Eskom	**Standard**	

Title: **Cloud Standard**

Document Identifier:	**240-150139783**
Alternative Reference Number:	
Area of Applicability:	**Eskom Holdings SOC Ltd**
Functional Area:	**Group IT - SEA**
Revision:	**1**
Total Pages:	**66**
Next Review Date:	**May 2022**
Disclosure Classification:	**Controlled Disclosure**

Compiled by	**Functional Responsibility**	**Authorized by**
E de Lange	**M Mokone**	**N Harris**
Chief Enterprise Architect – Strategy Execution and Architecture	**Senior Manager – Strategy Execution and Architecture**	**General Manager – Group IT**
Date: 31 May 2019	Date: 31|08|2019	Date: 6/09/2019

Content

Page

1. INTRODUCTION

Eskom GIT (Group Information Technology) adopted a cloud first IT (Information Technology) strategy that aims to promote the adoption of cloud services by Eskom. The cloud first strategy is supported by a cloud strategy [1] and a cloud policy [2]. The development of a cloud standard for Eskom was recommended to provide guidelines for the adoption of cloud services. This cloud standard depicts a neutral Cloud Reference Architecture and a supporting Cloud Taxonomy for Eskom that is derived from NIST (National Institute of Standard and Technology) [3].

The proposed Eskom Cloud Reference Architecture depicts a technology agnostic architecture that does not stifle innovation and is a generic high-level conceptual model that is effective for discussing Eskom's cloud requirements, structures and operations. The key architecture components related to cloud offerings and cloud services to be considered by Eskom are:

- Cloud service deployment, cloud service orchestration and cloud service management.
- Cloud business support mechanisms.
- Cloud customer management issues (contracts, accounting and pricing).
- Cloud provisioning, cloud configuration, cloud portability, cloud interoperability, cloud security, cloud privacy, cloud connectivity and cloud connectedness.

The Cloud Taxonomy defines the central elements associated with cloud (based on "Cloud Actors") and prescribes how cloud services within Eskom can be managed, provided and orchestrated in a secure manner. The "Cloud Actors" are the following:

- The "Cloud Consumer" – Eskom, the organisation that acquires cloud products or services.
- The "Cloud Provider" – The purveyor of cloud products or services to Eskom. The cloud products or services to be consumed by Eskom are Iaas (Infrastructure as a Service), PaaS (Platform as a Service) and SaaS (Software as a Service).
- The "Cloud Carrier" – Connects Eskom to the "Cloud Provider" and is responsible for transferring data between Eskom and the "Cloud Provider". This role could be fulfilled by Eskom Telecommunications and third party network providers.
- The "Cloud Broker" – The intermediate between Eskom and the "Cloud Provider". This role could be fulfilled by a VNS (Vendor Neutral Site) or Eskom's hardware and facilities.
- The "Cloud Auditor" – Conducts independent performance, security and monitoring as a VAS (Value Added Service) to Eskom. This role could be fulfilled by a CASB (Cloud Access Security Broker) or the Eskom GIT Information Security Department.

The traditional Eskom GIT service delivery model emphasises the procurement, maintenance, operations and support of the GIT hardware and software related infrastructure. This cloud standard aims to enable the Eskom business, represented by the various Eskom Divisional owners, to direct their attention to an innovative cloud IT service creation model. However, it is important to note that cloud products and services should only be considered by Eskom provided that the feasibility, viability and security of the potential cloud product or service are evaluated via the GIT RMO (Results Management Office) process which necessitates the development of a detailed BRS (Business Requirement Specification) and a business case. In many instances

Eskom already has the capabilities to enable cloud, i.e. “Cloud Carrier” (Eskom Telecommunications), “Cloud Provider” (Eskom Data Centre facilities) as well as “Cloud Auditor” capabilities (GIT Information Security platforms), respectively. These capabilities should therefore be considered to realise Eskom’s cloud intent. This should further be supported by considering the following minimum requirements for cloud adoption within Eskom:

- The cloud product or service should be economically viable (the costs should be lower than the traditional Eskom GIT service it replaces). The EVA (Economic Value Add) related to the cloud product or service, should also be positive. The promised economic benefits should be captured in the GIT BRP (Benefits Realisation Plan) and tracked over time.
- The cloud product or service should be technically feasible (provide the desired or improved QoS compared to the traditional GIT service it replaces). This can be managed via a SLA (Service Level Agreement) with the “Cloud Provider”.
- The cloud product or service should adhere to all Eskom security policies, standards and patterns to ensure that Eskom’s data confidentiality and data integrity is not compromised.
- Eskom is a NKP (National Key Point) and therefore a National Critical Information Infrastructure, which requires the protection of its information assets. Eskom’s cloud adoption intent should therefore recognise and adhere to the guidelines prescribed in the National Cybersecurity policy framework for South Africa [5] as well as the “Critical Infrastructure Protection Bill” of the Republic of South Africa [7].
- Privacy is paramount and therefore compliance to the POPIA (Protection of Personal Information Act) [8] as well as compliance to personal data protection legislation by Eskom is critical for cloud adoption. Transferring data cross border is an issue of sovereignty and is a data protection issue. Data sovereignty is the principle that electronic data is regulated by South Africa’s personal data protection regulatory landscape. Personal data protection laws contain data sovereignty principles in that they prevent the transfer of personal data to another country. Effort should therefore be made to comply with lawful personal data transfer related to employees, customers, suppliers and business partners. Eskom should only engage “Cloud Provider’s” whose data servers are located in South Africa and comply to South African personal data protection laws.
- In conclusion, Cloud services should only be considered by Eskom provided that it is lawful and after both asset and data classification is performed.

2. SCOPE

The objective of this cloud standard is to illustrate an overall cloud conceptual model for Eskom, by highlighting a neutral Cloud Reference Architecture and a supporting Cloud Taxonomy that are easy to understand. This will simplify discussions related to cloud within Eskom (how to categorise and compare cloud services, how to facilitate the analysis of candidate standards for security as well as how to provide a view of interoperability, portability and cloud reference implementations). Eskom requires a cloud standard to enjoy a successful cloud service delivery as a cloud standard will provide guidelines that will enable Eskom to consume cloud products and services reliably and securely, without compromising data portability and service interoperability. This cloud standard aims to improve confidence around feasible and viable cloud solutions to Eskom by providing a view on the number of different available cloud options. Identifying and recommending cloud standards and identifying a suitable vendor agnostic Cloud Reference Architecture for Eskom, are the objectives of this cloud standard. The formulation of this cloud standard provides an intermediate reference point from where discussions around cloud services can be formulated.

GWEA (Government-Wide Enterprise Architecture) provides enterprise architecture principles through its ICT (Information and Communication Technology) House of Values and associated TRM (Technology Reference Model), which emphasis lower cost, quantifying economic and technical value, increased productivity, security, interoperability, reduced duplication, economies of scale as well as Digital Inclusion (see Figure 1) [6].

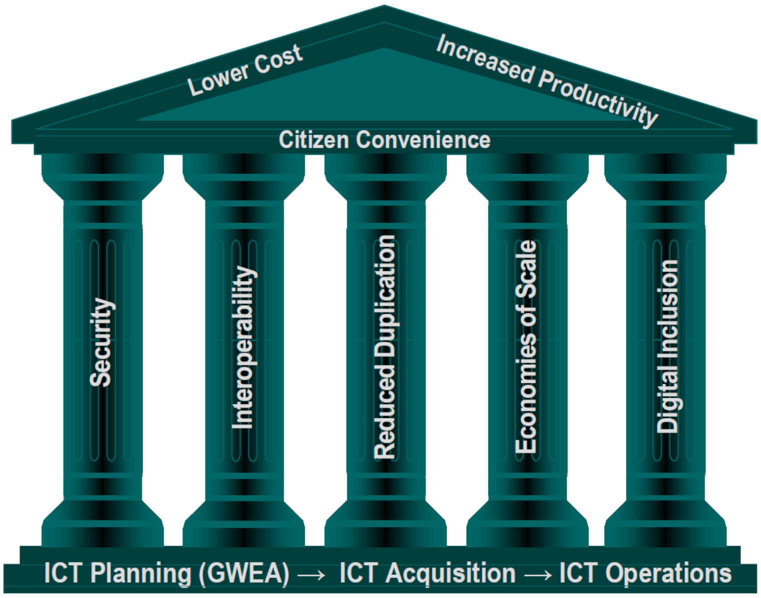
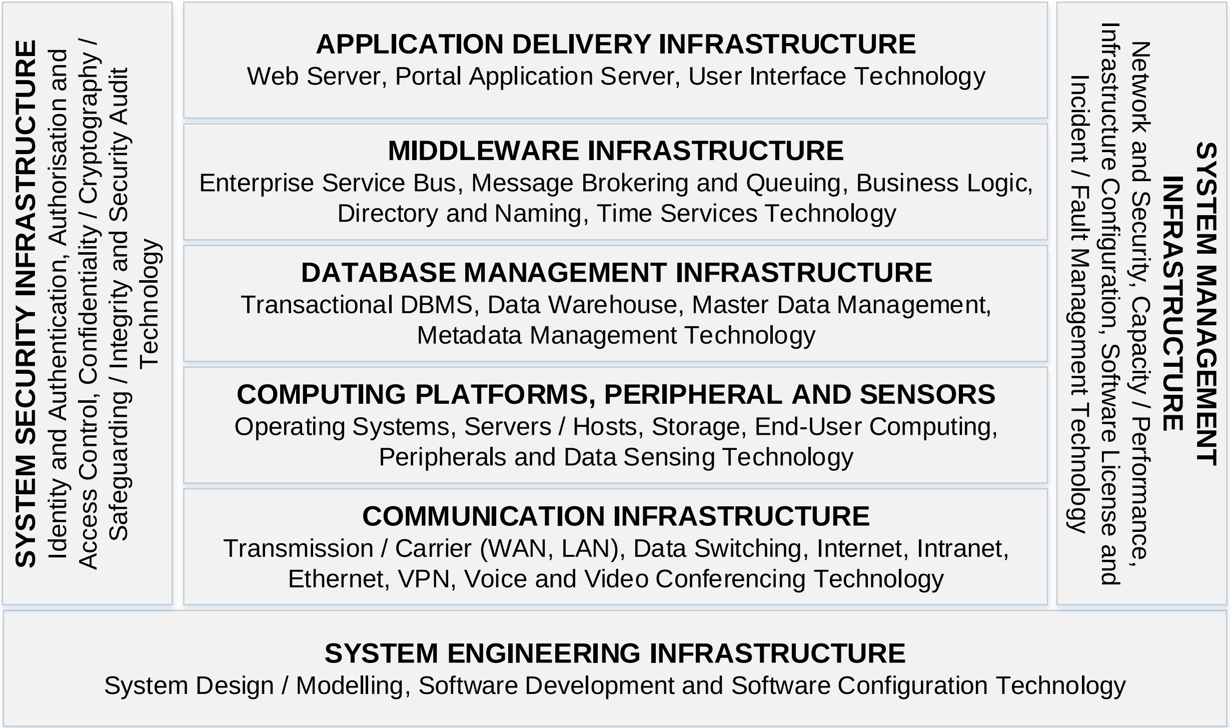


Figure 1: GWEA ICT House of Values

The GWEA House of Values was therefore recognised in deriving the Eskom cloud Reference Architecture and Cloud Taxonomy as it emphasises the various technology infrastructure domains that will be impacted by cloud adoption within Eskom (see Figure 2).



SYSTEM SECURITY INFRASTRUCTURE
Identity and Authentication, Authorisation and Access Control, Confidentiality / Cryptography / Safeguarding / Integrity and Security Audit Technology

APPLICATION DELIVERY INFRASTRUCTURE
Web Server, Portal Application Server, User Interface Technology

MIDDLEWARE INFRASTRUCTURE
Enterprise Service Bus, Message Brokering and Queuing, Business Logic, Directory and Naming, Time Services Technology

DATABASE MANAGEMENT INFRASTRUCTURE
Transactional DBMS, Data Warehouse, Master Data Management, Metadata Management Technology

COMPUTING PLATFORMS, PERIPHERAL AND SENSORS
Operating Systems, Servers / Hosts, Storage, End-User Computing, Peripherals and Data Sensing Technology

COMMUNICATION INFRASTRUCTURE
Transmission / Carrier (WAN, LAN), Data Switching, Internet, Intranet, Ethernet, VPN, Voice and Video Conferencing Technology

SYSTEM MANAGEMENT INFRASTRUCTURE
Network and Security, Capacity / Performance, Infrastructure Configuration, Software License and Incident / Fault Management Technology

SYSTEM ENGINEERING INFRASTRUCTURE
System Design / Modelling, Software Development and Software Configuration Technology

Figure 2: GWEA Technology Reference Model

The Eskom Cloud Reference Architecture defines a set of actors, activities and functions, which relates to an associated cloud Taxonomy for Eskom. The Eskom Cloud Reference Architecture contains a set of views and descriptions that are the basis for discussing the characteristics, use-cases and standards for cloud services. The actor / role-based model is intended to serve the expectations of the stakeholders (all Eskom Divisions) by allowing them to understand the overall view of roles and responsibilities in order to assess and assign risks. This Cloud Reference Architecture focuses on the requirements of "***what***" cloud services provide, not "***how to***" design cloud solutions and neither "***how to***" implement them. The Cloud Reference Architecture is intended to facilitate the understanding of the operational intricacies in cloud services within Eskom. It does not represent the system nor solution architecture of a specific cloud use-case, however it is a tool for describing, discussing and developing a system specific architecture using a common Cloud Reference Architecture that can be applied to any possible cloud-use case for Eskom.

2.1 Services Available in the Cloud

Cloud is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [4]. This cloud standard will contribute to the development of three cloud services for Eskom by providing a simple and unambiguous Cloud Taxonomy, i.e.:

- IaaS (Infrastructure as a Service).
- PaaS (Platform as a Service).

- SaaS (Software as a Service).

2.2 Cloud Deployment Models

This cloud standard also depicts four cloud deployment models for Eskom, which describes how the cloud infrastructure that delivers the cloud services can be shared (i.e. Private Cloud, Hybrid Cloud, Public Cloud and Community Cloud).

2.2.1 Private Cloud Deployment Model

A Private Cloud gives Eskom exclusive access to and usage of the infrastructure and computational resources. It may be managed either by Eskom or by a third party and may be hosted on Eskom's premises (On-Site Private Cloud) or outsourced to a hosting company (Outsourced Private Cloud). Figure 3 depicts an On-Site Private Cloud, while Figure 4 depicts an Outsourced Private Cloud.

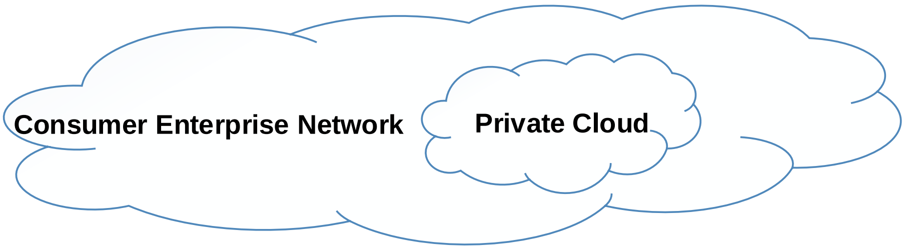


Figure 3: On-Site Private Cloud

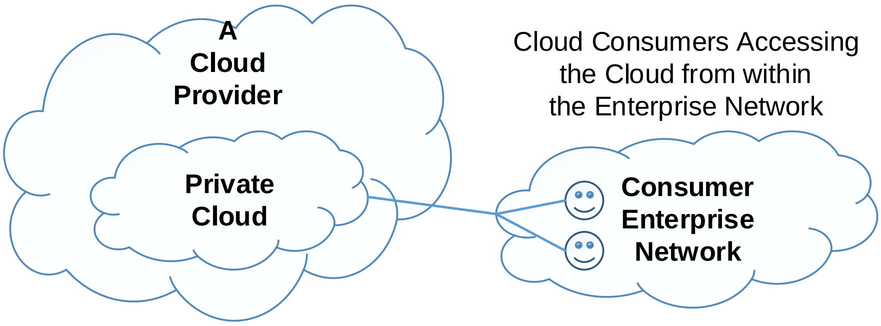

A Cloud Provider
Private Cloud
Cloud Consumers Accessing the Cloud from within the Enterprise Network
Consumer Enterprise Network

Figure 4: Out-Sourced Private Cloud

2.2.2 Hybrid Cloud Deployment Model

A Hybrid Cloud is a composition of two or more clouds (On-Site Private, On-Site Community, Off-Site Private, Off-Site Community or Public) that remain as distinct entities but are bound together by standardised or proprietary technology that enables data and application portability. Figure 5 presents a simple view of a Hybrid Cloud that could be built with a set of clouds in the five deployment model variants.

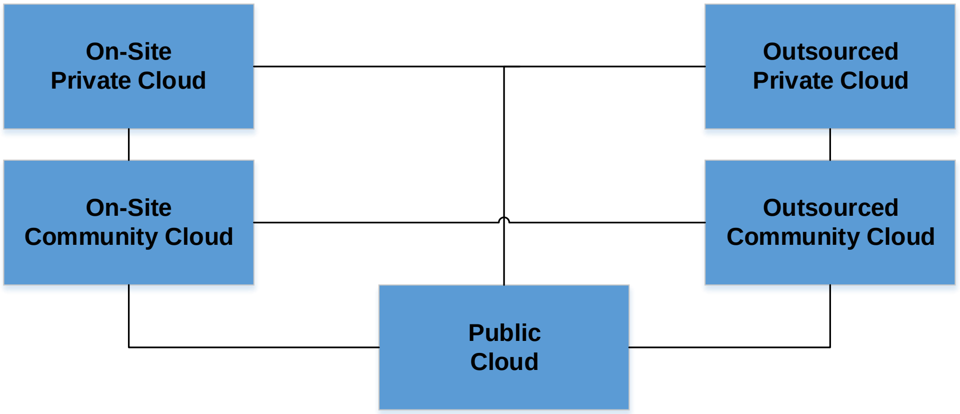


Figure 5: Hybrid Cloud

2.2.3 Public Cloud Deployment Model

The differences are based on how exclusive the computing resources are made to Eskom. A Public Cloud is one in which the cloud infrastructure and computing resources are made available to the general public over a public network. A Public Cloud is owned by an organisation selling “Cloud Services” and serves a diverse pool of clients (see Figure 6).

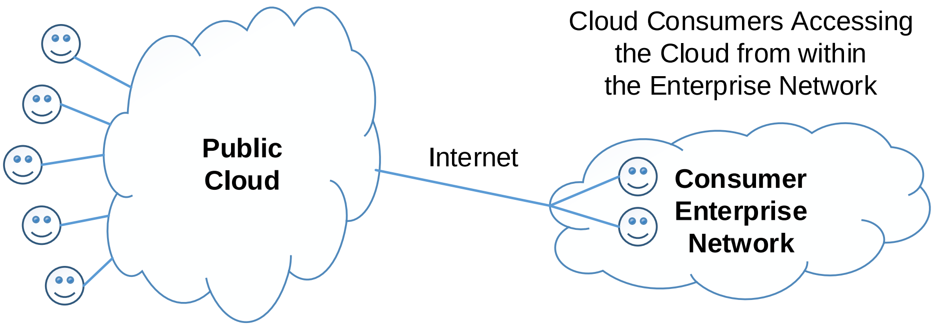

Cloud Consumers Accessing the Cloud from within the Enterprise Network
Public Cloud
Internet
Consumer Enterprise Network

Figure 6: Public Cloud

2.2.4 Community Cloud Deployment Model

A community cloud serves a group of “Cloud Consumers” which have shared concerns (i.e. mission objectives, security, privacy and compliance policy) rather than serving a single organisation as does a Private Cloud. Similar to private clouds, a community cloud may be managed by the organisation or by a third party and may be implemented on the customer premise (On-Site Community Cloud) or outsourced to a hosting company (Outsourced Community Cloud). Figure 7 depicts an On-Site Community Cloud comprised of a number of participant organisations. Eskom can access the local cloud resources and also the resources of other participating organisations through the connections between the associated organisations in a Community Cloud configuration. Figure 8 depicts an Outsourced Community Cloud, where the server side is outsourced to a hosting company. In this case, an Outsourced Community Cloud builds its infrastructure off premise and serves a set of organisations that request and consume cloud services.

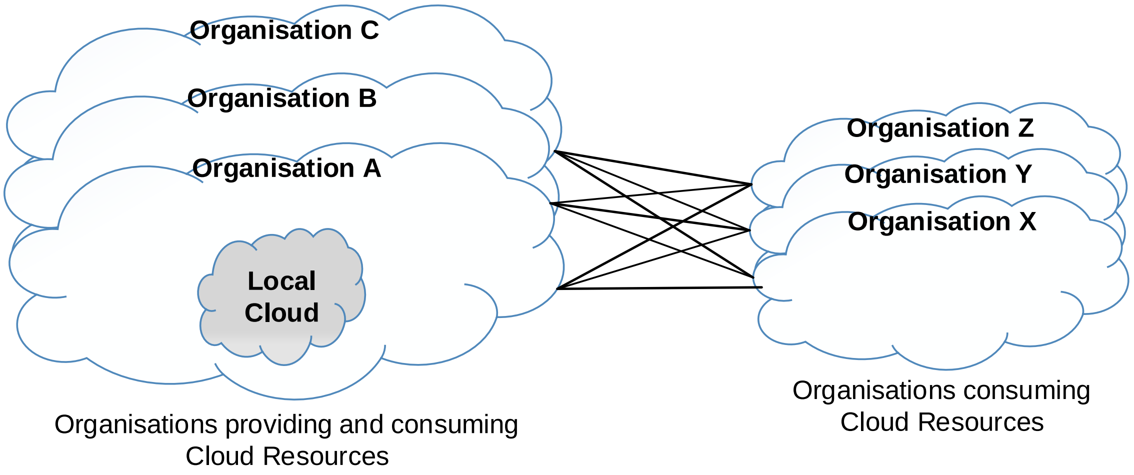


Figure 7: On-Site Community Cloud

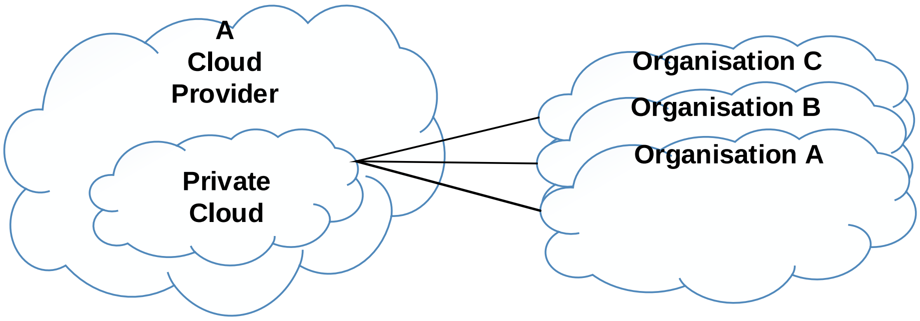


Figure 8: Outsourced Community Cloud

2.3 Essential Cloud Characteristics

This cloud standard discusses five essential cloud characteristics:

- **On-demand self service** - Computing capabilities (server time and network storage) can be automatically provisioned to Eskom without human interaction with the "Cloud Provider".
- **Broad network access** - Are available to Eskom over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (mobile phones, tablets, laptops and workstations).
- **Resource pooling** - The "Cloud Provider's" computing resources (storage, processing, memory and bandwidth) are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to Eskom's demand. There is a sense of location independence in that Eskom will have no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (country, state or datacenter).
- **Rapid elasticity** - Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To Eskom, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity and at any time.
- **Measured services** - Cloud systems automatically control and optimise resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (storage, processing, bandwidth and active user accounts). Resource usage can be monitored, controlled, audited and reported, providing transparency for both the "Cloud Provider" and Eskom.

3. ESKOM CLOUD REFERENCE ARCHITECTURE

Figure 9 depicts an overview of the proposed Eskom Cloud Reference Architecture derived from NIST and GWEA. The Cloud Reference Architecture for Eskom defines the major actors, their activities as well as their functions in cloud service provisioning. This Cloud Reference Architecture is a generic high-level architecture intended to facilitate the understanding of the requirements, uses, characteristics and standards of cloud service provisioning within Eskom. The conceptual Eskom Cloud Reference Architecture defines 5 major cloud actors and the scope of control between the "Cloud Consumer" and the "Cloud Provider" is being discussed.

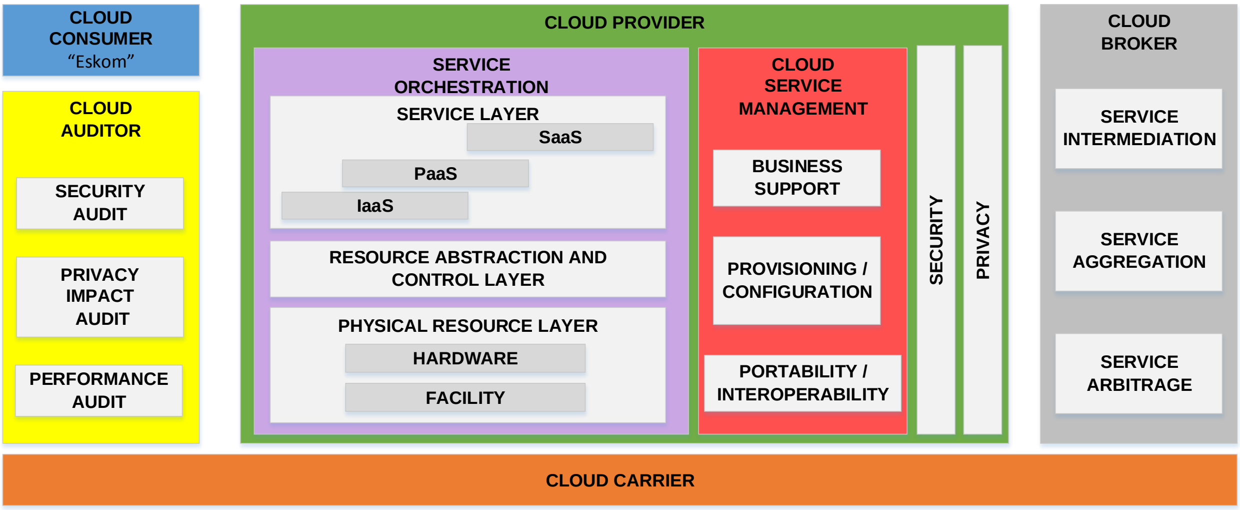


Figure 9: Proposed Eskom Cloud Reference Architecture

3.1 CLOUD CONSUMER

The "Cloud Consumer", represented by Eskom is the principal stakeholder for the cloud service. Eskom should consider cloud services from the cloud services catalog of the "Cloud Provider". Eskom can then request the appropriate cloud service from the "Cloud Provider". A contract should then be placed with the "Cloud Provider" that allows Eskom to use the cloud service. Eskom is then billed for the provisioned cloud service by the "Cloud Provider". The technical performance requirements for the "Cloud Provider" require SLAs. The SLAs will highlight the QoS (Quality of Service), security and remedies for performance failures. The "Cloud Provider" may also list in the SLA a set of promises (limitations and obligations) that explicitly can not be made to Eskom, which Eskom must accept. Eskom can freely choose a "Cloud Provider" with better pricing and more favourable terms. Typically, a "Cloud Provider's" pricing policy and SLAs are non-negotiable unless Eskom expects significant usage and might not be able to negotiate for better contracts. Depending on the requested service scenario, Eskom's activities and usage can be different. The specific SaaS, PaaS and IaaS services available to Eskom in the Cloud are depicted in Figure 10.

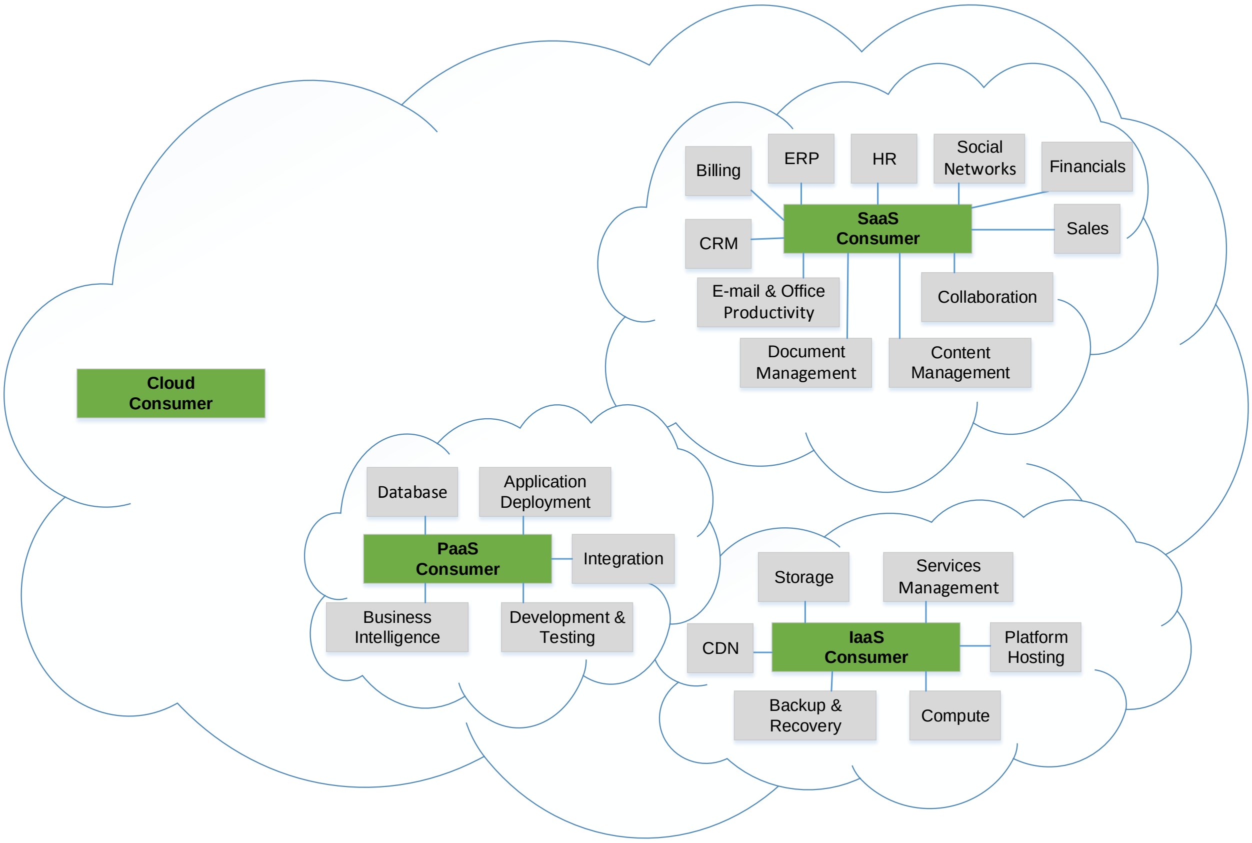


Figure 10: SaaS, PaaS and IaaS Services Available to Eskom in the Cloud

3.1.1 SaaS Applications Available to Eskom in the Cloud

SaaS applications in the cloud are made accessible via a network (the “Cloud Carrier”) to the SaaS consumer (Eskom). The “Cloud Provider” provides access to software applications via the “Cloud Carrier” to Eskom. Eskom can then have access to software applications, or software application administrators via the cloud. Eskom is billed for consuming SaaS based on the number of end-users, ToU (Time-of-Use), the network bandwidth consumed and the amount of data stored or the duration of stored data. SaaS applications available to Eskom are the following:

- **Email and Office Productivity** - Applications for email, word processing, spreadsheets and presentations.
- **Billing** - Application services to manage customer billing based on usage and subscriptions to products and services.
- **CRM (Customer Relationship Management)** - CRM applications that range from call center applications to sales force automation.
- **Collaboration** - Tools that allow Eskom to collaborate in workgroups, within the organisation and across the organisation.

- **Content Management** - Services for managing the production of and access to content for web-based applications.
- **Document Management** - Applications for managing documents, enforcing document production workflows and providing workspaces for the organisation or user-groups within the organisation to find and access documents.
- **Financials** - Applications for managing financial processes ranging from expense processing, invoicing and tax management.
- **HR (Human Resources)** - Software for managing HR functions within the organisation.
- **Sales** - Applications that are specifically designed for sales functions.
- **Social Networks** - Social software that establishes and maintains a connection among users that are tied in one or more specific types of interdependency (sentiment analysis).
- **ERP (Enterprise Resource Planning)** - Integrated system used to manage internal and external resources, including tangible assets, financial resources, materials and HR.

3.1.2 PaaS Applications Available to Eskom in the Cloud

Eskom can employ the tools and execution resources provided by "Cloud Provider's" to develop, test, deploy and manage applications hosted in a cloud environment (PaaS). Eskom can employ its own application developers whom can design and implement application software. Furthermore, Eskom's own application testers can run and test applications in cloud-based environments. Eskom can also publish applications into the cloud and deploy application administrators who can configure and monitor the performance of the application on the PaaS platform. Eskom can be billed according to processing, database storage and network resources consumed by the PaaS application as well as the the duration of the platform usage. PaaS applications available to Eskom are the following:

- **BI (Business Intelligence)** - Platforms for the creation of applications such as dashboards, reporting systems and data analysis.
- **Database** - Services offering scalable relational database solutions or scalable non-SQL datastores.
- **Development and Testing** - Platforms for the development and testing cycles of application development, which expand and contract as needed.
- **Integration** - Development platforms for building integration applications in the cloud and within the enterprise.
- **Application Deployment** - Platforms suited for general purpose application development. These services provide databases and web application runtime environments.

3.1.3 IaaS Applications Available to Eskom in the Cloud

Through IaaS, Eskom will have access to virtual computers, network accessible storage, network infrastructure components as well as other fundamental computing resources on which they can deploy and run arbitrary software. Through IaaS, Eskom can be a system developer, a system administrator as well as an IT manager who are interested in creating, installing, managing and monitoring services for IT infrastructure operations. Through IaaS, Eskom will be provisioned with the capabilities to access these computing resources and will be billed according to the amount or duration of the resources consumed (CPU hours used by virtual computers, volume and duration of data stored, network bandwidth consumed and the number of IP addresses used for certain intervals). IaaS applications available to Eskom are the following:

- **Backup and Recovery** - Services for backup and recovery of file systems and raw data stores on servers and desktop systems.
- **Compute -** Server resources for running cloud-based systems that can be dynamically provisioned and configured as needed.
- **CDN (Content Delivery Networks) -** CDNs store content and files to improve the performance and cost of delivering content for web-based systems.
- **Services Management -** Services or tools that manage cloud infrastructure platforms that often provide features that “Cloud Provider’s” do not provide or specialise in managing certain application technologies.
- **Storage -** Scalable storage capacity that can be used for applications, backups, archives and file storage.

3.2 “CLOUD PROVIDER”

A “Cloud Provider” is a person, an organisation or an entity that makes cloud services available to Eskom. A “Cloud Provider” can acquire and manage the cloud computing infrastructure required for providing cloud services to Eskom and are able to run the cloud software that provides the services and makes an arrangement to deliver the cloud services via network access through a “Cloud Carrier”. A ”Cloud Provider’s” activities can be grouped into 5 major areas (see Figure 11), which can be made available to Eskom and conducts its activities in the areas of service deployment, service orchestration, cloud service management, security and privacy.

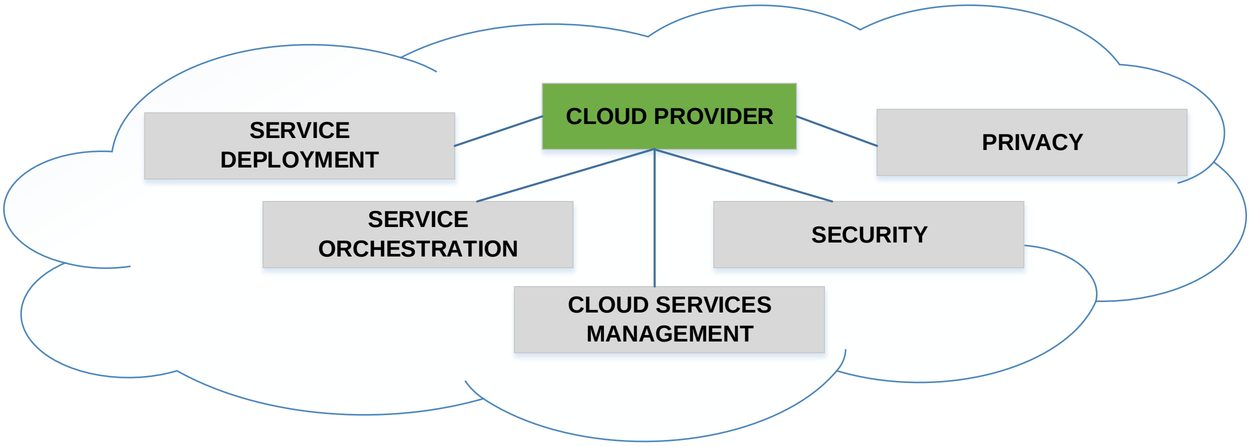


Figure 11: “Cloud Provider” Major Activities

3.2.1 “Cloud Provider” SaaS Applications

The “Cloud Provider” can on behalf of Eskom deploy, configure, maintain and update software applications on a cloud infrastructure at Eskom’s expected service levels. The “Cloud Provider” will assume most of the responsibilities in managing and controlling the applications as well as the infrastructure, while Eskom will have limited administrative control of the applications.

3.2.2 “Cloud Provider” PaaS Applications

The “Cloud Provider” can manage the computing infrastructure and the cloud software that provides the components (Runtime execution software stack, Databases and Middleware) on behalf of Eskom. The PaaS “Cloud Provider” can support the development, deployment and management of processes of Eskom by providing the tools (Integrated Development Environments, development versions of cloud software, Software Development Kits, deployment and management tools). Eskom will have control over the applications and possibly some of the hosting environment settings, but has no or limited access to the infrastructure underlying the platform (network, servers, OS’s or storage).

3.2.3 “Cloud Provider” IaaS Applications

The “Cloud Provider” acquires the physical computing resources underlying the services (servers, networks, storage and hosting infrastructure) required by Eskom. The “Cloud Provider” runs the cloud software necessary to make computing resources available to Eskom through a set of service interfaces and computing resource abstractions (VM’s and virtual interfaces). Eskom can then use these computing resources (virtual computer) for its fundamental computing needs compared to SaaS and PaaS “Cloud Consumers”. An IaaS “Cloud Consumer” has access to more fundamental forms of computing resources and thus has more control over the more software components in an application stack, including the OS (Operating System) and network. The IaaS “Cloud Provider”, has control over the physical hardware and cloud software that makes the provisioning of these infrastructure services possible (physical servers, network equipment, storage devices, host OS and hypervisors for virtualisation).

3.3 SCOPE OF CONTROL BETWEEN "CLOUD PROVIDER" AND CLOUD CONSUMER

The "Cloud Provider" and Eskom will share the control of resources in the cloud (see Figure 12). Different cloud service models will affect Eskom's control over the cloud computational resources. These differences using a classic software stack notation comprises of the application, middleware and OS layers. This analysis of controls over the application stack will help Eskom understand the responsibilities involved in managing the cloud application. The application layer includes software applications targeted at Eskom and end users or programs. The applications can be used by Eskom, or installed / managed / maintained by Eskom across PaaS, IaaS and SaaS platforms. The middleware layer provides the software building blocks (libraries, database and Java VM), allowing Eskom to develop software applications in the cloud. The middleware can be used by Eskom and can be installed / managed/maintained by Eskom or the "PaaS Provider". The OS layer includes the OS and drivers and can be hidden from Eskom. An IaaS cloud allows one or multiple guest OS's to run virtualised on a single physical host. Eskom will have broad freedom to choose which OS to be hosted among all the OS's that could be supported by the "Cloud Provider". Eskom should assume full responsibility for the guest OS's, while the "IaaS Provider" controls the host OS.

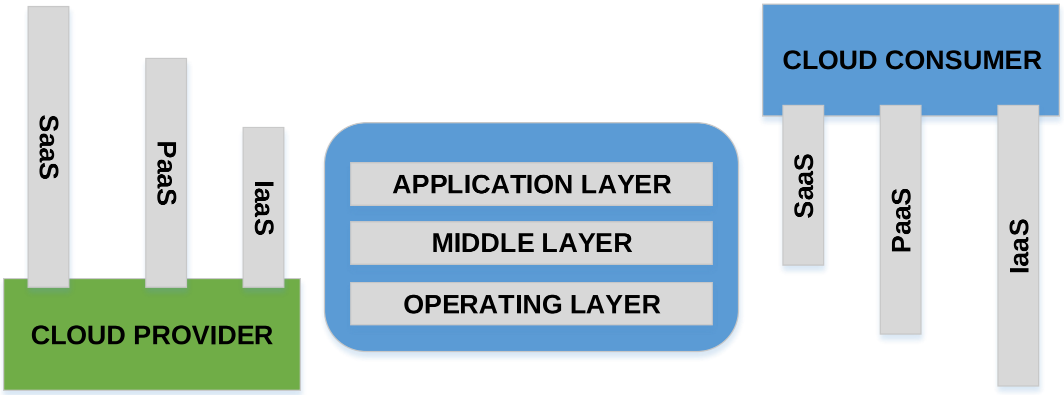


Figure 12: Scope of Control between "Cloud Provider" and "Cloud Consumer" (Eskom)

3.4 CLOUD AUDITOR

A "Cloud Auditor" is an independent examiner of cloud service controls and can evaluate the services provided by a "Cloud Provider" to Eskom in terms of security controls, privacy impact and performance. Audits are performed to verify conformance to standards by reviewing objective evidence. Auditing is therefore important for Eskom, as security controls are the management, operational and technical safeguards or countermeasures employed within IMS's (Information Management Systems) to protect the confidentiality, integrity and availability of the system as well as its information. For security auditing, a "Cloud Auditor" can make an assessment of the security controls in the IMS in order to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to the security requirements for the system. The security auditing should also include the verification of the compliance with regulation and the GIT information security policy. An auditor can be tasked with ensuring that the correct policies are applied to data retention according to relevant rules for the jurisdiction. The auditor may ensure that fixed content has been modified and that the legal and business data archival requirements have been satisfied. A privacy impact audit can help Eskom to comply with applicable privacy laws and regulations governing Eskom's privacy and to ensure confidentiality, integrity and availability of Eskom's PI (Personal Information) at every stage of development and operation.

3.5 CLOUD BROKER

As cloud computing evolves, the integration of cloud services can become too complex for Eskom to manage. Eskom may request cloud services from a "Cloud Broker", instead of contacting a "Cloud Provider" directly. A "Cloud Broker" is an entity that manages the use, performance and delivery of cloud services and negotiates relationships between "Cloud Provider's" and "Cloud Consumers". A "Cloud Broker" can provide services in three categories (see Table 1) to Eskom.

Service Intermediation	A "Cloud Broker" enhances a service by improving specific capabilities in providing VAS to Eskom. The improvement can be managing access to cloud services, performance reporting and enhanced security.
Service Aggregation	A "Cloud Broker" combines and integrates multiple services into one or more new services. The broker provides data integration and ensures the secure data movement between Eskom and multiple "Cloud Provider's".
Service Arbitrage	Service arbitrage is similar to service aggregation except that the services being aggregated are not fixed. Service arbitrage means a "Cloud Broker" has the flexibility to choose services from multiple agencies. The "Cloud Broker" can use a credit-scoring service to measure and select an agency with the best score.

Table 1: Three Service Categories for "Cloud Brokers"

3.6 CLOUD CARRIER

A "Cloud Carrier" acts as an intermediary that provides connectivity and transport of cloud services between Eskom and "Cloud Provider's". "Cloud Carriers" can provide access to Eskom through network, telecommunication and other access devices. Eskom can obtain cloud services through network access devices (i.e. computers, laptops, mobile phones and MID's). The distribution of cloud services is normally provided by network and telecommunication carriers or a transport agent, where a transport agent refers to a business organisation that provides physical transport of storage media such as high-capacity hard drives. The "Cloud Provider" will set up SLAs with a "Cloud Carrier" to provide services consistent with the level of SLAs offered to Eskom and may require the "Cloud Carrier" to provide dedicated and secure connections between Eskom and the "Cloud Provider's".

4. HIGH-LEVEL GENERIC CLOUD SCENARIOS

The “Cloud First” business use case requires more complex interactions between Eskom and the “Cloud Provider’s”. There are three generic scenarios from which interaction scenarios can be derived for Eskom (see Figure 13). These scenarios are considered to be Single Cloud or Multiple Cloud Systems.

4.1 Single Cloud System

- Scenario 1: Deployment on a single cloud system.
- Scenario 2: Manage resources on a single cloud system.
- Scenario 3: Interface enterprise systems to a single cloud system.
- Scenario 4: Enterprise systems migrated or replaced on a single cloud system.

4.2 Multiple Cloud Systems (serially, one at a time; or simultaneously, more than one at a time)

- Scenario 5: Migration between cloud systems.
- Scenario 6: Interface across multiple cloud systems.
- Scenario 7: Work with a selected cloud system.
- Scenario 8: Operate across multiple cloud systems.

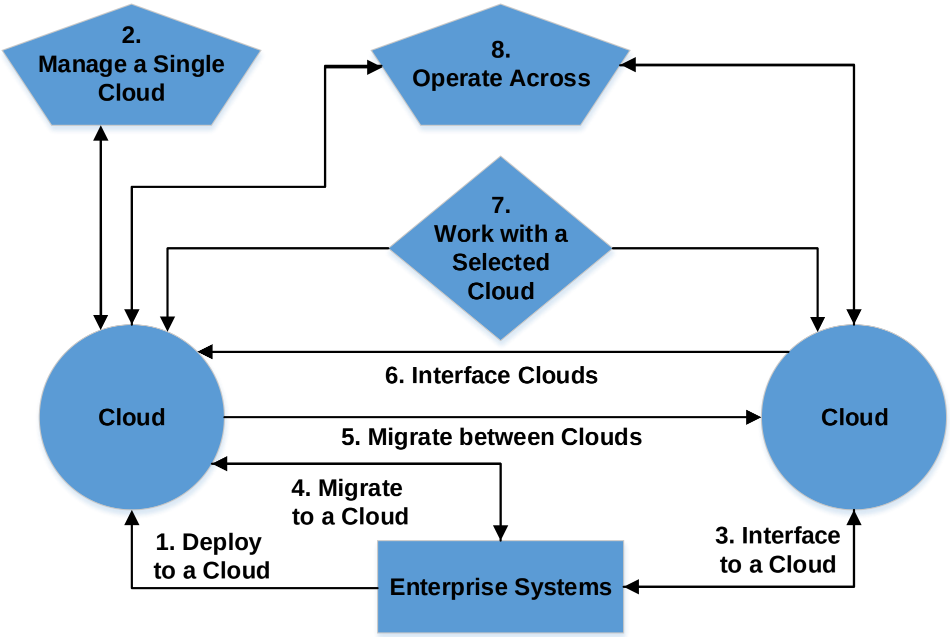


Figure 13: High-Level Generic Cloud Scenarios

4.3 Cloud Use Case Scenario for Various Interactions between the "Cloud Actors"

Figure 14 depicts the interaction between the various cloud actors. Eskom can request cloud services either directly from a "Cloud Provider" or via a "Cloud Broker". The "Cloud Auditor" conducts independent audits and may contact the cloud actors to collect the necessary information. The communication paths are provided by the "Cloud Carrier".

🟦	Communication path between ""Cloud Provider""and "Cloud Consumer"
🟥	Communication path for "Cloud Auditor" to collect auditing information
⬛	Communication path for "Cloud Broker" to provide service to a "Cloud Consumer"

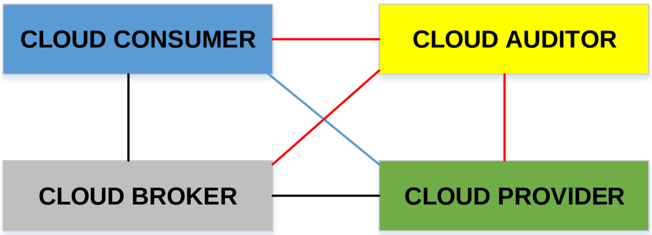


Figure 14: Various Interactions between the Cloud Actors

4.4 Cloud Use Case Scenario for "Cloud Auditors"

This scenario describes "Cloud Auditors" whom conducts independent assessments for cloud services during the operation and security of the cloud service implementation. The "Cloud Auditor" may interact with both Eskom and the "Cloud Provider" (see Figure 15).

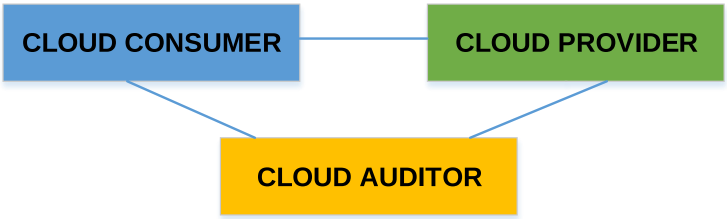


Figure 15: "Cloud Auditor" Scenario

4.5 Cloud Use Case Scenario for “Cloud Brokers”

Eskom may request a cloud service from a “Cloud Broker” (see Figure 16), instead of contacting a “Cloud Provider” directly. The “Cloud Broker” may create a new service by combining multiple services or by enhancing an existing service. In this scenario the “Cloud Provider’s” are invisible to Eskom and Eskom interacts directly with the “Cloud Broker”.

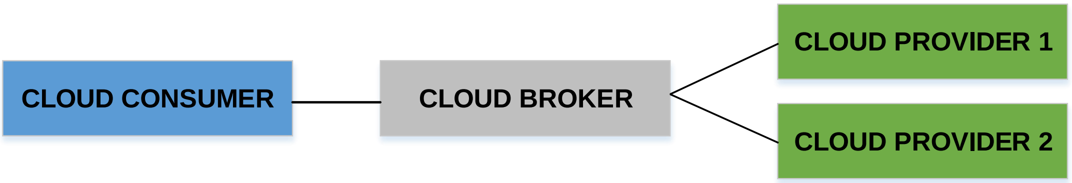


Figure 16: “Cloud Broker” Scenario

4.6 Cloud Use Case Scenario for “Cloud Carriers”

“Cloud Carriers” provide the connectivity and transport of cloud services from “Cloud Provider’s” to Eskom (see Figure 17). The “Cloud Provider” participates in and arranges for Eskom (SLA 1). A “Cloud Provider” arranges SLAs with a “Cloud Carrier” and may request dedicated and encrypted connections to ensure the “Cloud Services” are consumed at a consistent level according to the contractual obligations with Eskom. In this scenario, the “Cloud Provider” may specify its requirements on capability, flexibility and functionality in SLA2 in order to provide essential requirements in SLA1.

—	SLA between “Cloud Consumer” and ““Cloud Provider””
—	SLA between ““Cloud Provider”” and “Cloud Carrier”

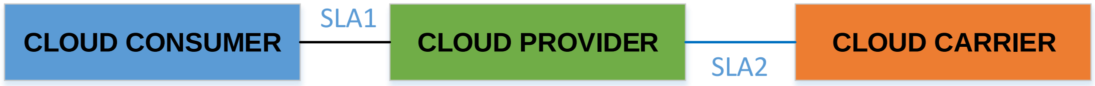


Figure 17: “Cloud Carrier” Scenario

5. FUNDAMENTAL DIMENSIONS TO THE SPECTRUM OF CLOUD USE CASES

These technical use cases must also be analysed in the context of their deployment models and the resultant way cloud actors must interact. These considerations identify two fundamental dimensions to the spectrum of cloud computing use cases. These deployment cases will drive the requirements for cloud standards for Eskom and can be identified through the summary matrix depicted in Table 2:

- Centralised vs. Distributed

- Within vs. Crossing Trust Boundaries

	a.) Within Trust Boundary	**b.) Crossing Trust Boundary**
1.) Centralised (One administrative cloud domain)	Deployment Case 1A	Deployment Case 1B
2.) Distributed (Crossing administrative cloud domains)	Deployment Case 2A	Deployment Case 2B

Table 2: Deployment Cases for High-Level Scenarios

5.1 Deployment Case 1

In the centralised deployment case, there is one “Cloud Provider” under consideration at a time. Each “Cloud Provider” may service Eskom. Eskom has a simple client-provider interaction with the “Cloud Provider”.

5.2 Deployment Case 1A

This is a Private Cloud within a single administrative domain and trust boundary wherein policy and governance can be enforced by nontechnical means. Use cases within this deployment case may require standards to support the following basic technical requirements:

- Simple, consumer-provider authentication.
- VM (Virtual Machine) management.
- Storage management.
- SLAs and performance / energy monitoring.
- Service discovery.
- Workflow management.
- Auditing.
- Virtual organisations in support of community cloud use cases.

5.3 Deployment Case 1B

This is a Public Cloud within a single administrative domain but is outside of any trust boundary. Eskom will be responsible to enforce policy and governance and must rely on the “Cloud Provider” to enforce policy and governance through technical means that are part of the infrastructure. This deployment case will require standards to support the following additional technical requirements:

- SLAs in support of governance requirements (e.g. national regulatory compliance).

- Stronger authentication mechanisms (e.g. PKI Certificates).
- Certification of VM isolation through hardware and hypervisor support.
- Certification of storage isolation through hardware support.
- Data encryption.

5.4 Deployment Case 2

In the distributed deployment case, Eskom could have an application that may be distributed across two or more “Cloud Provider’s” and administrative domains simultaneously. Eskom may have simple “Consumer-Provider” interactions with its application and the “Cloud Provider’s”. More complicated P2P (Peer-to-Peer) interactions may be required between Eskom and the “Cloud Provider” and also between the “Cloud Provider’s” themselves.

5.5 Deployment Case 2A

This deployment case is typically a federated cloud of two or more administrative cloud domains, but where the “Cloud Provider’s” can agree "out of band" how to mutually enforce policy and governance essentially establishing a common trust boundary. Use cases within this deployment case may require standards to support the following basic technical requirements:

- P2P service discovery.
- P2P SLA and performance monitoring.
- P2P workflow management.
- P2P auditing.
- P2P security mechanisms for authentication and authorisation.
- P2P virtual organisation management.

5.6 Deployment Case 2B

This is a Hybrid Cloud where applications cross a private-public trust boundary, or even span multiple public clouds, where both administrative domains and trust boundaries are crossed. Eskom will rely on the “Cloud Provider” to enforce policy and governance through technical means that are part of the infrastructure. Applications and services may be distributed and need to operate in a P2P manner. Use cases within this deployment case will require all the standards of the other deployment cases as well as more extensive technical requirements (i.e. P2P SLAs in support of governance requirements).

The use cases presented in this section should be analysed with regards to their possible cloud deployment scenarios to determine the requirements for cloud standards for Eskom. This analysis will subsequently be used to evaluate the likelihood of each of these deployment cases. Clearly the expected deployment of these use cases across the different deployment cases will not be uniform. This non-uniformity will assist in producing a prioritised roadmap for cloud standards.

Likewise, in reviewing existing standards, these use cases in conjunction with their possible deployment cases will be used to identify and prioritise gaps in available standards.

Based on this analysis, note that Scenarios 1 through 4 could be deployed on either a Private Cloud or a Public Cloud. Hence, different standards noted in deployment cases 1A and 1B will be required. Scenarios 5, 6, and 7 all involve the notion of the serial use of multiple clouds. Presumably these different clouds, used serially, could be either Private Cloud or Public Cloud. Hence, deployment cases 1A and 1B would also apply, but there are additional requirements to achieve portability (e.g. API commonality). Finally, Scenario 8 could involve a Federated / Community Cloud or a Hybrid Cloud. Hence, deployment cases 2A and 2B would apply.

5.7 Common Technical Requirements Across All Cloud Scenarios

The detailed technical use cases for this analysis that are common across all scenarios are summarised in Table 3.

Scenarios	Technical Requirements
1	Creating, accessing, updating, deleting, data objects in cloud systems.
2	Moving VMs and virtual appliances between cloud systems.
3	Selecting the best IaaS vendor for private externally hosted cloud system.
4	Tools for monitoring and managing multiple cloud systems.
5	Migrating data between cloud systems.
6	SSO to multiple cloud systems.
7	Orchestrated process across cloud systems.
8	Discovering cloud resources.
9	Evaluating SLAs and penalties.
10	Auditing Cloud Systems.

Table 3: Scenarios and Technical Requirements

6. SERVICE ORCHESTRATION

Service Orchestration refers to the composition of system components to support the “Cloud Provider’s” activities in arrangement, coordination and management of computing resources in order to provide cloud services to Eskom (see Figure 18). A three-layered model is presented, representing the grouping of three types of system components the “Cloud Provider’s” need to compose of to deliver their services.

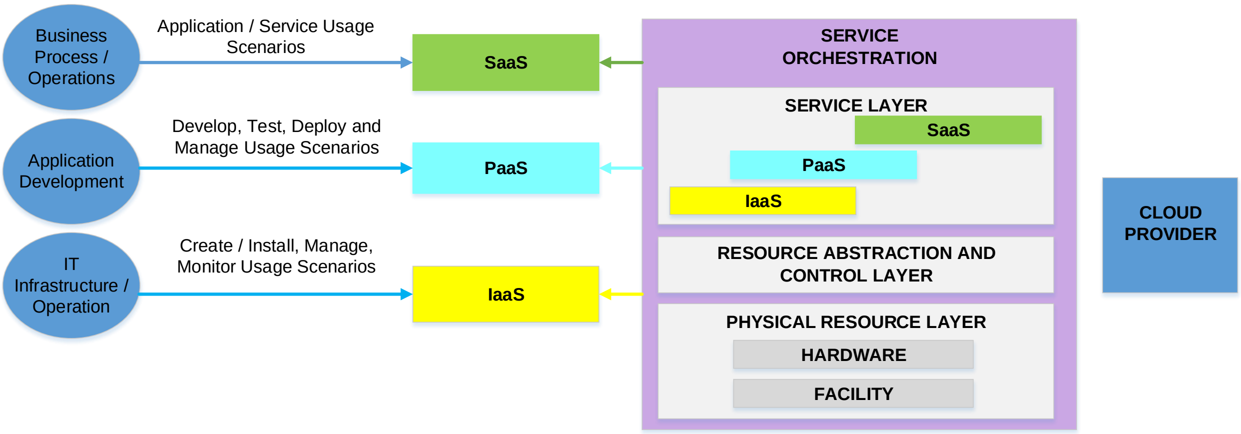

Business Process / Operations
Application Development
IT Infrastructure / Operation
Application / Service Usage Scenarios
Develop, Test, Deploy and Manage Usage Scenarios
Create / Install, Manage, Monitor Usage Scenarios
SaaS
PaaS
IaaS
SERVICE ORCHESTRATION
SERVICE LAYER
SaaS
PaaS
IaaS
RESOURCE ABSTRACTION AND CONTROL LAYER
PHYSICAL RESOURCE LAYER
HARDWARE
FACILITY
CLOUD PROVIDER

Figure 18: “Cloud Provider” Service Orchestration

6.1 Service Layer

The service layer is where the “Cloud Provider’s” define interfaces for Eskom to access the cloud. Access interfaces of each of the three service models are provided in this layer. It is possible, though not necessary, that SaaS applications can be built on top of PaaS components and PaaS components can be built on top of IaaS components. The optional dependency relationships among SaaS, PaaS and IaaS components are represented graphically as components stacking on each other, while the angling of the components represents that each of the service components can be independent (a SaaS application can be implemented and hosted on VM’s from an IaaS cloud or it can be implemented directly on top of cloud resources without using IaaS VM’s).

6.2 Resource Abstraction and Control Layer

This layer contains the system components that “Cloud Provider’s” use to provide and manage access to the physical computing resources through software abstraction (e.g. software elements such as hypervisors, VM’s, virtual data storage and other computing resource abstractions). The resource abstraction needs to ensure efficient, secure and reliable usage of the underlying physical resources. While VM technology is commonly used at this layer, other means of providing the necessary software abstractions are also possible. The control aspect of this layer refers to the software components that are responsible for resource allocation, access control and usage monitoring. This is the software fabric that ties together the numerous underlying physical resources and their software abstractions to enable resource pooling, dynamic allocation and measured services. Various open source and proprietary cloud software are examples of this type of middleware.

6.3 Physical Resources Layer

The physical resource layer includes all the physical computing resources. This layer includes hardware resources, i.e. computers (CPU and memory), networks (routers, firewalls, switches, network links and interfaces), storage components (hard disks) and other physical computing infrastructure elements. It also includes facility resources, i.e. HVAC (Heating, Ventilation and Air Conditioning), power, communications and other aspects of the physical plant. Following system architecture conventions, the horisontal positioning (the layering) in a model represents dependency relationships. The upper layer components are dependent on adjacent lower layers to function. The resource abstraction and control layer exposes virtual cloud resources on top of the physical resource layer and supports the service layer where cloud services interfaces are exposed to Eskom, while Eskom do not have direct access to the physical resources.

7. CLOUD SERVICE MANAGEMENT

Cloud Service Management includes all of the service-related functions that are necessary for the management and operation of those services required by or proposed to Eskom. Cloud service management can be described from the perspective of business support, provisioning, configuration as well as portability and interoperability requirements (see Figure 19).

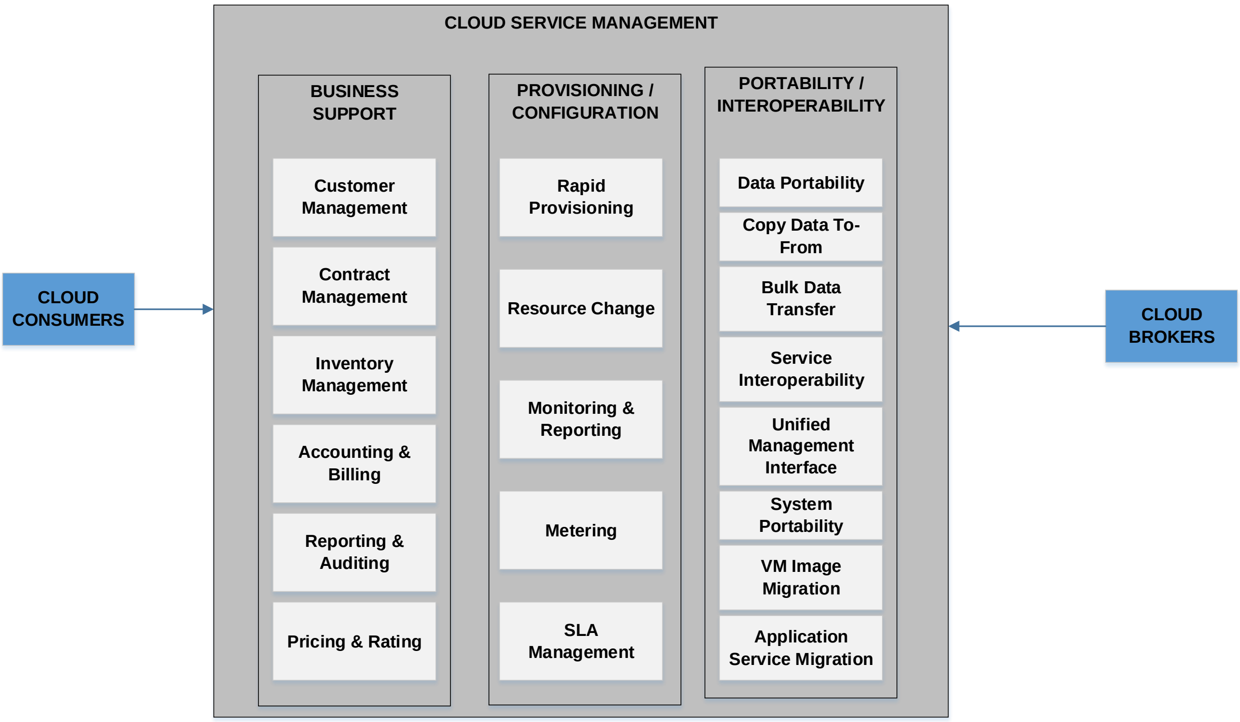


Figure 19: Cloud Service Management

7.1 Business Support

Business Support entails a set of business-related services and the associated supporting processes Eskom will need. It includes the components used to run business operations that are client-facing, i.e.:

- **Customer management** - Manage the Eskom account, the Eskom user profiles, open / close / terminate Eskom accounts, manage customer relationships by providing points-of-contact and resolving Eskom issues and problems.
- **Contract management** - Manage the Eskom service contracts and setup / negotiate / close / terminate the Eskom contract.
- **Inventory Management** - Set up and manage service catalogs for Eskom
- **Accounting and Billing** - Manage Eskom's billing information (billing statements, process received payments and track invoices).
- **Reporting and Auditing** - Monitor Eskom operations and generate reports.
- **Pricing and Rating** - Evaluate cloud services and determine prices, handle promotions and pricing rules based on Eskom's user profile.

7.2 Provisioning and Configuration

- **Rapid provisioning** - Automatically deploying cloud systems based on the requested service / resources / capabilities.
- **Resource changing** - Adjusting configuration / resource assignment for repairs, upgrades and joining new nodes into the cloud.
- **Monitoring and Reporting** - Discovering and monitoring virtual resources, monitoring cloud operations and events and generating performance reports.
- **Metering** - Providing a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth and active user accounts).
- **SLA management** - Encompassing the SLA contract definition (basic schema with the QoS parameters), SLA monitoring and SLA enforcement according to defined policies.

7.3 Portability and Interoperability

The proliferation of cloud computing promises cost savings in technology infrastructure and faster software upgrades. Eskom has a strong interest in moving to the cloud. However, the adoption of cloud computing depends greatly on how the cloud can address Eskom's concerns regarding security, portability and interoperability. For portability, Eskom are interested to know whether they can move their data or applications across multiple cloud environments at low cost and minimal disruption. From an interoperability perspective, Eskom is concerned about the capability to communicate between or among multiple clouds.

“Cloud Provider’s” should provide mechanisms to support data portability, service interoperability, and system portability. Data portability is the ability for Eskom to copy data objects into or out of a cloud or to use a disk for bulk data transfer. Service interoperability is the ability for Eskom to use their data and services across multiple “Cloud Provider’s” with a unified management interface. System portability allows the migration of a fully-stopped VM instance or a machine image from one “Cloud Provider” to another “Cloud Provider”, or migrate applications and services and their contents from one “Cloud Provider” to another.

It should be noted that various cloud service models may have different requirements related to portability and interoperability (e.g. IaaS requires the ability to migrate the data and run the applications on a new cloud). Thus, it is necessary to capture VM images and migrate to new “Cloud Provider’s” which may use different virtualisation technologies. Any provider-specific extensions to the VM images need to be removed or recorded upon being ported. While for SaaS, the focus is on data portability and thus it is essential to perform data extractions and backups in a standard format.

8. SECURITY

It is critical to recognise that security is a cross-cutting aspect of the architecture that spans across all layers of the Eskom Cloud Reference Architecture, ranging from physical security to application security. Security in cloud computing architecture concerns is not solely under the purview of the “Cloud Provider’s”, but also Eskom and other relevant actors. Cloud-based systems need to address security requirements such as authentication, authorisation, availability, confidentiality, identity management, integrity, audit, security monitoring, incident response and security policy management. While these security requirements are not new, this standard discusses cloud specific perspectives to help analyse and implement security in a cloud system. As Eskom moves to the cloud, it must be vigilant to ensure the security and proper management of NKP information to protect the privacy of South African citizens as well as ensure national security. Careful consideration should therefore be given to areas of cybersecurity, continuity of operations, IA (Information Assurance) and resilience.

The protection of the physical resource layer requires physical security that denies unauthorised access to the building, facility, resource, or stored information. “Cloud Provider’s” should ensure that the facility hosting cloud services is secure and that the staff has proper background checks (vetting). When data or applications are moved to the cloud, Eskom should ensure that the cloud offering satisfies the security requirements and enforces the compliance rules. Guidance in this regard should be sought from the SSA (State Security Agency) or “Cloud Auditors”. It is also important to note that security, compliance and policy requirements are a function of the legal jurisdiction of South Africa. An independent audit should be conducted to verify the compliance with regulations or security policies.

8.1 Cloud Service Model Perspectives

The three identified service models (SaaS, PaaS and IaaS) present Eskom with different types of service management operations and expose different entry points into cloud systems. This in turn create different attack surfaces for adversaries. Hence, it is important to consider the impact of cloud service models and their different issues in security design and implementation (e.g. SaaS provides Eskom with accessibility of cloud offerings using a network connection, normally over the Internet and through a Web browser). There has been an emphasis on Web browser security in

SaaS cloud system security considerations. Cloud Consumers of IaaS are provided with VMs that are executed on hypervisors on the hosts, therefore, hypervisor security for achieving VM isolation has been studied extensively for IaaS "Cloud Provider"s that use virtualisation technologies.

8.2 Implications of Cloud Deployments

The variations of cloud deployment models have important security implications as well. One way to look at the security implications from the deployment model perspective is the differing level of exclusivity of tenants in a deployment model. A private cloud is dedicated to Eskom, whereas a public cloud could have unpredictable tenants co-existing with each other. Therefore, workload isolation is less of a security concern in a private cloud than in a public cloud. Another way to analyse the security impact of cloud deployment models is to use the concept of access boundaries (e.g. an On-Site Private Cloud may or may not need additional boundary controllers at the cloud boundary when the private cloud is hosted on-site within Eskom's network boundary, whereas an Out-Sourced Private Cloud tends to require the establishment of such perimeter protection at the boundary of the cloud).

8.3 Shared Security Responsibilities

The "Cloud Provider" and Eskom have differing degrees of control over the computing resources in a cloud system. Compared to the traditional IT systems where Eskom has control over the whole stack of computing resources and the entire life-cycle of the systems, "Cloud Provider's" and Eskom collaboratively design, build, deploy and operate the cloud. The split of control means both parties now share the responsibilities in providing adequate protections to the cloud. Security is a shared responsibility and therefore security controls (i.e. measures used to provide protection) needs to be analysed in order to determine which party is in a better position to implement. This analysis needs to include considerations from a service model perspective, where different service models imply different degrees of control between "Cloud Provider's" and Eskom (e.g. account management controls for initial system privileged users in IaaS scenarios are typically performed by the IaaS Provider whereas application user account management for the application deployed in an IaaS environment is typically not the "Cloud Provider's" responsibility).

8.4 Privacy

The "Cloud Provider" should protect the assured properly and consistently during the collection, processing, communication, use and disposition of PI (Personal Information) and PII (Personally Identifiable Information) in the cloud. PII is the information that can be used to distinguish or trace an individual's identity (i.e. name, social security number, biometric records) or when combined with other personal or identifying information that is linked or linkable to a specific individual (i.e. date, place of birth, mother's maiden name). Though cloud computing provides a flexible solution for shared resources, software and information, it also poses additional privacy challenges to Eskom using the cloud. It is required, that Eskom and the "Cloud Provider" enter into a written (legal) agreement that clearly defines the roles and expectations of the parties. The three areas where the security and privacy for cloud computing are of particular interest to Eskom are:

- The internal control environment of a "Cloud Provider", including risks, controls, and other governance when that environment touches the provision of cloud services.

- The “Cloud Provider” shall engage with Eskom on all risks impacting the “Cloud Provider’s service to Eskom. The controls designed to reduce these risks shall be communicated to Eskom. The “Cloud Provider” shall define this process which will be included in the “Cloud Provider’s” SLA with Eskom. The risk methodology employed shall align to Eskom’s Enterprise Risk management framework, aligned to ISO 31000.
- Eskom shall have access to the “Cloud Provider’s” corporate audit trail, including workflow and authorisation, when the audit trail spans cloud services rendered to Eskom.
- The “Cloud Provider” shall provide assurance of the facilities for management and control of cloud services and how such facilities are secured.

With the advancement of technological innovation and cross-border trade, compliance with international personal data protection legislation and standards has become imperative [8]. This is due to the fact that non-compliance with personal data protection legislation could impede Eskom from transferring personal data cross-border, thereby hindering the Eskom business operations. Personal data protection legislation may potentially restrict Eskom’s ability to conduct international business trade if compliance is inadequate. Whether or not Eskom is being prevented from transferring personal data cross-border, it is an issue of data sovereignty, in addition to being a data protection issue.

Data sovereignty is the principle that data, especially in electronic form, is regulated by the laws of the country in which such data resides. Personal data protection laws contain data sovereignty principles in that they prevent the transfer of personal data to another country, unless certain conditions for such transfer are complied with under the laws of the country from which the personal data transfer is to be made. In the digitally disruptive age of the internet and electronic commerce (e-commerce) involving the cross-border flow of personal data, a high premium has been placed on personal data and its ability to either promote or hinder international trade. Hence, e-commerce has ushered in a new era of international trade, particularly on the resource-rich African continent, where business growth and FDI (Foreign Direct Investment) continually allow the harnessing of new opportunities.

Business in Africa is expanding at a rapid pace due to a proliferation of investment opportunities on the continent. To effectively conduct business in Africa, Eskom need to understand the African personal data protection regulatory landscape. Non-compliance with personal data protection legislation in Africa may potentially preclude Eskom from capitalising on their African exploits, by restricting their ability to transfer personal data to third parties beyond African borders, thus hindering business operations. In order for Eskom to facilitate the cross-border transfer of personal data between various geographical operations and optimise its business processes in Africa and beyond, Eskom should consider:

- The current African personal data protection regulatory landscape.
- The compliance challenges which this regulatory landscape precipitates for Eskom seeking to leverage off the vast investment opportunities in Africa.
- Understand how to potentially overcome pertinent personal data protection regulatory obstacles, while concurrently augmenting business growth, stakeholder confidence and market competitiveness.

A core theme with regard to international trade and personal data protection regulatory compliance is the issue of cross-border personal data transfers, which are necessary in order for Eskom to conduct business internationally. African personal data protection laws in African countries where they do exist, place restrictions on the transfer of personal data to third parties who are situated outside the borders of the country in which an organisation has a presence and from which the personal data is being transferred. However, these restrictions are not intended to be a barrier to Eskom or African (and global) business operations. Rather, they outline the conditions which must be fulfilled for cross-border personal data transfers to be within the limits of the relevant African personal data protection legislation.

In the event that these laws are not complied with, Eskom would not be able to lawfully transfer personal data (whether relating to customers, employees, suppliers, business partners or others) across borders as part of its business operations. This could potentially result in lost business opportunities and hamper Eskom’s ability to trade internationally, leading to a diminished geographical footprint which in turn, could result in reduced revenues and market competitiveness. This would entail the cross-border transfer of personal data to the “Cloud Provider’s” data centres (should they not be located in South Africa) and to the geographic location from which the data will be accessible by anyone within Eskom from any location. Eskom would have to ensure that it engages a “Cloud Provider” whose data servers are located in South Africa with adequate personal data protection laws. The African continent, for the most part, does not have personal data protection laws, other than a few countries.

8.4.1 Understanding the African Personal Data Protection Landscape

Figure 20 outlines the personal data protection coverage in Africa, which indicates that there is no unified approach to personal data protection across the African continent, with some countries having comprehensive personal data protection legislation in place and others have no legislation or constitutional protection. Adapting personal data compliance programmes to be in line with disparate legislation and regulation is no minor feat.

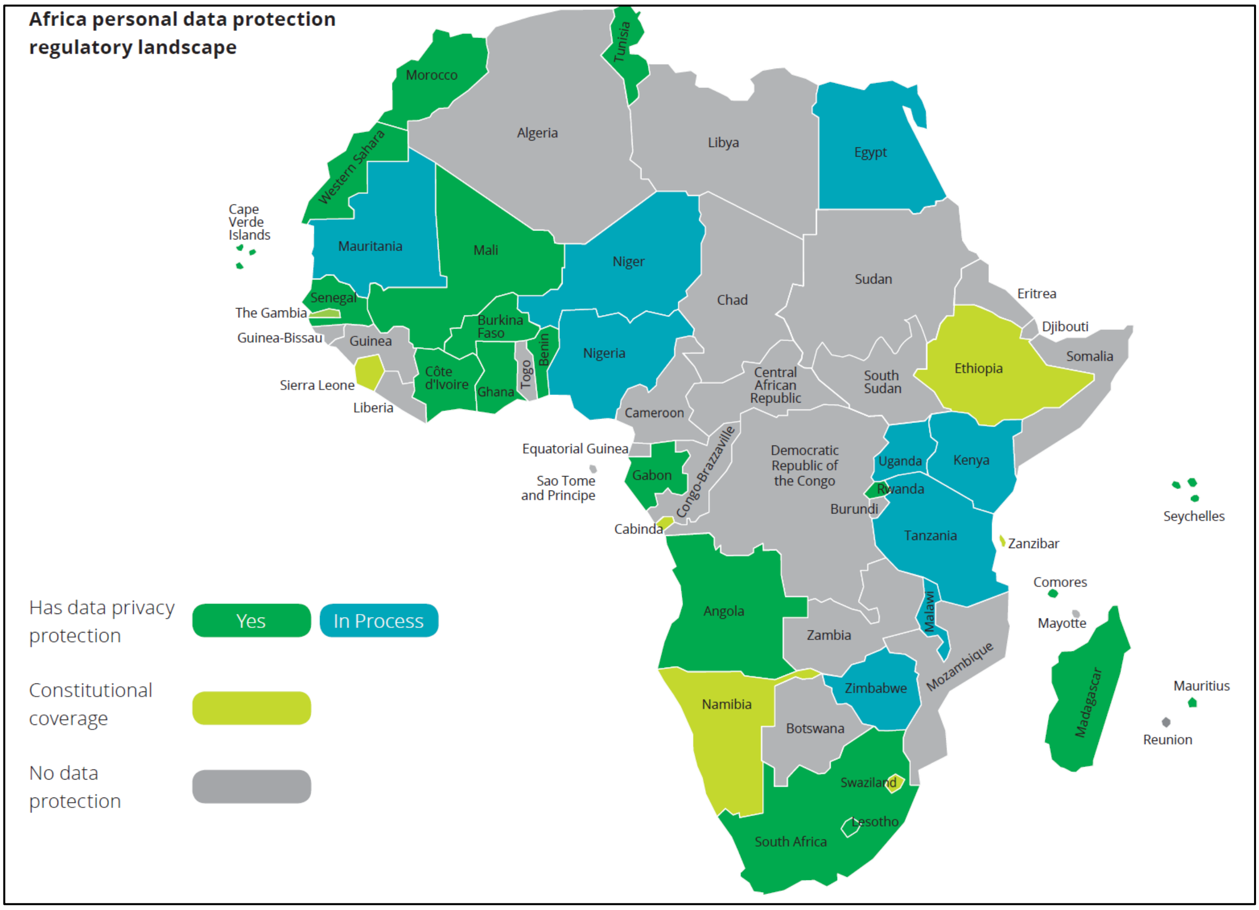


Figure 20: Africa Personal Data Protection Regulatory Landscape

There are currently 17 countries in Africa that have enacted comprehensive personal data protection legislation (i.e. Angola, Benin, Burkina Faso, Cape Verde, Gabon, Ghana, Ivory Coast, Lesotho, Madagascar, Mali, Mauritius, Morocco, Senegal, Seychelles, South Africa, Tunisia and Western Sahara). In addition, the AU (African Union) adopted the AU Convention on Cybersecurity and Data Protection (AU Convention) in June 2014. However, the AU Convention has not currently taken effect as it has, to date, not been ratified by 15 out of the 54 AU member jurisdictions. Nonetheless, the AU Convention does provide a personal data protection framework which African countries may potentially transpose into their national legislation and encourages African countries to recognise the need for protecting personal data and promoting the free flow of such personal data, taking global digitalisation and trade into account. In this regard, there are three countries (i.e. Kenya, Uganda and Zimbabwe) which have already enacted personal data protection legislation, the promulgation of which has not yet been made effective, as the laws are still in the form of bills. Tanzania is another country which is currently in the process of enacting personal data protection legislation.

8.4.2 Comparison with the European Union Personal Data Protection Regulatory Framework

The EU (European Union) personal data protection position is discussed in order to compare the AU (African Union) Convention personal data protection regulatory framework. The EU view is highlighted to demonstrate the benefit to Eskom in developing and implementing a comprehensive compliance programme to the African/South African personal data protection regulatory framework. The EU GDPR (General Data Protection Regulation) came into force on the 25th May 2018. The GDPR is automatically enforceable within EU member states. In contrast, the AU Convention will not have any legal force unless it is transposed into an African country's legislation. Furthermore, the EU is similar to Africa in the sense that there are disparate data protection legislative requirements across the various EU member states, which can present unique compliance challenges to organisations with an EU presence. Thus, the GDPR will unify the EU's personal data protection regime, thereby making it somewhat simpler for organisations with an EU presence (throughout several EU member states) to streamline their compliance activities across their EU footprint. It is easier to comply with a single piece of personal data protection legislation across multiple EU jurisdictions, as opposed to several disparate pieces of legislation within the region. It is elucidated organisations with an African presence may conduct their personal data protection compliance programmes to achieve adequate compliance with disparate Africa legislative regimes. The AU Convention does not currently have a "GDPR-equivalent" personal data protection framework in place. There are common personal data protection themes or principles contained in the legislation adopted by the African jurisdictions which have enacted comprehensive data protection legislation. These themes comprise of:

- Choice and consent.
- Data security.
- Data access and correction.
- Data quality and integrity.
- Data retention and destruction.
- Registration with a DPA (Data Protection Authority).
- Cross-border data transfers.
- Personal data breach notification.
- Appointment of a DPO (Data Protection Officer).

Despite most of the aforesaid personal data protection themes being contained in the legislation adopted by the above-mentioned African countries, there are particular principles that differ significantly from country to country. The pertinent personal data protection principles to which these differences relate, are:

- Registration with a DPA.
- Cross-border data transfers.
- Data breach notification.
- Appointment of a DPO.

Some jurisdictions require organisations to register with a DPA, while others do not. Moreover, 15 of the 16 above-mentioned African countries require that organisations put in place mechanisms for the cross-border transfer of personal data. The legislative disparities between the various African jurisdictions in respect of personal data protection may prove challenging to multinational organisations with an African presence. Accordingly, any compliance programmes will need to be tailored to account for these disparities. Lack of compliance will result in stiff penalties if all legislative nuances are not sufficiently addressed. Figure 21 demonstrates the challenges.

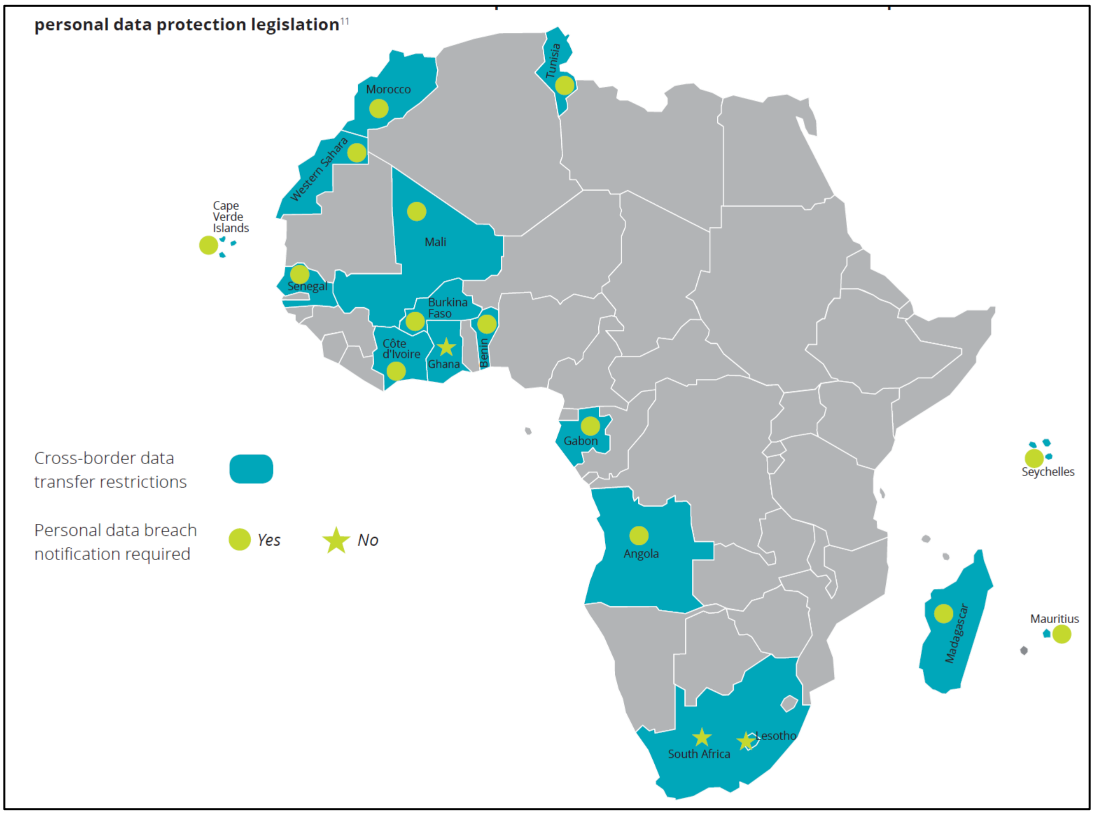


Figure 21: Cross-Border Data Transfer and Breach Notification Requirement in African Countries which have Adopted Personal Data Protection Legislation

It is evident from Figure 21 that while organisations with a presence in any of the above African jurisdictions will need to ensure that it has cross-border mechanisms in place within each relevant jurisdiction, it only needs to implement breach notification mechanisms within its business processes where it has a presence in Ghana and South Africa. However, international personal data protection best practice dictates that despite breach notification mechanisms not being required in all other jurisdictions, it will be imperative for Eskom to notify individuals if their personal data have been compromised during if a personal data breach does occur.

8.4.3 Existing Trends and Aggressiveness of African DPAs in Enforcing Personal Data Protection Legislation

Current statistics reflect DPA activity in countries such as Ghana and Mauritius as being more robust due to recent action taken or fines issued for non-compliance with relevant personal data protection legislation. The Ghanaian DPA has recently issued fines against certain organisations in the aviation industry for breaching the Ghanaian Data Protection Act. In respect of DPAs in countries such Senegal and Tunisia, there have not been any reports of particularly robust DPA activity. In contrast, the Moroccan DPA has recently investigated the data protection practices of several websites and applications which collect and process personal data in the context of providing online services. In countries such as Angola, Cape Verde, Madagascar, Mali and South Africa, there has been minimal DPA enforcement and activity (e.g. in South Africa, the

Information Regulator was only recently appointed and is still in the process of getting its administrative affairs in order). It is therefore evident that the legislative disparities as well as the disparities in DPA enforcement and activity across the African continent, will pose a compliance challenge to Eskom.

8.4.4 Potential Solutions for Multinational Organisations with an African Footprint to Overcome Compliance Challenges

Eskom with its African footprint must achieve optimal compliance with disparate, or even similar personal data protection regulations, especially in Africa. A high standard of personal data protection compliance should be applied (e.g. the EU's GDPR or South Africa's PPI Act 4 of 2013, POPI, which is modelled on the EU's personal data protection framework). If a higher compliance standard is applied, based on a particular country's legislative requirements, it would potentially streamline the compliance efforts within countries with a lower compliance standard, as there would potentially be automatic compliance due to not having to apply a lower standard of compliance. Thereafter, peculiar legislative requirements may be nuanced where necessary and complied with once the similar legislative requirements and common personal data protection principles and themes have been met. Accordingly, applying a "one-size-fits-all approach" would not be prudent in ensuring that all legislative requirements have been sufficiently covered.

8.4.5 Considering the Implementation of a Globally Endorsed Personal Data Protection Compliance Standard: a GDPR Standard

If the GDPR standard were to be applied by African organisations, this would ensure compliance with most, if not all African personal data protection requirements. Eskom should therefore develop a thorough understanding of the data protection legislation (if any) in the African jurisdictions in which they have a presence and map the similarities and differences relating to the common personal data protection themes, within every pertinent piece of personal data protection legislation. This will, as part of Eskom's personal data protection programme, enable more streamlined embedding of policies, processes and procedures within business processes to achieve a level of compliance which is mature, across its entire geographical footprint. Such an approach would enable Eskom's commercial relationships to be preserved while at the same time, achieving legislative compliance. Applying the GDPR standard would also allow for disparate cross-border data transfer requirements to be more easily complied with, since the GDPR (being a high global standard) sufficiently caters for most scenarios involving the cross-border transfer of personal data and the requirements that need to be adhered to in such circumstances.

8.4.6 Binding Corporate Rules

BCR's (Binding Corporate Rules) could be utilised within a group of undertakings to ensure compliance with cross-border transfers, thereby promoting Eskom's ability to trade internationally and expand its market share and market competitiveness. BCRs are effectively intra-group personal data protection policies and procedures. They will serve as a mechanism for Eskom to share personal data within the Eskom's group of undertakings, despite inadequant personal data protection legislation within its own and African jurisdiction. For cross-border data transfers to third parties outside of Eskom's group of undertakings, it would be prudent to engage in a binding contract with airtight personal data protection clauses to ensure the privacy and security of any personal data shared with such third parties. Furthermore, the countries which personal data is transferred to must be assessed from a data sovereignty perspective to ensure that there are no other laws which place the personal data at risk (e.g. is the government of South Africa able to subpoena such data or are there any other laws which dictate how personal data in South Africa is to be dealt with).

8.4.7 Conclusion

Eskom will need to set the ball in motion as far as understanding the South African and African personal data protection regulatory framework is concerned in order to ensure that Eskom is able to effectively capitalise on the vast investment opportunities in Africa. As personal data is the new currency with which to effectively conduct business operations globally, all stakeholders including Eskom's business partners would be confident in partnering with organisations who place a high premium on personal data protection on the African continent. Hence, Eskom should proactively address questions such as:

- Do we know and understand our geographical footprint, especially within Africa?
- Do we know whether there are personal data transfer restrictions in the African jurisdictions (and elsewhere) within which we have a presence?
- Are our cross-border operations legally compliant?

Eskom's Legal and Technology teams should assist the organisation to answering these questions effectively and structure its personal data protection compliance programmes accordingly.

9. CLOUD TAXONOMY

Taxonomy is the science of categorisation, or classification, of things based on a predefined system. Taxonomy contains a controlled vocabulary with a hierarchical tree-like structure (see Figure 22). This taxonomy is based on the Eskom Cloud Reference Architecture (i.e. a four-level taxonomy describing the key concepts associated with cloud computing):

- **Level 1 -** Is a set of obligations and behaviors as conceptualised by the associated actors in the context of cloud computing.
- **Level 2 –** An activity, which entails the general behaviors or tasks associated to a specific role.
- **Level 3 –** A component, which refer to the specific processes, actions, or tasks that must be performed to meet the objective of a specific activity.
- **Level 4 –** A sub-component, which present a modular part of a component.

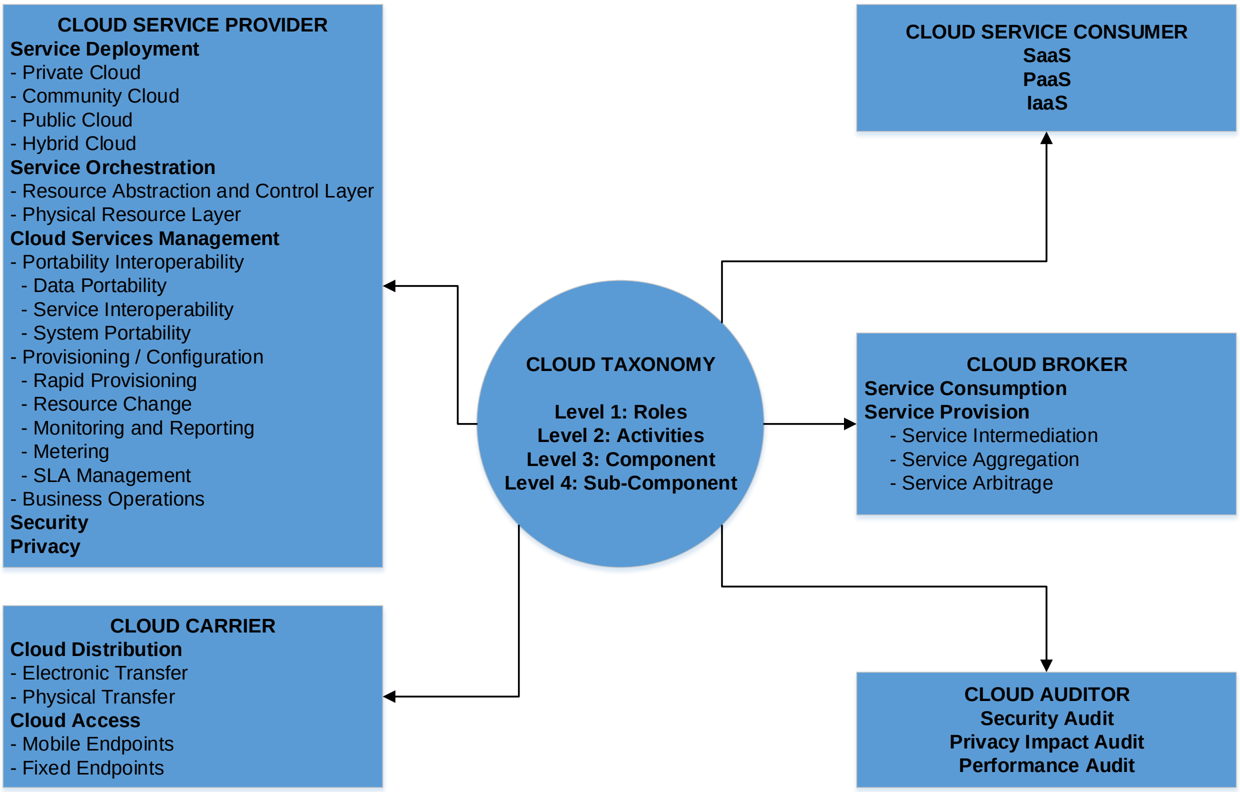


Figure 22: Cloud Taxonomy

9.1 First Level Terms

The First Level terms refers to the cloud actors:

- The “Cloud Consumer”
- The “Cloud Provider”
- The “Cloud Carrier”
- The “Cloud Broker”
- The “Cloud Auditor”

9.2 Second Level Terms

- **Cloud Distribution** – The process of transporting cloud data between “Cloud Provider’s” and Eskom.
- **Cloud Access** – To make contact with or gain access to Cloud Services by Eskom.
- **Service Deployment** – All activities needed to make a cloud service available to Eskom.
- **Service Orchestration** - The arrangement, coordination and management of cloud infrastructure to provide different cloud services to meet IT and business requirements.

- **Cloud Service Management** – Includes all the service-related functions necessary for the management and operations of those services required by or proposed to Eskom.
- **Security –** Refers to information security protecting information and IMS from unauthorised access, use, disclosure, disruption, modification, or destruction to provide Eskom with:
  - **Integrity** – Is guarding against improper information modification or destruction and includes ensuring information nonrepudiation and authenticity.
  - **Confidentiality -** Is preserving authorised restrictions on access and disclosure, including means for protecting personal privacy and proprietary information.
  - **Availability** - Is ensuring timely and reliable access to and use of information.
- **Privacy** - Information privacy is the assured, proper and consistent collection, processing, communication, use and disposition of disposition of PI and PII throughout its life cycle.

A formal information security governance framework establishes chains of responsibility, authority and communication. It describes the roles of people involved in the production cycle of content, their responsibilities, the ways in which they interact and the general rules and policies regarding the production of content. The category of cloud services offered by the “Cloud Provider” (IaaS, PaaS or SaaS) has an impact on the sharing of responsibilities between Eskom and the “Cloud Provider” in order to manage security and its associated risks. The responsibilities per offering are being discussed.

SaaS

The capability provided to Eskom is to use the “Cloud Provider’s” applications running on a cloud infrastructure. The applications are accessible from various “Cloud Provider’s” through a thin client interface such as a web browser (e.g. web-based email). Eskom 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.

- The “Cloud Provider” is responsible for the infrastructure, software and data. These aspects shall have appropriate coverage in the contract and the SLA between the “Cloud Provider” and Eskom.
- From a general governance perspective, “Cloud Provider’s” shall shall notify Eskom via a mutually agreed upon notification process, about the occurrence of any security incident in their system, regardless of the parties or data directly impacted.
- The “Cloud Provider” shall provide Eskom information about the location(s) of their data centers and allow Eskom to choose which of these location(s) to use for a given cloud service rendered to Eskom (see Figure 23).

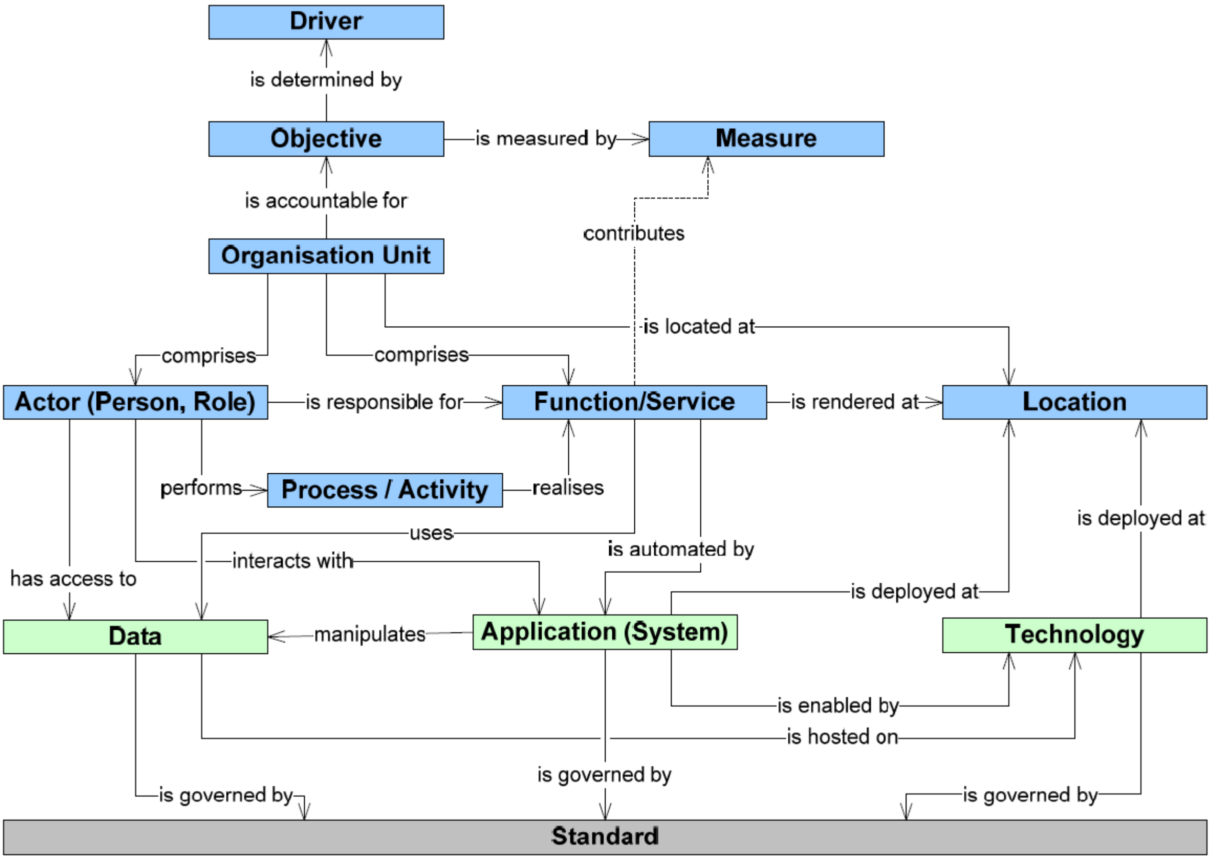


Figure 23: GWEA Meta Model

PaaS

The capability provided to Eskom is to deploy onto the cloud infrastructure Eskom-created or acquired applications created using programming languages and tools supported by the “Cloud Provider”. Eskom does not manage or control the underlying cloud infrastructure (i.e. network, servers, operating systems, or storage) but has control over the deployed applications and possibly application hosting environment configurations. For a PaaS offering, it is likely that much of the software stack is under the control of the “Cloud Provider” with the application code being the responsibility of the Eskom.

- **Service Consumption –** A “Cloud Broker” in the act of using a Cloud Service.
- **Service Provision –** A “Cloud Broker” in the act of providing a Cloud Service.
- **Security Audit** - Systematic evaluation of a cloud system by measuring how well it conforms to a set of established security criteria.
- **Privacy-Impact Audit** - Systematic evaluation of a cloud system by measuring how well it conforms to a set of established privacy-impact criteria.

- **Performance Audit** - Systematic evaluation of a cloud system by measuring how well it conforms to a set of established performance criteria.

IaaS

The capability provided to Eskom is to provision processing, storage, networks and other fundamental computing resources where Eskom is able to deploy and run arbitrary software, which can include operating systems and applications. Eskom 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). For IaaS, the provider shall supply and be responsible for securing basic computing resources (i.e physical and VM's, disks and networks). Eskom shall be responsible for securing the operating system, the entire software stack necessary to run applications as well as Eskom data placed into the cloud computing environment.

9.3 Third Level Terms

- **Service Intermediation** - An intermediation broker provides a service that directly enhances a given service delivered to Eskom and essentially adding value on top of a given service to enhance some specific capability.
- **Service Aggregation** - An aggregation brokerage service combines multiple services into one or more new services. It will ensure that data is modeled across all component services and integrated as well as ensuring the movement and security of data between Eskom and multiple providers.
- **Service Arbitrage** - Cloud service arbitrage is similar to cloud service aggregation. The difference between them is that the services being aggregated are not fixed. Indeed the goal of arbitrage is to provide flexibility and opportunistic choices for the service aggregator (e.g. providing multiple e-mail services through a "Cloud Provider" or providing a credit-scoring service that checks multiple scoring agencies and selects the best score).
- **Private Cloud** - The cloud infrastructure is operated solely for Eskom. It may be managed by Eskom or a third party and may exist on premise or off premise.
- **Community Cloud** - The cloud infrastructure is shared by several organisations and supports a specific community that has shared concerns (e.g. mission, security requirements, policy, and compliance considerations). It may be managed by Eskom or a third party and may exist on premise or off premise.
- **Public Cloud** - The cloud infrastructure is made available to the general public or a large industry group and is owned by a "Cloud Provider".
- **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 standardised or proprietary technology that enables data and application portability (e.g. cloud bursting for load-balancing between clouds).
- **Service Layer** - Defines the basic services provided by "Cloud Providers".

- **Physical Resource Layer** - Includes all the physical resources used to provide cloud services, most notably, the hardware and the facility.
- **Resource Abstraction and Control Layer** - Entails software elements, such as hypervisor, VM's, virtual data storage and supporting software components, used to realise the infrastructure upon which a cloud service can be established.
- **Portability** - The ability to transfer data from one system to another without being required to recreate or reenter data descriptions or to modify significantly the application being transported. The ability of software or of a system to run on more than one type or size of computer under more than one operating system.
- **Interoperability** - The capability to communicate, to execute programs, or to transfer data among various functional units under specified conditions.
  - **Provisioning / Configuration** – The process of preparing and equipping a "Cloud Provider" to allow it to provide services to Eskom.
  - **Mobile Endpoints** - A physical device, often carried by Eskom users that provides a man/machine interface to cloud services and applications. A Mobile Endpoint may use multiple methods and protocols to connect to cloud services and applications.
  - **Fixed Endpoints** - A physical device, fixed in its location that provides a man / machine interface to cloud services and applications. A fixed endpoint typically uses one method and protocol to connect to cloud services and applications.

9.4 Fourth Level Terms

- **Data Portability** – The ability to transfer data from one system to another without being required to recreate or reenter data descriptions or to modify significantly the application being transported.
- **Service Interoperability** - The capability to communicate, execute programs, or transfer data among various cloud services under specified conditions.
- **System Portability** - The ability of a service to run on more than one type or size of cloud.
- **Rapid provisioning** – Automatically deploying cloud system based on the requested service/resources/capabilities.
- **Resource change** – Adjust configuration/resource assignment for repairs, upgrades, and joining new nodes into the cloud.
- **Monitoring and Reporting** – Discover and monitor the virtual resources, monitor cloud operations and events as well as generate performance reports.
- **Metering** - Provide a measuring capability at some level of abstraction appropriate to the type of service (e.g, storage, processing, bandwidth and active user accounts).
- **SLA management** – Encompasses the SLA contract definition (basic schema with QoS parameters), SLA monitoring and SLA enforcement according to the defined policies.

10. CLOUD SECURITY STANDARDS

One approach to mapping cloud security standards is to map the relevant cloud standards against the Eskom Cloud Reference Architecture as the Eskom Cloud Refernce Architecture is as an integrated diagram of systems as well as organisational and process components. The Cloud Taxonomy provides further categorisations for the security, interoperability and portability aspects for cloud. While many standards are generally relevant to these cloud computing areas, the following sections will map those specifically relevant cloud standards and capture their standard maturity status. Some standards may apply to more than one category from the Cloud Taxonomy and therefore may be listed more than once and Eskom should therefore make use of these standards as sufficient guidelines to enable its cloud offering.

Cloud encompasses a variety of systems and technologies as well as service deployment and business models. Cloud has unique attributes (i.e. elasticity, rapid provisioning and releasing, resource pooling, multi-tenancy, broad-network accessibility and ubiquity) and can therefore realise various benefits for Eskom if adopted legally and ensuring that the data and systems affected are appropriately classified. However, it also entails specific security risks associated with the type of adopted cloud and deployment mode. To accelerate the adoption of cloud computing and to advance the deployment of cloud services, solutions coping with cloud security threats need to be addressed. Many of the threats that “Cloud Provider”s and Eskom will face can be addressed through traditional security processes and mechanisms (i.e. security policies, cryptography, identity management, intrusion detection/prevention systems and supply chain vulnerability analysis). However, risk management activities must be undertaken to determine how to mitigate the threats specific to different cloud models and to analyse existing standards for gaps that need to be addressed. Securing the information systems and ensuring the confidentiality, integrity and availability of information and information being processed, stored and transmitted are particularly relevant as these are the high-priority concerns and present a higher risk of being compromised in the cloud. Cloud implementations are subject to local physical threats as well as remote, external threats. Consistent with other applications of IT, the threat sources include accidents, natural disasters that induce external loss of service, hostile governments, criminal organisations, terrorist groups and malicious or unintentional vulnerabilities exploited through internal, external, authorised, or unauthorised access to the system. The complexity of the cloud supporting three service types and four deployment models and the cloud characteristics, specifically multi-tenancy, heighten the need to consider data and systems protection in the context of logical, physical boundaries and data flow separation. Possible types of security challenges for cloud services are:

- Confidentiality and integrity of data in transit to and from a “Cloud Provider” and at rest.
- Attacks which take advantage of the homogeneity and power of cloud computing systems to rapidly scale and increase the magnitude of the attack.
- Eskom’s unauthorised access (through improper authentication or authorisation, or exploit of vulnerabilities introduced maliciously or unintentionally) to software, data and resources provisioned to and owned by another authorised “Cloud Consumer”.
- Increased levels of network-based attacks that exploit software not designed for an Internet-based model and vulnerabilities existing in resources formerly accessed through private networks.
- Limited ability to encrypt data at rest in a multi-tenancy environment.

- Portability constraints resulting from the lack of standardisation of cloud services API's (Application Programming Interfaces) that preclude Eskom to easily migrate to a new cloud service provider when availability requirements are not met.
- Attacks that exploit the physical abstraction of cloud resources and exploit a lack of transparency in audit procedures or records.
- Attacks that take advantage of known, older vulnerabilities in VM's that have not been properly updated and patched.
- Attacks that exploit inconsistencies in global privacy policies and regulations.
- Attacks that exploit cloud computing supply chain vulnerabilities to include those that occur while cloud computing components are in transit from the supplier to the "Cloud Provider".
- Insider abuse of their privileges, especially "Cloud Provider's" personnel in high risk roles (e.g. system administrators).
- Interception of data in transit (man-in-the-middle attacks).

Some of the main security objectives for Eskom from the "Cloud Provider" should include:

- Protect Eskom's data from unauthorised access, disclosure, modification or monitoring. This includes supporting IAM (Identity and Access Management) and access control policies for authorised users accessing cloud services. This includes the ability of Eskom to make access to its data selectively available to other users.
- Prevent unauthorised access to cloud infrastructure resources. This includes implementing security domains that have logical separation between computing resources (e.g. logical separation of Eskom's workloads running on the same physical server by VM monitors [hypervisors] in a multi-tenant environment) and using secure-by-default configurations.
- Eskom's Web Application pattern should be used as a guideline to mitigate Internet threats.
- Challenges to prevent Internet browsers using cloud from attacks to mitigate end-user security vulnerabilities. This includes taking measures to protect internet-connected personal computing devices by applying security software, personal firewalls and patch maintenance.

Eskom should therefore include access control and intrusion detection as well as prevention solutions in its cloud implementations and conduct an independent assessment to verify that the solutions are installed and functional. This includes traditional perimeter security measures in combination with the domain security model. Traditional perimeter security includes restricting physical access to network and devices; protecting individual components from exploitation through security patch deployment; setting as default most secure configurations; disabling all unused ports and services; using role-based access control; monitoring audit trails; minimising privileges to minimum necessary; using antivirus software and encrypting communications. Trust boundaries between "Cloud Providers" and Eskom should be defined to ensure that the responsibilities to implement security controls are clearly identified. Eskom should also implement standardised API's for interoperability and portability to support easy migration of Eskom's data to other "Cloud Providers" when necessary.

10.1 Authentication and Authorisation

Table 4 maps the security standards for authentication and authorisation.

Categorisation	Standards	SDO
Authentication and Authorisation	RFC 5246 – SSL (Secure Sockets Layer) / TLS (Transport Layer Security)	IETF
	RFC 3820: X.509 - PKI (Public Key Infrastructure) Proxy Certificate Profile	IETF
	RFC5280: Internet X.509 - PKI Certificate and Certificate Revocation List (CRL) Profile	IETF
	RFC 5849 - OAuth (Open AuthoriSation Protocol)	IETF
	ISO/IEC 9594-8:2008 | X.509 - IT OSI (Open Systems Interconnection) - The Directory: Public-key and attribute certificate frameworks	ISO/IEC & ITU-T
	ISO/IEC 29115 | X.1254 - IT Security techniques Entity authentication assurance framework	ISO/IEC & ITU-T
	FIPS 181 - Automated Password Generator	NIST
	FIPS 190 - Guideline for the Use of Advanced Authentication Technology Alternatives	NIST
	FIPS 196 - Entity Authentication Using Public Key Cryptography	NIST
	OpenID Authentication	OpenID
	XACML (eXtensible Access Control Markup Language)	OASIS
	SAML (Security Assertion Markup Language)	OASIS

Table 4: Authentication and Authorisation

10.2 Confidentiality

Categorisation	Standards	SDO
Confidentiality	RFC 5246 – SSL / TLS	IETF
	KMIP (Key Management Interoperability Protocol)	OASIS
	XML Encryption Syntax and Processing	W3C
	FIPS 140-2 - Security Requirements for Cryptographic Modules	NIST
	FIPS 185 – EES (Escrowed Encryption Standard)	NIST
	FIPS 197 – AES (Advanced Encryption Standard)	NIST
	FIPS 188 - Standard Security Label for Information Transfer	NIST
	CAC (Common Access Control) 8201	FIPS

Table 5: Confidentiality

10.3 Identity Management

Categorisation	Standards	SDO
Identity Management	X.idmcc - Requirement of IdM in Cloud Computing	ITU-T
	FIPS 201-1 – PIV (Personal Identity Verification) of Federal Employees and Contractors	NIST
	SPML (Service Provisioning Markup Language)	OASIS
	WS (Web Services) Federation Language (WS-Federation) Version 1.2	OASIS
	WS-Trust 1.3	OASIS
	SAML	OASIS
	OpenID Authentication 1.1	OpenID Foundation

Table 6: Identity Management

10.4 Security Controls

Categorisation	Standards	SDO
Security Controls	Cloud Controls Matrix Version 1.3	CSA
	ISO/IEC 27001:2005 – IT Security Techniques Information Security Management Systems Requirements	ISO/IEC
	ISO/IEC WD TS 27017 – IT Security techniques - Information security management - Guidelines on information security controls for the use of cloud computing services based on ISO/IEC 27002	ISO/IEC
	ISO/IEC 27018 - Code of Practice for Data Protection Controls for Public Cloud Computing Services	ISO/IEC
	ISO/IEC 1st WD 27036-4 – IT Security techniques – Information security for supplier relationships – Part 4: Guidelines for security of cloud services	ISO/IEC

Table 7: Security Controls

10.5 Integrity

Categorisation	Standards	SDO
Integrity	XMLDSig (XML signature)	W3C
	FIPS 180-4 – SHS (Secure Hash Standard)	NIST
	FIPS 186-4 – DSS (Digital Signature Standard)	NIST
	FIPS 198-1 – HMAC (The Keyed-Hash Message Authentication Code)	NIST

Table 8: Integrity

10.6 Security Monitoring and Incident Response

Categorisation	Standards	SDO
Security Monitoring and Incident Response	ISO/IEC WD 27035-1 – IT Security techniques - Information security incident management - Part 1: Principles of incident management	ISO/IEC
	ISO/IEC WD 27035-3 – IT Security techniques - Information security incident management - Part 3: Guidelines for CSIRT operations	ISO/IEC
	ISO/IEC WD 27039; IT - Security techniques - Selection, deployment and operations of IDS (Intrusion Detection Systems)	ISO/IEC
	ISO/IEC 18180 – IT Specification for the XCCDF (Extensible Configuration Checklist Description Format) Version 1.2 (NIST IR 7275)	ISO/IEC
	X.1500 - Cybersecurity information exchange techniques	ITU-T
	X.1520: Common vulnerabilities and exposures	ITU-T
	X.1521 - Common Vulnerability Scoring System	ITU-T
	PCI Data Security Standard	PCI
	FIPS 191 - Guideline for the Analysis of LAN (Local Area Network) Security	NIST

Table 9: Security Monitoring and Incident Response

10.7 Availability

Categorisation	Available Standards	SDO
Availability	ATIS-02000009 - Cloud Services Lifecycle Checklist	ATIS
	ISO/PAS 22399:2007 - Societal security - Guideline for incident preparedness and operational continuity management	ISO

Table 10: Availability

10.8 Security Policy Management

Categorisation	Standards	SDO
Security Policy	ATIS-02000008 – TIE (Trusted Information Exchange)	ATIS
	FIPS 199 - Standards for Security Categorisation of Federal Information and Information Systems	NIST

Management	FIPS 200 - Minimum Security Requirements for Federal Information and Information Systems	NIST
	ISO/IEC 27002 - Code of practice for information security management	ISO/IEC
	XACML	OASIS

Table 11: Security Policy Management

10.9 Interoperability Standards

Categorisation	**Available Standards**	**SDO**
Service Interoperability	CIMI (Cloud Infrastructure Management Interface)	DMTF
	IEEE P2301, Draft Guide for CPIP (Cloud Portability and Interoperability Profiles)	IEEE
	IEEE P2302, Draft SIIF (Standard for Intercloud Interoperability and Federation)	IEEE
	Y.3520 - Cloud computing framework for end to end resource management.	ITU-T
	CAMP (Cloud Application Management Platform)	OASIS
	OCCI (Open Cloud Computing Interface)	OGF
	DFDL (Data Format Description Language)	OGF
	TOSCA (Topology and Orchestration Specification or Cloud Applications),Version 1.0 Committee Specification Draft 06 / Public Review Draft 01	OASIS
	CDMI (Cloud Data Management Interface), also approved as ISO/IEC 17826:2012, IT – CDMI	SNIA

Table 12 – Interoperability Standards

10.10 Portability Standards

Categorisation	**Available Standards**	**SDO**
Data Portability	CDMI	SNIA
System Portability	OVF (Open Virtualisation Format), OVF 1.0, also approved as INCITS 469-2010 & ISO/IEC 17203: 2011	DMTF
	OVF 2.0	DMTF
	IEEE P2301 - Draft Guide for CPIP (Cloud Portability and Interoperability Profiles)	IEEE
	TOSCA,Version 1.0 Committee Specification Draft 06 / Public Review Draft 01	OASIS

Table 13 – Portability Standards

10.11 Performance Standards and Service Agreements

There are numerous reasons why cloud computing standards for performance are needed in today's market. Eskom need to be able to objectively determine the costs and benefits of moving to cloud services to validate claims of performance by "Cloud Provider's" and to objectively compare services from multiple providers in order to better meet a specific need. Determining performance involves establishing a set of metrics that will provide a clear picture of how a given cloud service performs. This is complex due to the fact that specific metrics and standards will be needed for not only specific categories of services, but also due to the domains in which they are needed. Standards might be needed for attributes that are associated with the service such as network performance. Additionally, standards are needed that measure attributes specific to cloud service such as VM performance. While not an exhaustive list, other potential performance aspects relevant to the cloud include:

- Manage and Benchmark performance.
- Cloud service life cycle elements.
- Negotiation performance.
- Instantiation performance and Termination performance.
- Performance testing, Monitoring and Auditing.

These performance standards will be of interest to all stakeholders involved in cloud computing. Eskom and the "Cloud Providers" will use these standards and metrics as a basis for creating measurable and enforceable SLA contracts. "Cloud Auditors" will be able to measure performance for Eskom. "Cloud Brokers" will need these standards to ensure that Eskom's specific needs are met. "Cloud Provider"s will be performing self-evaluations on their own offerings. The topic of performance includes considerations related to monitoring, reporting, measuring, scaling and right-sizing cloud resources to meet the expected or experienced demand. This area deserves careful consideration, as it relates directly to the factors that control the potential cost savings to Eskom from the use of cloud.

Performance can potentially be scaled to meet conditions of anticipated or real-world demand, within the parameters of a cloud service agreement. It is therefore crucial that such agreements contain all necessary parameters that relate to the conditions for delivery of the associated cloud service or product. Only by careful measurement and by proper anticipation of peak workload conditions, backed by appropriate service remedies, credits, or penalties and appropriate fallback arrangements, can true cost savings be realised with proper delivery of services. Eskom should be careful to include suitable performance, monitoring and emergency metrics and conditions into the cloud service master agreement and associated SLA. These elements, reflecting Eskom's given mission and goals, will help to ensure that Eskom pay only for needed services.

Cloud services are particularly well suited to deployment of automated terms and conditions for the delivery of these services. While the basic parameters, legal and cost controls for cloud services require Eskom approval and human-mediated review, automated tools should be deployed where appropriate to ensure conditions such as failover in the event of cloud service component failure or compromise and scaling to meet emergent needs or to grow or shrink service delivery according to cost and / or demand and other relevant features. Wherever possible, standards-based methods for monitoring, measuring and scaling delivery of the resources to meet Eskom's missions should be pursued. Performance standards are needed for cloud service agreements and for cloud service monitoring (see Table 14).

Categorisation	Available Standards	SDO
Service Agreements	TOSCA,Version 1.0 Committee Specification Draft 06 / Public Review Draft 01	OASIS
	GB917 - SLA Management Handbook, Release 3.1	TM Forum
	GB963 - Cloud SLA Application Note, Version 1.2	TM Forum
	TR178 - Enabling End-to-End Cloud SLA Management, Version 0.4	TM Forum
	TR194 - Multi-Cloud Service Management Accelerator Pack - Introduction, Release 1.0	TM Forum
	TR195 - Multi-Cloud Service Management Pack - Business Guide, Release 1.0	TM Forum
	TR196 - Multi-Cloud Service Management Pack - Technical Guide, Release 1.0	TM Forum
	TR197 - Multi-Cloud Service Management Pack – SLA Business Blueprint	TM Forum
	TR198 - Multi-Cloud Service Management Pack – Developer Primer	TM Forum

Table 14 – Performance Standards and Service Agreements

10.12 Accessibility Standards

Accessibility is relevant to cloud computing services at the application level where a human interacts with an application. This is where accessibility is measured. Therefore, many of the existing accessibility standards for ICT applications are relevant to cloud computing applications. Table 16 lists accessibility standards, which may be relevant for Eskom cloud applications.

Categorisation	Available Standards	SDO
Accessibility	Section 508 standards (Technical Standards 1194.21 Software applications and operating systems; 1194.22 Web-based intranet and internet information and applications; and 1194.23 Telecommunications products)	US Access Board
	W3C WCAG (Web Content Accessibility Guidelines) 2.0	W3C
	ISO 9241-20:2008, Ergonomics of human-system interaction - Part 20: Accessibility guidelines for ICT equipment and services	ISO/IEC
	ISO 9241-171:2008, Ergonomics of human-system interaction -- Part 171: Guidance on software accessibility	ISO/IEC
	ISO/IEC 24751-1:2008, IT - Individualised adaptability and accessibility in e-learning, education and training -- Part 1: Framework and reference model	ISO/IEC
	ANSI/HFES 200 Human Factors Engineering of Software User Interfaces (Parts 1, 2, and 3)	ANSI

Table 15 – Accessibility Standards

10.13 The Internal Control Environment of a "Cloud Provider"

As a baseline, Eskom shall request a report of the "Cloud Provider's" operations by independent auditors. The "Cloud Provider" shall offer access to audit events, log and report information relevant to Eskom's specific data or applications within an upfront agreed time frame which shall be specified in the contract. The "Cloud Provider" shall ensure the following before Eskom can consume a cloud service:

- At a minimum, virtual isolation of Eskom's applications and data in a shared multi-tenant environment.
- Provide protection of Eskom's assets from unauthorised access by the "Cloud Provider's" staff or the "Cloud Provider's" 3rd party service providers.
- Provide protection of Eskom's assets from accidental or unintentional access by Eskom's employees and 3rd party service providers.

10.14 Corporate Audit Trail

The "Cloud Provider" shall provide Eskom with access to the "Cloud Provider's" event, logs and audit trails that prove the enforcement of the "Cloud Provider's" security controls. The independent auditors to shall assure Eskom that all the necessary information relating to the use of particular applications and data against all security and compliance policies established by the "Cloud Provider" or Eskom is being logged and stored appropriately by the "Cloud Provider". This information includes at a minimum AAA (Authentication, Authorisation and Accounting). The "Cloud Provider" shall ensure that Eskom has complete visibility into the security controls that relate to its data and applications and shall be responsible for the routine flow of audit information form the "Cloud Provider" to Eskom. This flow may take the form of security logs and reports on an agreed upon schedule. The "Cloud Provider" shall be required to supply the above information via APIs or web services from all the audit facilities pertaining to Eskom's applications and data and this data flow shall be encrypted. The "Cloud Provider" shall ensure the timely notification of exceptional security alerts, events or incidents. The incident management process shall be documented and audited. The audited data shall have the necessary meta data associated with it to enable forensic analysis on how the incident occurred and the assets that were compromised.

10.15 Facilities for Management and Control of Cloud Services

A "Cloud Provider" may provide facilities such as service catalogues, subscription services, payment processes, the provision of streams of operational event data and logs, usage metering data, facilities for configuring services including the addition and removal of user identities and the management of authorisations. Eskom shall ensure the security audit extends to these facilities as well as to the main services of the "Cloud Provider" (see Table 16).

Standards Requirement	Certification Requirement
The "Cloud Provider" shall conform to ISO/IEC 27000 series	"Cloud Provider" shall provide ISO/IEC 27001 Certification
	"Cloud Provider" shall provide ISO/IEC 27017

	certification
The "Cloud Provider" shall comply to SSAE16 for cloud services with financial activities	"Cloud Provider" shall provide SSAE16 certification
Eskom's Information Security Log Management standard (240-106914007).	

Table 16:Operational and Business Process Audit Standards Requirement

10.16 People, Roles and Identities

The use of cloud services means that employees of both Eskom and the "Cloud Provider" shall have the ability to access Eskom's cloud hosted systems, hence the "Cloud Provider" shall ensure the following measures are in place:

- The "Cloud Provider" shall have processes approved by Eskom and functionality that govern who has access to the Eskom's data and applications.
- The "Cloud Provider" shall allow Eskom to assign and manage the roles and associated levels of authorisation for each of their users in accordance with Eskom's security policies and apply the principle of least privilege.
- The "Cloud Provider" shall have a secure system for provisioning and managing unique identities for their users and services. This IAM (Identity and Access Management) functionality shall support simple resources allowing for Eskom's application and service workflows.
- Any user access to the "Cloud Provider's" management platform, regardless of role or entitlement, shall be monitored and logged to provide auditing of all access to Eskom data and applications.

The "Cloud Provider" shall use Eskom's KMS (Key Management System) to safeguard cryptographic keys and passwords. The "Cloud Provider" shall allow for multifactor authentication to a user's device (hardware or virtual). The capabilities required to manage the people, roles and identities is depicted Table 17: Capabilities Required to Manage People, Roles and Identities.

Capabilities	**Eskom's Requirement of the Capability**
FIM (Federated Identity Management), EIP (External Identity Providers)	The Cloud service shall integrate with Eskom's current IAM solution.
Identity Provisioning and Delegation	The "Cloud Provider" shall allow Eskom to administer their own users. Thus, the "Cloud Provider" should support delegated administration. If the cloud service cannot integrate with Eskom's IAM solution, the "Cloud Provider" is required to provide tools for the onboarding and offboarding of users.
SSO (Single Sign-On), Single Sign-Off	The "Cloud Provider" shall offer SSO for access across multiple services offered by the "Cloud Provider" based on standards such as SAML 2.0, OAuth or WS-Federation.
Identity and Access Audit	The "Cloud Provider" shall provide auditing logs, reports alerts and notifications in order to monitor user access both for Eskom's and its auditors needs.
Robust Authentication	"Cloud Provider" shall support strong authentication using MFA and or biometric authentication for high value assets hosted in the cloud service. The strong authentication shall apply both to the "Cloud Provider" administrative and Eskom access
Service ID and API Keys	With the cloud native microservices approach, Eskom also need to manage the identity and access of services. This is typically done through use of the service ID which is an identity that can be used by an application or service. The developer can also create and associate API keys with the service ID, which is used to authenticate and access other services based on the policy and permissions set. If the cloud service supports API integration the "Cloud Provider" shall allow for Service ID and use of API Keys.

Table 17: Capabilities Required to Manage People, Roles and Identities

Standards Requirement	**Certification Requirement**
"Cloud Provider" shall support federated ID and SSO based on one or more of the following standards: • OAuth 2.0 • WS-Federation • OpenID • SCIM	"Cloud Provider" shall have ISO/IEC27001certification.
"Cloud Provider" needs to provide access and security policy decisions leveraging industry standard protocols such as XACML.	"Cloud Provider" shall have ISO/IEC 27017 or equivalent certification.
The "Cloud Provider" shall support the following security certificates: • PKCS	

• X.509 • OpenPGP	
Eskom's Information Security Logical Access Control standard (32-351).	

Table 18: Manage People, Roles and Identities Standards Requirement

10.17 Protection of Data

Data is at the core of Eskom's security concern irrespective of the infrastructure used and cloud computing does not change this. The following security considerations shall apply to the cloud service:

- Data at rest - held on some form of storage system.
- Data in motion - being transferred over some form of communication link.
- Data in process - data in memory being used by application code.

When Eskom's data is in motion the following standards shall be applied at a minimum (see Table 19).

Type of Data Flow	Requirement
Connections from Eskom over the internet to cloud service	HTTPS
Bulk Data Transfers	SFTP
Eskom employees to Cloud Service	VPN using IPSec or SSL
Secure and private connections between two connected applications	TLS

Table 19: Data in Flow Security Requirements

When Eskom's data is at rest in a cloud service the principle of encrypting sensitive data at rest shall be taken. "Cloud Provider" shall comply to the following:

- The US FIPS 140-2 standard can be used as guidance with regards which data at rest encryption algorithm.
- The encryption keys shall not be stored alongside the data. For IaaS and PaaS the keys shall be stored by Eskom and passed to the application as and when needed.

In Eskom various data types are created and consumed, therefore controls must be in place for the storage and processing of this data. Table 20 specifies the minimum requirements that need to be met per data classification type from a cloud perspective. Prior to moving data into the cloud an assessment of the data needs to be done to classify it (both data and asset) acceding to its sensitive and criticality.

Data Classification	**Guideline**
Public	Can be processed and/or stored in a Cloud environment subject to the implementation of the Security Controls for the Cloud.
Controlled Disclosure	Can be processed and/or stored in a Cloud environment subject to the implementation of the Security Controls for the Cloud.
Confidential	The DC (Data Centres) of the “Cloud Provider”, including backup DCs, shall be in sovereign regions with privacy and data governance laws at least equal to those of South Africa. Eskom information shall not be stored in data centres based in countries with authoritarian laws that make provision for the seizure of information belonging to any organisation during an unrelated legal matters.
	User and Service authentication shall be done using the current Eskom IAM solution.
Secret	Application processing shall be done on physical or virtual servers that is exclusively for the use of Eskom, its subsidiaries and users (e.g. a SaaS instance that is not shared with a non-Eskom entity).
	Eskom Information shall not share storage services with a non-Eskom entity.
Top Secret	Application processing shall be done on physical or virtual servers that is exclusively for the use of Eskom, its subsidiaries and users (e.g. a SaaS instance that is not shared with a non-Eskom entity).
	Eskom Information shall not share storage services with a non-Eskom entity

Table 20: Data Classification Guidelines

Standards Requirement	**Certification Requirement**
“Cloud Provider” shall be ISO/IEC 27002	“Cloud Provider” shall supply the appropriate certification
“Cloud Provider” shall be ISO/IEC 27017	“Cloud Provider” shall supply the appropriate certification
“Cloud Provider” shall conform to ISO/IEC 27040:2015 for data storage	
Eskom’s Web Services Security Standard, 240-1070077584 - Web Services Security Standard	
Eskom’s Information Security Encryption Standard	
Eskom’s information Security System Classification	

Table 21: Data Protection Standards

10.18 Security Provisions for Cloud Applications

Application security poses specific challenges to both the “Cloud Provider” and Eskom. If an application is compromised, it can create financial liability, reputational damage, legal liability, health and environment safety risk, to both the “Cloud Provider” and Eskom. A threat and vulnerability assessment process of the services rendered to Eskom shall be established between Eskom and the “Cloud Provider”. This assessment and design of controls shall be monitored and assessed (by the “Cloud Provider” in collaboration with Eskom) for effectiveness periodically e.g. every 6 months. In order to protect an application from various types of breaches it is important to understand the application security policy considerations based on the different cloud deployment models. Table 23 highlights the application policy requirements of Eskom.

Deployment Type	**Application Security Policy requirement**
IaaS	Eskom is responsible for the deployment of the software stack and for all aspects that pertain to this stack, including the application of the security patches.
	Eskom is required to develop and regularly test the incident response procedures based in the shared responsibilities between Eskom and the “Cloud Provider”.
PaaS	The “Cloud Provider” shall provide Eskom with security reports on a regular basis.
	“Cloud Provider” is responsible in securing the infrastructure, operating systems and middleware.
SaaS	Application-tier security policy controls are mostly the responsibility of the “Cloud Provider” and are dependent upon terms in the contract and SLA. Eskom shall ensure that these terms meet their confidentiality, integrity, and availability requirements.
	Eskom shall have knowledge of how their data is protected against administrative access by the provider.
	Eskom shall have knowledge of the location of the data storage.

Table 23:Cloud Application Security Standard

Standards Requirement	**Certification Requirement**
“Cloud Provider” shall be ISO/IEC27001	“Cloud Provider” shall supply the appropriate certification.
“Cloud Provider” shall be ISO/IEC 27018	“Cloud Provider” shall supply the appropriate certification.

Table 24: Certification Requirements

10.19 Cloud networks and connections

A “Cloud Provider” shall allow legitimate network traffic and block malicious network traffic. The following external network controls need to be provided by the “Cloud Provider” (see Table 25).

“CLOUD PROVIDER” Responsibility	**Requirement**
Traffic Screening	“Cloud Provider” shall screen traffic from known malware ports, if the “Cloud Provider” does not allow for this Eskom shall need to fulfil this requirement.
	“Cloud Provider” shall supply Eskom with a copy of the firewall block list.
	The “Cloud Provider” providers firewall shall allow for IPv6 and protect against IPv6 and IPv4 attacks.
	The provider should allow for geographic restriction of network traffic.
Intrusion detection and prevention	The cloud service shall have intrusion detection and/or prevention systems (IDS/IPS) for a cloud service.
Logging and notification	“Cloud Provider” and Eskom shall have visibility into the network health.
	“Cloud Provider” is required to segregate the network logging information pertaining to Eskom data in motion.

Table 25: External Network Controls

Internal network security differs from external network security in that we assume that any attackers have already made it through the external defences, either via an attack or, more commonly, because the attackers are legitimately authorised for a different part of the network. After a user is allowed access to a portion of the “Cloud Provider's” network, the provider has the following responsibilities with respect to internal network security (see Table 26).

"CLOUD PROVIDER" Responsibility	**Guidance**
Tools to protect Eskom from the "Cloud Provider's" other customers	The "Cloud Provider" shall be able to provide VLAN and Virtual Private Cloud capabilities to Eskom. This dedicated VLAN shall be capable of connecting to Eskom's network in a secure client to site configuration. The "Cloud Provider" shall ensure that the appropriate firewalls are implemented. If dedicated VLANs are not available, the "Cloud Provider" may use hypervisor-based filters such as e-tables on Linux to control traffic at a virtual switch level.
Tools to allow Eskom to implement network segmentation	The "Cloud Provider" shall allow Eskom to create multiple layers of network security within the deployment, such as the creation of a DMZ (Demilitarized Zone) and multiple back-end network zones for different types of systems, e.g. Eskom may want to create: • Two different DMZ network segments for production and test. • Separate back end segments for production and test. • A separate administration segment.
Protect the "Cloud Provider's" network	The "Cloud Provider" is required to protect its own network such that an attack cannot come from the "Cloud Provider's" control network. The "Cloud Provider" is required to provide this assurance to Eskom via an audit or certification.
Monitor for intrusion attempts	"Cloud Provider" shall have activity auditing and logging as part of their preventive security measures as well as incident response and forensics. Audit information and logs should be subject to appropriate security controls to prevent unauthorised access, destruction, or tampering. "Cloud Provider" shall have processes for alerting Eskom about both successful and unsuccessful internal network attacks.

Table 26: "Cloud Provider" Internal Network Security Responsibilities

10.20 Physical Infrastructure and Facilities Security

The security of a cloud service also depends on the security of the physical infrastructure and facilities of the "Cloud Provider". Eskom shall get assurance from the "Cloud Provider" that appropriate security controls are in place. This assurance shall be provided by means of having the following security controls (see Table 27):

- Physical Infrastructure and facilities should be held in secure areas. A physical security perimeter should be in place to prevent unauthorised access, allied to physical entry controls to ensure that only authorised personnel have access to areas containing sensitive infrastructure. Appropriate physical security should be in place for all offices, rooms, and facilities that contain physical infrastructure relevant to the provision of cloud services.
- Protection against external and environmental threats. Protection should be provided against fire, floods, lightning, earthquakes, civil unrest or other potential threats that could disrupt cloud services.

- Controls should be applied to prevent malicious actions by any personnel who have access to secure areas.
- Controls should be in place to prevent loss, theft, damage or compromise of assets.
- Supporting utilities such as electricity supply, gas supply, telecommunications and water supply should have controls in place. Controls are required to prevent disruption to cloud services either by failure of a utility supply or by malfunction (e.g. water leakage). This may require the use of multiple routes and multiple utility suppliers.
- Controls are needed to protect power cabling and telecommunications cabling to prevent accidental or malicious damage.
- Controls should be in place to perform necessary preventive maintenance of all equipment to ensure that services are not disrupted through foreseeable equipment failures.
- Controls are required on the removal of assets to avoid theft of valuable and sensitive assets.
- Controls are required for the disposal of any equipment and particularly any devices which might contain data such as storage media.
- Appropriate controls need to be in place for the staff working at the facilities of a "Cloud Provider", including any temporary or contract staff.
- The provider should have appropriate backup of data, redundancy of equipment, and continuity plans for handling equipment failure situations

Standards Requirement	**Certification Requirement**
"Cloud Provider" shall conform to ISO/IEC27002	"Cloud Provider" shall supply the appropriate certification.
"Cloud Provider" shall conform to ISO/IEC 27017	"Cloud Provider" shall supply the appropriate certification.

Table 27: Physical Infrastructure and Facilities Security

10.21Cloud Service Agreement

Cloud service involves two organisations – Eskom and the "Cloud Provider" and the respective security responsibilities need to be documented clearly. This can be done in the CSA (Cloud Service Agreement), which specifies the terms of the contract between Eskom and the "Cloud Provider".

It shall be explicit in the CSA that any requirements that is placed on the "Cloud Provider" shall also pass on to any peer "Cloud Provider"s that the provider may use in order to supply any part of their service(s). The CSA should explicitly document that "Cloud Provider's" shall notify Eskom in a timely manner of the occurrence of any breach of their system, regardless of the parties or data directly impacted. The provider should:

- Include specific pertinent information in the notification.
- Stop the data breach as quickly as possible.
- Restore secure access to the service as soon as possible.
- Apply best-practice forensics in investigating the circumstances and causes of the breach.
- Make long-term infrastructure changes to correct the root causes of the breach and ensure that it does not recur.
- Test the effectiveness of the repair.

10.22 Cloud GRC Standards and Certification Requirements

The Cloud GRC (Governance, Risk and Compliance) standards and certifications requirements (see Table 28) that the “Cloud Provider” should comply with to meet Eskom’s Cloud GRC requirements.

Standards and Legislative Requirement	Certification Requirement
The “Cloud Provider” shall comply a minimum of one of the following; COBIT, ISO/IEC2000 and ITIL.	“Cloud Provider” shall supply the appropriate certification
“Cloud Provider” shall conform to the following standards to ensure information systems security (ISO/IEC 27001 and ISO/IEC 27002)	“Cloud Provider” shall supply the 27001 certifications
“Cloud Provider” shall conform to: • ISO/IEC 27017 • ISO/IEC 27018 (Applicable to workloads that contain PII)	“Cloud Provider” shall supply the 27017 or equivalent certification
“Cloud Provider” shall conform to the following South African and International regulation: • PIA • POPIA • Cyber Security Bill • Critical Infrastructure Bill • GDPR • National Key points Act (Act No. 102 of 1980)	“Cloud Provider” shall attest that their cloud service complies to the mentioned regulation
“Cloud Provider” with card payment information workloads shall conform to PCI-DSS	“Cloud Provider” shall supply the PCI-DSS certification
“Cloud Provider” shall conform to SSAE 16 if the workload has an impact on financial activities.	“Cloud Provider” shall provide SSAE 16 certification
NIST Cloud Security Framework	
NIST SP 800-53 R4	
Eskom Information Secuirty Policy	
NISTIR 7628 guideline	

Table 28:Cloud GRC Standards and Certification Requirements

11. EXIT PROCESS

From a security perspective, it is important that once the Eskom has completed the termination process, "reversibility" is achieved - i.e., Eskom’s data should not remain with the “Cloud Provider”. The provider shall ensure that any copies of the data are permanently erased from their environment, wherever the copies may have been stored (including backup locations as well as online data stores). The data derived by the cloud service which was held by the “Cloud Provider” needs to be cleansed of information pertaining to Eskom. A process of sanitisation of the “Cloud Provider’s” infrastructure and applications, upon contract termination, hosting Eskom’s information and data shall be documented and approved by Eskom. The “Cloud Provider” shall provide evidence of sanitisation to Eskom upon contract termination. During the exit process however, Eskom needs to be able to ensure transition without loss or breach of data. Therefore, process shall allow for Eskom to retrieve the data in a secure form and backups shall be retained for an agreed period of time until the exit process is complete.

12. REFERENCES

[1] “Cloud Adoption Strategy”; Document Identifier: 240-125797682, GIT SEA, 1 February 2017

[2] “Cloud Policy”; Document Identifier: 240-134085928, 14 December 2018

[3] “NIST Cloud Computing Reference Architecture”; Special Publication 500-292, September 2011

[4] “NIST Cloud Computing Standards Roadmap”, Special Publication 500-291, Version 2, July 2013

[5] “National Cybersecurity Policy Framework for South Africa”, SSA (State Security Agency), Government Gazette, 4 December 2015

[6] “GWEA (Government-Wide Enterprise Architecture Framework Implementation Guide”; Revision 1.2, June 2010

[7] “Critical Infrastructure Protection Bill”; Republic of South Africa, 2015

[8] “Privacy is Paramount”, Personal Data Protection in Africa, Deloitte, 2017

13. GLOSSARY

AES – Advanced Encryption Standard
ANSI – American National Standards Institute
API – Application Programming Interface
AU – African Union
BCR – Binding Corporate Rules
BCR – Business Corporate Rule
BI – Business Intelligence
BRP – Benefits Realisation Plan
BRS – Business Requirement Specification
CAC – Common Access Control
CAMP – Cloud Application Management Platform

CASB – Cloud Access Security Broker

CDN – Content Delivery Network

CIM – Common Information Model

CIMI – Cloud Infrastructure Management Interface

CMDI – Cloud Data Management Interface

CPU – Central Processing Unit

CRM – Customer Relationship Management

CSA – Cloud Service Agreement

DFDL – Data Format Description Language

DMDI - Cloud Data Management Interface

DMTF - Distributed Management Task Force

DPA – Data Protection Authority

DPO – Data Protection Officer

DSS – Digital Signature Standard

EES – Escrowed Encryption Standard

EIP – External Identity Providers

ERP – Enterprise Resource Planning

EU – European Union

EVA – Economic Value Add

FIM – Federated Identity Management

GDPR – General Data Protection Regulation

GIT – Group Information Technology

GWEA – Government-Wide Enterprise Architecture

HMAC – The Keyed-Hash Message Authentication Code

HR – Human Resources

HVAC – Heating, Ventilation and Air Conditioning

IA – Information Assurance

IaaS – Infrastructure as a Service

IAM – Identity and Access Management

ICT – Information and Communication Technology

IDE – Integrated Development Environment

IMS – Information Management System

IP – Internet Protocol

IT – Information Technology

KMIP – Key Management Interoprability Protocol

KMS – Key Management System

LAN – Local Area Network

MID – Mobile Internet Devices

NIST – National Institute of Standards and Technology

NKP – National Key Point

oAuth – Open Authorisation Protocol

OCCI - Open Cloud Computing Interface

OS – Operating System

OSI – Open Systems Interconnection

OVF - Open Virtualisation Format
P2P – Peer-to-Peer
PaaS – Platform as a Service
PI – Personal Information
PII – Personally Identifiable Information
PIV – Personal Identity Verification
PKI – Public Key Infrastructure
POPI – Protection of Personal Information
POPIA – Protection of Personal Information Act
QoS – Quality of Service
RMO – Results Management Office
SaaS – Sotware as a Service
SAML – Security Assertion Markup Language
SDK – Software Development Kits
SHS – Secure Hash Standard
SIIF – Standard for Intercloud Interoperability and Federation
SLA – Service Level Agreement
SNIA – Storage Networking Industry Association
SPML – Service Provisioning Markup Language
SSA – State Security Agency
SSL – Secure Sockets Layer
SSO – Single-Sign-On
TIE – Trusted Information Exchange
TLS – Transport Layer Security
TOSCA - Topology and Orchestration Specification or Cloud Applications
ToU – Time-of-Use
TRM – Technology Reference Model
VAS – Value Added Services
VM – Virtual Machine
VNS – Vendor Neutral Site
WCAG – Web Content Accessibility Guidelines
WS – Web Services
XACML – Extensible Access Control Markup Language
XCCDF – Extensible Configuration Checklist Description Format
XMLDSig – XML Signature

14. Acceptance

This document has been seen and accepted by:

Name	Designation
Nico Harris	Acting General Manager IT
Varsha Pillay	Senior Manager – Business Solutions & Shared Services (Acting)

Name	**Designation**
Nomsa Vanda	Senior Manager – Analytics Centre of Excellence (Acting)
Grasswell Mabudusha	Senior Manager – IM Business Relationship Management
Ian Marks	Senior Manager – Office of the Chief Information Officer (Acting)
Maureen Mokone	Senior Manager – Business Process Management & SEA
Sham Dhrampal	Corporate Specialist (SSE) – Enterprise Architecture
Brenda Thomo	Senior Manager – IM Operations (Acting)
Nhlanhla Tshabalala	Senior Manager - ITSO TSG (Acting)
EAB Committee	
EARC Committee	

15. Revisions

Date	**Rev.**	**Compiler**	**Remarks**
May 2019	1	E. de Large	New document

16. Development Team

The following people were involved in the development of this document:

- Ezzard De Lange

17. Acknowledgements

None