

## **CLOUD COMPUTING GUIDELINE DOCUMENT**

### **Contents**

|                                                       |   |
|-------------------------------------------------------|---|
| 1. EXECUTIVE SUMMARY .....                            | 2 |
| 2. INTRODUCTION .....                                 | 2 |
| 3. PURPOSE .....                                      | 3 |
| 4. RELEVANT LEGISLATION, STANDARDS and POLICIES ..... | 3 |
| 5. CLOUD COMPUTING DEFINITION AND BASELINE .....      | 5 |
| 6. NERSA CLOUD COMPUTING GUIDELINES .....             | 8 |

## **1. EXECUTIVE SUMMARY**

A surge in remote working has put the focus on Cloud Computing (CC) to support work-from-home requirements, maintain business continuity and build business resilience.

In 2020 an International Data Group Incorporated (IDG) survey reported that 81% respondents are already using computing infrastructure or having applications in the cloud compared to 73% in 2018. Another 12% plan to adopt cloud-based applications in the next 12 months and 6% plan to do so in the next 1 to 3 years. Cloud adoption has reached more than two-thirds in every industry, though adoption is higher in education (88%), manufacturing (87%), and healthcare (86%), than in financial services (75%) and government/non-profit (71%).

“By 2022, 75% of organizations that implemented work-from-home policies for their workforce during COVID-19 will retain the remote working options for their employees,” said Ed Anderson, Distinguished VP Analyst, during his presentation at virtual Gartner IT Symposium/Xpo® 2020. “Cloud adoption will continue to accelerate as key workloads are needed to support remote workers and maintain data center operations.”

In February 2022 the Department of Public Service and Administration (DPSA) published the “DETERMINATION AND DIRECTIVE ON THE USAGE OF CLOUD COMPUTING SERVICE IN THE PUBLIC SERVICE” document (Annexure A). The purpose of this document is stated as ‘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’.

The COVID-19 disruption, forced NERSA to also implement Cloud Computing (CC). In June 2020 NERSA implemented Ms Teams to facilitate virtual meetings. Teams is a collaboration platform that unifies chat, voice, video and file sharing. It's designed to be used by local, remote and distributed work groups. Irrespective the rich features within Teams at NERSA the application is only used for virtual meetings.

In a post-pandemic world, there will be opportunity to move key workloads to the cloud for the benefits it offers today and to prepare for the next unforeseen disruption. Organisations of all types should sensibly evaluate which CC service model; private, public, community or hybrid suites their line of business. Which Cloud orchestration; software as a service (SaaS), infrastructure as a service (IaaS) or platform as a service (PaaS) best suites which business process. Which workloads can be moved to the cloud environment given aspects of data confidentiality and need for security.

NERSA management will use this document as a guideline to determine which workloads may move to the Cloud as well as which service provider to use given the sensitivity of NERSA data and the strict operating environment.

## **2. INTRODUCTION**

In July 2020, NERSA requested the State Security Agency's guidance on the adoption of cloud computing technology as part of the ICT Strategy of NERSA (Annexure D). The

State Security Agency (SSA) responded to NERSA and indicated that they did not have a legislative directive or minimum security specifications on the usage of cloud technology. However, SSA was in the process of developing cloud computing guidelines and had in the interim, recommended the following security principles for consideration by NERSA when implementing cloud computing (Annexure E):

- Physical and environment security;
- Business continuity management (in terms of ICT) and incident response;
- Network inventory and configuration management;
- Data encryption;
- Access control, monitoring and logging;
- Network security and monitoring;
- Identity and Access Management;
- Legislative and Regulatory Framework.

### **3. PURPOSE**

At face value the decision to adopt a Cloud strategy seems to be an obvious yes. The Cloud offer benefits of economies of scale, reduced capex, improve access, agility, leverage global workforce and gain access to advanced capabilities. However, on closer inspection it becomes clear that the decision to implement a Cloud solution is not an easy one.

This document will be used as a guideline by NERSA management when faced with the decision of Cloud implementation.

### **4. RELEVANT LEGISLATION, STANDARDS and POLICIES**

- a) Chapter 2: Bill of Rights, Section 32 Access to Information of the Constitution of the Republic of South Africa, 1996;
- b) State Information Technology Agency Act, 1998 (Act 88 of 1998); to provide for the establishment of a company that will provide information technology, information systems and related services to, or on behalf of, participating departments and in regard to these services, act as an agent of the South African Government; and to provide for matters connected therewith
- c) The Protection of Personal Information, 2013 (Act No. 4 of 2013): to promote the protection of personal information processed by public and private bodies, to introduce certain conditions so as to establish minimum requirements for the processing of personal information.

- d) Promotion of Access to Information Act, 2000 (Act No. 2 of 2000): the constitutional right of access to any information held by the State and any information that is held by another person and that is required for the exercise or protection of any rights; and to provide for matters connected therewith.
- e) Critical Infrastructure Protection Act, 2019 (Act No. 8 of 2019) to provide for measures to be put in place for the protection, safeguarding and resilience of critical infrastructure;
- f) Electronic Communications Security (PTY) Ltd Act. 2002 (Act No. 68. 2002): to ensure that critical electronic communications are protected and secure.
- g) The Consumer Protection Act No. 68 of 2008: spells out the rights of the Consumer and the responsibilities of the supplier;
- h) 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;
- i) Public Service Act, 1994 (PSA) and Public Service Regulations (PSR), 2016 as amended;
- j) Chapter 5: Public Administration Management Act 2014, section 14 Use of Information and Communication Technologies in Public Administration;
- k) Electronic Communications and Transaction Act 2002 (ECTA) Provides for identification, protection and management of critical data and critical databases. It further provides that these databases should be declared by the Minister for protection of National Security or economic and social wellbeing of the country.
- l) Regulation of Interception of Communications and Provision of Communication-Related Information Act: to regulate the interception of certain communications, the monitoring of certain signals and radio frequency spectrums and the provision of certain communication-related information.
- m) Protection of Information Act, 1982 (Act no 84 of 1982): To provide for the protection from disclosure of certain information; and to provide for matters connected therewith.
- n) Promotion of Administrative Justice Act 3 OF 2000 Act 3 of 2000: the right to administrative action that is lawful, reasonable and procedurally fair and to the right to written reasons for administrative action.

- o) Criminal Procedure Act, 1977 (Act No.51 of 1977): to make provision for procedures and related matters in criminal proceedings
- p) Minimum Information Security Standards: access to classified information should be controlled, encryption devices should be used on electronic equipment that transmits classified information in order to prevent interception by unauthorised people.
- q) Minimum Physical Security Standards: The implementation of physical security measures to deter, delay, detect or prevent unauthorized intrusion to an Institution or Department.
- r) General Data Protection Regulation: rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.
- s) NERSA Security Policy: to support the national interest and NERSA's business objectives by protecting the employees, information, assets of NERSA and assure the continued delivery of services to South African citizens
- t) The draft Public Service Cloud Computing Standard: to facilitate and or stimulate the use of Cloud-based computing services as the technology enabler for the digitally transformed public service.

## **5. CLOUD COMPUTING DEFINITION AND BASELINE**

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

There is a need to distinguish between “cloud services” and “cloud-based services”. Cloud services are utilised (“...on demand at any time, through any access network, using any connected devices that use cloud computing technologies”. Furthermore, cloud services use software and applications that are located on the cloud and not on the users’ own devices. Cloud-based services include mass market applications i.e. social media and webmail offered over the internet, whereby the does not reside on individuals’ devices but is stored remotely in a data centre.

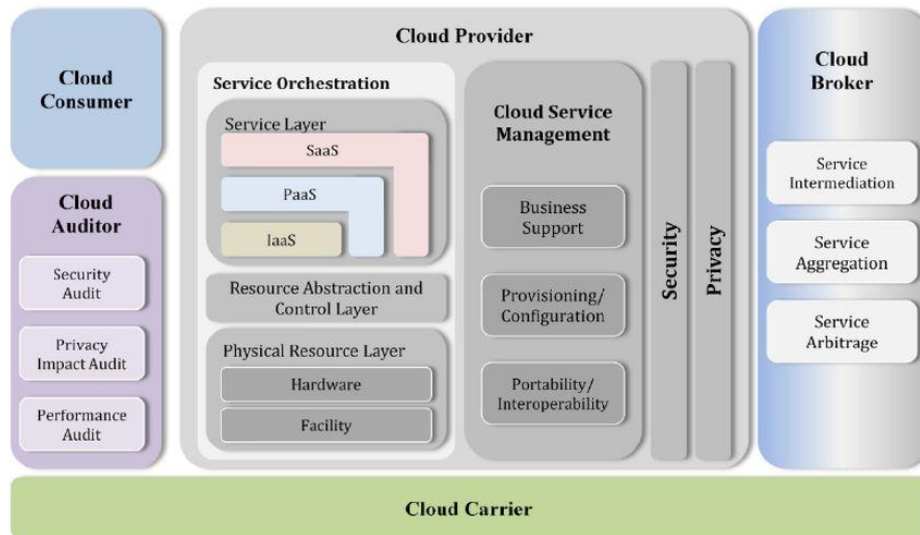
Cloud Computing (CC) is an information and communication system that offers a variety of on-demand services. The term CC does not have a clear definition. The National Institute of Standards and Technology (NIST) defines cloud computing as, “a model of enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and

services) that can be rapidly provisioned and released with minimal management effort, or service-provider interaction”.

Different organisations, create their own specifications. However, most organisations have minimum characteristics that the environment must subscribe to in order to qualify as a CC. Some of these characteristics are: it is virtual, flexible and scalable, open (closed), accessible, safe and available.

In an effort to avoid confusion herewith a basic understanding of some of the terminologies within the CC environment and how NERSA interpret them. Below is the NIST Cloud Computing Conceptual Reference Model.

## Conceptual Reference Model



4/13/2019

NIST Reference Architecture

6

### Cloud Consumer

A person or organisation using CC services. It agrees with the provider in some form of use of its environment, which is usually confirmed by some form of Service Level Agreement (SLA) document.

### Cloud Auditor

An independent entity that can perform control of the CC environment.

### Cloud Provider

Entity that cares about the operation of the entire CC environment that it offers to its users. They manage the entire infrastructure and are responsible the functionality and flawlessness of the whole environment.

#### Cloud Broker

An intermediary, is the entity that controls the use, delivery of services, and the relationship between the consumer and service provider.

#### Cloud Carrier

The Carrier entity is an interface that provides interconnection between other CC environments.

#### Service Orchestration

There are three basic Cloud service models:

- Software as a Service (SaaS)

SaaS get defined as a service category where the user has an application available from the service provider. With this model the user does not manage any CC infrastructure. The term SaaS is often associated with business applications and outsourcing. SaaS applications are normally charged in the form of a user fee.

SaaS is the most visible part of the CC environment from the end user's perspective. To control such an application, the user can use dedicated application, but more popular is using the web interface. Benefits of this category is that the user does not have to install a client application but just a web browser that is already standard on almost every device. Examples of these solutions are Office 365 from Microsoft, storage services such as Google Drive, Dropbox and OneDrive.

Two main disadvantages of this category is security and availability. Some users may have a problem placing company information outside the organisation if the policy does not support it. Availability of data might be compromised if the service provider is not geographically well located.

- Platform as a Service (PaaS)

PaaS get defined as a service category where the user run their applications using the programming language, libraries, services and utilities provided by the service provider. The customer does not manage the infrastructure on which the application is deployed but at the same time it has full administrative access to its application. PaaS offers the consumer with a platform in the CC environment where the consumer can run their own suite of applications or use its own support platform for existing applications.

- Infrastructure as a Service (IaaS)

IaaS get defined as a service category where the consumer has the freedom to create basic computer resources (computing power, storage, networking,...). The user does not manage the infrastructure on which the computer resources are running but has control over everything that runs on it.

IaaS is designed for the more experienced consumer because it requires knowledge of operating system administration. With this type of service, the user manages the entire infrastructure itself, starting with servers, with the operating system, databases and networking.

The CC environment is characterised by the following deployment models:

- Private Cloud

A private cloud is used by one CC customer only. The CC environment can be managed by the customer themselves or by a third-party. The customer can also grant access to their CC environment to other users.

- Community Cloud

A Community Cloud is defined as an infrastructure that is used by a particular community with common interest. Like a private cloud a community cloud can be managed by the community or third-party.

- Public Cloud

A Public Cloud is defined as an infrastructure that is available to the general public. It can be managed by a private organisation, an academic institution, a government institution, or a combination of them.

- Hybrid Cloud

A Hybrid Cloud is defined as an infrastructure that is made up of multiple infrastructures (private, community and public CC). These infrastructures are deployed independently but are also interconnected by technologies that enable data and application portability.

## **6. NERSA CLOUD COMPUTING GUIDELINES**

Given the nature of NERSA's business and the sensitivity of the information in its possession the decision of what information to put on the cloud will not be made by one person or department. The use of cloud services or cloud-based services will be subjected to company approved evaluation processes. At a minimum the evaluation criteria will include:

### **6.1 Before acquiring and implementing cloud computing services.**

- Ensure compliance to the guidelines as received from SSA;

- Ensure that all data is classified according to the according to the classification system prescribed in the Minimum Information Security Standards (MISS);
- As far as practically possible, avoid moving data classified as “Secret” or “Top Secret”, to the Public, Hybrid or Community Clouds;
- As far as practically possible, ensure that data that is intended for general public consumption, such as data hosted on public-facing websites, is moved to a Public Cloud;
- Ensure that data always reside in the borders of South Africa. Where, such is not practically possible, ensure that section provisions of section 72 of the POPI Act are complied with;
- The Head of Department is accountable for managing the risks to NERSA even concerning services provided by service providers/contractors;
- A comprehensive Risk Assessment is undertaken for each cloud service that NERSA intends to use. The details of the Risk Assessment must be captured in the business case and presented to the Audit and Risk Committee;
- Ensure that a Cloud Readiness Assessment is conducted before the decision is made to move to cloud-based computing services;
- Ensure that a Business Case is developed. The Business Case must include at a minimum:
  - The scope of the Cloud Services required;
  - The budget over the short, medium and long term;
  - A calculation of the Total Cost of Ownership over the medium and long term;
  - The Human resource skills required to support the cloud services environment;
  - The infrastructure required to enable the proper operation of the cloud service (Broadband connectivity etc.);
  - The intended benefit to NERSA through the use of the cloud service;
  - The detailed outcome of the Risk Assessment, a summary of the key risks, and the recommendations for mitigation;
- Ensure that the Business Case is approved before the Cloud Services are consumed, and reviewed at regular intervals;
- Ensure that a valid contract exists between NERSA and the Cloud Service Provider (CSP) before utilising a cloud service;
- At a minimum the contract must:
  - Explicitly state that NERSA 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);

- State that data processing (mining) shall be carried out in a manner provided for by the POPI Act and shall be authorized by NERSA;
- Identify the actual geographic locations where data storage and processing will occur;
- Confirm the jurisdiction which governs the operation of the contract;
- Confine data storage and processing to specified locations where the regulatory framework and technical infrastructure allow NERSA to maintain adequate control over the data;
- Make provisions for the safe return/transfer of data should the cloud service provider be the subject of a takeover;
- Specify what will happen to the data, applications, infrastructure, etc., (e.g. transfer to a new provider, returned to NERSA, permanently deleted) once the Contract ends;
- 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).
- May enter into a medium-term contract (that is, contract period of more than 3 years but less than 5 years) for cloud services. NERSA 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 NERSA has entered into a medium-term contract but wishes to terminate such a contract prior to its expiry date, NERSA must ensure that there are no damages for early termination payable or ensure that it is aware of any potential damages that may flow for early termination.

## **6.2 During Cloud Service Consumption.**

- Ensure the security of the data in line with the existing NERSA information security policy;
- Ensure that access rights to data stored or processed in the Cloud are regularly reviewed;
- Cloud Service Subscription levels can be scalable up or down according to demand, resulting in variable costs. NERSA must ensure that officials are not able to scale up cloud services without proper authorization;
- Ensure that an inventory of Assets (Data or applications) is developed and maintained during the contract period;
- Ensure that NERSA's Business Continuity plans are updated following the implementation of the cloud service and ensure that NERSA conducts regular business continuity testing;

- Ensure that mechanisms exist to backup NERSA's data. Backups of data must be regularly reviewed to ensure that the risk of data loss is minimised.

### **6.3 Cloud Service Termination**

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