and guidelines*
e) *ISO/IEC 27000 series. The Government is committed to and will continue contributing to the development of international cloud standards via its work with the ISO on the Joint Technical Committee 1SC27 and SC28.*

7.4 The mitigation of risks should include, but is not limited to:
a) data location and retrieval,
b) legal and regulatory risk,
c) information governance and management,
d) business continuity, security,
e) privacy and licensing
f) business continuity and disaster recovery plans must be well documented and tested.

7.5 Depending upon the service type, business need and delivery model adopted, an understanding and mitigation of risks will be required, including, but not limited to:

7.5.1 **Business continuity (**ISO22301**)** - As with all ICT delivery options, business continuity and disaster recovery plans must be well documented and tested.
7.5.2 **Data location and retrieval** – Data residence and sovereignty needs to be understood and implications managed, reference POPI Act.
7.5.3 **Legal and regulatory** – As with all emerging technologies there is little legal precedent and many untested areas. This needs to be monitored as case law evolves.
7.5.4 **Information governance and management** – Departments must ensure cloud service providers and their service offerings comply with all applicable South Africa information management frameworks.
7.5.5 **Privacy** – Departments must ensure cloud service providers and their service offerings meet all applicable South African legislative requirements relating to the privacy of information.

[7] https://oag.treasury.gov.za/RMF/Pages/s305InternalAudit.aspx

7.5.6 **Security** - Departments must ensure cloud service providers and their service offerings meet all applicable South African legislative requirements relating to the security of information.

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

8 INFORMATION AND DATA MANAGEMENT

8.1 The *National Archives and Records Service of South Africa Act (Act. No. 43 of 1996, as amended* is the primary instrument regarding the creation, management, protection and on-going accessibility of records of public offices in South Africa.

8.2. Departments must ensure that records and data created, stored or managed in the cloud remain accessible and retrievable in order to meet regulatory requirements for information access, e.g. under *National Archives and Records Service of South Africa Act (Act. No. 43 of 1996, the Protection of Personal Information (POPI) Act No. 4 of 2013*, and *the Promotion of Access to Information Act 2 of 2000 (PAIA)*. POPI and PAIA also give individuals the right to access their personal and health information held by public sector departments. The broad issues to be considered include:

a) is department access to data guaranteed?

b) can department provide relevant information to third parties (such as to individuals to whom the data relates or regulators monitoring compliance with legislative requirements)?

c) can the department audit data access?

d) how will system administrators or staff of the cloud service provider be prevented from unauthorised access to the data?

8.3 National Archives and Records Service of South Africa Act (Act. No. 43 of 1996 provides further guidance in the *Standard on records management.*

8.4 Security

8.4.1 The *CGICT Policy Framework* establishes that public service departments must develop departmental information security strategy that ensure that classified information, intellectual property and personal information are protected within ICT systems according to its security plan.

8.4.2 Departments must ensure that any cloud-based service complies with the department's Information Security Policy and the requirements of the CGICT Policy Framework. Relevant international standards include *ISO/IEC 27001 Information technology – Security techniques – Information security management systems* and *ISO/IEC 27018*.

8.5 Privacy

8.5.1 The collection, storage, access, use and disclosure of personal information is governed by POPI Act and PAIA. Where the use of cloud computing requires the transmission or storage of personal information, including health information, departments must ensure that their arrangements comply with relevant privacy and disclosure requirement to a minimum of the ISO 27018 standard.

8.5.2 A department must not do anything, or engage in any practice, that contravenes an Information Protection Principle or a Health Privacy Principle applying to the department. Particular areas of cloud services which may affect data privacy include:

a) disclosure of personal information to a cloud service provider should be encrypted to a minimum of ISO/IEC 18033, which specifies encryption systems (ciphers) for the purpose of data confidentiality.

b) data security and safeguards against misuse or loss, unauthorised access, use, or alteration

c) ensuring ongoing accessibility for the department and for data subject via a request to the department

d) legislative environment and governing data laws in the location where data is stored

e) determining who has control of data at the end of a contract should be clearly addressed in the contract.

f) authorised data retention and disposal should be clearly addressed in the contract.

8.6 If a department shares with or transfers personal information to a contracted cloud service provider and the cloud service provider simply holds the data and acts according to the instructions of the department, then disclosure will not be considered to have occurred. If the cloud service provider uses the data provided for its own purposes, this may be unauthorised access, use, modification or disclosure.

8.6.1 Departments must ensure that contractual arrangements with a cloud service provider explicitly address this, and take such security safeguards as are reasonable in the circumstances to prevent unauthorised access or use. These arrangements will need to take into account circumstances that may include where one or more functions of an agency are outsourced to a provider, or where a cloud service provider is asked to perform some action on the personal information that they had previously only been storing.

8.7 Standards

8.7.1 Consideration of the use the and adoption of international standards, covering, among others, security, interoperability, and data portability are recommended in order to reduce the risk of technology lock-in and inadequate data portability. Standards from the International Standards Organisation (ISO), in particular the ISO27000 series, ISO39500 and the ISO22300 series, as well as specific cloud standards, such as ISO17788 provide for this. A list of current applicable standards is included in the Appendix.

8.8 Change management

8.8.1 Departments will need to consider the existing organisational environment when adopting new delivery models. The transition to an as-a-service model may have significant change implications. Moving to a cloud environment may require departments to reconsider business design and enterprise architecture, particularly where cloud services interface with internal business processes and systems. This can affect capability requirements across the department.

8.8.2 Adoption of a cloud service should be viewed as part of a larger business reengineering project, rather than as a purely IT-related project. Early engagement across the department on the change implications of transitioning to an as-service model will allow departments to more easily take advantage of associated opportunities to improve business efficiency.

8.9 Technical considerations

8.9.1 The use of a cloud service will require consideration of specific technical requirements including LAN, WAN and bandwidth, security, compatibility with the various browser technologies, and implications for longer-term data integration.

8.9.2 In order to achieve the levels of automation and virtualisation required in a cloud service, most providers offer a standard operating system with no, or limited, customisation. While improving cost effectiveness, this may increase complexity for departments when integrating cloud services with legacy environments or with different cloud service providers.

8.9.3 A comprehensive assessment of the internal technical environment prior to implementation will contribute to a smoother migration, fewer unexpected costs and more timely delivery against project timeframes. While the effort, time and cost associated with remediating the internal technical environment may be high, it is an exercise that may need to be performed only once, after which the department should be able to source additional cloud-based services more easily and more cost effectively.

8.10 Contract terms

International best practices on government cloud computing contracts indicate that departments should address the following when creating a cloud computing contract:

8.10.1 Selecting a Cloud Service: Choosing the appropriate CSP and deployment model (see Appendix 1) is the critical first step in procuring cloud services;

8.10.2 CSP and End-User Agreements: Terms of Service and all CSP/contracting department required agreements need to be integrated fully into the cloud contracts;

8.10.3 Service Level Agreements (SLA): SLAs need to define performance with clear terms and definitions, demonstrate how performance is measured, and what enforcement mechanism are in place to ensure SLAs are met and in conformance with ISO 19806, Cloud computing, Service Level Agreement (SLA) framework;

8.10.4 CSP, Department, and Integrator Roles and Responsibilities: Careful delineation between the responsibilities and relationships among department, integrators, and CPS are needed in order to effectively manage cloud services;

8.10.5 Standards: The use of the ISO 17789 cloud reference architecture (see appendix 1) as well as department involvement in standards are necessary for cloud procurements;

8.10.6 Security: Departments must clearly detail the requirements for CSPs to maintain the security and integrity of data existing in a cloud environment. At a minimum this should be in conformance with ISO 27017, Security Techniques, code of practice for information security controls based on ISO/IEC 27002 for cloud services.;

8.10.7 Privacy: If cloud services host "privacy data", departments must adequately identify potential privacy risks and responsibilities and address these in the contract. At a minimum this should be in conformance with ISO 27018, Security Techniques, code of practice for the protection of personally identifiable information (PII) in public clouds acting as PPI processors;

8.10.8 Promotion of Access to Information Act (PAIA) and Protection of Personal Information Act (POPI): Departments must ensure that all data stored in a CSP environment is available for appropriate handling under the PAIA and POPI.

8.10.9 Legal Discovery: Departments must ensure that all data stored in a CSP environment is available for legal discovery by allowing all data to be located, preserved, collected, processed, reviewed, and produced; and

8.10.10 Electronic Records (E-Records): Departments must ensure CSP's understand and assist departments in compliance with South Africa National Archive Act and obligations under this law.

Prior to signing a cloud computing contract, Departments should ensure that their contract:

a) Details the process by which a CSP stores, searches, and collects information;
b) Clarifies who (Department or CSP) will pay for requests/searches and how the information will be identified;
c) Defines what abilities a CSP has to search and retrieve specific information by source;
d) Addresses potential data access issues or cross-border transfer issues that may arise from data located in other jurisdictions;
e) Clearly identifies procedures in place for proper chain of custody. Ideally chain of custody should be automated to eliminate erroneous access of data and to immediately identify individuals accessing data; and
f) identifies what access methods/protocols will be available for access by external services/applications.

By addressing the elements above and including all necessary stakeholders when creating cloud computing contracts (e.g. GCIO, SITA, Privacy, Records, PFMA, and procurement staff), departments will be able to more effectively procure and manage IT as a service.

8.11 Skills and capabilities

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

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

.

9 CLOUD SERVICE PROVIDER COMPLIANCE AND ACCREDITATIONS

9.1 Global Cloud Accreditations

The following global cloud accreditations are prescribed for a Cloud Service Provider to hold :

□ CIS Benchmark
□ CSA-STAR attestation
□ CSA-STAR certification
□ CSA-STAR self-assessment
□ ISO 20000-1:2011
□ ISO 22301
□ ISO 27001
□ ISO 27017
□ ISO 27018
□ ISO 27701
□ ISO 9001
□ SOC
□ WCAG

9.2 Industry Specific Cloud Accreditations

The Province of KwaZulu Natal has a vision to be a gateway to the world. As responsible global citizens, the Cloud Service Provider should attest to compliance in these industry specific accreditations to demonstrate capability of both local and global relevance.

□ 23 NYCRR Part 500
□ AFM + DNB (Netherlands)
□ APRA (Australia)
□ AMF and ACPR (France)
□ CDSA
□ CFTC 1.31 (US)
□ DPP (UK)
□ EBA (EU)
□ FACT (UK)
□ FCA (UK)
□ FDA CFR Title 21 Part 11
□ FERPA
□ FFIEC (US)
□ FINMA (Switzerland)
□ FINRA 4511
□ FISC (Japan)
□ FSA (Denmark)
□ GLBA
□ GxP
□ HDS (France)
□ HIPAA / HITECH
□ HITRUST
□ KNF (Poland)
□ MARS-E
□ MAS + ABS (Singapore)
□ MPAA
□ NBB + FSMA (Belgium)
□ NEN-7510 (Netherlands)
□ NERC
□ NHS IG Toolkit (UK)
□ OSFI (Canada)
□ PCI DSS
□ RBI + IRDAI (India)
□ SEC 17a-4
□ SEC Regulation SCI
□ Shared assessments
□ SOX
□ TISAX (Germany)
□ TruSight

9.3 Multi Cloud Environment

Where a cloud service is expected to straddle multiple cloud service providers due to technical, jurisdiction or other relevant reasons then it is expected that all the cloud service providers have the equivalent compliance accreditations in order to have the entire service ecosystem at an equivalent compliance level.

The security and technical plans are to ensure that data in transit is not compromised and the end result subscribes to the ICT integrity and vision of the province.

Further, a deviation application must be supplied to the Office of The Premier and relevant governance departments from the Accounting Officer. This must be discussed and deliberated upon by the provincial GITO committee and other existing structures.
Such application must complete all the necessary checklists detailed in this policy and then provide all criteria that is non-compliant with associated reasons and business case implications.

10 CLOUD SECURITY PRINCIPLES

10.1 The benefit of migrating government workloads and data onto government cloud is the ability to enhance overall data security. Cloud service providers engaged by government department will be required to meet international security standards, and ensure appropriate certification. They will abide by all relevant industry standards, for example, international security standards such as ISO 27001.

10.2 Government departments should collaborate with SITA to establish a security framework which applies a risk management approach towards its own data control requirements (see Data Classification), and align this with international standards and certifications, as well as industry standards. The precise level of security requirements for contracted cloud services should be determined by the contracting department based on an assessment of data risk. Stipulated security controls can include any one or more of the following:

a) Physical and environmental security
b) Business continuity management and incidence response
c) Inventory and configuration management
d) Data encryption
e) Access controls, monitoring and logging
f) Network security and monitoring.

Security Framework

10.3 Managing the security of contracted cloud services is a responsibility that is shared between the contracting department and the cloud service provider. The contracting department as data controller is responsible for information security and defining security controls in the cloud, and align to it. The (CSP) is responsible for the security of the cloud services under contract as a data processor.

In short the data itself remains under the ownership and control of the department at all times, with the CSP as data processor. The level of responsibility on both parties depends on the cloud deployment model type, and departments should be clear as to their responsibilities in each model

10.4 Data security depends upon:

a) Meeting security requirements for each data classification level; and
b) Employing standardized tools and procedures for audit.

10.5 Data Classification

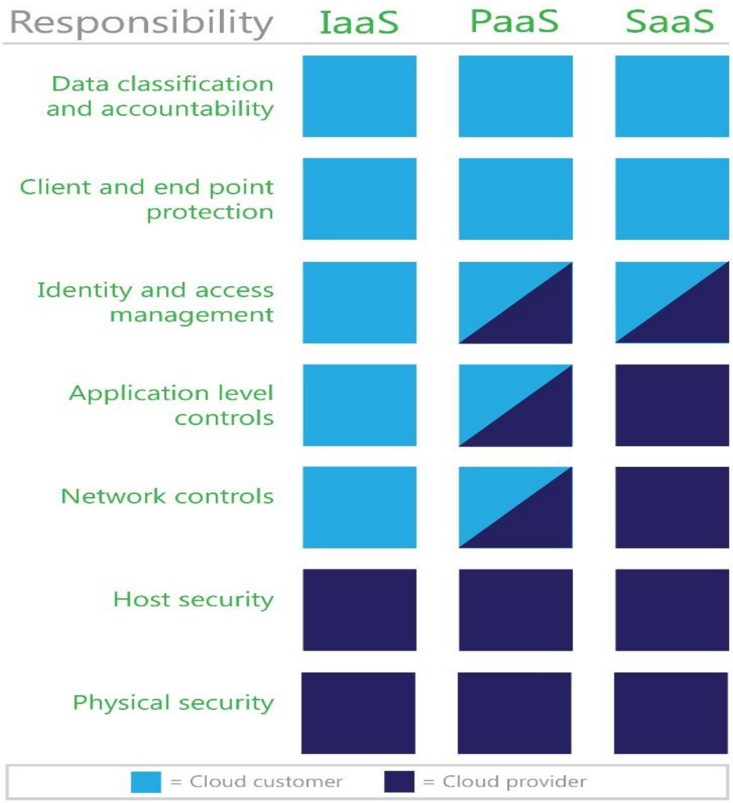
10.5.1 Successful data classification in a department requires broad awareness of the department's needs and a thorough understanding of where the department's data assets reside.

10.5.2 Data exists in one of three basic states: at rest, in process, and in transit. All three states require unique technical solutions for data classification, but the applied principles of data classification should be the same for each.

10.5.3 Roles and responsibilities in cloud computing

10.5.3.1 Data classification responsibilities will vary based on which cloud service model is in place, as shown in the following figure 1. The three primary cloud service models are infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). Implementation of data classification mechanisms will also vary based on the reliance on and expectations of the CSP.

Figure 1 Roles and Responsibilities in cloud data classifications



Responsibility	IaaS	PaaS	SaaS
Data classification and accountability	🟦	🟦	🟦
Client and end point protection	🟦	🟦	🟦
Identity and access management	🟦	🟦/⬛	🟦/⬛
Application level controls	🟦	🟦/⬛	⬛
Network controls	🟦	🟦/⬛	⬛
Host security	⬛	⬛	⬛
Physical security	⬛	⬛	⬛

🟦 = Cloud customer ⬛ = Cloud provider

10.5.3.2 Departments are responsible for classifying their data, CSP should make written commitments to departments about how they will secure and maintain the privacy of the department data stored within their cloud. These commitments should include information about privacy and security practices, data use limitations, and regulatory compliance. In addition, cloud providers should make certifications and audit reports that demonstrate compliance with standards such as the International Organization for Standardization (ISO) and South African security legal prescripts.

10.5.3.3 Data that is classified as confidential needs to stay confidential when at rest, in process, and in transit.

10.5.3.4 Departments should not migrate data to a cloud provider that cannot address their data protection needs.

10.5.3.5 **IaaS provider**. From a data classification perspective, IaaS provider requirements are limited to ensuring that the virtual environment can accommodate data classification capabilities and customer compliance requirements. IaaS providers have a smaller role in data classification because they only need to ensure that department data addresses compliance requirements.

However, CSP must still ensure that their virtual environments address data classification requirements in addition to securing their data centres.

10.5.3.6 **PaaS providers**. Responsibilities may be mixed, because the platform could be used in a layered approach to provide security for a classification tool. PaaS providers may be responsible for authentication and possibly some authorization rules, and must provide security and data classification capabilities to their application layer. Much like IaaS providers, PaaS providers need to ensure that their platform complies with any relevant data classification requirements.

10.5.3.7 **SaaS providers** will frequently be considered as part of an authorization chain, and will need to ensure that the data stored in the SaaS application can be controlled by classification type. SaaS applications can be used for Line of Business (LOB) applications, and by their very nature need to provide the means to authenticate and authorize data that is used and stored

10.5.4 Classification Process

10.5.4.1 To implement data classification it is recommended that departments use the **PLAN**, **DO, CHECK, ACT** model[8]

1. **PLAN**. Identify data assets, a data custodian to deploy the classification program, and develop protection profiles.
2. **DO**. After data classification policies are agreed upon, deploy the program and implement enforcement technologies as needed for confidential data.
3. **CHECK**. Check and validate reports to ensure that the tools and methods being used are effectively addressing the classification policies.
4. **ACT**. Review the status of data access and review files and data that require revision using a reclassification and revision methodology to adopt changes and to address new risks.

10.5.4.2 When classifying a file or resource that combines data that would typically be classified at differing levels, the highest level of classification present should establish the overall classification. For example, a file containing sensitive and restricted data should be classified as restricted.

[8] Trustworthy Computing | Data classification for cloud readiness, Microsoft, 2014

Table 1 Data Classification

Sensitivity	**Classification 1**	**Classification 2**
High	Restricted	Restricted
Medium	For internal use only	Sensitive
Low	Public	Unrestricted

10.5.4.3 Confidential (restricted). Information that is classified as confidential or restricted includes data that can be catastrophic to one or more individuals and/or organizations if compromised or lost. Such information is frequently provided on a "need to know" basis and might include:

a) **Personal data**, including personally identifiable information such as government ID number or national identification numbers, passport numbers, credit card numbers, driver's license numbers, medical records, and health insurance policy ID numbers.
b) **Financial records**, including financial account numbers such as checking or investment account numbers.
c) **Business material**, such as documents or data that is unique or specific intellectual property.
d) **Legal data**, including potential attorney-privileged material.
e) **Authentication data**, including private cryptography keys, username password pairs, or other identification sequences such as private biometric key files.

Data that is classified as confidential frequently has regulatory and compliance requirements for data handling.

10.5.4.4 For internal use only (sensitive). Information that is classified as being of medium sensitivity includes files and data that would not have a severe impact on an individual and/or organization if lost or destroyed. Such information might include:

a) Email, most of which can be deleted or distributed without causing a crisis (excluding mailboxes or email from individuals who are identified in the confidential classification).
b) Documents and files that do not include confidential data.

Generally, this classification includes anything that is not confidential. This classification can include most business data, because most files that are managed or used day-to-day can be classified as sensitive. With the exception of data that is made public or is confidential, all data within a business organization can be classified as sensitive by default.

10.5.4.5 Public (unrestricted). Information that is classified as public includes data and files that are not critical to business needs or operations. This classification can also include data that has deliberately been released to the public for their use, such as marketing material or press announcements. In addition, this classification can include data such as spam email messages stored by an email service.

10.5.5 Minimum Information Security Standards[9] (MISS) Classification

10.5.5.1 All official matters[10] requiring the application of security measures (exempted from disclosure) must be classified "Restricted", "Confidential", "Secret" or "Top Secret".

Sensitivity	**MISS Classification**
High	Secret or Top Secret
Medium	Confidential
Low	Restricted

10.5.5.2 Restricted

a) ***Definition***: **RESTRICTED** is that classification allocated to all information that may be used by malicious/opposing/hostile elements to hamper activities or inconvenience an institution or an individual.

b) ***Test***: Intelligence/information must be classified as **RESTRICTED** when the compromise thereof could hamper or cause an inconvenience to the individual or institution.

c) ***Explanation***: **RESTRICTED** is used when the compromise of information can cause inconvenience to a person or institution, but cannot hold a threat of damage. However, compromise of such information can frustrate everyday activities.

10.5.5.3 Confidential

a) ***Definition***: The classification **CONFIDENTIAL** should be limited to information that may be used by malicious/opposing/hostile elements to harm the objectives and functions of an individual and/or institution.

b) ***Test***: Intelligence/information must be classified **CONFIDENTIAL** when compromise thereof can lead to:

i. the frustration of the effective functioning of information or operational systems;
ii. undue damage to the integrity and/or reputation of individuals;
iii. the disruption of ordered administration within an institution; and
iv. adverse effect on the non-operational relations between institutions.

[9] Minimum Information Security Standards (MISS), 1996

[10] The MISS, applies to:

a) public bodies rendering a public service (both those subject to the Public Service Act and those subject to any other law)
b) private bodies processing information that is of importance to national interests.

c) ***Explanation***: **CONFIDENTIAL** is used when compromise of information results in:

i. undue damage to the integrity of a person or institution, but not entailing a threat of serious damage. The compromise of such information, however, can frustrate everyday functions, lead to an inconvenience and bring about wasting of funds;

ii. the inhibition of systems, the periodical disruption of administration (e.g. logistical problems, delayed personnel administration, financial relapses, etc) that inconvenience the institution, but can be overcome; and

iii. the orderly, routine co-operation between institutions and/or individuals being harmed or delayed, but not bringing functions to a halt.

10.5.5.4 Secret

a) ***Definition***: **SECRET** is the classification given to information that may be used by malicious/opposing/hostile elements to disrupt the objectives and functions of an institution and/or state.

b) ***Test***: Intelligence/information must be classified as SECRET when the compromise thereof:

i. can disrupt the effective execution of information or operational planning and/or plans;

ii. can disrupt the effective functioning of an institution;

iii. can damage operational relations between institutions and diplomatic relations between states;

iv. can endanger a person's life.

c) ***Explanation***: **SECRET** is used when the compromise of information:

i. can result in the disruption of the planning and fulfilling of tasks, i.e. the objectives of a state or institution in such a way that it cannot properly fulfil its normal functions; and

ii. can disrupt the operational co-operation between institutions in such a way that it threatens the functioning of one or more of these institutions.

10.5.5.5 Top Secret

a) ***Definition***: **TOP SECRET** is the classification given to information that can be used by malicious/opposing/hostile elements to neutralise the objectives and functions of institutions and/or state.

b) ***Test***: Intelligence/information must be classified **TOP SECRET** when the compromise thereof:

i. can disrupt the effective execution of information or operational planning and/or plans;
ii. can seriously damage operational relations between institutions;
iii. can lead to the discontinuation of diplomatic relations between states; and
iv. can result in the declaration of war.

c) ***Explanation***: **TOP SECRET** is used when the compromise of information results in :
i. the functions of a state and/or institution being brought to a halt by disciplinary measures, sanctions, boycotts or mass action;
ii. the severing of relations between states; and iii. a declaration of war.

10.5.6 Define data ownership

10.5.6.1 The Department that originates/owns the data is deemed to be the Data Controller; the CSP is deemed is deemed to be the Data Processor and has no rights as to ownership of the data. Departments must establish a clear custodial chain of ownership for all data assets. The following table identifies different data ownership roles in data classification efforts and their respective rights.

Role	Create	Modify/delete	Delegate	Read	Archive/restore
Owner	x	x	x	x	x
Custodian			x		
User*		x		x	

*Users may be granted additional rights such as edit and delete by a custodian

10.5.6.2 The data asset owner is the original creator of the data, who can delegate ownership and assign a custodian. When a file is created, the owner should be able to assign a classification, which means that they have a responsibility to understand what needs to be classified as confidential based on their organization's policies. All of a data asset owner's data can be auto-classified as for internal use only (sensitive) unless they are responsible for owning or creating confidential (restricted) data types.

10.5.6.3 The data asset custodian is assigned by the asset owner (or their delegate) to manage the asset according to agreements with the asset owner or in accordance with applicable policy requirements. Ideally, the custodian role can be implemented in an automated system. An asset custodian ensures that necessary access controls are provided and is responsible for managing and protecting assets delegated to their care. The responsibilities of the asset custodian could include:

a) Protecting the asset in accordance with the asset owner's direction or in agreement with the asset owner
b) Ensuring that classification policies are complied with

c) Informing asset owners of any changes to agreed-upon controls and/or protection procedures prior to those changes taking effect

d) Reporting to the asset owner about changes to or removal of the asset custodian's responsibilities

10.5.7 Reclassification

10.5.7.1 Reclassifying or changing the classification state of a data asset needs to be done when the data controller determines that the data asset's importance or risk profile has changed. This effort is important for ensuring that the classification status continues to be current and valid.

10.5.7 Data retention, recovery, and disposal

10.5.7.1 Data recovery and disposal, like data reclassification, is an essential aspect of managing data assets. The principles for data recovery and disposal would be defined by a data retention policy in conformance with ISO 22301 (Business continuity) and ISO 19806 (Cloud SLA) and enforced in the same manner as data reclassification; such an effort would be performed by the data owner.

10.5.7.2 Failure to have a data retention policy could mean data loss or failure to comply with regulatory and legal discovery requirements. Defining a policy for confidential data can ensure that data is stored and removed based on best practices. In addition, an archival policy can be created to formalize an understanding about what data should be disposed of and when. Data retention policy should address the required regulatory and compliance requirements, as well as corporate legal retention requirements.

10.5.8 Mitigation and Back-Up

10.5.8.1 Departments need to have in place mitigation and redundancy contingencies. It is the responsibility of each government department to ensure that they have a mitigation and back-up plan for their data and services. These plans need to ensure at a minimum:

- Having service continuity in times of disaster or emergency
- No government data loss occurs without recovery
- Be in conformance with ISO 22301 (Business continuity)

10.5.8.2 A mitigation and back-up plan should include backing-up data in a second location in two regions so as to ensure (i) full data protection, (ii) continued and uninterrupted service, and (iii) data recovery.

11 ROLES AND RESPONSIBILITIES

11.1 This policy was first drafted by the DPSA and the national policy developed is currently awaiting national approval. It was developed and reviewed by GITOC for the intention of implemented by Government departments. Any changes or deviations from this policy will need a review by the provincial GITOC. Once the national DPSA policy is approved, the provincial policy will be reviewed for subscription to the national DPSA policy.

11.2 The implementation of the policy will be monitored by the KwaZulu Natal province and will governed by DPSA and GITOC until the national DPSA policy is approved.

11.3 In addition, the following roles and responsibilities for each stakeholder, involved with the policy implementation, have been listed below.

11.3.1 *Government* Department

a) The Heads of the Government departments are responsible for ensuring all aspects of this policy and guidelines are applied within their department.
b) All Government employees involved in procuring cloud based services, applications or platform hosting services for the Government department must adhere to this policy.
c) The business owner is responsible for the application functionality and support.
d) The business owner will ensure optimal sizing and detailed analysis of usage, incorporating seasonal spikes in workloads, to enable accurate budgeting for the cloud services required.
e) Monitoring and ensuring the performance of the applications is as per the stated SLA.
f) The department shall monitor usage of the cloud services and provide a monthly usage report to DPSA/NT. This is to ensure that the usage does not exceed the budgeted limit for the department.

11.3.2 SITA

a) Act as the government cloud service provider to government departments, subject to all the compliance requirements of the cloud service providers being met.
b) Assist the departments to ensure relevant SLAs are defined for the applications based on the department requirements.
c) Continue to monitor and govern existing SLAs agreed with departments.
d) Provide support and guidance to departments in assessment and identification of applications to move to the cloud, where requested.
e) Provide technical support to modify applications and get them cloud ready, where SITA has demonstrated capable and trained skills to effectively conduct such exercises.

11.3.3 DPSA

a) DPSA will maintain an oversight on the implementation of this policy.
b) DPSA will audit the government entities for compliance at its discretion, at regular intervals as well as on an ad hoc basis.
c) Shall act as the arbitrator in cases if dispute between the various government departments

11.3.4 Provincial GITOC

a) GITOC set the strategic direction for Cloud initiative and oversight the Cloud Strategy implementation.

12 GUIDELINES STEPS

12.1 Experience with cloud internationally has revealed practical lessons that departments can incorporate into their approaches to maximise the benefits of cloud and help address key considerations.

12.1.1 Define the desired business outcomes and appropriate use cases, and validate with internal and external stakeholders and peers as necessary.
Ensure non-business critical elements are removed.

12.1.2 Assess information requirements in terms of privacy, security, sensitivity, access and regulatory compliance.

12.1.3 Start with non-critical systems with less information sensitivity in transitioning to the cloud.

12.1.4 Understand the business and technological impacts of the transformation on processes, people and policies. Understand system and business process integration requirements.

12.1.5 Invest effort in developing intellectual property that defines the business capabilities and processes that are being enabled with cloud solutions. Collaborate on and share this intellectual property with peers and industry as a way to achieve better solution designs.

12.1.6 Be pragmatic, and balance risk and reward when choosing a solution.

12.1.7 Align the application workload with business strategy.

12.1.8 Consider how to leverage solutions from other common law jurisdictions, such as the Uganda, Rwanda, Australia, New Zealand or the United Kingdom, or building on already-established initiatives in other departments.

12.1.9 Use refresh points as triggers for evaluating cloud options.

12.1.10 Apply leadership, collaborative approaches and innovation in strategic cloud procurements.

13 CLOUD FIRST POLICY BENEFITS

The benefits realized by governments that adopt a cloud environment are numerous, including but not limited to:

13.1 **Improved business engagement** across the organization by aligning IT to program and business objectives;

13.2 **Cultural shift to higher value work** because there is no need to oversee procurement of IT commodities, or provision underlying infrastructure and systems; therefore, this evolves the role of IT as a "value creator" (i.e., from "IT delivery" to "service delivery");

13.3 **Support sustainability measures** by more efficiently aligning resource capacity with actual demand and consumption, minimizing government waste by reducing excess computing capacity and power consumption;

13.4 **Enhanced end-to-end service delivery** by making information more easily accessible, allowing for nimbler response times to citizens, businesses and stakeholders;

13.5 **Innovate the public service** by tapping into private-sector innovation in the cloud computing arena, and identifying new opportunities for collaboration;

13.6 **Better enabled to adopt and try new technologies** and services on a limited scale before deploying nationally;

13.7 **Realized cost savings** by paying for only what is consumed (purchased "as-service"), thereby ensuring taxpayers' Rands are well spent;

13.8 **Fuel an entrepreneurial culture** both inside and outside government, stimulating the economy and innovation ecosystem; and

13.9 **Enhanced reputation** by promoting open government and fostering public engagement.

13.10 **Efficiency improvements** by using the cloud computing model for IT services, the government will be able to reduce data centre infrastructure expenditure

13.11 **Better utilisation of ICT Assets** with cloud computing, IT infrastructure resources are pooled and shared across large numbers of applications and organizations. Cloud computing can complement data centre consolidation efforts by shifting workloads and applications to infrastructures owned and operated by third parties

13.12 **Reduce duplication c**loud computing will help departments to mitigate the fragmented data, application, and infrastructure silo issues and funding models by focusing on IT services as a utility.

13.13 **Data centre consolidation c**loud computing can accelerate data centre consolidation efforts by reducing the number of applications hosted within government-owned data centres. For those that continue to be owned and operated directly by departments (e.g., by implementing private IaaS clouds), environments will be more interoperable and portable, which will decrease data centre consolidation and integration costs because it reduces unnecessary heterogeneity and complexity in the IT environment.

14 APPENDICES

APPENDIX 1 CLOUD COMPUTING DEFINITION

NIST has identified five essential characteristics of cloud computing: on-demand service, broad network access, resource pooling, rapid elasticity, and measured service. This is now formalised within the ISO 17788 standard.

Cloud computing is defined to have several deployment models, each of which provides distinct trade-offs for departments which are migrating applications to a cloud environment. NIST defines the cloud deployment models as follows:

a) ***Private cloud***. The cloud infrastructure is operated solely for an organisation. It may be managed by the organisation or a third party and may exist on premise or off premise.

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

c) ***Public cloud***. The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.

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

Cloud computing can also categorized into service models. These are defined by NIST to be:

a) **Cloud Software as a Service (SaaS).** The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

b) **Cloud Platform as a Service (PaaS).** The capability provided to the consumer is the ability to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

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

ON-PREMISE VS CLOUD – WHAT IS THE DIFFERENCE

Some of the fundamental differences between a traditional on premise solution and a cloud-based solution is around the areas of ownership, management responsibility and control of the underlying resources comprising the solution stack, as depicted in Figure below.

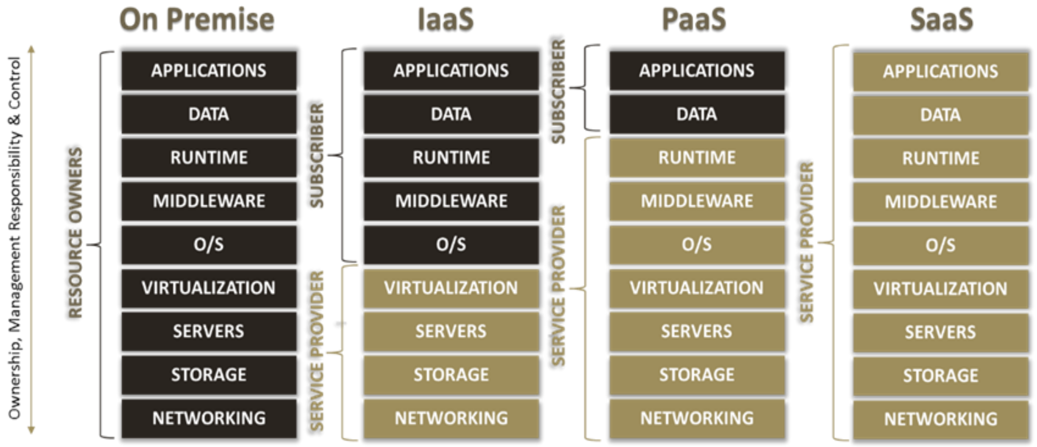


Figure 1: On-Premise vs Cloud Service Models (according to NIST)

For a traditional On-Premise solution, all three of these areas reside with the resource owner, which may be the end-user customer itself, or could be outsourced partly or in its entirety to a 3rd party service provider, typically as a hosted or managed service.

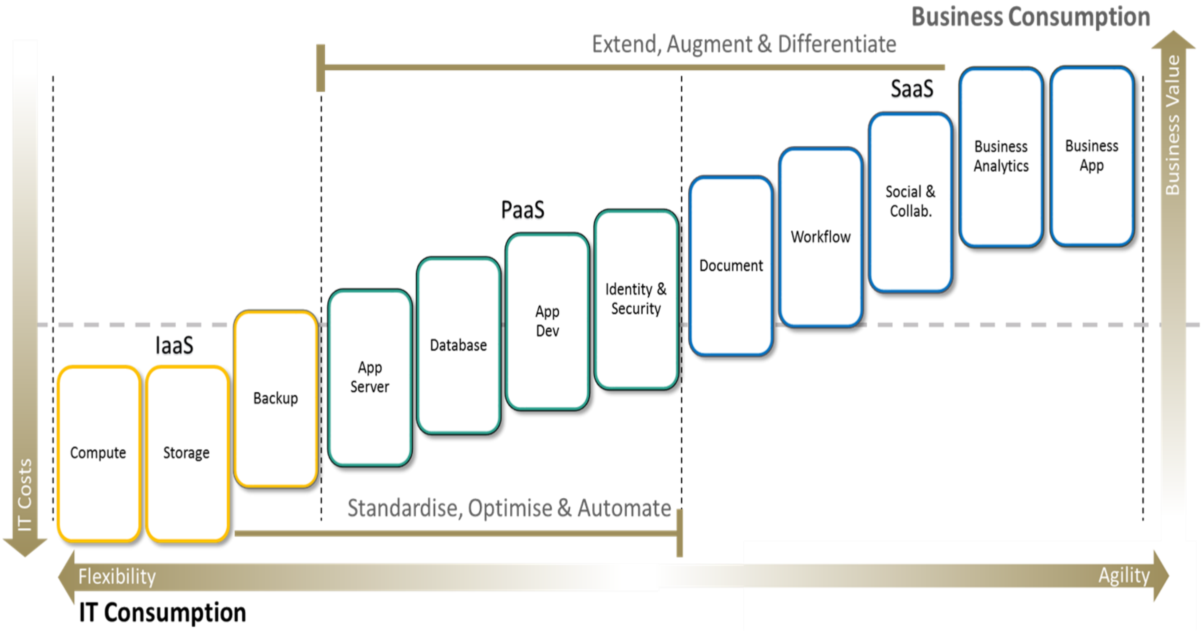


Figure 2: The Cloud Continuum

The main differences between an On-Premise and a Cloud solution is depicted in Figure 2, and the matching implication of each as it relates to IFMS is further outlined in Table 1.

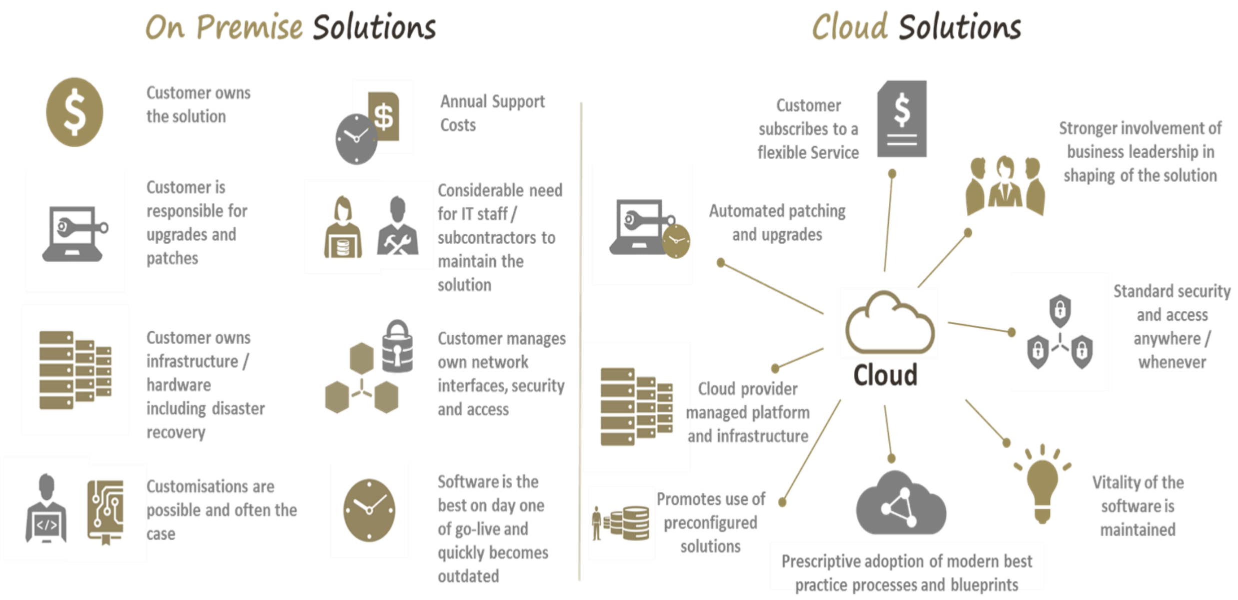

On Premise Solutions
Customer owns the solution
Annual Support Costs
Customer is responsible for upgrades and patches
Considerable need for IT staff / subcontractors to maintain the solution
Customer owns infrastructure / hardware including disaster recovery
Customer manages own network interfaces, security and access
Customisations are possible and often the case
Software is the best on day one of go-live and quickly becomes outdated
Cloud Solutions
Customer subscribes to a flexible Service
Stronger involvement of business leadership in shaping of the solution
Automated patching and upgrades
Standard security and access anywhere / whenever
Cloud
Cloud provider managed platform and infrastructure
Promotes use of preconfigured solutions
Vitality of the software is maintained
Prescriptive adoption of modern best practice processes and blueprints

Figure 3: Difference between On-premise and Cloud Solutions

On-Premise	Cloud
Customer owns and maintains the solution	Customer subscribes to a flexible service
Software is the best on day one of go-live and quickly becomes outdated	Vitality of the software is maintained
Requirements-driven implementation is the norm	Prescriptive adoption of modern best practice processes and blueprints
Customisations are possible and often the case	Promotes use of preconfigured solutions
Implementation is typically led and managed by IT	Stronger involvement of business leadership in shaping of the solution
Long, arduous implementation cycles is typically the norm	Quicker setup and agile implementation methods are available
Annual Support Costs	Subscription based commercial model
Considerable need for IT staff / subcontractors to maintain the solution	Maintenance of the solution is the responsibility of the cloud provider
Customer is responsible for upgrades and patches	Automated patching and upgrades
Customer owns infrastructure / hardware including disaster recovery	Cloud provider managed platform and infrastructure
Customer manages own network interfaces, security and access	Standard security and access anywhere / whenever

Table 1: On-Premise vs Cloud Relevance for SAAS

15 TEMPLATES

1 PRIVACY CHECKPOINTS TEMPLATE FOR A CLOUD SOLUTION[11]

The Privacy Checkpoint Document is available from the KZN Office of the Premier for completion.

2 LEGAL CHECKLIST TEMPLATE FOR A CLOUD SOLUTION[12]

The Legal Document is available from the KZN Office of the Premier for completion and further elaborates on the ISO/IEC 19086-1 standard.

3 BUSINESS CASE TEMPLATE FOR CLOUD SOLUTION[13]

A detailed Business Case template for the province of Kwazulu Natal has been drafted and is available from the KZN Office of the Premier.

[11] Adopted from Privacy and Cloud Computing for Australian Government 2013

[12] Adopted from Negotiating the cloud – legal issues in cloud computing agreements. Australian Government, 2012

[13] Adopted from A Guide to Implement Cloud Services, Australian Government, 2012

16 REFERENCES

i. ISO/IEC 27000 family - Information security management systems
https://www.iso.org/isoiec-27001-information-security.html

ii. ISO/IEC 17788:2014. Cloud computing https://www.iso.org/standard/60544.html

iii. ISO/IEC 17789:2014. Cloud computing (reference architecture)
https://www.iso.org/standard/60545.html

iv. ISO/IEC 19086-3:2017 Cloud computing -- Service level agreement (SLA) framework
https://www.iso.org/standard/67547.html

v. ISO/IEC 38505-1:2017 Governance of IT/ data
https://www.iso.org/standard/56639.html

vi. ISO 22301:2012 Business continuity management systems
https://www.iso.org/standard/50038.html

vii. '2017_Modernising_public_sector_through_cloud_South-Africa_RANITP.pdf'. Accessed 19 February 2018.
https://researchictafrica.net/wp/wpcontent/uploads/2018/01/2017_Modernising_public_sector_through_cloud_SouthAfrica_RANITP.pdf.

viii. Australian-Government-Cloud-Computing-Policy-3.pdf'. Accessed 3 March 2018.
https://www.finance.gov.au/sites/default/files/australian-government-cloud-computing-policy3.pdf.

ix. Cloud Computing Policy'. Office of the Chief Information Officer, 31 October 2016.
https://ocio.commerce.gov/page/cloud-computing-policy.

x. 'Cloud Policy'. Office of the Government Chief Information Officer (blog), 24 May 2016.
https://gcio.wa.gov.au/2016/05/24/cloud-policy-2/.

xi. 'Cloud-Computing-Policy-March-1-2015.pdf'. Accessed 3 March 2018.
https://www.cbu.ca/wpcontent/uploads/2015/07/Cloud-Computing-Policy-March-1-2015.pdf.

xii. 'Cloud-Computing-Policy.pdf'. Accessed 3 March 2018.
https://carleton.ca/secretariat/wpcontent/uploads/Cloud-Computing-Policy.pdf.

xiii. 'Cloud-Computing-Transforming-the-Government-of-Canada-for-the-Digital-Economy.pdf'. Accessed 15 February 2018. http://itac.ca/wp-content/uploads/2015/08/Cloud-ComputingTransforming-the-Government-of-Canada-for-the-Digital-Economy.pdf.

xiv. 'Cloud-Policy-2014-Final.pdf'. Accessed 3 March 2018. https://www.tcd.ie/about/policies/assets/pdf/Cloud-Policy-2014-final.pdf.

xv. 'Cloud policy-APPROVED -2014-07-7-FINAL.pdf'. Accessed 3 March 2018. https://it.tufts.edu/sites/default/files/cloudpolicy-APPROVED%20-2014-07-7-FINAL.pdf.

xvi. 'Digital-by-Default-a-Guide-to-Transforming-Government.pdf'. Accessed 17 February 2018. https://www.mckinsey.com/~/media/mckinsey/industries/public%20sector/our%20insights/transforming%20government%20through%20digitization/digital-by-default-a-guide-totransforming-government.ashx.

xvii. 'Discussion_Paper_on_Policy_Legal_Issue_sin_Cloud_0.pdf'. Accessed 17 February 2018. https://www.dsci.in/sites/default/files/Discussion_Paper_on_Policy_Legal_Issue_sin_Cloud_0. pdf.

xviii. 'Draft Administrative Order : Cloud First Policy, December 20, 2014'. iGovPhil Program (blog). Accessed 3 March 2018. http://i.gov.ph/govcloud/policies/draft-administrative-order-cloud-firstpolicy-december-20-2014/.

xix. 'Federal-Cloud-Computing-Strategy.pdf'. Accessed 19 February 2018. https://www.dhs.gov/sites/default/files/publications/digital-strategy/federal-cloud-computingstrategy.pdf.

xx. 'GI-Cloud Strategic Direction Report(1)_0.pdf'. Accessed 3 March 2018. http://meity.gov.in/writereaddata/files/GI-Cloud%20Strategic%20Direction%20Report%281%29_0.pdf.

xxi. 'Government Cloud First Policy - GOV.UK'. Accessed 15 February 2018. https://www.gov.uk/guidance/government-cloud-first-policy.

xxii. Hinshelwood, Martin. 'Government Cloud First Policy'. Martin Hinshelwood - naked Agility Ltd, 10 May 2017. https://nkdagility.com/government-cloud-first-policy/.

xxiii. 'iGA_Cloud-First_Policy_V1.0.pdf'. Accessed 3 March 2018. http://www.nea.gov.bh/Attachments/iGA_Cloud-First_Policy_V1.0.pdf.

xxiv. 'Information Security Guideline 2011.pdf'. Accessed 19 February 2018.
http://www.lssa.org.za/upload/documents/Information%20Security%20Guideline%202011.pdf xxv.

http://www.lssa.org.za/upload/documents/Information%20Security%20Guideline%202011.pdf. xxvi.

'Information Security Guideline 2011.pdf'. Accessed 19 February 2018.

http://www.lssa.org.za/upload/documents/Information%20Security%20Guideline%202011.pdf.

xxvii. 'ISACA-Guiding-Principles.pdf'. Accessed 4 March 2018. http://www.eurogeography.eu/SoC/sofia-workshop/SoC-implementation/ISACA-GuidingPrinciples.pdf.

xxviii. 'ISO/IEC 27017 Cloud Security'. Accessed 19 February 2018. http://webcache.googleusercontent.com/search?q=cache:WjZv6j2EG88J:www.iso27001security.com/html/27017.html+&cd=1&hl=en&ct=clnk&gl=za.

xxix. 'IT Contro Objectives for Cloud Computing.pdf'. Accessed 3 March 2018. https://www.isaca.org/chapters2/kampala/newsandannouncements/Documents/IT%20contro%20objectives%20for%20Cloud%20computing.pdf.

xxx. 'nistspecialpublication800-145.pdf'. Accessed 15 February 2018. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.

xxxi. 'POV_SevenPillarsforBecomingaDigitalGovernmentOrganization.pdf'. Accessed 17 February 2018. http://assets.unisys.com/Documents/Global/POVPapers/POV_SevenPillarsforBecomingaDigitalGovernmentOrganization.pdf.

xxxii. Secretariat, Treasury Board of Canada, and Treasury Board of Canada Secretariat. 'Government of Canada Cloud Adoption Strategy'. Guidance. aem, 29 June 2016. https://www.canada.ca/en/treasury-board-secretariat/services/information-technology/cloudcomputing/government-canada-cloud-adoption-strategy.html.

xxxiii. 'Why Agencies Must Use Cloud Services | ICT.govt.nz'. Accessed 15 February 2018. https://www.ict.govt.nz/guidance-and-resources/using-cloud-services/why-agencies-must-usecloud-services/.