the dpsa

Department:
Public Service and Administration
REPUBLIC OF SOUTH AFRICA

Private Bag X916, PRETORIA, 0001 Tel: (012) 336 1000, Fax: (012) 326 7802
Private Bag X9148, CAPE TOWN, 8000 Tel: (021) 467 5120, Fax:(021) 467 5484

Enquiries : Ayanda Nkundla
Tel No. : (012) 336 1250 / 061 442 0471
Email : ayanda.nkundla@dpsa.gov.za

TO ALL HEADS OF NATIONAL AND PROVINCIAL DEPARTMENTS

CIRCULAR NO. 01 OF 2022

PUBLIC SERVICE CLOUD COMPUTING DETERMINATION AND DIRECTIVE AWARENESS

1. The Minister for Public Service and Administration has approved the Public Service Cloud Computing Determination and Directive (Attached) for implementation by the departments. The Determination and Directive is issued in terms of section 3(1) (f) (g) & (i) of Public Service Act, 1994.

2. The purpose of the Determination and Directive is to provide clear guidance to Public Service departments on adopting and using Cloud Computing services and technologies.

3. The prescripts set out in the Determination and Directive must be applied to all Cloud Services where Government data is either stored and or processed.

MS YOLISWA MAKHASI
DIRECTOR-GENERAL MINISTER FOR THE PUBLIC SERVICE AND ADMINISTRATION
DATE: 02/02/2022

Staatsdiens en Administrasie • Ditirelo tsa Puso le Tsamaiso • Ditshebeletso tsa Mmušo le Tsamaiso • uMnyango wemiSebenzi kaHulumeni nokuPhata
Muhasho wa Tshumelo ya Muvuso na Vhulanguli • Kgoro ya Ditirelo tša Mmušo • Ndzanwulo ya Vutirela-Mfumo na Valawuri
LiTiko le Tebasebenti bahulumende nekuPhatsa • Isebe leNkonzo ka Rhulumente noLawulo • UmNyango wemiSebenzi ka Rhulumende nokuPhata

DETERMINATION AND DIRECTIVE ON THE USAGE OF CLOUD COMPUTING SERVICES IN THE PUBLIC SERVICE

TABLE OF CONTENTS

DEFINITIONS

TERM	DEFINITION
ACT	Public Service Act, 1994
BIG DATA	Refers to data that is so large, fast or complex that it's difficult or impossible to process using traditional methods
BUSINESS CASE	A business case is a document where a proposed action is presented and coherently supported with detailed reasoning and expected net benefits for the business.
CLOUD WORKLOAD	Is a specific application, service, capability or a specific amount of work that can be run on a cloud resource. Virtual machines, databases, containers, Hadoop nodes and applications are all considered cloud workloads.
CONFIDENTIAL DATA	Access to confidential data requires specific authorization and/or clearance. Types of confidential data might include Social Security numbers, cardholder data, M&A documents, and more. Usually, confidential data is protected by laws like HIPAA and the PCI DSS.
CSP	Cloud service provider: A third-party company offering a cloud-based platform, infrastructure, application, or storage services.
DATA CLASSIFICATION	Refers to a process of organising data by relevant categories so that it may be used and protected more efficiently.
DATA MINING	Data mining is defined as a process used to extract usable data from a larger set of any raw data. It implies analysing data patterns in large batches of data using one or more software.
DATA PROCESSING	Data processing occurs when data is collected and translated into usable information. Usually performed by a data scientist or team of data scientists, it is important for data processing to be done correctly as not to negatively affect the end product, or data output.
DATA RESIDENCY	Refers to the physical or geographic location of an organization's data or information.
DATA SECURITY SOLUTIONS	Work by providing visibility and security at the same time
DATA SOVEREIGNTY	Describes the legal principle that information (generally in electronic form) is regulated or governed by the legal regime of the country in which that data resides.
DEPARTMENT	National department, a National government component, the Office of a Premier, a Provincial department or a provincial government component.
DETERMINATION AND DIRECTIVE	The Determination to provide clear guidance on the adoption and use of cloud computing in the public service and the Directive on numerous issues to be considered by departments before, during and after acquiring cloud-based computing services.
DPSA	Department of Public Service and Administration
eGSIM	eGovernment Service and Information Management
HEAD OF DEPARTMENT(HOD)	The incumbent of a post mentioned in column 2 of Schedule 1, 2 or 3 and it includes any employee acting in such post.
IaaS	Infrastructure as a service: is a cloud computing offering in which a vendor provides users access to computing resources such as storage, networking, and servers.
ICT	Information and communication technology refers to all communication technologies.

IP	Intellectual property refers to creations of the mind, such as inventions; literary and artistic works; designs; and symbols, names and images used in commerce.
ISO	International Organization for Standardization
IT	Information technology is the use of any computers, storage, networking and other physical devices, infrastructure and processes to create, process, store, secure and exchange all forms of electronic data.
MISS	Minimum Information Security Standards, data and information classification
MPSA	Minister for the Public Service and Administration
MSP	Managed service provider
NIST	The National Institute of Standards and Technology
OPEN DATA	Means data that is made freely available to everyone for use, re-use and republishing as they wish, subject to ensuring the protection of privacy, confidentiality and security in line with the Constitution.
OPEN DATA PRINCIPLES	Government data shall be considered open if it is made public in a way that complies with the principles: Complete; Primary; Timely; Accessible; Machine processable; Non-discriminatory; Non-proprietary; License-free.
PaaS	Platform as a service is a service provider that offers access to a cloud-based environment in which users can build and deliver applications.
PERSONAL INFORMATION	Means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person.
PSR	The Public Service Regulations , 1996
PUBLIC DATA	This type of data is freely accessible to the public (i.e. all employees/company personnel). It can be freely used, reused, and redistributed without repercussions. An example might be first and last names, job descriptions, or press releases.
RACI	Responsible, accountable, consulted, informed
SaaS	Software as a service is a service provider that delivers software and applications through the internet.
SECRET DATA	The classification level applied to information the unauthorized disclosure of which reasonably could be expected to cause serious damage to national security that the original classification is able to identify or describe.
SLA	Service level agreement defines the level of service you expect from a vendor, laying out the metrics by which service is measured, as well as remedies or penalties should agree-on service levels not be achieved.
TCO	Total cost of ownership is the metric that organizations use to quantify and measure cloud adoption success.

1. INTRODUCTION

1.1. Rapid advancements in information and communication technology have made it difficult for Government departments to keep up and or sustain investment in this area. This has further ensured that the required and appropriate skills remain concentrated outside departments and or the public sector in general.

1.2. Cloud computing services can provide government departments with access to on-demand ICT hardware and software resources over the Internet. These include ICT resources, such as computing power, data storage capacity, software services and operating system functionality. These resources run on computer servers, storage devices, and networking equipment located in physical data centers operated by a cloud service provider (CSP). The service provider is responsible for the security, maintenance, and backup of the hardware, software, and data stored in these facilities, freeing up the department to focus on its core service delivery functions.

1.3. The economic efficiencies, privacy and information security concerns, environmental impact (carbon emissions) issues associated with technological practices as well as the general opportunities associated with technological developments particularly in the area of cloud computing services have further prompted the issuing of this determination and directive.

2. PURPOSE

2.1. The purpose of this Determination and Directive is to provide clear guidance on the adoption and use of cloud computing services in the public service.

3. AUTHORISATION

3.1. This Determination and Directive is issued by the MPSA in terms of section 3(1) (f) (g) & (i) of Public Service Act, 1994.

4. SCOPE OF APPLICATION

4.1. This Determination and Directive applies to all departments and its employees employed in terms of the Act and the members of the services only in so far as the provisions of the Determination and Directive are not contrary to the laws governing their employment.

4.2. Furthermore, the prescripts set out in this determination and directive must be applied to all cloud services where Government data is either stored and or processed.

5. Regulatory Framework (provides the context within which the Determination And Directive exists)

5.1. Constitution of the Republic of South Africa, 1996.

5.2. Public Service Act, 1994, Section 3(1) (f) (g) & (i).

5.3. The Protection of Personal Information Act 4 of 2013(POPI), Section 72.

5.4. Promotion of Access to Information Act 2 of 2000 (PAIA), Section 63-66.

6. Implementation Of The Determination And Directive

6.1. The prescripts set out herein must be applied to every Cloud service where government data will either be stored and or processed before implementing the cloud service.

6.2. Where a department had implemented a cloud solution before the approval date of this Directive, the Head of Department must ensure that a risk assessment is conducted and a risk assessment report is tabled at the departmental risk committee.

6.3. The Head of Department must ensure that all requirements of this determination and directive are met within 6 months of the approval and publication of this determination and directive.

7. Non-Compliance Management

7.1. Failure to comply with this Determination and Directive will be dealt with in line with the provisions of the Public Service Act, 1994, section 16A and 16B.

8. Date Of Implementation

8.1. This Determination and Directive shall come into effect on the date of signature by the MPSA.

9. Provisions On The Usage Of Cloud Computing Services

There are numerous provisions to be considered by departments before, during, and after acquiring cloud-based computing services. The following points outline the provisions:

9.1. What is cloud computing?

Cloud computing is a model for enabling 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. This cloud model promotes availability and is composed of **three service models** and **four deployment models**.

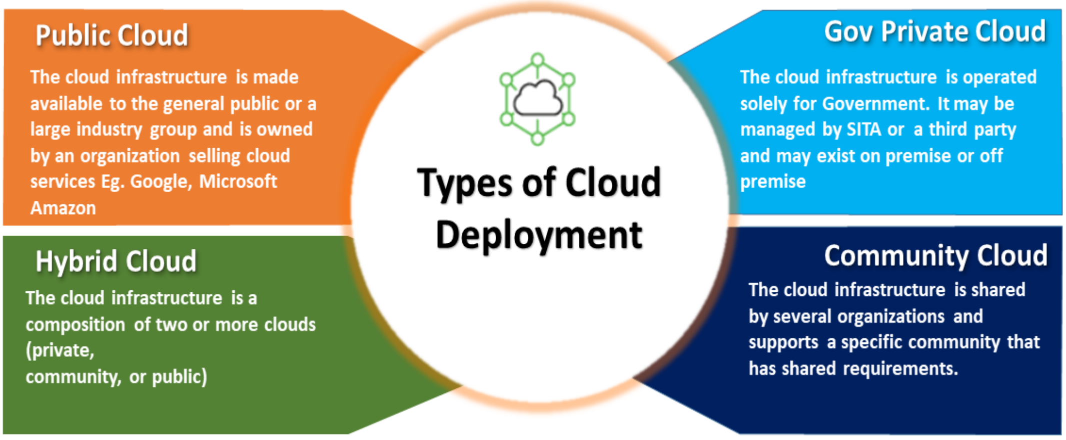
Public Cloud
The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services Eg. Google, Microsoft Amazon
Types of Cloud Deployment
Gov Private Cloud
The cloud infrastructure is operated solely for Government. It may be managed by SITA or a third party and may exist on premise or off premise
Hybrid Cloud
The cloud infrastructure is a composition of two or more clouds (private, community, or public)
Community Cloud
The cloud infrastructure is shared by several organizations and supports a specific community that has shared requirements.

Figure 1. Cloud Deployment Models adapted from NIST

Cloud Service Models

Software as a Service (SaaS): The capability provided to a department is to use the provider's applications running on a cloud infrastructure. The applications are accessible through a web browser (e.g. Gmail). The department does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities.

Platform as a Service (PaaS): Departments develop applications using the Cloud Service provider's hosted hardware and software platforms. The department 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.

Infrastructure as a Service (IaaS): The capability provided to the department is to provision processing, storage, networks, and other fundamental computing resources where the department is able to deploy and run arbitrary software, which can include operating systems and applications. The department 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).

9.2. GENERAL CLOUD CONSIDERATIONS

9.2.1. The Head of Department must ensure that Cloud Services are the first option explored before any on-premise infrastructure investment is made. This option must be fit for purpose, and preference (not exclusive use) must be given to private government cloud where the capability exists.

9.2.2. The Head of Department must ensure that the proposed cloud-based computing services and/or solutions are **fit-for-purpose** and **appropriate** for the delivery of the respective department processes. This must be applied to all cloud services, whether long-term or short-term, and care should be taken to only procure services when they are ready to be consumed to avoid fruitless and wasteful expenditure.

9.2.3. The Head of Department must ensure that the proper procurement processes concerning the procurement of ICT goods and services/Cloud are followed.

9.2.4. The Head of Department must ensure that scaling up of cloud services is based on operational requirements, rather than purchasing upfront and not utilizing until the operational need arises.

9.3. BEFORE ACQUIRING AND IMPLEMENTING CLOUD SERVICES

9.3.1. The Head of Department must ensure that **all data** is **classified** according to the classification system prescribed in the Minimum Information Security Standards (MISS).

9.3.2. The Head of Department must, as far as practically possible, **avoid** moving data classified as **“Secret"** or **“Top Secret**”, to the **Public, Hybrid or Community Clouds.**

9.3.3. The Head of Department must as far as practically possible, ensure that data that is intended for general public consumption, such as data hosted on Departmental public-facing websites, is moved to a Public Cloud.

9.3.4. The Head of Department must ensure that data always resides within the borders of South Africa. Where such is not practically possible, the Head of Departments must ensure that provisions of section 72 of the POPI Act are complied with.

9.3.5. The Head of Department is **accountable** for managing the risks to the Department even concerning services provided by service providers/contractors.

9.3.6. The Head of Department must ensure that a comprehensive **Risk assessment** is undertaken for each cloud service that the Department intends to utilise. The details of the risk assessment must be captured in the relevant business case and presented to the Department Risk Committee.

9.3.7. The Head of Department must ensure that a Cloud Readiness Assessment is conducted **before** the decision is made to move to cloud-based computing services. The Cloud Readiness Assessment Checklist *(Appendix A)* can be used to guide departments.

9.3.8. The Head of Department must ensure that a **Business Case** is developed. The Business Case must include at a minimum:

a) The scope of the Cloud Services required;

b) The budget over the short, medium and long term;

c) A calculation of the Total Cost of Ownership over the medium and long term;

d) The Human resource skills required to support the cloud services environment;

e) The infrastructure required to enable the proper operation of the cloud service (Broadband connectivity etc);

f) The intended benefit to the department through the use of the cloud service.

g) The detailed outcome of the Risk Assessment, a summary of the key risks, and the recommendations for mitigation.

9.3.9. The Head of Department must ensure that the **Business Case is approved before** the Cloud Services are consumed, and reviewed at regular intervals.

9.3.10. The Head of Department must ensure that a **valid contract** exists between the Department and the CSP before utilising a cloud service.

9.3.11. At a minimum the contract must:

a) Explicitly state that the department is the owner of all rights, title, and interest in the data and that all data will be maintained, backed up and secured until returned on termination of the agreement (unless other provisions are made for the migration, transfer or destruction of the data).

b) State that data processing (mining) shall be carried out in a manner provided for by the POPI Act and shall be authorized by the Department.

c) Identify the actual geographic locations where data storage and processing will occur.

d) Confirm the jurisdiction which governs the operation of the contract.

e) Confine data storage and processing to specified locations where the regulatory framework and technical infrastructure allow the department to maintain adequate control over the data.

f) Make provisions for the safe return/transfer of data should the cloud service provider be the subject of a takeover.

g) Specify what will happen to the data, applications, infrastructure, etc., (e.g. transfer to a new provider, returned to the department, permanently deleted) once the Contract ends.

h) Define contract provisions relating to the migration of data on termination of the contract (i.e. CSP takes full responsibility for data migration and or who plays what role during data migration).

9.3.12. The Head of Department may enter into a medium-term contract (that is, contract period of more than 3 years but less than 5 years) for cloud services. The Head of Department must ensure that such a medium-term contract makes provisions for early termination and must agree at the time of contracting on the method of calculation for damages, should damages be applicable. In the event that a Department has entered into a medium-term contract but wishes to terminate such a contract prior to its expiry date, the Head of Department must ensure that there are no damages for early termination payable by the Department or ensure that it is aware of any potential damages that may flow for early termination.

9.4. DURING CLOUD SERVICE CONSUMPTION

9.4.1. The Head of Department must ensure the security of the data in line with the existing departmental information security policy.

9.4.2. The Head of Department must ensure that access rights to data stored or processed in the Cloud are regularly reviewed.

9.4.3. Cloud Service Subscription levels can be scalable up or down according to demand, resulting in variable costs. The Head of Department must ensure that officials are not able to scale up cloud services without proper authorisation.

9.4.4. The Head of Department must ensure that an inventory of Assets (Data or applications) is developed and maintained during the contract period.

9.4.5. The Head of Department must ensure that the department's Business Continuity plans are updated following the implementation of the cloud service and ensure that the department conducts regular business continuity testing.

9.4.6. The Head of Department must ensure that mechanisms exist to backup departmental data. Backups of data must be regularly reviewed to ensure that the risk of data loss is minimised.

9.5. CLOUD SERVICE TERMINATION

9.5.1. At the termination of the agreement with a CSP, the Head of Department must ensure that **all data** and/or **applications** that belong to the Department are transferred to a new provider, returned to the department and/or permanently deleted.

9.6. GENERAL

9.6.1. Departments must submit copies of the following to the DPSA before acquiring and deploying cloud services :

9.6.1.1. The approved Business Case aligned to the prescripts set out in 9.3.8 above.

9.6.1.2. Evidence of having complied with the requirements set out in 9.3.6 above.

APPROVED BY THE MINISTER FOR PUBLIC SERVICE AND ADMINISTRATION

9.6. GENERAL

9.6.1. Departments must submit copies of the following to the DPSA before acquiring and deploying cloud services :

9.6.1.1. The approved Business Case aligned to the prescripts set out in 9.3.8 above.

9.6.1.2. Evidence of having complied with the requirements set out in 9.3.6 above.

APPROVED BY THE MINISTER FOR PUBLIC SERVICE AND ADMINISTRATION

MS AYANDA DLODLO, MP
MINISTER FOR THE PUBLIC SERVICE AND ADMINISTRATION
DATE: 14\01\2022

10. Cloud Computing Policy. Office of the Chief Information Officer, 31 October 2016. Available at: https://ocio.commerce.gov/page/cloud-computing-policy.
11. Cloud Policy. Office of the Government Chief Information Officer (blog), 24 May 2016. Available at: https://gcio.wa.gov.au/2016/05/24/cloud-policy-2/.
12. Cloud-Computing-Transforming-the-Government-of-Canada-for-the-Digital-Economy.pdf. Available at: http://itac.ca/wp-content/uploads/2015/08/Cloud-Computing-Transforming-the-Government-of-Canada-for-the-Digital-Economy.pdf [Accessed 15 February 2018].
13. LSSA – An introduction to cloud computing, v2 September 2014.pdf. Available at: http://www.lssa.org.za/upload/documents/LSSA%20Introduction%20to%20cloud%20computing%20v2%20September%202014.pdf.
14. Cloud Security Guidance IBM Recommendations for the Implementation of Cloud Security. Available at: http://www.redbooks.ibm.com/abstracts/redp4614.html?Open.
15. Are You Rather a SI, ISV, MSP, VAR or a Reseller? Available at: https://ormuco.com/blog/cloud-provider-rather-si-isv-msp-var-reseller.
16. Multi-cloud strategy: Pros, cons and tips. Available at: https://www.cio.com/article/3441856/multi-cloud-strategy-pros-cons-and-tips.html#:~:text=Multi%2Dcloud%20defined&text=Gartner%20has%20a%20more%20formal,says%20Gartner%20analyst%20David%20Smith.
17. How to Avoid Cloud Vendor Lock-in with Four Best Practices. Available at: precisely.com | 877 700 0970.
18. Gartner, Inc. (2020). Decision Model to Optimize Risk, Value and Cost, ID: G00466040. Gartner, Inc.

19. How TCO Benefits Make Cloud Computing a No-Brainer for Many SMBs and Mid-Market Enterprises, https://knowledgehubmedia.com/tco-benefits-cloud-computing-nobrainer-smbs-midmarket-enterprises/
20. Section 72 (Transfers of personal information outside Republic) of the Protection of Personal Information Act, 2013 (Act No. 4 of 2013). https://popia.co.za/section-72-transfers-of-personal-information-outside-republic/
21. SaaS vs PaaS vs SaaS Enter the Ecommerce Vernacular: What You Need to Know, Examples & More, https://www.bigcommerce.com/blog/saas-vs-paas-vs-iaas/
22. Big Data, https://www.sas.com/en_za/insights/big-data/what-is-big-data.html
23. Open Government Data Principles, https://public.resource.org/8_principles.html
24. 4 Ways to Classify Data , https://kirkpatrickprice.com/blog/classifying-data/
25. Cloud Workloads, https://www.delltechnologies.com/en-us/learn/cloud/cloud-workloads.htm#:~:text=A%20cloud%20workload%20is%20a,are%20all%20considered%20cloud%20workloads.
26. What is Intellectual Property?, https://www.wipo.int/about-ip/en/
27. What is data processing?; https://www.talend.com/resources/what-is-data-processing/
28. Data Mining, https://economictimes.indiatimes.com/definition/data-mining
29. What is a Business Case?, https://www.myaccountingcourse.com/accounting-dictionary/business-case
30. IMB Cloud Education , https://www.ibm.com/za-en/cloud/learn/iaas-paas-saas
31. What is an SLA? Best practices for service-level agreements, https://www.cio.com/article/2438284/outsourcing-sla-definitions-and-solutions.html

32. The total cost of ownership for Cloud, https://www.ibm.com/garage/method/practices/discover/total-cost-ownership-cloud/

33. Information technology, https://www.google.com/search?q=what+is+information+technology+definition&sxsrf=ALeKk007SzYrqrtXb9rm4X_iM9yPpCcmhQ%3A1625202893420&ei=zaDeYOWRGeTC8gKE9YuADQ&oq=what+is+Information+technology+de&gs_lcp=Cgdnd3Mtd2l6EAEYATICCAAyAggAMgIIADICCAAyAggAMgIIADIGCAAQFhAeMgYIABAWEB4yBggAEBYQHjIGCAAQFhAeOgcIABBHELADSgQIQRgAUMSCBljwiwZgg58GaAFwAngAgAHFBIgBrgySAQkyLTEuMS4xLjGYAQCgAQGqAQdnd3Mtd2l6yAEIwAEB&sclient=gws-wiz

34. ICT Definition, https://techterms.com/definition/ict

APPENDIX A – CLOUD READINESS ASSESSMENT CHECKLIST

Moving your IT systems to the Cloud offers many benefits including reduced costs, flexibility, increased efficiency, and in many cases, better performance and security. SaaS, PaaS, and IaaS all present several key differences in terms of security, performance, reliability, and management. This guide will help you assess your readiness to transition to cloud computing and identify any areas that need to be re-evaluated.

After reading through these checklists and determining your department's current cloud computing readiness, you'll have the tools you need to start preparing for your transition.

1. WILL MY DEPARTMENT BENEFIT FROM TRANSITIONING SERVICES TO THE CLOUD?

Although most departments will benefit from transitioning some or all of their IT services into the Cloud, not all will. Start with these questions to help determine whether your department should transition to cloud computing.

What is your department's current IT infrastructure expenditure?	
Is Cloud computing likely to reduce costs?	
How much does usage fluctuate over time?	
Would your department benefit from a more elastic solution?	
Does your department need to add applications or functionality but cannot make a large capital expenditure for additional IT infrastructure?	

Is your IT department able to effectively provide maintenance and security, and maximise efficiency for your IT infrastructure?	
Will your department benefit strategically or financially from a reduction in IT focus?	
Does your department have a BCM (Business Continuity Management Planning (BCM)) in place?	
Does your department need to secure sensitive data on proprietary servers?	
Will the increased accessibility of the Cloud improve your company's performance?	

Table 1

Use these questions to get a brief overview of your company's current Cloud Computing readiness and to identify areas that need to be addressed.

What is the extent of your department's current IT usage?	
How quickly would you like to transition to the Cloud?	
Have you prepared a cost-benefit analysis?	
Do you have a team capable of managing the transition?	
Have you classified your data?	
Are you prepared to transition data securely?	
Do you plan to use IaaS, PaaS, or SaaS?	
Will the increased accessibility of the Cloud improve your department's performance?	

Table 2

Security is a key concern in using Cloud Computing technology. This checklist will help you identify key considerations for safely transitioning and securing data.

Outlining the security plan

Have you made an outline of your top security goals and concerns?	
What types of assets will be managed by the system?	
Have key assets been listed and rated based on their sensitivity?	
How assets are currently managed and how will this change when transitioned to the Cloud?	
Has the right cloud delivery model been assigned based on the assets' sensitivity?	
Has the network topology been mapped?	

Table 3

Enumerating safeguards and vulnerabilities

Have the security controls been enumerated, verified, and evaluated?	
Will all sensitive data stored in the Cloud be encrypted?	
Are remote connections to the Cloud properly encrypted?	
Have you evaluated the security risk of the server's physical location?	
Are the servers housed in guarded and locked rooms?	
Have all vulnerabilities been identified and addressed?	
Are staff properly trained on the new security protocols?	

Table 4

Complying with regulations

Have you reviewed your cloud service provider's security policies?	
Do they comply with POPI Act, PAIA, ECT Act or other regulations your data may be subject to?	
Have you drafted any contracts or agreements with your cloud service provider to bridge compliance gaps?	

Table 5

2. PERSONNEL CONSIDERATIONS

A department's staff must be properly prepared for the cloud computing transition to ensure that it does not interfere negatively with day-to-day operations. Use these questions to make sure your team is ready.

Preparing your cloud adoption team

Who will be heading the effort to move systems to the Cloud?	
Has a team been assembled to plan and execute cloud adoption?	
Who are the key human resource assets for the plan?	
Is management in full support of the adoption strategy?	
Do you need to bring on additional staff or consultants to help adopt Cloud computing technology?	

Table 6

Training the staff

How will using cloud computing affect the everyday operations of the department?	
Will staff need to learn new skills to function after the transition?	
Has a training plan been drafted?	
Is there a team in place to train staff on the new technology?	
Are staff aware of any changes to security protocol that cloud adoption will bring?	

Table 7

Reconfiguring the ICT department

Do the current IT employees have the expertise to properly maintain the new systems?	
Will this change necessitate hiring additional staff?	
Will this change require that certain staff members be redeployed?	

Table 8

3. LOCATION CONSIDERATIONS

Moving to cloud computing means your servers will be physically located in another place. This can have ramifications for your IT infrastructure's speed, security and reliability.

Where is the cloud service provider located?	
Is the location near your user base (customers or staff)?	
Will speed be adversely affected by the server's location?	
Can you visit the data centre where your Cloud will be hosted?	

Table 9

4. RELIABILITY

Ensuring the reliability of your IT infrastructure is a critical step in transitioning to cloud computing. Make sure the Cloud will be as reliable as in-house IT infrastructure by going through the following checklist.

Assessing the cloud provider's reliability

Does your cloud service provider have a reputation for reliability?	
How long have they been operational?	
What is their average uptime over the past three years?	
Do they have a reliability guarantee?	
Do they use reliability safeguards like backup power sources and redundant servers?	
Will they promptly inform you of any planned or unplanned outages?	
Is the cloud service provider regularly assessed by a third-party auditor?	
Does the cloud provider offer comprehensive support?	
Will your in-house IT team be responsible for support?	

Table 10

Making a continuity plan

Do you have a backup system if the Cloud goes down for any reason?	
Is there a contingency plan to continue mission-critical functions if the Cloud cannot be accessed?	
Will you store copies of your data in-house?	
Is your data safe-harbored with a third party who can protect against data loss?	

Table 11

5. PERFORMANCE CONSIDERATIONS

One of the primary concerns when moving to the Cloud is how it will affect performance. In many cases speed can be improved when using cloud computing solutions. Answer the following questions to make sure your performance is not adversely affected by a transition to the Cloud.

Is the cloud provider's hardware sufficient to handle your workload?	
Will you be using the public or private Cloud?	
Will you be using dedicated hardware?	
What steps will the cloud provider take to ensure consistent performance?	
Does the cloud provider make any performance guarantees?	
Will the cloud solution offer the same or better performance compared to an in-house solution?	

Table 12

6. FINANCIAL CONSIDERATIONS

Most departments can save considerably when moving systems and applications into the Cloud. Use this checklist to help you consider the total financial impact of the move.

Cloud provider fees

What are the initial set-up fees?	

How complex is the pricing model? Is it transparent?	
Can the provider increase fees at regular intervals?	

Table 13

Migration costs

Will there be additional human resource costs associated with the transition?	
Will there be additional hardware costs associated with the transition?	
What will be the cost of an outage during migration?	

Table 14

Planning the financial impact

Is your department moving to the Cloud to take advantage of reduced overhead?	
How will the transition costs and provider fees be offset by potential savings?	
How will moving to the Cloud affect your IT costs?	
Have you drafted a cost-benefit analysis for the move?	
How will your department finance the transition?	
What to do with your IT hardware that has not reached end of life?	

Table 15

7. LEGAL CONSIDERATIONS

Although often overlooked, legal considerations are extremely important when moving to the Cloud. Use this checklist to make sure the transition is made legally.

Understanding the legal agreement with your cloud provider

Have you read the cloud provider’s standard contract and or Service level agreement (SLA)?	
How does the contract affect your data’s property rights?	
Do you have the full legal rights to the data you will be moving to the Cloud?	
Is the cloud provider’s privacy policy compatible with your department’s?	
Does the cloud provider have the right to access your data?	
If hosted in another country, which law applies to you?	

Table 16

Complying with regulations

Is your data subject to any government regulations?	
Does the cloud provider comply with those regulations?	
Who is legally responsible for your data’s security?	
Are you able to audit your cloud provider’s compliance with regulations?	

Table 17

Terminating the service

What are the terms of cancellation?	
What will happen to your data after the service is terminated?	

Table 18