TRANSNET

delivering freight reliably

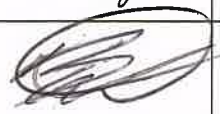
Transnet Cloud Standard

Version Number	*V1.0*
Next Review Date	*2 years from the final approval date*
Standard Owner	*Mark Snyders: GM Technology Innovation & Digital Transformation*
Signature	Mark A Snyders
Standard Sponsor	*Pandelani Munyai: Group Chief Information Officer*
Signature	
Date Approved	3 June 2024

Approved by:

	Name	Designation	Approval Signature	Date	E-Mail	Contact Number
Subject Matter Expert	Shawn Norton	Snr Manager: Group ICT Infrastructure		May 31, 2024	Shawn.Norton@transnet.net	083 795 1575
Subject Matter Expert	Sibusiso Mthimunye	Cyber Security Specialist	 Sibusiso Mthimunye (May 30, 2024 12:27 GMT+2)	May 30, 2024	Sibusiso.Mthimunye@transnet.net	084 245 7086

I hereby acknowledge that a search has been conducted and that the Standard is not duplicated or in conflict with any other Transnet Standards.

	Name	Designation	Approval Signature	Date	E-Mail	Contact Number
Owner	Mark Snyders	GM Technology Innovation & Digital Transformation	Mark A Snyders	May 30, 2024	Mark.Snyders@transnet.net	083 308 6550
Sponsor	Pandelani Munyai	Group Chief Information Officer			Pandelani.Munyai@transnet.net	011 308 3071

Final Approval

RR Thipe

ICT Architecture Review Council

16.09.2024

Date Approved

Summary of Version Control

Version Number	Effective Date	Summary of Changes
1.0	*November 2018*	• *Initial Cloud Policy*
1.0	*May 2024*	• *Initial Cloud Standard*

TRANSNET

Table of Contents

1. INTRODUCTION

This Cloud Standard sets out the rules by which decisions to consume cloud services must be made and managed in Transnet. Transnet has clear set of objectives as articulated in its strategy, currently the Shareholder Compact, Corporate plan, and all applicable Governance structures. It is also Transnet's objective to accelerate the digital roadmap which has cloud-based technologies as one of the critical enabling blocks. The era of sensor technologies, predictive capabilities and Internet of Things has led to "Big Data" requiring increased processing power and consumptive models of IT. With the physical world forming part of the enterprise so rapidly, Transnet is facing serious challenges and if these are not addressed by adaptation then we face extinction. Smart consumption of IT as a commodity is now critical not only for IT, but for business as well.
Transnet is putting into place the standard, skills, and tools necessary to accelerate the adoption of cloud and to become less technology-centric and more outcome-focused.
Through this standard, Transnet endorses the use of cloud services in enabling its operations. The standard further provides guidelines in the use of cloud services for Software as A Service (SaaS), Platform as a Service (PaaS), and all other "XaaS" with respect to access, management, and protection of data for all its stakeholders:

- Vendors.
- Transnet contractors.
- Transnet employees.
- Transnet partners.
- Transnet clients when interacting or who can provide appropriate levels of protection and recovery for Transnet's information.

While cloud storage of files can expedite collaboration and sharing of information anytime, anywhere, and with anyone, there are some guidelines that must be in place for the kind and type of internal information that is appropriate for storing and sharing using these services.

2. PURPOSE

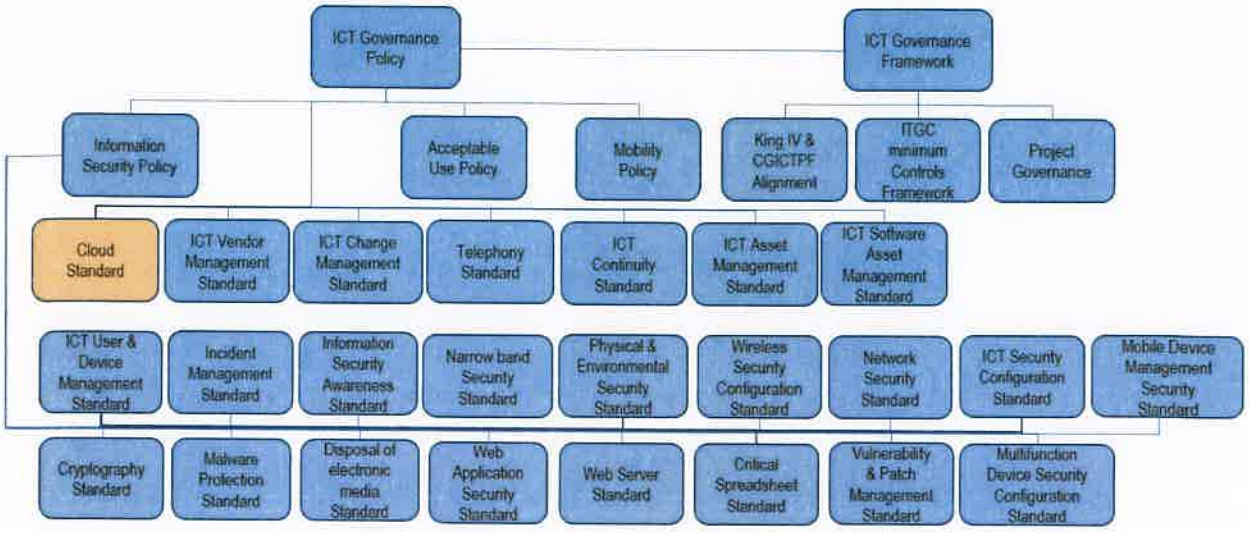
This Standard identifies the minimum baseline configuration and security requirements and provides related 'good practice' for effective and efficient management of the Cloud computing environment within Transnet.

With the modernisation and transformation of the Transnet IT installed base, commoditising IT moves to the centre to enable agility, speed of processing and speed of response. This modernisation will also make Transnet a critical player in the Transport and Logistics industry not only in South Africa, but globally.

It is also the purpose of this standard to encourage consumption of cloud-based services by all Transnet stakeholders within a secure environment. The intention is to move away from unnecessary ownership of ICT infrastructure and let Transnet consume it on a usage basis where appropriate.

Within the context of the Transnet Information Security Management System (ISMS), The Cloud Standard supports the ICT Governance Policy and the ICT Governance Framework as depicted below:

ICT Policies, Standards & Frameworks



3. SCOPE

This standard applies to all Transnet systems deployed within cloud environments. This standard also applies to all system owners and custodians where applicable. Any cloud-based solution must, at minimum meet the requirements in this standard. There are cloud-based solutions available that are not able to have certain elements of this standard applied, in which case they will be evaluated at the design stage at which point, exemption may be sought from the relevant Governance Committee(s).

This standard pertains to all external cloud services, e.g., cloud-based email, document storage, Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS), Management-as-a-Service (MaaS), Platform-as-a-Service (PaaS), etc. Personal accounts are excluded.

If you are not sure whether a service is cloud-based or not, please contact your ICT team.

4. DEFINITIONS AND ABBREVIATIONS

For ease of reference words, expressions and abbreviations used in the standard are defined below.

Azure Fabric: Azure Service Fabric is a distributed systems platform that makes it easy to package, deploy, and manage scalable and reliable microservices and containers.

CGICTPF: Corporate Governance of Information and Communications Technology Policy Framework. DPSA framework instituted by cabinet. December 2013. Transnet falls within the scope of the framework for implementation as a state-owned entity.

Cloud (Definition of cloud from NIST): Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Cloud computing: Is defined as the utilization of servers or information technology hosting of any type that is not controlled by, or associated with, Transnet for services such as, but not limited to, social networking applications (e.g., blogs and wikis), file storage (Drop Box), and content hosting (publishers textbook add-ons).

CMDB: Configuration Management Database is an ITIL term for a database used by an organization to store information about hardware and software assets (commonly referred to as configuration items).

DOA: Delegation of Authority provides Signature Authority to certain individuals based on their level in the organization to approve various transactions.

DPSA: Department of Public Service and Administration.

GICTF: Governance of ICT Framework. An abstraction that defines the elements for the effective and efficient directing and controlling of ICT resources to facilitate the achievement of company strategic objectives.

ICT: Information and Communications Technology.

Infrastructure as code (IaC): Is the managing and provisioning of infrastructure through code instead of through manual processes.

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

ISO 27001: Is an international standard to manage information security.

IT and Digital Governance Framework - An abstraction that defines the elements that support the effective and efficient directing and controlling of ICT resources (people, process, and technology) to facilitate the achievement of Transnet's strategic objectives.

MaaS (Management as a Service): Cloud-based service model that provides businesses with outsourced management solutions for various aspects of their operations. MaaS involves the delegation of tasks related to IT infrastructure, applications, security, or other business processes to a third-party service provider. E.g., Software managed for Transnet with Transnet specific configuration requirements.

NIST: The National Institute of Standards and Technology is an agency of the United States Department of Commerce whose mission is to promote American innovation and industrial competitiveness.

OMS: Operations Management Suite (OMS) is an advanced, comprehensive offering that brings together four complementary Azure services: Backup, Site Recovery, Log Analytics and Automation and is one of the tools Microsoft leverages when providing managed Azure consulting services.

Platform as a Service (PaaS): The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools

supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

Portability- The ability to transfer data from one system to another without being required to recreate or re-enter data descriptions or to modify significantly the application being transported. 2. 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. 3. Of equipment, the quality of being able to function normally while being conveyed. (Source: NIST Cloud Taxonomy)

Private Cloud - The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise. (Source: NIST Cloud Taxonomy) It is a Cloud ecosystem or platform specifically for an organisation with its own rules and governance and for its own consumption only. The platform is not a shared platform and can be across multiple cloud providers. The classification of data will be according to data classification policies i.e., which data is for public consumption, and which is for Private Consumption.

Probity - Strict adherence to a code of ethics based on undeviating honesty, especially in commercial (monetary) matters and beyond legal requirements.

Public Cloud - The cloud infrastructure is made available to the public or a large industry group and is owned by an organization selling cloud services. (Source: NIST Cloud Taxonomy)

Regulatory Requirements -Any legislation applicable to Transnet, i.e., legislation as set out in the Transnet Regulatory Universe as amended from time to time. e.g., National Treasury Regulations and the Public Finance Management Act No 1 of 1999 (PFMA).

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

Terraform: Terraform uses declarative syntax to describe your Oracle Cloud Infrastructure (OCI) infrastructure and then persist it in configuration files that can be shared, reviewed, edited, versioned, preserved, and reused.

TCP / UDP: Transmission Control Protocol (TCP) / User Datagram Protocol (UDP).

Transnet: "The Company" or "The Group" - Transnet SOC Ltd.

5. ROLES AND RESPONSIBILITIES

5.1. ICT Architecture Review Council

- Responsible for the final approval of all Transnet ICT Standards.
- Responsible for providing approval for any new cloud deployments.

5.2. GM: Technology Innovation & Digital Transformation

- Owner of the standard.
- Responsible for overseeing the development, enforcement, and measurement of this standard.
- Reviews and supports waivers that have been compiled for exception from compliance with this standard.
- Overall accountability for overseeing assurance reviews to ensure compliance with this standard.

5.3. Information Security, Governance, Risk and Compliance Committee

- Responsible to manage and co-ordinate ICT risk mitigation and governance activities across the Group and to co-ordinate activities regarding the protection of Transnet's information assets.
- Participate in the development and maintenance of the standard and/or related processes.
- The committee is responsible for recommending Transnet ICT standards to the ICT Architecture Review Council for final approval.
- ISGRC committee members participate in the development and maintenance of the standard and the related procedures.
- Report compliance to the GM: Technology Innovation & Digital Transformation.

5.4. GM: Enterprise Technology Services

- Ensure the standard is communicated to all parties (including third parties) that are responsible for designing, developing, and managing web-based applications in the Transnet environment.
- Ensure implementation of this standard.

5.5. Operating Division Information Security Liaison

- Facilitate the implementation of the standard in the OD by communicating the requirements, providing technical assistance with implementation, and reporting adherence to the standard.
- Co-ordinate the compliance with this standard.

5.6. Vendor Manager

- Ensure that compliance requirements for this standard are included in vendor/supplier contracts and requirements of any engagement that involves the design, development and/or implementation of web applications.

5.7. Transnet Operating Division ICT

- Communicate requirements of the standard to all ICT departments and relevant third parties.
- Establish mechanisms and controls to ensure compliance to this standard within your respective operating division.
- Participate in the on-going maintenance, review, and enhancement of this standard.

5.8. Vendors, Third-Party Suppliers System Owners/Custodians

- Ensure that the requirements of this standard are formally adopted and enforced during the design, acquisition, implementation, or deployment of computer/information systems in the Transnet environment.

5.9. Transnet Group Change Advisory Board (CAB)

- Responsible for providing final approval for any new or changes to cloud deployments.

6. REQUIREMENTS

The following stipulations must be complied with to ensure that Transnet Cloud services are efficiently managed:

6.1. GENERAL:

6.1.1. Cloud based solutions and services will be the first consideration for Transnet when new applications or solutions are considered.

6.1.2. The consumption of Public Cloud solutions must comply with the principle of portability as defined in this standard and be in line with both the letter and spirit of this standard.

6.1.3. A business case for cloud based versus on premise solutions must be completed each time a new solution is considered.

6.1.4. For all cloud-based solutions, there must be a clear and approved DR (Disaster Recovery), back up procedures and standards and integration requirements if any. Ease of integration with core systems must be assured.

6.2. COST MANAGEMENT:

Cost management for Cloud managed Services	
Justification / Description	The effectiveness of Cost Management depends on the controls implemented to mitigate associated risks. Below are the controls that must be complied with to ensure effective cost management.
Standard Requirements	The following requirements must be complied with: **6.2.1. <u>Cloud Procurement:</u>** Any end user, working group, or department looking to use cloud services for either single project based work or ongoing work, must ensure that: **6.2.1.1.** In situations where cloud service providers have pre-drafted contracts, these must be reviewed by the relevant Transnet's legal department in consultation with the ICT department prior to these being accepted. **6.2.1.2.** For any cloud services that require individual users to agree to terms of service or usage, the office of the relevant Transnet's legal department in consultation with the ICT department will review such documents and determine if end users can agree on an

	individual basis or identify any needed changes. This is to mitigate the risk that employees may inadvertently bind Transnet by simply clicking "Yes", "Okay", "Accept" without realising that there is an underlying contract that may bind Transnet. **6.2.1.3.** Any usage of cloud services must include a Disaster Recovery and Business Continuity capabilities where in the event of a data disaster Transnet is able to recover any lost data. **6.2.1.4.** All Transnet RFS's (Request for Services) for cloud-based services will be written in line with this standard. **6.2.1.5.** The contract must specifically state what data Transnet owns. It must also classify the type of data shared in the contract according to the Transnet's classification policy. **6.2.1.6.** The contract must specify how the cloud-computing vendor can use Transnet's data. Vendors cannot use Transnet's data in any way that contravenes South African law or infringe on Transnet data ownership rights. **6.2.1.7.** IT-related risks must be identified, recorded, evaluated, mitigated, and monitored, and reported in accordance with the approved Transnet ERM (Enterprise Risk Management) framework and policy. **6.2.1.8.** Without compromising the Transnet Supply Chain policies and procedures, all information technology acquisition activities, including hardware, software, telecom, and professional services, must be managed through the appropriate ICT governance structures and in line with the Transnet Delegation Framework. **6.2.1.9.** Heads of ICT must establish formal processes for ICT value optimisation to continually evaluate the portfolio of ICT- enabled investments, direct value management principles and practices and monitor key goals and metrics. **6.2.1.10.** As a transition, any cloud solution currently deployed will be deemed to comply with this standard but will be assessed by the relevant CIO to determine if it materially complies with this standard. If after such an assessment is done it is determined that the solution does not comply, cost effective mitigation actions will be undertaken to address the said non-compliance. **6.2.1.11.** There must be a clearly documented exit plan i.e., timelines, cost and approved procedures for all cloud-based solutions and services. This is in effect, to secure Transnet's ability to continue operations in the event a cloud service provider is unable to provide service, or the service level is no longer acceptable to Transnet. The exit plan must form part of the contract specifying the format in which data must be returned and the process of how data will be securely deleted.

	6.2.2. Resource Cost Management: Any end user, working group, or department looking to use cloud services for either single project based work or ongoing work, must ensure that: **6.2.2.1.** A multi-disciplinary cloud cost management team must be established and tasked with oversight and implementation of cost-related strategies. **6.2.2.2.** Cost optimisation KPIs must be developed and tracked. **6.2.2.3.** Start and stop of workloads during times when not required (e.g., December holidays / quiet periods) must be configured. **6.2.2.4.** Implement auto-scaling to dynamically adjust resource capacity based on workload fluctuations, ensuring optimal performance while minimizing costs during off-peak hours. **6.2.2.5.** Regularly review and optimize the allocation of cloud resources to ensure they are appropriately sized for the workload demands, thus avoiding over-provisioning and unnecessary costs. (Resource Right-Sizing). **6.2.2.6.** Implement monitoring controls on resource utilization to identify underutilized or idle resources, allowing for timely decommissioning or downsizing to prevent unnecessary expenditure. **6.2.2.7.** Utilize reserved instances or savings plans for predictable workloads to benefit from discounted pricing compared to on-demand usage (Reserved Instances and Savings Plans). **6.2.2.8.** Leverage spot instances or low-priority virtual machines for non-critical, fault-tolerant workloads to take advantage of cost savings during periods of low demand (Spot Instances and Low-Priority VMs).

	6.2.2.9. Establish lifecycle policies to automatically archive or delete unused resources, such as snapshots, storage, and temporary instances, to prevent unnecessary storage costs (Lifecycle Management). **6.2.2.10.** Enforce tagging standards to categorize resources by owner, department, project, or environment, enabling accurate cost allocation and facilitating cost accountability (Tagging and Cost Allocation). **6.2.2.11.** Set up cost alerts and budgets to notify stakeholders when spending exceeds predefined thresholds, enabling proactive cost management and preventing budget overruns (Cost Alerts and Budgets). **6.2.2.12.** Implement storage optimization such as tiered storage, data compression, and deduplication, to minimize storage costs while maintaining data accessibility and performance (Optimized Storage Solutions). **6.2.2.13.** Foster a culture of continuous optimization by regularly reviewing and refining cost-saving strategies based on evolving business needs, technological advancements, and cloud provider offerings (Continuous Optimization). **6.2.2.14.** Provide ongoing training to educate users on cost-effective cloud resource management practices, empowering them to make informed decisions that align with cost-saving objectives. **6.2.2.15.** Engage in regular negotiations with cloud service providers to explore cost-saving opportunities, such as volume discounts, reserved capacity commitments, or customized pricing models.

6.3. SECURITY BASELINE:

Security configuration requirements for all Cloud Systems.	
Justification / Description	The effectiveness of Cloud services depends on how it is implemented within an organization. Below are the controls that must be complied with when configuring cloud services.
Standard Requirements	The following requirements must be complied with: **6.3.1.** **Data protection:** **6.3.1.1.** All cloud-based Transnet Data, both structured and unstructured, will be managed in line with data classification policy and standard. **6.3.1.2.** Microsoft OneDrive is the authorised cloud platform for storing and sharing company information. Any other public cloud-based services example Google drive, iCloud, and/or Dropbox must not be used for sharing and/or storing company information. Cloud based services hosted by third parties must be approved prior unless explicitly approved for business use. **6.3.1.3.** If at any point the flow of data will contain personally identifiable information (PII), credit card numbers, data covered under POPI Act, confidential corporate data or any other sensitive or regulated data, the data must be encrypted two ways (to and from the cloud provider) and when in storage (refer to section 6.4.3 "Tagging"). **6.3.1.4.** Any usage of cloud services must adhere to all applicable laws, Policies, Standards, and regulations governing Transnet. **6.3.2.** **AZURE: Role Based Access Control (RBAC):** All deployments must have RBAC provisioned through the relevant portal / mechanisms to ensure roles are provisioned at the fabric layer and not only on the Virtual Machines (VMs). The principle of least privilege access applies. Role changes must be tracked, and role assignment alerts must be enabled.

Refer to the below list of available built-in RBAC roles available within Microsoft Azure:

Built-in role	Description
Owner	Let's you manage everything, including access to resources.
Contributor	Let's you manage everything except access to resources.
Reader	Let's you view everything, but not make any changes.
AcrImageSigner	acr image signer
AcrQuarantineReader	acr quarantine data reader
AcrQuarantineWriter	acr quarantine data writer
API Management Service Contributor	Can manage service and the APIs
API Management Service Operator Role	Can manage service but not the APIs
API Management Service Reader Role	Read-only access to service and APIs
Application Insights Component Contributor	Can manage Application Insights components
Application Insights Snapshot Debugger	Gives user permission to use Application Insights Snapshot Debugger features
Automation Job Operator	Create and Manage Jobs using Automation Runbooks.
Automation Operator	Automation Operators can start, stop, suspend, and resume jobs
Automation Runbook Operator	Read Runbook properties - to be able to create Jobs of the runbook.
Azure Stack Registration Owner	Let's you manage Azure Stack registrations.
Backup Contributor	Let's you manage backup service, but can't create vaults and give access to others
Backup Operator	Let's you manage backup services, except removal of backup, vault creation and giving access to others
Backup Reader	Can view backup services, but can't make changes
Billing Reader	Allows read access to billing data
BizTalk Contributor	Let's you manage BizTalk services, but not access to them.
CDN Endpoint Contributor	Can manage CDN endpoints but can't grant access to other users.
CDN Endpoint Reader	Can view CDN endpoints but can't make changes.

	CDN Profile Contributor	Can manage CDN profiles and their endpoints but can't grant access to other users.	
	CDN Profile Reader	Can view CDN profiles and their endpoints but can't make changes.	
	Classic Network Contributor	Let's you manage classic networks, but not access to them.	
	Classic Storage Account Contributor	Let's you manage classic storage accounts, but not access to them.	
	Classic Storage Account Key Operator Service Role	Classic Storage Account Key Operators are allowed to list and regenerate keys on Classic Storage Accounts	
	Classic Virtual Machine Contributor	Let's you manage classic virtual machines, but not access to them, and not the virtual network or storage account they're connected to.	
	ClearDB MySQL DB Contributor	Let's you manage ClearDB MySQL databases, but not access to them.	
	Cosmos DB Account Reader Role	Can read Azure Cosmos DB account data. See DocumentDB Account Contributor for managing Azure Cosmos DB accounts.	
	Data Factory Contributor	Create and manage data factories, as well as child resources within them.	
	Data Lake Analytics Developer	Let's you submit, monitor, and manage your own jobs but not create or delete Data Lake Analytics accounts.	
	Data Purger	Can purge analytics data	
	DevTest Labs User	Let's you connect, start, restart, and shutdown your virtual machines in your Azure DevTest Labs.	
	DNS Zone Contributor	Let's you manage DNS zones and record sets in Azure DNS but does not let you control who has access to them.	
	DocumentDB Account Contributor	Can manage Azure Cosmos DB accounts. Azure Cosmos DB is formerly known as DocumentDB.	
	Intelligent Systems Account Contributor	Let's you manage Intelligent Systems accounts, but not access to them.	
	Key Vault Contributor	Let's you manage key vaults, but not access to them.	
	Lab Creator	Let's you create, manage, delete your managed labs under your Azure Lab Accounts.	

	Log Analytics Contributor	Log Analytics Contributor can read all monitoring data and edit monitoring settings. Editing monitoring settings includes adding the VM extension to VMs; reading storage account keys to be able to configure collection of logs from Azure Storage; creating and configuring Automation accounts; adding solutions; and configuring Azure diagnostics on all Azure resources.	
	Log Analytics Reader	Log Analytics Reader can view and search all monitoring data as well as and view monitoring settings, including viewing the configuration of Azure diagnostics on all Azure resources.	
	Logic App Contributor	Let's you manage logic app, but not access to them.	
	Logic App Operator	Let's you read, enable, and disable logic app.	
	Managed Identity Contributor	Create, Read, Update, and Delete User Assigned Identity	
	Managed Identity Operator	Read and Assign User Assigned Identity	
	Monitoring Contributor	Can read all monitoring data and edit monitoring settings. See also Get started with roles, permissions, and security with Azure Monitor.	
	Monitoring Reader	Can read all monitoring data (metrics, logs, etc.). See also Get started with roles, permissions, and security with Azure Monitor.	
	Network Contributor	Let's you manage networks, but not access to them.	
	New Relic APM Account Contributor	Let's you manage New Relic Application Performance Management accounts and applications, but not access to them.	
	Reader and Data Access	Let's you view everything but will not let you delete or create a storage account or contained resource. It will also allow read/write access to all data contained in a storage account via access to storage account keys.	
	Redis Cache Contributor	Let's you manage Redis caches, but not access to them.	
	Resource Policy Contributor (Preview)	(Preview) Backfilled users from EA, with rights to create/modify resource policy, create support ticket and read resources/hierarchy.	
	Scheduler Job Collections Contributor	Let's you manage Scheduler job collections, but not access to them.	

	Search Service Contributor	Let's you manage Search services, but not access to them.	
	Security Admin	In Security Center only: Can view security policies, view security states, edit security policies, view alerts and recommendations, dismiss alerts and recommendations	
	Security Manager (Legacy)	This is a legacy role. Please use Security Administrator instead	
	Security Reader	In Security Center only: Can view recommendations and alerts, view security policies, view security states, but cannot make changes	
	Site Recovery Contributor	Let's you manage Site Recovery service except vault creation and role assignment	
	Site Recovery Operator	Let's you failover and failback but not perform other Site Recovery management operations	
	Site Recovery Reader	Let's you view Site Recovery status but not perform other management operations	
	SQL DB Contributor	Let's you manage SQL databases, but not access to them. Also, you can't manage their security-related policies or their parent SQL servers.	
	SQL Security Manager	Let's you manage the security-related policies of SQL servers and databases, but not access to them.	
	SQL Server Contributor	Let's you manage SQL servers and databases, but not access to them, and not their security -related policies.	
	Storage Account Contributor	Let's you manage storage accounts, but not access to them.	
	Storage Account Key Operator Service Role	Storage Account Key Operators are allowed to list and regenerate keys on Storage Accounts	
	Storage Blob Data Contributor (Preview)	Allows for read, write, and delete access to Azure Storage blob containers and data	
	Storage Blob Data Reader (Preview)	Allows for read access to Azure Storage blob containers and data	
	Storage Queue Data Contributor (Preview)	Allows for read, write, and delete access to Azure Storage queues and queue messages	
	Storage Queue Data Reader (Preview)	Allows for read access to Azure Storage queues and queue messages	
	Support Request Contributor	Let's you create and manage Support requests	

Traffic Manager Contributor	Let's you manage Traffic Manager profiles but does not let you control who has access to them.
User Access Administrator	Let's you manage user access to Azure resources.
Virtual Machine Administrator Login	- Users with this role can login to a virtual machine with Windows administrator or Linux root user privileges.
Virtual Machine Contributor	Let's you manage virtual machines, but not access to them, and not the virtual network or storage account they're connected to.
Virtual Machine User Login	Users with this role can login to a virtual machine as a regular user.
Web Plan Contributor	Let's you manage the web plans for websites, but not access to them.
Website Contributor	Let's you manage websites (not web plans), but not access to them.

6.3.3. Network Security Groups (NSG) and Default Configurations:

6.3.3.1. Configuration of the NSGs comprises of defaults loaded by the Azure Fabric for basic protection and custom rules that are configured once the NSG has been deployed.

6.3.3.2. NSG security rules are evaluated by priority using the 5-tuple information (source, source port, destination, destination port and protocol) to allow or deny the traffic. A Flow record is created for existing connections, communication is allowed or denied based on the connection state of the flow records, this allows NSG to be stateful. If you specify an outbound security rule to any address over port 80, for example, it is not necessary to specify an inbound security rule for the response to the outbound traffic. You only need to specify an inbound security rule if communication is initiated externally. The opposite is also true. If inbound traffic is allowed over a port, it is not necessary to specify an outbound security rule to respond to traffic over the port. An existing connection must not be interrupted when you remove a security rule that enabled the flow. Traffic flows are interrupted when connections are stopped, and no traffic is flowing on either direction for at least a few minutes.

A breakdown of the fields and associated options are noted below:

Priority:	*Rules are processed in priority order, the lower the number, the higher the priority. It is recommended to leave gaps between rules - 100, 200, 300, etc. - so that it's easier to add new rules without having to edit existing rules*

Name:	*Name of the rule to distinguish it from others. This is a unique identifier for each rule*
Port:	*This specifies on which ports traffic will be allowed or denied by this rule.* *Provide a single port such as 80; a port range such as 1024-65535 or a comma-separated list of single ports and/or port ranges such as 80, 1024-65535. Provide and asterisk (*) to allow traffic on any port.*
Protocol:	*This is the traffic protocol being allowed/denied through the NSG. I.e., All / TCP / UDP*
Source:	*The source filter can be Any, a specific address / address range or a default tag. It specifies the incoming traffic source IP range that will be allowed or denied by this rule.*
Destination:	*The destination filter can be Any, an IP address/range, or a default tag. It specifies the outgoing traffic for a specific destination IP address range that will be allowed or denied by this rule.*
Action:	*This is noting whether you are allowing or denying traffic through based on the settings configured*

6.3.4. Augmented Security Rules

6.3.4.1. An additional form of security rules is available using Augmented security rules to make rule management easier for predetermined sources and destinations. This list is controlled by Microsoft and cannot be edited to suit a customer's unique requirements due to the functionality being part of the Azure Fabric.

6.3.4.2. *"Augmented rules simplify security definition for virtual networks, allowing you to define larger and complex network security policies, with fewer rules. You can combine multiple ports, multiple explicit IP addresses, Service tags, and Application security groups into a single, easily understood security rule. Use augmented rules in the source, destination, and port fields of a rule. When creating a rule, you can specify multiple explicit IP addresses, CIDR (Classless Inter-Domain Routing) ranges, and ports. To simplify maintenance of your security rule definition, combine augmented security rules with service tags or application security groups."*

Below is a selection of the Service Tags available when configuring NSG rules:

Virtual Network	*This tag includes the virtual network address space (all CIDR ranges defined for the virtual network), all connected on-premises address spaces, and peered virtual networks or virtual network connected to a virtual network gateway.*

	Azure Load Balancer	*This tag denotes Azure's infrastructure load balancer. The tag translates to an Azure datacenter IP (Internet Protocol) address where Azure's health probes originate. If you are not using the Azure load balancer, you can override this rule.*
	Internet	*This tag denotes the IP address space that is outside the virtual network and reachable by the public Internet. The address range includes the Azure owned public IP address space.*
	Azure Traffic Manager	*This tag denotes the IP address space for the Azure Traffic Manager probe IPs. More information on Traffic Manager probe IPs can be found in the Azure Traffic Manager FAQ.*
	Storage	*This tag denotes the IP address space for the Azure Storage service. If you specify Storage for the value, traffic is allowed or denied to storage. If you only want to allow access to storage in a specific region, you can specify the region. For example, if you want to allow access only to Azure Storage in the East US region, you could specify Storage.EastUS as a service tag. The tag represents the service, but not specific instances of the service. For example, the tag represents the Azure Storage service, but not a specific Azure Storage account. All address prefixes represented by this tag are also represented by the Internet tag.*
	SQL	*This tag denotes the address prefixes of the Azure SQL Database and Azure SQL Data Warehouse services. If you specify SQL for the value, traffic is allowed or denied to SQL. If you only want to allow access to SQL in a specific region, you can specify the region. For example, if you want to allow access only to Azure SQL Database in the East US region, you could specify SQL. EastUS as a service tag. The tag represents the service, but not specific instances of the service. For example, the tag represents the Azure SQL Database service, but not a specific SQL database or server. All address prefixes represented by this tag are also represented by the Internet tag.*
	Azure Cosmos DB	*This tag denotes the address prefixes of the Azure Cosmos Database service. If you specify AzureCosmosDB for the value, traffic is allowed or denied to AzureCosmosDB. If you only want to allow access to AzureCosmosDB in a specific region, you can specify the region in the following format AzureCosmosDB.[region name].*

Azure Key Vault	*This tag denotes the address prefixes of the Azure Key Vault service. If you specify AzureKeyVault for the value, traffic is allowed or denied to AzureKeyVault. If you only want to allow access to AzureKeyVault in a specific region, you can specify the region in the following format AzureKeyVault.[region name].*

6.3.5. Default NSG Rules on Deployment

When a NSG is deployed there is a predetermined set of default rules applied. The Change Advisory Board (CAB) process must be followed for the approval of creating custom security groups.

Below is a breakdown of the default rules applied:

6.3.5.1. Inbound Default rules

Allow VNet In Bound

Priority	Source	Source ports	Destination	Destination ports	Protocol	Access
65000	Virtual Network	0-65535	Virtual Network	0-65535	All	Allow

Allow Azure Load Balancer In Bound

Priority	Source	Source ports	Destination	Destination ports	Protocol	Access
65001	Azure Load Balancer	0-65535	0.0.0.0/0	0-65535	All	Allow

Deny All Inbound

Priority	Source	Source ports	Destination	Destination ports	Protocol	Access
65500	0.0.0.0/0	0-65535	0.0.0.0/0	0-65535	All	Deny

6.3.5.2. Outbound Default rules

Allow Vnet Out Bound

Priority	Source	Source ports	Destination	Destination ports	Protocol	Access
65000	Virtual Network	0-65535	Virtual Network	0-65535	All	Allow

Allow Internet Out Bound

Priority	Source	Source ports	Destination	Destination ports	Protocol	Access
65001	0.0.0.0/0	0-65535	Internet	0-65535	All	Allow

Deny All Out Bound

Priority	Source	Source ports	Destination	Destination ports	Protocol	Access
65500	0.0.0.0/0	0-65535	0.0.0.0/0	0-65535	All	Deny

Refer to the Transnet Web Server Standard and the Network security Standard. (Transnet Standards)

6.4. RESOURCE CONSISTENCY

Resource consistency on all cloud Systems	
Justification / Description	The effectiveness of a resource consistency depends on how it is implemented within an organization. Below are the controls that must be compiled with when initiating cloud services: Virtual systems must be clearly identified and documented to enable the effective management of cloud infrastructure.
Standard Requirements	The following requirements must be complied with: **6.4.1. <u>Maintain a CMDB of all workloads deployed:</u>** **6.4.1.1.** All deployments of cloud-based solutions to be documented on the Transnet CMDB. **6.4.1.2.** Changes to cloud-based deployments can be maintained through Infrastructure as code (IaC) (e.g., Terraform declarative configuration files, deployed via pipeline and source controlled) **6.4.2. <u>Data Classifications and Restrictions:</u>** All data moving to and through Transnet's usage of cloud services are subject to and must adhere to organizationally defined data classification levels. This classification includes all the levels as defined in the Classification Policy (Data for public consumption and data for private consumption). The Group CIO may after consultation with Chief Corporate and Regulatory Officer determine how Transnet data is to be managed whilst on the cloud platform. **6.4.3. <u>Tagging Definitions and Standards:</u>** **6.4.3.1. Database Server:** 1) Environment - AZ (AZURE) 2) OS version - W (windows) / L (Linux) 3) OD - TCC 4) Abbreviated Application (workload)- PRIM (Primavera) 5) Database - DB 6) Number - 101 following 102 following 103 7) Stored Data Classification level - Public/Confidential/Secret 8) Business Unit - HR/Marketing/ICT/Finance 9) Development / Production - Dev / Prod Example: AZWTCCPRIMDB_HR_Prod101

	6.4.3.2. Resource Group: 1) Group - RG 2) Operating Division - TCC 3) Abbreviated Application (Workload) - PRIM (Primavera) Example: RG–TCC–PRIM **6.4.3.3. Server:** 1) Environment - AZ (AZURE) 10) OS version - W (windows) / L (Linux) 2) Operating Division - TCC 3) Abbreviated Application (Workload) - PRIM (Primavera) 4) Server - SRV 5) Number - 101 following 102 following 103 6) Stored Data Classification level - Public/Confidential/Secret 7) Business Unit - HR/Marketing/ICT/Finance 8) Development / Production - Dev / Prod Example: AZWTCCPRIMSRV_FIN_Dev101

6.5. CLOUD DEPLOYMENTS

Cloud Deployments	
Justification / Description	The effectiveness of Cloud services depends on how it is implemented within an organization. Below are the controls that must be complied with when configuring cloud services.
Standard Requirements	The following requirements must be complied with: **6.5.1. General Requirements:** **6.5.1.1.** Transnet must have a single tenant with operating divisions configured as departments under the single subscription. Each OD (Operating Division) will then register accounts and subscriptions under the relevant OD. **6.5.1.2.** Any cloud workloads must go to Change Advisory Board (CAB) for formal approval (including DEV, QA, and Production systems). **6.5.1.3.** For all cloud deployments (e.g., SaaS, PaaS, IaaS), at minimum obtain an annual SOC (Security Operations Center) Type 2 report and/or ISO 27001 certification from the contracted cloud service provider (CSP) / operating service provider (OSP) and ensure they meet the minimum requirements. **6.5.1.4.** Use of cloud computing services for work purposes must be formally authorized by the Operating division head of ICT or DOA (Delegation of Authority). The OD head of ICT or DOA must certify that security, privacy, and all other IT management requirements will be adequately addressed by the cloud computing vendor. **6.5.1.5.** Before entering into any new contract or agreement with a cloud vendor, a thorough due diligence must be conducted to ensure that the vendor's services align with the security, privacy, compliance, and operational requirements of Transnet. This aims to minimize risks, safeguard sensitive information, and ensure the continuity of our operations while leveraging the benefits of cloud-based services. This due diligence process includes at a minimum the following steps: 1) **Security Assessment:** Evaluating the vendor's security measures, including data encryption practices, access controls, network security protocols, and incident response procedures. 2) **Privacy Compliance:** Verifying that the vendor complies with applicable privacy regulations, such as GDPR, CCPA, HIPAA, or any other relevant standards, and assessing their data handling and privacy protection mechanisms. 3) **Compliance Certification:** Confirming that the vendor adheres to industry-specific compliance standards, such as SOC 2, ISO 27001, PCI DSS, or others relevant to our business operations.

Cloud Deployments	
	4) **Data Residency and Sovereignty:** Ensuring that the vendor's data storage and processing locations comply with our legal and regulatory requirements regarding data residency and sovereignty. 5) **Service Level Agreements (SLAs):** Reviewing SLAs to understand the vendor's commitments regarding uptime, performance, support, and resolution times for issues or disruptions. 6) **Vendor reputation and Reliability:** Assessing the vendor's reputation, reliability, financial stability, and track record of delivering high-quality services to other clients. 7) **Exit Strategy and Data Portability:** Establishing procedures and mechanisms for data migration, termination of services, and ensuring data portability in the event of contract termination or vendor changes. 8) **Risk Management:** Identifying and mitigating potential risks associated with the vendor's services, including vendor lock-in, service disruptions, data breaches, and legal liabilities. **6.5.1.6.** For any cloud services that require users to agree to terms of service, such agreements must be reviewed and approved by the OD Head of ICT or DOA. **6.5.1.7.** The use of such services must comply with Transnet Acceptable Use and Transnet Information Security Policy. **6.5.1.8.** The use of such services must comply with all laws and regulations governing the handling of personally identifiable information, corporate financial data or any other data owned or collected by Transnet. **6.5.1.9.** The OD Head of ICT or DOA decides what data may or may not be stored in the Cloud. **6.5.1.10.** Below is a set of standards that must be applied to all cloud-based deployments. Due to the list of available services or workloads this document does not provide granular detail for configuration standards and therefore require that the cloud administrator ensures that

deployments are done looking at best-practise while ensuring all standards noted in this document are adhered to.

6.5.2. Generic standards across subscriptions:

- **6.5.2.1.** All deployments to have anti-malware installed.
- **6.5.2.2.** All deployments to be placed in the South African region.
- **6.5.2.3.** All disks and databases deployed to have encryption.
- **6.5.2.4.** All workloads, components, resource groups to be tagged for their purpose – Tagging definition and standard to be defined.
- **6.5.2.5.** All passwords created during deployment are to be either 42 characters or use certificate authentication. The password may be securely stored in a PAM (Privileged Access Management) or password manager.
- **6.5.2.6.** All IP addresses to be dynamic unless there is a business and technical need for static IP addressing.

6.5.3. Production deployments:

- **6.5.3.1.** All production deployments to be part of high availability sets.
- **6.5.3.2.** All production deployments to have OMS (Operations Management Suite) monitoring.
- **6.5.3.3.** All production deployments to have backup and disaster recovery enabled.
- **6.5.3.4.** All production deployments to have change tracking enabled.
- **6.5.3.5.** All production deployments to have alerts enabled and configured.
- **6.5.3.6.** Use of Premium disks is limited to deployments that require high Input/Output rates.
- **6.5.3.7.** All production deployments to have disks managed as part of the managed disks feature.
- **6.5.3.8.** All production deployments to have Just in Time VM (Virtual Machine) access enabled.
- **6.5.3.9.** The use of external IP addresses is limited to workloads that need direct internet facing connections. By default, all workloads will have this disabled as all traffic will route through load balancers. However, this is a workload and design dependant.
- **6.5.3.10.** Regular reviews and monitoring must be performed for external facing IPs. Alerts must be configured for the creation of public IPs.
- **6.5.3.11.** All VMs are to have disk encryption enabled.

6.5.4. Development and Testing deployments

- **6.5.4.1.** Dev/Test deployments not to have high availability outside of the High availability PoC (Proof of Concept).
- **6.5.4.2.** Masking requirements for the usage of production data in development/test environments in cloud computing:
  1) **Data Anonymization:** Ensure that personally identifiable information (PII), such as names, addresses, social security numbers, and other sensitive data, is anonymized or replaced with

synthetic data that retains the format and structure but does not contain real information.

2) **Tokenization:** Implement tokenization techniques to replace sensitive data with randomly generated tokens while preserving referential integrity and ensuring that the tokens cannot be reverse engineered to retrieve the original data.
3) **Pseudonymization:** Use pseudonymization methods to replace identifiable information with pseudonyms or aliases, which are reversible only with access to a separate mapping table stored securely and accessible only to authorized personnel.
4) **Subset Selection:** Limit the amount of production data used in development/test environments by selecting a subset of records or data fields that are necessary for testing purposes while excluding unnecessary or sensitive information.
5) **Data Masking Techniques:** Employ data masking techniques such as substitution, shuffling, encryption, or format-preserving encryption to obfuscate sensitive data while maintaining its usability for testing and development activities.
6) **Dynamic Data Masking:** Implement dynamic data masking mechanisms that dynamically conceal sensitive data in real-time based on user roles and privileges, ensuring that unauthorized users do not have access to sensitive information even within the development/test environment.
7) **Data De-identification:** De-identify sensitive data by removing direct identifiers and suppressing quasi-identifiers to minimize the risk of re-identification while maintaining the utility of the data for testing and development purposes.
8) **Data Lifecycle Management:** Establish policies and procedures for the lifecycle management of masked production data in development/test environments, including data generation, masking, storage, usage, and disposal, to ensure compliance with regulatory requirements and minimize data exposure.
9) **Monitoring and Auditing:** Implement monitoring and auditing mechanisms to track and log access to masked production data in development/test environments, detect unauthorized access or usage, and maintain accountability for data handling activities.

6.5.4.3. OMS (Azure Operations Management Suite) monitoring is required on Dev/Test deployments as it is best for pre-production environments to be mirrors of production. Not having OMS monitoring during the Dev and Testing phase may introduce risks or result in outages, when released to production.

6.5.4.4. Disaster recovery is not required on Dev/Test workloads.

6.5.4.5. Cost management visibility alerts must be configured for Dev/Test deployments.

6.5.4.6. Premium storage is not to be used for dev test deployments.

6.5.4.7. Disks to be managed as part of the managed disks feature.

Cloud Deployments	
	6.5.4.8. Just in time VM access can be enabled depending on technical requirement. **6.5.4.9.** No Dev Test deployment is to use public IP addresses unless there is a technical and business requirement that is approved. **6.5.4.10.** Disk encryption is not mandatory and is at the discretion of the business owner. **6.5.4.11.** All Dev test deployments to have auto-shutdown enabled.

7. EXCEPTIONS

Conformance with this standard is mandatory and whilst the necessary care must be taken to ensure that the requirements within this standard are as practical as possible, situations may arise where compliance to specific requirements may not be feasible/possible. For all cases where compliance to a specific requirement is not possible, an exemption or exception must be formally submitted in line with the deviation process. Such deviation requests must be submitted to the GM: Technology Innovation & Digital Transformation for preliminary investigations and considerations. Only the Information Security, Governance, Risk and Compliance Committee has the authority to formally approve deviations from this standard.

8. REFERENCES

The Standard must be read in conjunction with the following related internal and external requirements:

8.1. INTERNAL DOCUMENTS:

- Information Security Policy.
- Information Classification Policy & Standard.
- Cryptography Standard.
- Enterprise Risk Management Strategy and Framework.
- ICT Continuity Standard.
- ICT Physical and environmental Security Standard.
- ICT Vulnerability & Patch Management Standard.
- Network Security Standard.
- Web Server Standard.
- Incident Management Standard.
- User and Device Management Standard.

8.2. EXTERNAL DOCUMENTS:

- Azure Well-Architected Framework.
- The Protection of Personal Information Act, 2013 (Act No 4 of 2013).
- The King IV Report on Corporate Governance for South Africa.
- Electronic Communications Act 36 of 2005.
- Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002.

9. VIOLATIONS OF THE STANDARD

Each employee is responsible for complying with the Cloud Standard requirements. Violation of any provision of this Standard will result in one or more of the following:

- Total or partial limitation of an employee's or third party's access to some or all of Transnet's systems.
- Initiation of legal action by Transnet including, but not limited to, criminal or civil prosecution under the applicable law.
- Transnet requiring the violator to provide restitution for any improper use of service.
- Disciplinary sanctions against employees.
- Invocation or legal remedies such as those included in contractual agreements and Service Level Agreements including cancellation of contracts with third parties.