APLU
AFRICAN PROCUREMENT LAW UNIT

POLICY POSITION PAPER

Public Procurement of Cloud Services in South Africa

African Procurement Law Unit

May 2026

Public Procurement of Cloud Services in South Africa

Policy Position Paper

Published by

African Procurement Law Unit

Authors

Prof Geo Quinot

Mr Joshua Swart

May 2026

Cite as: Quinot, G & Swart, J (2026) *Public Procurement of Cloud Services in South Africa: Policy Position Paper* (Stellenbosch: APLU).

www.africanprocurementlaw.org

TABLE OF CONTENT

ABBREVIATIONS

4IR	Fourth Industrial Revolution
AfCFTA	African Continental Free Trade Area Agreement
AGSA	Auditor-General of South Africa
AI	Artificial Intelligence
AWS	Amazon Web Services
C&DTI Roadmap	Communications & Digital Technology Infrastructure Roadmap
CDO	Chief Data Officer
CISPE	Cloud Infrastructure Service Providers in Europe
CKO	Chief Knowledge Officer
COBIT	Control Objectives for Information and Related Technologies
CSPs	Cloud Service Providers
DCDT	Department of Communications and Digital Technologies
DGPF	Digital Government Policy Framework
DHA	Department of Home Affairs
DPSA	Department of Public Service and Administration
DSTI	Department of Science, Technology and Innovation
DSU	Digital Service Unit
ECA	Electronic Communications Act 36 of 2005
ECTA	Electronic Communications and Transactions Act 25 of 2002
GCC	General Conditions of Contract
GDPR	General Data Protection Regulation (EU) 2016/679
GDS	Government Digital Service (UK)
GIS	Geographic Information Systems
GITOC	Government Information Technology Officers Council
GPC	Government Private Cloud
GWEA	Government-Wide Enterprise Architecture
IaaS	Infrastructure as a Service
ICASA	Independent Communications Authority of South Africa Act 13 of 2000
ICT	Information Communication Technology
IDWG	Inter-Departmental Working Group
IMC	Inter-Ministerial Committee
ITIL	Information Technology Infrastructure Library
ITU	International Telecommunication Union

KM	Knowledge Management
MFMA	Municipal Finances Management Act 56 of 2003
MISS	Minimum Information Security Standards
MSPs	Managed Service Providers
NIST	National Institute of Standards and Technology
NDP	National Development Plan
NT	National Treasury
OaaS	Outcome as a Service
OCDS	Open Contracting Data Standard
OCPO	Office of the Chief Procurement Officer
OECD	Organisation for Economic Cooperation and Development
PaaS	Platform as a Service
PAM Act	Public Administration Management Act 11 of 2014
PAYG	Pay-as-you-go
PFMA	Public Finance Management Act 1 of 1999
PPA	Public Procurement Act 28 of 2024
PPO	Public Procurement Office
PPP	Public Private Partnerships
POPIA	Protection of Personal Information Act 4 of 2014
PSA	Public Service Act, 1994
SaaS	Software as a Service
SARS	South African Revenue Service
SCC	Special Conditions of Contract
SCM	Supply Chain Management
SCOPA	Standing Committee on Public Accounts
SDIA	Spatial Data Infrastructure Act 54 of 2003
SDIC	State Digital Infrastructure Company
SEDA	Small Enterprise Development Agency
SITA	State Information Technology Agency
SLA	Service Level Agreement
SME	Small and Medium Enterprises
SSA	State Security Agency
TCO	Total Cost of Ownership
XaaS	Anything as a Service

1 EXECUTIVE SUMMARY

South Africa stands at a decisive juncture in its digital transformation trajectory. Over the past two years, government has adopted an ambitious suite of policy instruments advancing a cloud-first and digital public infrastructure (DPI) agenda, including the National Data and Cloud Policy (2024), the Digital Government Policy Framework, the Communications and Digital Technology Infrastructure Roadmap (2024), and the Roadmap for the Digital Transformation of Government (2025). Collectively, these instruments articulate a clear policy direction: the transition toward interoperable, data-driven governance enabled by cloud infrastructure.

However, this policy trajectory is not matched by the legal and operational framework governing public procurement. Public procurement regulation, as currently set out under the Public Finance Management Act 1999 (PFMA), Local Government: Municipal Finance Management Act 2003 (MFMA), Preferential Procurement Policy Framework Act 2000 (PPPFA) and several ancillary statutory instruments, remains structurally oriented toward the acquisition of static goods and services. These instruments presuppose fixed specifications, predetermined outputs, linear tender processes and static pricing models. By contrast, cloud computing and DPI operate through fundamentally different modalities, including consumption-based pricing, modular deployment, continuous iteration and platform-based service ecosystems.

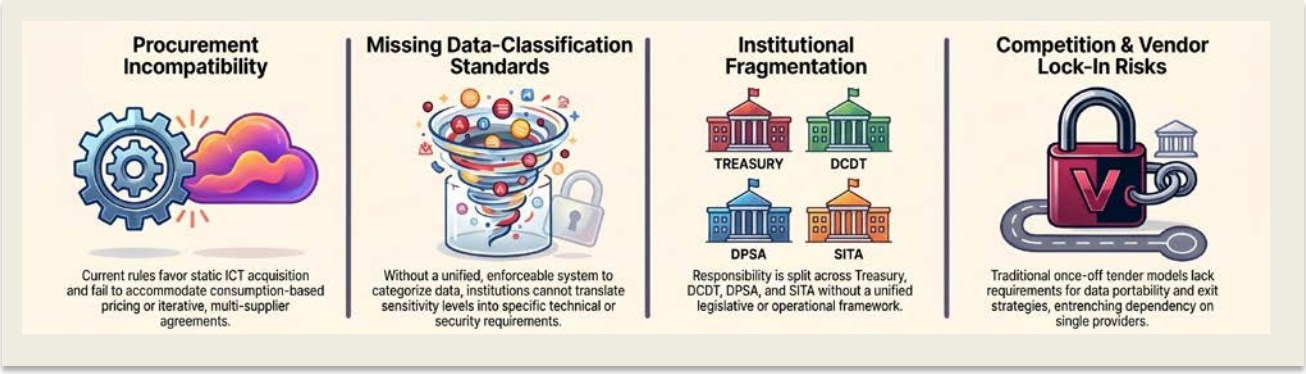
The result is a structural misalignment between policy ambition and legal operability. Public institutions are required to implement cloud-first and digital-government strategies while remaining bound to procurement rules that do not permit their effective execution. In practice, this produces implementation delays, fragmented adoption, increased audit exposure, and a reliance on deviations or bespoke arrangements that undermine legal certainty.

The Public Procurement Act 2024 (PPA), while not yet in operation, offers a critical opportunity to realign South African public procurement practice in relation to cloud computing. The imminent promulgation of the PPA Regulations represents a critical inflection point. These regulations will determine whether South Africa's procurement framework evolves to accommodate digital infrastructure, or whether existing constraints are entrenched.

This paper is therefore positioned as an intervention in both the public cloud policy development *and* public procurement reform in South Africa. Specifically, the paper analyses the interaction between these developments. The ultimate aim is to inform the continued development of South Africa's public procurement system, currently primarily through the development of the PPA Regulations, to align procurement law with the technical and commercial realities of cloud computing and DPI.

1.1 Structural Constraints in the Current Framework

The analysis identifies four systemic constraints that must be addressed to enable a functional digital procurement regime.



1.1.1 Procurement incompatibility

Existing procurement rules do not adequately accommodate the defining characteristics of cloud services and digital infrastructure. They do not provide for consumption-based pricing models, iterative or phased procurement, or multi-supplier framework agreements. As a result, departments are required to interpret digital procurement through frameworks designed for static ICT acquisition, leading to procedural uncertainty, compliance risk and implementation delays.

1.1.2 The absence of a binding data-classification framework

South Africa lacks a unified and enforceable system for classifying public data in a manner that can be operationalised within cloud environments. While the Protection of Personal Information Act 2014 (POPIA) and related instruments establish substantive data-protection obligations, they do not provide a mechanism for translating data sensitivity into procurement requirements, deployment models or technical safeguards. The continued reliance on the Minimum Information Security Standard (MISS), which predates modern cloud architectures, exacerbates this gap. The absence of classification standards undermines lawful deployment, inhibits interoperability and creates systemic uncertainty across government.

1.1.3 Institutional fragmentation

Responsibility for digital policy, procurement regulation, data governance and implementation is distributed across multiple institutions, including National Treasury (NT), the Department of Communications and Digital Technologies (DCDT), the Department of Public Service and Administration (DPSA), the State Information Technology Agency (SITA), the Information Regulator and the Presidency's Digital Service Unit (DSU). These institutions operate without a unified legislative or operational framework, resulting in overlapping mandates, inconsistent standards and limited accountability. The current role of SITA, in particular, reflects a structural misalignment between its statutory mandate and its operational capacity.

1.1.4 Competition and lock-in risks

Traditional once-off tender models, combined with static contracting approaches, increase the risk of long-term vendor dependency. In the absence of enforceable requirements for interoperability, portability and exit, procurement decisions may entrench incumbent providers and limit future competition. Comparative experience demonstrates that these risks are not inherent to cloud markets but arise from procurement design.

1.2 Central finding

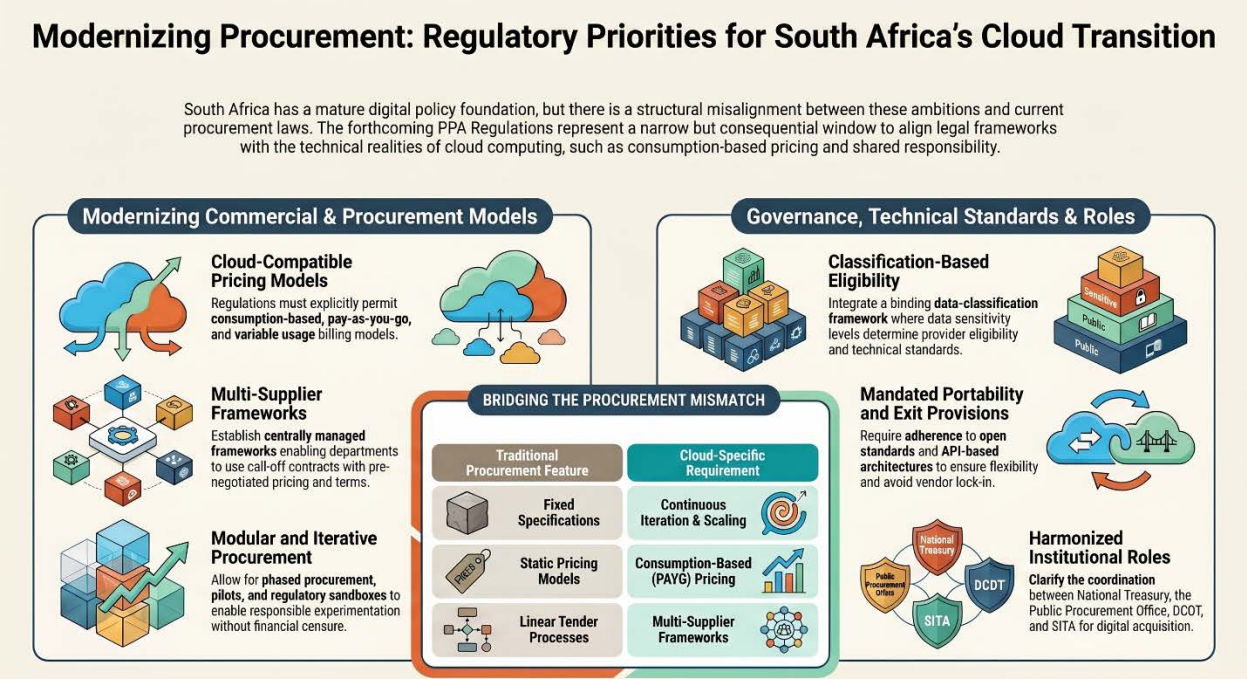
The central finding of this paper is that South Africa's digital transformation challenge is no longer one of policy formulation, but of legal and institutional operability.

Jurisdictions that have successfully implemented cloud-enabled government have done so by adapting procurement frameworks to the technical and commercial realities of digital infrastructure. South Africa faces the same imperative: digital policy must now be translated into enforceable procurement rules, standards and institutional arrangements.

The PPA provides a critical opportunity to achieve this translation, especially through the drafting of detailed implementation regulations under the Act.

1.3 Regulatory Priorities for the PPA Regulations

To enable lawful, secure and scalable cloud adoption and DPI development, the PPA Regulations should incorporate the following elements.



1.3.1 Recognition of cloud-compatible pricing and contracting models

The Regulations should explicitly permit consumption-based pricing, including pay-as-you-go and variable usage billing, as well as multi-year commitment structures and hybrid pricing models appropriate to cloud services.

1.3.2 Establishment of multi-supplier framework agreements

The Regulations should provide for centrally managed, multi-supplier frameworks enabling departments to procure cloud and digital infrastructure services through call-off contracts in a clear legal structure. Such frameworks should include continuous provider accreditation, standardised contractual terms and pre-negotiated pricing mechanisms.

1.3.3 Enabling modular and iterative procurement methods

The Regulations should permit phased procurement, pilot programmes and iterative contracting approaches appropriate to digital infrastructure, including mechanisms for scaling from innovation to pilot to full deployment. Importantly, the Regulations should allow for regulatory sandboxes that would enable responsible experimentation in a lawful manner, where the lack of success of a procured solution would not lead to public finance management censure.

1.3.4 Integration of data classification into procurement eligibility

A national, binding data-classification framework should be developed and incorporated into procurement processes, such that classification levels determine provider eligibility, deployment models and minimum technical standards.

1.3.5 Mandating interoperability, portability and exit provisions

Procurement instruments should require adherence to open standards, API-based architectures and enforceable exit mechanisms, ensuring that public institutions retain flexibility and avoid long-term lock-in.

1.3.6 Clarification of institutional roles and coordination mechanisms

The Regulations should support a coherent allocation of responsibilities across NT, the (to-be-created) Public Procurement Office (PPO) in NT, DCDT, SITA and other relevant institutions, ensuring alignment between policy, regulation and implementation in respect of public cloud procurement.

1.4 Strategic opportunity

South Africa possesses a mature digital ecosystem, including significant hyperscaler investment, a growing domestic partner network and a well-developed policy foundation for digital transformation. The primary constraint now lies in the procurement and governance framework through which this ecosystem is accessed.

The forthcoming PPA Regulations present a narrow but consequential window of opportunity. If procurement rules are aligned with the requirements of cloud computing and DPI, South Africa can transition rapidly toward a scalable, interoperable and secure digital state. If not, digital transformation efforts will remain constrained by legal uncertainty, institutional fragmentation and suboptimal procurement design.

Final Insight

South Africa's strategic digital ambition is clear and internationally aligned. The infrastructure foundation is advanced, and the cloud ecosystem is deep. The structural limitations now sit squarely in procurement law, data-governance standardisation, and mandate coordination. The countries that have succeeded in cloud adoption did not attempt to "fit cloud into traditional procurement." They adapted procurement to cloud and South Africa faces the same choice.

If it embeds classification, establishes a cloud-specific multi-framework mechanism, modernises procurement rules and clarifies institutional mandates, a lawful, secure, scalable cloud-first government becomes fully achievable.

South Africa has already made the policy decision to pursue digital transformation. The remaining question is whether its public procurement system will enable that decision to be realised.

The trajectory of digital public infrastructure in South Africa will ultimately be determined not by technological capability, but by the legal architecture through which that capability is procured and governed.

2 INTRODUCTION

South Africa stands at a critical juncture in the evolution of its public procurement system and its digital transformation agenda. The enactment of the PPA signals a decisive effort to consolidate and modernise the legal framework governing public procurement across all spheres of government. Yet, the true operational significance of this reform lies in the forthcoming Regulations, which will determine how procurement is implemented in practice, including the methods, pricing structures and institutional arrangements through which goods and services are acquired.

At the same time, the government has articulated an increasingly coherent policy vision for digital transformation. Recent instruments, including the National Data and Cloud Policy (2024), the Digital Government Policy Framework, the Communications and Digital Technology Infrastructure Roadmap (2024), and the Roadmap for the Digital Transformation of Government (2025), collectively advance a "cloud-first" approach to public service delivery. These policies position cloud computing and DPI as foundational enablers of a more integrated, data-driven and responsive state.

However, the implementation of this vision is contingent upon the legal and institutional mechanisms through which digital services are procured. Public procurement functions as the primary interface between policy ambition and operational execution. It is through procurement that digital infrastructure is acquired, markets are shaped and state capability is realised. In this respect, the relationship between digital policy and procurement law is not incidental, but determinative.

> **"the relationship between digital policy and procurement law is not incidental, but determinative"**

A central concern addressed in this paper is the extent to which the public procurement framework, soon to be consolidated under the PPA, supported by a range of ancillary regulatory instruments and institutional arrangements governing ICT procurement, remains aligned with the operational realities of (public) cloud computing. The prevailing procurement paradigm is structured around the acquisition of discrete goods and services, characterised by fixed specifications, predetermined outputs, linear tender processes and static pricing models. By contrast, cloud computing operates through consumption-based pricing, on-demand scalability, continuous iteration and platform-based service delivery.

This divergence gives rise to a structural misalignment between South Africa's digital policy objectives and the legal framework through which those objectives must be implemented. The consequence is not merely conceptual, but operational. Procurement officials are required to interpret and apply legacy supply chain management frameworks to cloud-based services, often resulting in risk-averse practices,

delays in implementation and reliance on ad hoc or exceptional procurement mechanisms. Financial management systems, in turn, are required to accommodate variable and consumption-based expenditure within budgeting frameworks designed for fixed commitments. At an institutional level, fragmentation across key actors, including NT, DCDT, DPSA, SITA and the Information Regulator, further compounds uncertainty and inconsistency in practice.

This misalignment is particularly evident in the regulatory instruments and guidance currently governing public ICT and cloud procurement. Existing circulars and procurement instructions, while intended to provide oversight and control, operate within a procurement paradigm that does not accommodate the core characteristics of cloud computing. In doing so, they have the effect of constraining agile and scalable procurement approaches, thereby constituting a primary structural barrier to the implementation of cloud-first strategies.

The imminent promulgation of the PPA Regulations therefore presents a critical opportunity to address these challenges. The Regulations will define the permissible procurement methods, pricing models and contracting mechanisms applicable to digital infrastructure. In this sense, they represent a pivotal point at which procurement law may either evolve to support public cloud computing and DPI, or entrench existing constraints in a new regulatory form.

Against this backdrop, this paper examines the extent to which the current procurement framework enables or constrains the acquisition of cloud services, identifies key gaps and structural misalignments, and advances targeted regulatory interventions aimed at aligning procurement law with the requirements of digital public infrastructure. The analysis is informed by comparative international experience, recognising that jurisdictions which have successfully implemented cloud-enabled government have done so through procurement systems that accommodate consumption-based services, enable framework-based procurement and integrate data governance considerations into procurement design.

The paper proceeds on the basis that South Africa's digital transformation challenge is no longer one of policy articulation, but of legal and institutional operability. In this regard, procurement law is understood not only as a mechanism for acquiring goods and services, but as a critical instrument for shaping markets, enabling innovation and determining the trajectory of the digital state.

2.1 Purpose and scope of the paper

The purpose of this paper is to analyse the intersection between South Africa's cloud-related policy instruments and its public procurement framework, with particular emphasis on the extent to which the latter enables or constrains the implementation of cloud-first strategies. It seeks to identify areas of misalignment between policy ambition and procurement operability, and to propose targeted interventions, particularly within the forthcoming PPA Regulations, that may support a more coherent and enabling framework for the procurement of digital infrastructure.

The scope of the paper includes an examination of relevant legislative instruments, policy frameworks and institutional arrangements, as well as an assessment of public procurement practices as they relate to public cloud computing. The analysis is both doctrinal and functional, recognising that legal design and operational implementation are closely intertwined in the public procurement context.

2.2 Context: Digital transformation and cloud adoption in South Africa

South Africa's approach to digital transformation reflects a broader global shift toward the use of cloud computing as the backbone of public service delivery. Cloud infrastructure underpins a range of digital public infrastructure components, including identity systems, data exchange platforms and digital payments, which together enable more integrated and efficient government services.

In the domestic context, government policy has increasingly emphasised the importance of shared digital infrastructure, interoperability and data-driven governance. These objectives are framed within a broader commitment to improving service delivery, enhancing administrative efficiency and supporting economic development through digital innovation.

Notwithstanding these policy developments, the implementation of cloud-based systems within the public sector remains uneven. This is attributable, in part, to the constraints imposed by existing procurement frameworks, which have not evolved at the same pace as digital policy. As a result, there is a growing recognition that procurement reform is a necessary condition for the realisation of South Africa's digital transformation objectives.

> **"procurement reform is a necessary condition for the realisation of South Africa's digital transformation objectives"**

2.3 What are cloud services - basic terminology, frames, ecosystem

2.3.1 Cloud Computing Fundamentals

Cloud computing delivers computing resources, including servers, storage, networking, applications, analytics, and artificial intelligence, on-demand via the internet. Unlike traditional IT infrastructure, cloud services operate on a pay-as-you-go model, similar to utility services where organisations pay only for actual consumption. This represents a fundamental shift from capital-intensive, dedicated IT resources to flexible, service-based models that have transformed public sector procurement approaches.

2.3.2 Cloud Service Models

Cloud service models take the following forms.

Infrastructure as a Service (IaaS): Virtual IT Foundations

IaaS provides organisations with fundamental computing resources, servers, storage capacity, networking capabilities, and operating systems, delivered virtually through the cloud. Rather than purchasing, housing, and maintaining physical hardware in government-owned data centres, organisations rent these resources on-demand from cloud providers. This model is comparable to leasing office space instead of

constructing a building: organisations access the infrastructure they need, scale it up or down based on requirements, and pay only for what they use. IaaS eliminates the significant upfront capital expenditure traditionally required for IT infrastructure whilst providing flexibility to respond rapidly to changing operational needs.

Platform as a Service (PaaS): Ready-Made Development Environments

PaaS offers a complete development and deployment environment in the cloud, enabling organisations to build, test, and run applications without managing the underlying infrastructure complexity. Think of PaaS as a fully equipped workshop where developers can focus on creating applications rather than maintaining the tools and facilities. The cloud provider handles servers, storage, networking, databases, middleware, and development tools, whilst government entities concentrate on developing applications that serve citizens. This approach accelerates digital service delivery, reduces technical overhead, and allows IT teams to focus on innovation rather than infrastructure maintenance.

Software as a Service (SaaS): Ready-to-Use Applications

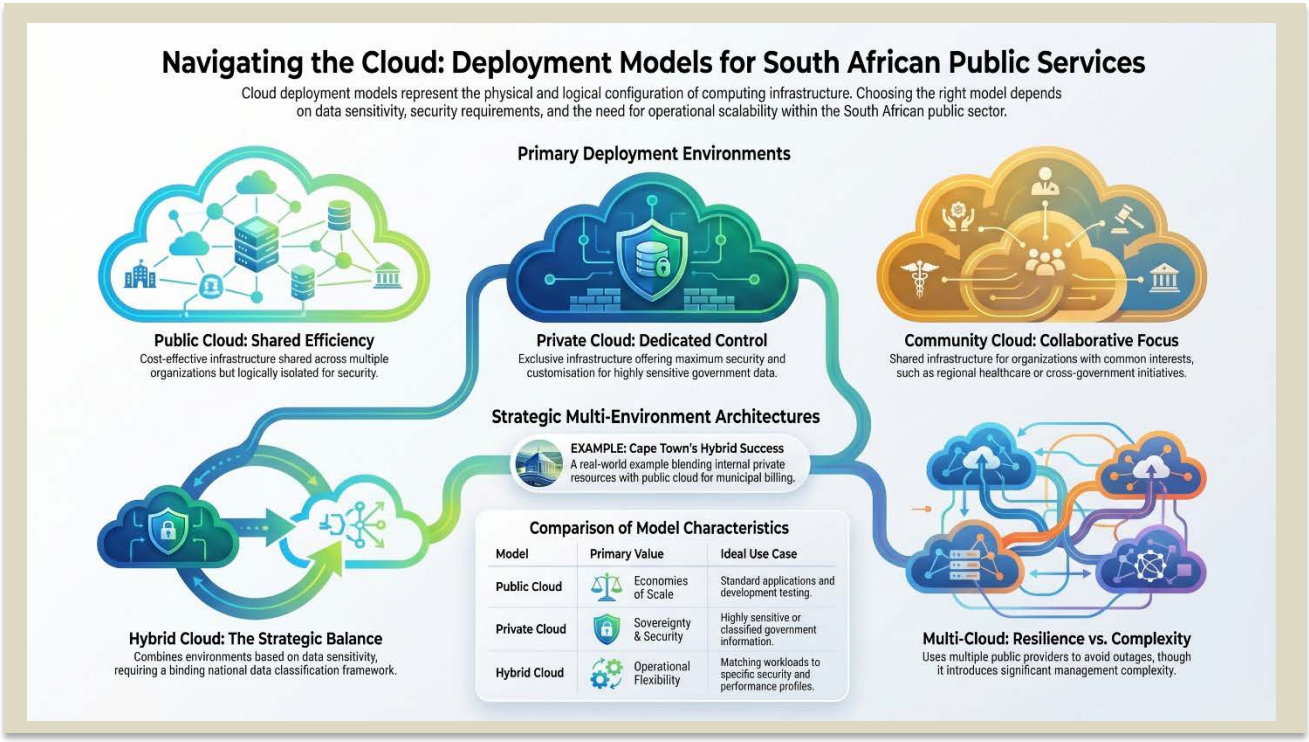
SaaS delivers fully functional applications over the internet on a subscription basis. Instead of purchasing software licences, installing applications on individual computers, and managing updates and security patches, organisations access software directly through web browsers. Common examples include email services, document collaboration tools, and customer relationship management systems. The cloud provider manages all aspects of the application, hosting, maintenance, security updates, and infrastructure, whilst users simply log in and work. This model eliminates the burden of software maintenance, ensures all users access the latest version, and converts large upfront software costs into predictable operational expenses. For public sector organisations, SaaS enables rapid deployment of citizen-facing services without extensive IT infrastructure investment.

Outcome as a Service (OaaS): Results-Focused Cloud Solutions

OaaS represents the most comprehensive cloud service model, where providers deliver specific business results or outcomes rather than merely providing technology or platforms. Instead of purchasing infrastructure, development environments, or applications, organisations contract for measurable outcomes such as "improved citizen service response times" or "reduced processing costs by 20%". The service provider assumes full responsibility for selecting, deploying, and managing whatever combination of technologies, processes, and expertise is required to achieve the agreed outcome. This model shifts risk from the public sector organisation to the provider, who is compensated based on successfully delivering the specified results. For government agencies, OaaS offers the advantage of focusing on policy objectives and citizen needs rather than technical implementation, whilst ensuring accountability through outcome-based performance metrics. This approach is particularly valuable when organisations lack internal technical expertise or wish to modernise services rapidly without building extensive in-house capabilities.

2.3.3 Cloud Deployment Models

Cloud services can be deployed via different models.



Public Cloud: Shared Infrastructure for All

Public cloud infrastructure is made available for use by any organisation or individual through a cloud service provider. The infrastructure, including servers, storage, and networking, is owned and operated by the cloud provider (such as commercial vendors, academic institutions, or government entities) and housed in the provider's data centres. Multiple organisations share the same physical infrastructure, though their data and applications remain isolated and secure. This model offers the greatest cost efficiency through economies of scale, as infrastructure costs are distributed across many users. Public cloud is particularly suitable for standard applications, development and testing environments, and services that do not involve highly sensitive data. Government agencies benefit from paying only for resources used without the burden of maintaining physical infrastructure.

Private Cloud: Dedicated Infrastructure for Single Organisations

Private cloud infrastructure is reserved exclusively for a single organisation, such as a government department or public body with multiple divisions. Whilst the infrastructure serves only one organisation, it may be owned and managed by the organisation itself, a third-party provider, or a combination of both. The infrastructure can be located on the organisation's premises (on-site) or hosted at an external facility (off-site). Private cloud offers the highest level of control, customisation, and security, making it ideal for

handling sensitive data, classified information, or applications with strict regulatory requirements. This model suits government agencies requiring enhanced data sovereignty, specialised security configurations, or compliance with specific legal frameworks, though typically at higher cost than public cloud.

Community Cloud: Shared Infrastructure for Collaborative Groups

Community cloud infrastructure serves a specific group of organisations with common interests, objectives, or requirements, such as public sector bodies collaborating on shared services, health organisations with similar regulatory obligations, or local authorities working on joint initiatives. The infrastructure may be owned and operated by one or more member organisations, a dedicated third party, or a collaborative arrangement, and can be located on or off members' premises. This model enables organisations to share costs whilst maintaining higher security and compliance standards than public cloud. Community cloud is particularly valuable for cross-government initiatives, regional partnerships, or sector-specific services where organisations benefit from shared resources whilst maintaining appropriate data protection and governance aligned with their collective mission, security requirements, and policy considerations.

Hybrid Cloud: Integrated Multi-Environment Strategy

Hybrid cloud refers to the coordinated use of two or more distinct cloud environments, typically a combination of public, private or community clouds, linked through standardised interfaces that allow controlled data exchange and workload mobility. Although each environment remains technically and administratively separate, they function as part of a unified architectural strategy that allocates workloads according to their sensitivity, performance profiles and regulatory requirements. In government contexts, this often takes the form of retaining highly sensitive or regulated datasets within a private or sovereign cloud, while consuming scalable public-cloud services for less sensitive workloads or variable-demand computing needs.

Critically, however, hybrid cloud is not simply a technical configuration choice. A lawful and effective hybrid strategy presupposes a clear, binding data-classification framework that determines which categories of information may reside in which environments and under what security controls. Without such classification, hybrid deployments can become inconsistent, expose agencies to compliance risk and undermine interoperability. When anchored in a robust classification regime, hybrid cloud offers strategic flexibility: agencies can maintain strict control over sensitive operations while leveraging the elasticity and innovation of public-cloud platforms for appropriate workloads, achieving a more balanced, context-responsive digital architecture.

Multi-Cloud Deployment

Multi-cloud refers to the intentional use of more than one public-cloud provider for different components of a system or portfolio of workloads. Its recent prominence is largely a response to high-visibility outages, which has led some institutions to consider multi-cloud as a resilience measure. However, the model carries significant trade-offs. Multi-cloud can reduce dependency on a single provider and, for certain

workloads, improve continuity of operations. Yet it also introduces substantial complexity: agencies must duplicate tooling, security controls and integration layers across providers, often at considerable cost. Without architectures designed specifically for cross-cloud portability, resilience gains are frequently marginal while expenditure increases sharply.

For the South African public sector, multi-cloud should therefore be treated as a specialised, not default, deployment model. It is suitable only where a clear operational need exists and where workloads are engineered for genuine cross-cloud failover or interoperability. In most cases, especially legacy or monolithic government systems, the governance, cost and compliance burdens may outweigh any resilience benefit. A lawful procurement approach must therefore require agencies to justify multi-cloud adoption through structured needs assessment, cost–benefit analysis and explicit alignment with data-classification and interoperability requirements.

2.3.4 The Need for Cloud-Specific Procurement

Traditional IT procurement methods designed for hardware, software, and data centre acquisitions are inadequate for cloud services. Cloud procurement requires distinct approaches to pricing, contract governance, terms and conditions, security, and service level agreements (SLA). A cloud-centric acquisition process enables public sector organisations to realise key benefits including access to innovation, increased agility, improved security, compliance governance, and cost efficiencies. Applying conventional procurement methods undermines these advantages.

2.3.5 Direct and Indirect Procurement Routes

Public sector organisations can procure cloud services through two channels: directly from hyperscale Cloud Service Providers (CSPs) or indirectly through CSP partners such as Managed Services Providers (MSPs) and solutions providers. Cloud acquisition strategies must clearly distinguish between cloud technologies (compute, networking, storage) provided by CSPs and hands-on labour services (professional services, consulting, managed services) required to utilise those technologies. These components can be purchased as a comprehensive solution or separately, each with distinct roles, responsibilities, terms, and service-level agreements.

2.3.6 The Shared Responsibility Model

The shared responsibility model delineates the respective security obligations of cloud providers and public bodies. CSPs assume responsibility for security “of the cloud,” encompassing physical data-centre infrastructure, underlying hardware, virtualisation layers, core networking, and the integrity of foundational platform services. Public institutions, by contrast, remain responsible for security “in the cloud,” including data protection, identity and access management, encryption, application-layer controls, access governance and the configuration of cloud-native services.

In the South African context, this model has an additional procurement-law dimension. Many public bodies procure cloud services indirectly through accredited partners, resellers or managed-service

providers to address internal capacity constraints. These intermediary arrangements can also support socio-economic policy objectives. For example, SITA-governed procurement is subject to requirements that a portion of eligible spend be directed to black-owned SMMEs, and indirect cloud procurement through partner ecosystems can provide a lawful mechanism for meeting such obligations without compromising technical standards or security requirements.

When properly governed, the shared responsibility model therefore serves both a security function, by clarifying control boundaries, and a procurement function, by creating structured opportunities for compliant participation by local SMMEs in value-added cloud services. However, realising these socio-economic benefits requires strong governance and clear contracting to ensure that responsibility boundaries are understood, monitored and enforceable.

2.4 Cloud services landscape in South Africa

2.4.1 Players

South Africa hosts the most mature and competitive cloud services ecosystem on the continent yet holds vast room for improvement. The local market is led by global hyperscalers and supported by a growing base of regional and local providers:

Global players:

Amazon Web Services (AWS), Microsoft Azure, and Google Cloud are the key international providers with local data centres in Johannesburg and Cape Town. Their market entry has been catalytic for the local ecosystem, spurring demand for XaaS offerings.

Telecom operators:

Major telcos such as Vodacom, MTN and Telkom have repositioned as hybrid cloud and managed service providers, leveraging their existing infrastructure and customer bases.

South African government:

The South African Revenue Service (SARS) has migrated elements of its taxpayers portal and analytics workloads to the cloud to improve uptimes and processing efficiency. The Department of Health used cloud-based systems for managing COVID-19 vaccination data and digital health records. The Department of Home Affairs (DHA) is exploring a secure cloud architecture under its *Modernisation Programme* for digitising the National Population Register and e-ID services. The *City of Cape Town's Data Strategy* has adopted a multi-year digital transformation programme aimed at improving public service delivery, data transparency and citizen engagement. Cloud infrastructure is set to host municipal applications, including geographic information systems (GIS), billing, customer portals and internal collaboration tools. This hybrid model combines private cloud resources managed internally with public cloud services (from AWS and Azure) for scalability and analytics.

Systems integrators and MSPs:

Firms like Dimension Data, BCX, EOH and Liquid Intelligent Technologies act as intermediaries, bundling cloud with connectivity, cybersecurity and business continuity services.

Local hosting firms:

Data centre specialists like Teraco, African Data Centres, and Cloud Africa provide colocation and private cloud infrastructure that support both hyperscalers and enterprises. Local providers ensure data localisation and compliance with POPIA.

Emerging innovators:

A layer of small and medium providers offer niche SaaS or industry-specific cloud products, especially in fintech, agritech and public sector digitisation.

2.4.2 Structure of the sector - Public-Sector Digitisation and Cloud Integration

A practical illustration of the layered structure of South Africa's cloud ecosystem can be seen in the City of Cape Town's Data Strategy. The municipality has adopted a hybrid-cloud model that blends locally managed private cloud systems with public cloud services from global hyperscalers such as AWS and Microsoft Azure. At the infrastructure layer (IaaS), the City relies on cloud-hosted computing and storage to manage large datasets, including GIS and municipal billing data. These workloads are hosted partly through local data centre operators such as Teraco to maintain compliance with POPIA and emerging data residency expectations under the National Cloud and Data Policy.

At the platform layer (PaaS), the City leverages cloud development and analytics environments to process real-time data from sensors across transport, water, and energy networks. This platform capability enables predictive maintenance and improved urban planning, demonstrating how local governments can use cloud-based analytics to support evidence-based policy. Finally, at the software layer (SaaS), the City has adopted cloud-hosted collaboration tools and citizen service applications, from e-billing to digital permit systems, which allow secure access for staff and citizens alike.

Similar initiatives reinforce the structural interdependence of South Africa's cloud sector. SARS uses cloud-based analytics to enhance tax compliance, the Department of Health employs cloud solutions to manage vaccination and digital health data, and the DHA is developing a secure cloud architecture for digitising identity records. These examples demonstrate how the public sector is increasingly positioned as both a user and driver of the national cloud ecosystem. By utilising multi-layered cloud services, public institutions are helping to shape a more resilient, interoperable, and data-driven governance infrastructure - a key condition for the successful roll-out of a cloud-first procurement policy.

2.4.3 Business models

The commercial structure of South Africa's cloud ecosystem reflects a mix of consumption-based, subscription-based and service-integrated models, each with distinct procurement implications. Importantly, cloud services cannot be reduced to "subscription models": different providers and service

categories apply materially different commercial logics that affect budgeting, contracting and value-for-money assessments in the public sector.

Consumption-based Pay-as-you-go (PAYG) Models:

Most hyperscalers operate primarily or exclusively on a pure consumption model, where customers pay only for the resources used, without upfront fees or mandatory long-term commitments. This model aligns with on-demand scalability and reduces capital expenditure but creates complexity for public entities that must forecast variable usage within annual budgeting cycles.

Reserved capacity and enterprise commitment models:

Some providers also offer options for reserved instances, committed-use discounts, or enterprise-wide agreements. These are not subscriptions in the traditional sense, but structured commitments in exchange for predictable pricing. Such models can provide stability but require careful contractual oversight to avoid inflexible long-term lock-in.

Hybrid and Private-Cloud service models:

Telecommunications firms and managed service providers offer private-cloud or hybrid-cloud solutions on a mixture of fixed-fee, consumption-based or capacity-based pricing. These are often used in sectors with regulatory or sovereignty constraints.

Managed Cloud Services and Systems Integration:

MSPs derive recurring revenue from migration, optimisation, monitoring and cybersecurity services. These arrangements are frequently structured as monthly recurring service contracts and play a crucial role where government entities lack in-house capability.

Colocation and Data-Centre Leasing Models:

Colocation operators charge for physical space, power, cooling and cross-connects. This remains a significant component of the overall cloud ecosystem, supporting hyperscaler presence and enterprise hosting, and operates largely outside subscription or consumption models.

SaaS Licensing and Subscription Models:

SaaS vendors typically use subscription or licence-based models, often tiered by functionality, user count or compliance requirements. This remains the predominant model for application-layer solutions.

Channel, Reseller and Partner Ecosystems:

Hyperscalers rely on certified partners for sales, implementation and ongoing support. These partners operate under diverse commercial structures: resale margins, managed-service fees, project-based engagements or value-added consulting. This ecosystem expands local participation and can support procurement transformation, including socio-economic objectives.

Taken together, these business models illustrate that South Africa's cloud economy is not driven solely by subscription revenue but by a layered mix of consumption, commitment, service-integration and partnership-based arrangements. For public procurement, this diversity requires clear guidance on

contracting, forecasting and evaluation, particularly where PAYG models interact with annual appropriations, or where partner ecosystems create indirect procurement routes that must still comply with legal, financial and socio-economic mandates.

2.4.4 Regulatory and Policy Context

While South Africa's technical ecosystem is relatively advanced, the regulatory framework remains fragmented. Key instruments such as the Electronic Communications and Transactions Act 2002 (ECTA), POPIA, and the Cybercrimes Act 2020 provide the legal basis for digital transactions, data protection, and cybersecurity. However, institutional coordination between SITA, NT, and the Information Regulator is still evolving.

The PPA presents an opportunity to harmonise procurement law with digital-era requirements, embedding data protection, electronic signatures, and cybersecurity compliance into procurement practice. The successful rollout of a cloud-first policy for public procurement will depend on clarifying these institutional roles, updating outdated municipal SCM regulations, and ensuring alignment between technology policy and procurement law.

2.4.5 Key Insight

South Africa's cloud landscape reflects both technological maturity and policy flux. While global investment has built a strong infrastructure base, public-sector digital transformation and procurement reform remain the most critical levers for accelerating widespread, secure, and equitable cloud adoption. The country's ability to harmonise its legal and institutional frameworks will determine whether it can sustain a cloud-first transition that balances innovation, sovereignty, privacy and public accountability.

3 METHODOLOGY

The methodology adopted in this paper involves a desktop analysis of regulatory instruments impacting on public procurement of cloud services. The research team identified all relevant policy instruments by way of a comprehensive review of South African statutory law, including both primary and secondary instruments. This review was supplemented by an institutional review of all public entities potentially involved in cloud procurement. The aim of this second step was to identify any further relevant policy documents.

3.1 Policy review

Each policy identified is reviewed in terms of a standardised review framework and a qualitative rating assigned to each element in the framework. This is followed by a gap analysis of the policy in relation to public cloud services procurement.

3.2 Policy review framework

All policies are reviewed in terms of the following review framework.

3.2.1 Thematic lenses

Category	Key Questions / Indicators
1. Legal Clarity	Is the document legally binding or policy-based? Are roles, definitions, and procedures clear?
2. Policy Coherence	Are there overlaps or contradictions with other frameworks (e.g., procurement vs ICT policy)?
3. Procurement Compatibility	Does the policy enable or restrict agile, cloud-specific procurement approaches?
4. Market Access and Competition	Are there barriers to entry for SMEs and new cloud providers?
5. Digital Sovereignty & Security	Are data localisation, residency, or ownership requirements well-defined and practical?
6. Institutional Mandates	Are institutional roles (e.g., SITA, Treasury, DCDT) clearly aligned for implementation?
7. Implementation Feasibility	Are timeframes, funding, capacity, and enforcement mechanisms realistic and actionable?
8. Alignment with Global Best Practice	Does the document reflect international norms (e.g. modular procurement, interoperability)?

3.2.2 Rating system

A qualitative rating in relation to procurement of cloud solutions is assigned to the policy for each of the eight thematic lenses, using the following rating system.

Rating	Description
Strong	Clear, enabling, and aligned with best practices
Moderate	Some clarity but room for improvement; potential ambiguities or bottlenecks
Weak	Lacks clarity or conflicts with other frameworks; risks blocking outcomes

3.2.3 Findings

Based on the policy review and gap analysis, findings are formulated for each regulatory instrument (or set of instruments) pertaining to cloud procurement.

These findings are consequently consolidated into an overarching set of findings regarding the policy environment pertaining to cloud procurement in South Africa.

3.4 Benchmark against international experiences

The findings flowing from the analysis of the South African policy environment are compared to selected foreign examples and international principles.

4 POLICY REVIEW AND GAP ANALYSIS

4.1 Introduction

South Africa does not have a consolidated, overarching policy instrument governing the procurement of cloud solutions in the public sector. Rather, a wide range of different policy instruments impact on such procurement. These are spread out across several core institutional environments, primarily DCDT, DPSA, SITA, NT, Presidency (DSU). Each environment approaches the cloud procurement function from the perspective of its own institutional mandate with little cross-functional alignment. In this section, the main policy instruments impacting on procurement of cloud solutions by the public sector are analysed.

The policy instruments analysed can be broadly categorised into three main categories as follows.

Category	Instrument	Date	Implementing Authority
Public procurement instruments	Public Procurement Act (PPA)	2024	NT
	SITA Act & Regulations (as amended)	1998, 2005, 2025	DPSA DCDT
	General Conditions of Contract (GCC)	2010	NT
ICT and cloud policy instruments	National Data and Cloud Policy	2024	DCDT
	draft Digital Government Policy Framework (DGPF)	2024	DPSA
	South Africa's Communications & Digital Technology Infrastructure Roadmap (the C&DTI Roadmap)	2024	DCDT
	Roadmap for the Digital Transformation of Government	2025	DSU, NT, DCDT
	Public Service Act (PSA): Determination and Directive on the Usage of Cloud Computing Services in the Public Service	2022	DPSA
	PSA: Public Service Data Governance Framework	2024	DPSA
	PSA: Determination and Directive on the Implementation of Knowledge Management in the Public Service	2025	DPSA
	PSA: Determination and Directive on the Implementation of Data Governance in the Public Service	2025	DPSA
	PSA: Determination and Directive on Digital Public Services Standard	2025	DPSA
	Eskom Cloud Standard Policy	2019	Eskom
General policy instruments impacting across the spectrum irrespective of subject matter	Protection of Personal Information Act (POPIA)	2013	Information Regulator, Department of Justice
	Minimum Information Security Standard (MISS)	1996	State Security Agency

4.2 Public Procurement Act 28 of 2024

The promulgation of the PPA in July 2024 represents the most significant regulatory development in public procurement law in South Africa since the introduction of the country's modern public procurement system in 2000. However, the PPA is not yet in operation, pending the creation of detailed Regulations to give effect to the Act. Once in effect, the PPA will replace all existing regulatory instruments governing public procurement generally. A limited number of specific regulatory regimes for public procurement will remain in place under the PPA. One of the aims of the PPA is to "create a single framework that regulates public procurement". The PPA explicitly includes procurement of ICTs, which is viewed as part of "infrastructure" as defined by the Act: "'infrastructure' means the physical facilities or structures and systems, including digital or analogue communications systems that are required to provide services to the public directly or indirectly".

4.2.1 GAP Analysis

The policy review (see ***Addendum A at 9.1.1***) identified the following gaps.

Policy Area	Gap Identified	Implication
System Architecture & Timelines	No statutory timeline/phasing plan for the national platform; "progressive" rollout is undefined.	Risk of uneven adoption and prolonged dual systems; need PPO instruction with milestones, cutover windows, and minimum viable components.
Standards & Interoperability	The Act mandates interoperable open data, but no schema/API/security standard is specified.	Fragmentation and vendor lock-in if each organ digitises differently.
Data Classification & Publication	The Act expands publication/access but leaves the classification taxonomy (open/limited/confidential/PII) and redaction rules to later instruments. No clear alignment to data classification frameworks under other legislative regimes, such as DPSA policies.	Over- or under-disclosure risks (legal challenge or opacity). Need a standard classification and release schedule with POPIA-aligned redaction and explicit linkages to data classifications in other contexts (e.g. DPSA).
Identity, Access, Audit	No detail on who authenticates whom, role-based access, audit logging, and key management for the platform.	Security/control variance; harder incident forensics. PPO must prescribe identity & access baselines, immutable audit and key custody.
Municipal Adoption	PPO instructions are not automatically binding on municipalities (rely on guidelines/circulars and council adoption).	Heterogeneous municipal digitisation; need provincial treasury playbooks and model policies to drive convergence. Greatly undermines "one system" objective.
Method Support in the System	Procurement methods will be set by regulation; the platform must support them, but details are pending.	Early tenders risk rework once methods/frameworks are prescribed; maintain configurable workflows with versioning.
Readiness & Legacy Migration	"Readiness assessments" are required but criteria & migration rules are not defined.	Data quality gaps; audit trail discontinuities. PPO needs migration standards (ETL templates, master-data routines, archival policies).
Hosting & Sovereignty	Act mentions hosting options for procurement data but no residency/DR baseline.	Inconsistent resilience, sovereignty and POPIA alignment; PPO should fix in-country primary, defined DR RPO/RTO, and backup/retention norms.
Transparency vs Confidentiality	The Act allows public scrutiny while protecting candid deliberations/confidential info, but categories/tests are not defined.	Disputes and Tribunal reviews on disclosure decisions. Need publish-by-default lists, harm tests, and exemption reasons templates.

Funding & Capacity	The statute establishes duties (national system, analytics, databases) but does not itself ring-fence funding; commencement is phased.	Pace of digitisation depends on Treasury allocations; risk of delays without earmarked budgets and skills programmes.

4.2.2 Findings

The PPA introduces several provisions that may significantly complicate cloud solution procurement for South African public entities. However, right at the outset, it must be noted that the Act itself only provides a broad framework for procurement law. The specific rules will only emerge once regulations are promulgated under the Act.

The PPA's emphasis on standardised procurement processes, transparency and accountability remains grounded in a model of procurement that presupposes fixed specifications, predetermined outputs and static pricing. While these features are appropriate for traditional goods and services, they do not readily accommodate cloud computing, which is characterised by consumption-based pricing, on-demand scalability, continuous iteration and platform-based delivery. Within this structurally constrained environment, the provisions of the PPA introduce additional layers of complexity, but do not in themselves constitute the primary barrier to cloud adoption. Among these considerations, the preferential procurement framework introduced by the PPA presents a set of secondary, but nonetheless significant, considerations for cloud procurement. The requirement for pre-qualification criteria and mandatory subcontracting to small enterprises, cooperatives and entities owned by designated groups necessitates the structuring of bids through local partnerships. Given that major cloud service providers are typically large multinational corporations, compliance with these provisions will depend on the development of credible local partner ecosystems capable of delivering implementation, support and related services. While this may create opportunities for domestic participation and skills development, it also introduces complexity in bid structuring and contract management.

Similarly, the potential designation of cloud services or related infrastructure for local production and content requirements may give rise to additional compliance obligations. These could include requirements relating to data localisation, domestic hosting of infrastructure, or the generation of economic value within South Africa through investment in data centres, research and development, or associated services. While such measures may align with broader industrial policy objectives, they must be carefully calibrated to avoid unintended constraints on access to globally integrated cloud services.

In operational terms, the PPA introduces additional layers of complexity through the requirement for procurement to be conducted via a centralised ICT-enabled system, incorporating standardised data structures and an electronic marketplace. While these developments may enhance transparency and efficiency over time, they must be adapted to accommodate the multi-year, consumption-based expenditure profiles associated with cloud services. The shift from capital expenditure to operational expenditure models presents particular challenges for budgeting and financial management frameworks that remain oriented toward fixed commitments.

Crucially, the framework nature of the PPA creates significant regulatory latitude. The Act does not prescribe fixed procurement methods, pricing models, or contracting structures for digital services. As a result, it neither resolves nor definitively entrenches the misalignment identified above. Rather, it transfers the responsibility for resolving this misalignment to the forthcoming Regulations.

> **“ the principal barrier to cloud procurement in South African procurement law is not legislative prohibition, but regulatory inertia within a system that has yet to adapt to the realities of digital service delivery ”**

Accordingly, the primary finding is not that the PPA, in and of itself, precludes effective cloud procurement, but rather that, in the absence of deliberate regulatory intervention, it risks entrenching a procurement paradigm that is not aligned with digital service delivery. The extent to which the Act enables or constrains cloud adoption will therefore depend on how this regulatory space is utilised in the development of the PPA Regulations. An important characteristic of the PPA in this regard is the ample scope for differentiation within the Regulations. The Act provides explicit authorisation for different regulatory treatment of different categories of procurement, which opens the door to tailored approaches to procurement of cloud services. In this sense, the principal barrier to cloud procurement in South African procurement law is not legislative prohibition, but regulatory inertia within a system that has yet to adapt to the realities of digital service delivery.

4.3 General Condition of Contract

The General Conditions of Contract (GCC) is published by NT as a standard set of contract terms that all public entities must use as a template for procurement contracts. While use of the GCC is mandatory, entities are entitled to depart from the GCC by means of special conditions of contract (SCC), tailored to the particular context.

4.3.1 GAP Analysis

The policy review (see ***Addendum A at 9.1.2***) identified the following gaps.

Policy Area	Gap Identified	Implication
Digital Contract Execution & Signature	GCC does not specify electronic signature, non-repudiation, or “when is a digital signed contract binding.”	Without supplementary clauses, a digital system may struggle to ensure legal enforceability of contracts signed in the system. Need SCC or rider specifying valid e-signature standards (e.g. X.509, PKI) and process.
Auditability & Immutable Logs	GCC does not require contracts to maintain immutable audit trails, version history, or tamper detection.	The system must add audit logging “on top” of GCC obligations to track who viewed, modified, or accepted contract terms; useful for disputes or regulatory oversight.

Clause Trigger Logic & Automation	Many GCC clauses are conditional (e.g. penalties, termination, variation). But GCC text is not coded; there is no built-in logic for digital triggers.	The digital system must build clause engines that interpret events (late delivery, failure to perform test, warranty breach) and trigger notifications, penalties, or escalations in line with GCC semantics.
SCC Integration & Overrides	GCC requires that SCC take precedence where conflict exists. But in digital context, handling overrides must be carefully versioned and tracked.	The platform must support dynamic layering: base GCC + SCC templates + amendments, with conflict resolution logic and traceability.
Data Classification & Confidentiality	GCC clauses discuss inspections, use of contract documents, intellectual property, confidentiality, etc., but they don't define data classes, redaction, or digital confidentiality levels.	The system should incorporate data classification schemes (public, internal, confidential, personal data) and enforce redactions, access control, and encryption where required.
Platform Responsibility & Liability	GCC doesn't name the software provider or platform as a party; liability rests with supplier and purchaser.	When contract execution is mediated by a digital platform, clarify in SCC or system terms whether the platform is agent, facilitator, or neutral, and what liability it bears (integrity, availability).
Interfacing with Procurement Lifecycle	GCC assumes independent contract documents, delivery notices, design, etc. But in a digital procurement platform, contract, delivery, inspections, payment, etc. are phases.	The system must integrate GCC contract lifecycle with procurement workflow (e.g. bid evaluation → contract award → contract module → delivery acceptance → invoice → payment).
Version Control and Amendments	GCC allows amendments (variation orders, contract amendments), but no built-in version control for multiple amendments.	Digital systems must preserve version histories of contracts and amendments, allow rollback or audit, and ensure that each party has visibility on changes.
Force Majeure / Exception Handling	Clause for "force majeure" exists, but no standardised digital protocol for declaring or processing force majeure events.	The platform needs a force majeure event module: notification, automatic suspension of penalties, extension of times, and audit trail of event justification.
Performance Guarantees & Securities	GCC includes performance securities, warranties, guarantees – often in paper form.	Digital procurement systems should support digital escrow / bond mechanisms, or track performance guarantee issuance, expiry, claims, and release electronically.
Terminations, Disputes & Appeals	GCC provides for termination, dispute resolution (arbitration/boards) etc. But no digital docketing, case tracking, evidence linking.	Add a dispute management module that tracks notices, hearings, evidence, timelines, and links to contracts, audit logs.

4.3.2 Findings

The GCC provides a stable, legally enforceable baseline for government procurement contracts, covering delivery, payment, risk, termination, variation, inspections, warranties, etc. However, the GCC was designed for a predominantly manual, paper-based procurement world and lacks built-in mechanisms for digital contract execution, auditability, versioning, or integration with an e-procurement engine. To deploy GCC effectively in a national digital procurement system, the platform must wrap GCC in a digital contract engine: interpret clauses, enforce event triggers, version control, electronic signature support, layered SCC overrides, immutable logs, and dispute-management modules. In effect, GCC becomes the "legal vocabulary," and the digital system is its executable runtime. Meeting that approach requires adding system architecture, metadata models, identity and access control, classification, and liability binding clauses.

4.4 National Data and Cloud Policy

The National Data and Cloud Policy was published on 31 May 2024 in the *Government Gazette* in line with the Electronic Communications Act 2005 (ECA). The Policy states its aims as follows:

> "The National Data and Cloud Policy is a framework aimed at efficiently managing and utilizing data through cloud computing technologies. Its primary goals are to enhance government service delivery and foster socio-economic development by promoting data-driven decision making and creating data-based tradable goods and services, thereby supporting an emerging digital economy."

4.4.1 Gap Analysis

The policy review (see ***Addendum A at* 9.1.3**) identified the following gaps.

Policy Area	Gap Identified	Implication
Procurement Alignment	No explicit link to NT procurement reforms (e.g. PPA, GCC).	Lack of integration may prevent legal enforcement of cloud-first, open competition objectives, and may delay implementation given uncertainty about future procurement and hence contractual arrangements.
SITA Mandate and Capacity	SITA is given a central, determinative role while its current capacity constraints are noted but no clear intervention formulated to capacitate it.	Creates significant execution risk; departments may be bottlenecked by SITA or may bypass it, in which case the absence of dedicated procedures to procure solutions will emerge as a new gap.
Procurement Methods for Cloud Services	Absence of guidance on fit-for-purpose procurement (e.g. framework arrangements, modular contracting, dynamic purchasing).	Restricts agility in selecting and updating CSPs or onboarding niche providers.
Data Classification and Interoperability	While the policy proposes data classification, it lacks specificity and binding operational standards.	Impedes appropriate procurement and contractual provisions dealing with data. Risks inconsistent implementation across departments.
Competition and Vendor Lock-In	Acknowledges risk of CSP dominance but lacks procurement safeguards like data portability mandates.	Public buyers may be locked into proprietary platforms, raising cost and switching barriers.
Regulatory Coherence	Overlap between DPSA, DCDT, SITA, sectoral regulators without defined coordination protocol.	Risk of duplicated efforts and regulatory conflict.
Enforcement and Accountability	No enforcement provisions or KPIs to monitor departmental compliance with cloud-first directives.	Departments may ignore policy without consequence.
International Benchmarking	References AU/UN protocols but lacks comparative examples from countries with successful cloud procurement.	Missed opportunity to localise proven practices (e.g., Kenya's ICT Authority, UK's G-Cloud).
Funding & Resource Mobilisation	Calls for large-scale broadband and cloud infrastructure but lacks funding strategy or fiscal envelope.	Creates implementation paralysis or misaligned expectations.
Legal Effect	Policy lacks legal binding authority without associated regulations or legislative amendments.	Risk of inconsistent implementation or disregard by departments.

4.4.2 Findings

The vision put forward in the Policy is forward-looking and values-aligned with international trends (cloud-first, digital trust, open data). Procurement remains a major blind spot. Institutional execution risks are high, especially due to SITA's central role and current constraints and vagueness around the creation and implementation of a data classification framework. Legislative follow-through and alignment are needed: regulations, directives, or amendments to support implementation. Best practice benchmarking is partial; stronger comparative alignment with model jurisdictions could improve credibility and adaptability.

Despite the Policy's ambitious goals, cloud-first adoption, data-sharing, digital trust, it does not provide or mandate any concrete changes to public procurement systems that would enable those goals to be implemented through contracting mechanisms. The Policy also does not provide any clarity or direction on the alignment of key implementation tools, such as a data classification framework and interoperability framework, with public procurement systems, which raises material concerns regarding feasibility of implementation.

4.5 Government Digital Strategy

4.5.1 Draft Digital Government Policy Framework

The DPSA published a draft Digital Government Policy Framework (DGPF) in terms of the Public Service Act, 1994 in the *Government Gazette* on 20 September 2024. The aims of the DGPF are as follows:

> "The purpose of the DGPF is to provide guiding principles to identify and develop policies required to transform the public service using digital technologies. The DGPF will lead to a comprehensive and coherent approach to leverage digital technologies to deliver public services, improve the efficiency and effectiveness of government operations, and foster a citizen-centric approach to governance. The DGPF also establishes a digital-first mindset across all government departments and government agencies, promotes collaboration and coordination among government entities, and ensure (sic) digital initiatives align with the government's overall strategic objectives."

4.5.1.1 Gap Analysis

The policy review (see ***Addendum A at 9.1.4***) identified the following gaps.

Policy Area	Gap Identified	Implication
Procurement Alignment	DGPF mentions procurement reform but does not align with the PPA or define cloud procurement procedures.	Departments lack legal and procedural clarity for digital and cloud acquisitions; potential compliance conflicts with PFMA/MFMA/PPPFA; with increased procurement risk.
SITA Mandate and Capacity	SITA remains the default ICT procurement gatekeeper for departments, but DGPF proposes a new "digital transformation component."	Mandate confusion risks duplication or paralysis; no clarity on how digital procurement oversight transitions from SITA to a new entity; no clarity on alignment between new entity and PPO regarding procurement.

Procurement Methods for Cloud Services	The DGPF encourages modernised procurement but lacks operational guidance (framework agreements, consumption-based billing).	Public entities cannot effectively or lawfully procure scalable cloud services; delays in adopting cloud-first practices.
Data Classification and Interoperability	Advocates a "Whole-of-Government Data Framework" but no classification schema or interoperability standard yet exists.	Inconsistent data handling, interoperability failures, and POPIA non-compliance risks across departments.
Competition and Vendor Lock-In	PPPs are encouraged but not balanced with open competition safeguards.	Cloud and software monopolies may emerge, limiting local participation and innovation.
Regulatory Coherence	Overlaps among DPSA, DCDT, DSU and SITA with no legislative harmonisation plan. Relationship with subsequent policy documents unclear.	Confused accountability for digital transformation; fragmented implementation.
Enforcement and Accountability	No enforcement body or monitoring metrics defined; success relies on voluntary compliance.	Weak accountability undermines results; departments may deprioritise digital transformation.
International Benchmarking	Cites OECD and World Bank frameworks but lacks measurable targets (e.g., digital maturity index).	Difficult to benchmark progress or evaluate impact internationally.
Funding & Resource Mobilisation	ICT budgets remain departmental; no mechanism for pooled funding or shared infrastructure financing.	Fragmented spending limits scalability, increases duplication, and wastes resources; limits resources available to build central capacity and implementation.
Legal Effect	Policy guidance only; not legally binding until incorporated into future procurement regulation.	Cannot compel compliance or procurement change; remains advisory; existing procurement regulatory frameworks override these guidelines creating reduced incentives to pursue innovative procurement in support of this policy.

4.5.1.2 Findings

The draft DGPF represents an important step towards consolidating South Africa's fragmented digital governance landscape, aligning with international best practice frameworks from the OECD and World Bank. However, the analysis reveals fundamental limitations that undermine its transformative potential. As an advisory framework lacking legislative force, the DGPF cannot compel compliance or override existing procurement regulations, rendering it largely aspirational. Critical implementation gaps persist across procurement alignment, institutional coordination, and enforcement mechanisms. The framework fails to

- reconcile overlapping mandates between DPSA, SITA, and DCDT,
- provide operational guidance for cloud service procurement under the PPA, or
- establish a national data classification schema required for interoperability and POPIA compliance.

Whilst the DGPF articulates sound principles around digital-first governance, citizen centricity, and whole-of-government data management, these remain unenforceable without supporting legislation. The absence of defined funding mechanisms, performance metrics, and accountability structures—combined with fragmented ICT budgets and unclear pathways for private sector participation—suggests that without substantial legislative reform and institutional restructuring, the policy risks becoming another

unimplemented framework in South Africa's digital transformation journey. The realisation of the vision formulated in the DGPF thus greatly depends on associated policy and regulatory reforms.

The draft nature of the DGPF and its relationship with the more recent Roadmap for the Digital Transformation of Government (see 4.5.3 below) raise serious questions about its currency as an expression of government intent.

4.5.2 South Africa's Communications & Digital Technology Infrastructure Roadmap

On 28 October 2024, the Minister of Communications and Digital Technologies launched the government's plan, under the heading South Africa's Communications & Digital Technology Infrastructure Roadmap (the C&DTI Roadmap), setting out the current administration's high-level strategy for the digital transformation of South Africa's economy and society.

The C&DTI Roadmap centres on communications and digital technology infrastructure, which is the backbone and enabler of connectivity, broadband, digital networks and infrastructure. The focus is thus on the foundational infrastructure required to support digital transformation. In contrast, the Roadmap for the Digital Transformation of Government of May 2025 (see 4.5.3 below) is a broader, whole-of-government roadmap for how to deliver digital public services by leveraging digital public infrastructure. The Roadmap for the Digital Transformation of Government explicitly links to the infrastructure objective, e.g. it defines DPI as a key enabler, and emphasises data-exchange, trusted channels, etc. The infrastructure layer as envisaged under the C&DTI Roadmap must facilitate and support the DPI (in terms of networks, data centre capacity, interoperability standards).

4.5.2.1 Gap Analysis

The policy review (see ***Addendum A at 9.1.5***) identified the following gaps.

Policy Area	Gap Identified	Implication
Procurement Alignment	C&DTI Roadmap does not provide cloud/XaaS-specific procurement pathways; must rely on generic PFMA/MFMA + Treasury Regulations and ICT procurement notes.	Risk of delays/contestation; projects need explicit procurement mappings and (where applicable) SITA/other deviation justifications.
SITA Mandate & Capacity	C&DTI Roadmap depends on ICT backbone actors, incl. SITA; governance and delivery weaknesses can slow DPI/cloud tracks.	Programme risk unless capacity is augmented and accountability clarified in delivery plans.
Procurement Methods for Cloud Services	No standardised terms for consumption billing, portability, or multi-tenant cloud in C&DTI Roadmap text.	Contract ambiguity and lock-in risk unless departments impose cloud-specific T&Cs and evaluation criteria.
Data Classification & Interoperability	High-level intent; lacks detailed, government-wide data-classifications and DPI interoperability profiles.	Integration/security gaps; POPIA compliance risk; inconsistent implementations across departments.
Competition & Vendor Lock-In	Infrastructure ambitions are compatible with open models but need enforceable openness requirements.	Without explicit portability/interoperability clauses, vendor lock-in and switching costs rise.
Regulatory Coherence	State Digital Infrastructure Company (SDIC) delays and shifting roles across DCDT/SITA/NT create moving parts. Fuzzy	Delivery friction unless a single compliance and governance map is adopted per project.

	relationship with Roadmap for the Digital Transformation of Government.	
Enforcement & Accountability	C&DTI Roadmap is directional; it needs measurable KPIs, milestones, and audit trails.	Weak accountability could erode trust and funding continuity. Reinforced by DCDT APP/AR emphasis on oversight.
International Benchmarking	Global DPI/cloud playbooks exist but are not yet embedded as binding norms.	Missed efficiency/security gains; harder comparability for investors and partners.
Funding & Resource Mobilisation	Multi-year capital + Opex (cloud) mix not laid out within the C&DTI Roadmap text.	Budget rigidity or underfunding of Opex-heavy DPI/cloud operations.
Legal Effect	Roadmap is a policy/speech-level instrument; not prescriptive law or formal policy document.	Needs translation into directives, standards, and SCM templates to have binding effect in procurements.

4.5.2.2 Findings

The C&DTI Roadmap sets a clear political and strategic signal for scalable, interoperable digital infrastructure, but its deliverability relies on downstream instruments: NT-compliant procurement routes, cloud-specific contracting standards (portability, security, performance), and clarified roles among DCDT, SITA and a still-delayed SDIC. Departmental projects that anchor to the C&DTI Roadmap should therefore package: (i) a compliance map to PFMA/MFMA & PPPFA (and in future, PPA), (ii) cloud/DPI technical baselines (interoperability, data classification, POPIA controls), and (iii) assurance-ready contracts with measurable KPIs and auditability. International guidance favours open, interoperable DPI. Embedding those requirements into tenders and SLAs will bring the C&DTI Roadmap in line with global best practice while reducing lock-in risk and improving investor confidence.

4.5.3 South Africa's Roadmap for the Digital Transformation of Government

In May 2025, the South African Government launched the Roadmap for the Digital Transformation of Government (the Digital Transformation Roadmap). The Roadmap was approved by Cabinet and its implementation is spearheaded by the newly-created DSU in The Presidency. The President describes the Digital Transformation Roadmap as follows:

> "This roadmap … sets out a focused plan to modernise how we deliver services by investing in shared systems, improving coordination and removing the barriers that make it difficult for people to get what they need. The roadmap outlines better ways to verify identity, reduce fraud, share data safely, make and receive payments and access services through a single trusted platform."

The Digital Transformation Roadmap intends, among others, to unify "previously fragmented digital initiatives into a comprehensive, whole-of-government vision" and "to modernise public service delivery". The Roadmap was accompanied by a comprehensive resource document (dated April 2025) as well as a "Desktop diagnostic on the state of digital transformation of the public sector in South Africa" (dated October 2024).

4.5.3.1 Gap Analysis

The policy review (see ***Addendum A at 9.1.6***) identified the following gaps.

Policy Area	Gap Identified	Implication
Procurement Alignment	The Roadmap does not align digital transformation goals with existing procurement frameworks or procurement rules nor does it suggest future interventions for such alignment under the PPA.	Legacy procurement models could slow digital rollout and limit agile or service-based acquisitions.
SITA Mandate & Capacity	Roles between SITA, the new DSU, and other ICT bodies (e.g. GITOC) remain unclear, with capacity gaps unresolved.	Institutional overlap and weak capability may stall coordinated implementation.
Procurement Methods for Cloud Services	There's no specific guidance on cloud-friendly or agile procurement methods.	Departments may default to outdated models unsuited to scalable, subscription-based services and/or be averse to pursue innovative approaches for fear of irregular procurement.
Competition & Vendor Lock-In	No detailed measures to ensure open standards or prevent vendor dominance in digital infrastructure.	Risk of dependency on large vendors and limited participation of local innovators.
Regulatory Coherence & Accountability	Legislative integration and enforcement mechanisms are vague.	Implementation may rely on voluntary compliance, reducing oversight and impact. Uncertainty may lead to fear of non-compliance and inaction.
International Benchmarking	No reference to global best practices in digital government procurement, despite explicitly noting several case studies of successful digitalisation.	Missed opportunities to adopt proven models and accelerate reform, including under the PPA.
Funding & Resource Mobilisation	Funding mechanisms and budget alignment for digital initiatives are undefined.	Projects risk fragmentation or stalling due to unclear financial pathways.
Legal Effect	The Roadmap has policy weight but no binding legal force.	Without statutory backing, reforms may lack enforceability and consistency.

4.5.3.2 Findings

The Digital Transformation Roadmap represents a significant policy milestone towards a digitally integrated state, yet its practical effect is constrained by weak linkages to existing procurement and data governance frameworks. The most pressing gap lies in the absence of a comprehensive data classification and interoperability regime, which is essential for ensuring secure, privacy-compliant, and efficient data exchange across departments as well as appropriate procurement practices. Without clear standards on how data is categorised, stored, and shared, interoperability will remain fragmented and expose government systems to security and privacy risks as well as inappropriate contractual arrangements in the critical startup phase.

Equally, the lack of structured competition safeguards in digital procurement - particularly for cloud and infrastructure services - poses a risk of vendor lock-in and limits opportunities for local and regional suppliers to participate in the state's digital transformation agenda. Open standards, multi-vendor frameworks, and transparent contracting models should therefore be prioritised to foster a competitive digital ecosystem.

Overall, while the Roadmap articulates a forward-looking vision, it requires complementary regulatory instruments and procurement reforms to operationalise its ambitions in a manner that secures data sovereignty, promotes market diversity, and ensures long-term digital resilience within the public sector.

The South African Government's strategy regarding digital transformation has taken material shape over the past two years with the publication of the draft DGPF, the C&DTI Roadmap and most recently, the Digital Transformation Roadmap. These policy documents signal a clear commitment to significant digital transformation in the public sector. The operational dimension, specifically in relation to public procurement, remains largely underdeveloped, which poses a significant risk to the achievement of this commitment.

4.6 DPSA Determinations and Directives under the Public Service Act

The Public Service Act, 1994 authorises the Minister of Public Service and Administration to establish norms and standards relating to information management, e-Government and ICT related matters for the public service. To this end, the Minister has issued a range of relevant instruments relating to digital services. These include:

- Determination and Directive on the Usage of Cloud Computing Services in the Public Service
- Public Service Data Governance Framework
- Determination and Directive on the Implementation of Knowledge Management in the Public Service
- Determination and Directive on the Implementation of Data Governance in the Public Service
- Determination and Directive on Digital Public Services Standard

A combined analysis of these instruments from the perspective of procurement of cloud services is done below.

4.6.1 Gap analysis

The policy review (see ***Addendum A at* 9.1.7**) identified the following gaps.

Policy Area	Gap Identified	Implication
1. Procurement Alignment	All directives are silent or peripheral on procurement methodology. No guidance on agile contracting, consumption-based pricing, cloud marketplaces, modular procurement, or iterative approaches. Governance-first sequencing (establish committees → develop policies → procure technology) creates "wait states" that delay cloud adoption. Instruments mandate establishing databases/platforms but provide no procurement pathways.	Departments will default to traditional, slow RFP processes incompatible with cloud service delivery models. Governance overhead (committee approvals, policy compliance, security protocols) introduces bureaucratic friction that conflicts with agile cloud procurement. Risk of 6+ month procurement cycles for services that should be provisioned in days/weeks. Traditional line-item budgeting cannot accommodate variable, consumption-based cloud costs.
2. SITA Mandate & Capacity	Complete silence on SITA's role across all documents. No clarity on: (i) whether SITA's transversal contract mandate applies to cloud services; (ii) SITA's capacity to provide/broker cloud	Fundamental uncertainty about procurement authority—departments don't know if they must use SITA transversal contracts or can procure

	platforms; (iii) coordination protocols between SITA and departments; (iv) exemption mechanisms for departments to procure directly; (v) SITA's technical capacity for cloud vendor assessment. Cloud Circular requires DPSA approval but doesn't specify SITA's involvement. Documents create parallel governance structures (DGCs, KMCs, CDOs) with no interface to SITA.	independently. Risk of conflicting mandates: directives assign responsibilities to Heads of Department while SITA Act centralises ICT procurement. Without SITA coordination, departments may duplicate cloud contracts, miss economies of scale, or face legal challenges for bypassing SITA mandates. DPSA approval requirement may exceed ministerial authority if it usurps SITA's statutory role.
3. Procurement Methods for Cloud Services	No recognition of cloud-specific procurement characteristics: (i) subscription vs. perpetual licensing; (ii) pay-per-use vs. fixed costs; (iii) rapid provisioning vs. 6-month tenders; (iv) trial-and-iterate vs. waterfall implementation; (v) API-driven marketplaces vs. RFPs; (vi) multi-year flexibility vs. 3-5 year lock-ins. Cloud Circular requires 6-month compliance for existing solutions (section 6.3) but provides no guidance on procurement methods. TCO calculations required (9.3.8c) but no frameworks provided for comparing cloud OpEx vs. on-premises CapEx.	Procurement frameworks designed for capital asset acquisition cannot accommodate operational cloud expenditure. Departments cannot leverage cloud marketplace provisioning (e.g., AWS Marketplace, Azure Marketplace) due to lack of regulatory recognition. Long procurement cycles negate cloud's speed advantages—by the time a 6-month tender completes, the technology landscape has shifted. Risk of vendor lock-in through multi-year contracts without flexibility for emerging providers or technology shifts. Traditional TCO models undervalue cloud benefits (elasticity, reduced maintenance, rapid innovation).
Competition & Vendor Lock-In	All documents are entirely silent on: (i) SME participation and vendor diversity; (ii) measures to prevent lock-in; (iii) open standards and interoperability requirements; (iv) preferences for emerging/innovative providers; (v) evaluation criteria favouring innovation over incumbency. Governance requirements (comprehensive security protocols, mature compliance capabilities, regulatory knowledge) create de facto advantages for large, established vendors. Data residency requirements (Cloud Circular section 9.3.3: "within the Republic") may limit competition by excluding global hyperscalers' default regions. No provisions for competitive re-evaluation or contract flexibility.	Market dominated by 3-5 large vendors (Microsoft, AWS, Google, Oracle, local incumbents). SMEs and innovative providers cannot compete due to compliance barriers and bureaucratic complexity. Departments risk 5-10 year lock-ins with limited ability to switch providers or leverage multi-cloud approaches. Missed opportunities for South Africa's developmental procurement objectives (B-BBEE, local content, technology transfer). Without interoperability requirements, proprietary platforms create exit barriers. Global hyperscalers may decline participation if data residency rules are economically unviable, limiting competition to expensive local alternatives.
5. Regulatory Coherence & Accountability	Fragmented regulatory landscape with unclear hierarchy: (i) Data Governance Directive mandates CDO appointment but doesn't clarify relationship to GITO/CIO; (ii) Knowledge Management Directive creates parallel structures (KMC, CKO, KM practitioners) with no integration mechanisms; (iii) Cloud Circular references PFMA but doesn't specify Treasury approval thresholds; (iv) No clarity on overlap with SITA Act, PFMA, or Provincial autonomy. Potential contradiction: directives assign procurement authority to accounting officers while SITA Act centralises ICT procurement.	Departments face conflicting obligations without legal mechanism to resolve tensions. Example: Data Governance requires comprehensive security protocols vs. Cloud Circular emphasises user experience—departments cannot balance competing mandates. Risk of parallel governance: departments establish separate DGCs, KMCs, and cloud oversight committees, creating coordination inefficiencies and duplicated bureaucracy. Legal vulnerability: accounting officers may be sanctioned for non-compliance with directives while simultaneously violating

		SITA mandates or Treasury regulations. Departments paralysed by regulatory uncertainty, defaulting to inaction rather than risking non-compliance.
6. International Benchmarking	Strong alignment with international data governance standards (DAMA DMBOK, COBIT, CMMI, ISO 30401, ISO 9001) but weak alignment with cloud-era best practices. No reference to: (i) ISO/IEC 17788/17789 (cloud computing standards); (ii) DevOps/DataOps approaches; (iii) API-first architecture; (iv) microservices and serverless models; (v) data mesh or federated architectures; (vi) multi-cloud and hybrid cloud patterns. Cloud Circular and Digital Standard describe aspirational technology stacks without learning from proven international implementations. Data residency requirements more restrictive than comparators (EU GDPR allows adequacy mechanisms; UK permits overseas processing with safeguards).	South Africa reinvents cloud governance rather than adopting proven models from UK Government Cloud, US FedRAMP, Australia Digital Transformation Agency, or Singapore GovTech. Missed opportunity to leverage internationally recognized certifications (ISO 27001, SOC 2, FedRAMP) to streamline vendor assessment—departments must create criteria from scratch. Technology approaches reflect 2010s thinking (database-centric, committee-driven) rather than 2020s cloud-native practices (distributed, API-first, agile). Restrictive data residency may limit access to best global cloud services without evidence that localisation improves security or sovereignty. Risk of technological isolation if requirements diverge too far from international norms.
7. Funding & Resource Mobilisation	No budget allocations or funding mechanisms specified across any document. Cloud Circular requires TCO calculations but provides no budgeting guidance for variable cloud costs. Digital Standard describes extensive technology requirements with no cost estimates or affordability assessment. Directives mandate: (i) establishing Data Governance Offices and KM infrastructure with no staffing budgets; (ii) appointing CDOs/CKOs from existing staff (no new positions); (iii) specialised skills training with no training budgets; (iv) 6-month compliance for existing solutions with no remediation funding. No differentiation by department size/capacity—same requirements for small departments as large ones. No centralised funding, shared services, or pooled resources.	Traditional line-item budgeting incompatible with elastic cloud costs—departments cannot plan for variable spending that changes monthly. Unfunded mandates force departments to absorb substantial costs from existing budgets: governance infrastructure, staff training, technology upgrades, compliance audits. Aspirational requirements without affordability assessment lead to partial implementation or failure. Capacity gaps remain unfunded—specialised cloud skills do not exist in public service and cannot be developed without investment. Departments duplicate efforts without economies of scale—each procures independently rather than leveraging shared services. Smaller departments overwhelmed by requirements they cannot afford, creating two-tier implementation (well-resourced vs. under-resourced departments). Risk of non-compliance not due to resistance but due to inability to fund requirements.
8. Legal Effect	No hierarchy established between documents if they conflict. No amendment procedures, review cycles, or sunset provisions—policies remain binding even as technology evolves. DPSA approval requirement may exceed ministerial authority and create administrative overreach. Interaction with PFMA unclear—no specification of Treasury approval thresholds. Data Governance and Knowledge Management Directives have strong legal authority but create obligations without clearly defining relationships to other laws.	Risk of legal challenges: DPSA veto power over cloud solutions vulnerable to challenge as potential unlawful act (exceeding ministerial authority). Departments cannot resolve conflicting mandates (e.g., security protocols vs. user experience) without legal hierarchy. Regulatory obsolescence risk: cloud technology evolves every 6-12 months, but policies lack review mechanisms—requirements become outdated yet remain

		legally binding. Provincial governments may challenge directives as infringing on provincial competence under Schedule 4/5 of Constitution. Interaction with PFMA creates risk: departments may violate financial regulations while attempting compliance with directives (e.g., variable cloud costs exceeding virement limits). Legal uncertainty deters innovation—departments choose non-compliance or inaction over risking sanctions for unclear violations.

4.6.2 Findings

The suite of policy instruments issued by the DPSA, including the Determination and Directive on the Usage of Cloud Computing Services, the Data Governance Framework, and associated digital governance directives, establishes a comprehensive administrative framework for the adoption and governance of digital technologies within the public service. These instruments are legally authoritative and demonstrate strong alignment with recognised international standards, including DAMA-DMBOK, COBIT and ISO frameworks.

At a foundational level, the framework introduces a sophisticated model of data governance, in which data classification serves as a primary determinant of cloud deployment decisions. Government data must be categorised according to the MISS, with classification levels directly informing permissible deployment environments. These requirements extend into procurement design, necessitating that service level agreements, technical specifications, and outsourcing arrangements incorporate classification-based controls, security protocols, and jurisdictional considerations. In this respect, the DPSA instruments provide a robust governance architecture for managing data in cloud environments.

Notwithstanding these strengths, the combined effect of these instruments is to impose a governance model that is structurally misaligned with the operational characteristics of cloud computing. This misalignment constitutes the primary constraint on effective cloud procurement within the South African public sector.

Most critically, the Cloud Computing Directive adopts a governance-first approach that prioritises ex ante control, risk mitigation and institutional readiness. Departments are required to undertake extensive preparatory processes prior to procurement, including the development of business cases, total cost of ownership (TCO) analyses, risk assessments, data classification exercises, and compliance evaluations, often coupled with centralised approval requirements. While these measures are consistent with public administration principles, they are premised on a model of technology acquisition that assumes stability, predictability and pre-defined system architectures.

Cloud computing operates on fundamentally different principles. It is characterised by consumption-based pricing, rapid provisioning, elastic scaling, and iterative deployment. The requirement to fully

define, justify and stabilise cloud solutions prior to procurement introduces a structural tension between governance requirements and technological reality. In practice, this results in procurement processes that are slow, rigid and incompatible with cloud service delivery models.

This constraint is compounded by the absence of procurement-specific guidance across the broader DPSA policy framework. While the directives establish extensive governance structures, including Data Governance Committees, Knowledge Management frameworks, and digital oversight roles, they are largely silent on procurement methodology. There is no recognition of cloud-specific procurement mechanisms such as modular contracting, cloud marketplaces, subscription-based pricing models, or iterative acquisition strategies. As a result, departments default to traditional procurement approaches, including lengthy request-for-proposal processes and fixed-term contracting models that negate the inherent advantages of cloud computing.

The governance-first sequencing embedded in the directives further exacerbates this constraint. Departments are required to establish institutional structures, develop policies, and ensure compliance readiness prior to initiating procurement processes. This creates operational "wait states" that delay cloud adoption and inhibit the rapid deployment of digital services. In a technological environment characterised by continuous evolution, such delays materially undermine the effectiveness of cloud-based solutions.

In addition, the framework exhibits significant gaps in relation to market design and competition. The directives do not address vendor diversity, interoperability standards, or mechanisms to mitigate vendor lock-in. Nor do they provide guidance on enabling participation by small and medium-sized enterprises. Instead, the cumulative compliance burden, including security protocols, governance requirements, and regulatory complexity, creates structural advantages for large, established providers, potentially limiting competition and innovation within the cloud services market.

Institutional fragmentation further complicates the procurement landscape. The directives do not clearly define the roles and relationships between key entities, including SITA, NT, DCDT, and provincial or local governments. This creates uncertainty regarding procurement authority and coordination, particularly given the potential overlap between DPSA directives and the statutory mandate of SITA in relation to ICT procurement. The absence of clear coordination mechanisms risks duplication, inefficiency, and legal ambiguity.

Finally, the framework fails to address the fundamental incompatibility between traditional public sector budgeting models and the consumption-based nature of cloud services. While the Directive requires TCO assessments, it provides no guidance on how departments should manage variable operational expenditure within rigid line-item budgeting systems. This creates a practical barrier to adoption, as departments are unable to align financial planning processes with the dynamic cost structures of cloud computing.

The central finding arising from this analysis is that the primary barrier to effective cloud procurement in South Africa is not the absence of policy, but the interaction between a governance framework designed

for legacy ICT systems and a technology paradigm that requires flexibility, modularity and continuous adaptation. The DPSA directives, and in particular the Cloud Computing Directive, embody this structural misalignment.

Accordingly, any effort to reform public procurement to support digital public infrastructure must engage directly with this constraint. Without aligning governance instruments with the realities of cloud service delivery, there is a material risk that forthcoming procurement reforms, including the PPA Regulations, will be implemented within an administrative framework that continues to inhibit, rather than enable, digital transformation.

4.7 SITA Rules and Procurement Policy

The most comprehensive current set of rules governing all ICT procurement, including cloud procurement is that created in terms of the SITA Act. The Act and the regulations made under the Act provide a comprehensive regulatory framework for ICT procurement. In terms of section 7(3) of the SITA Act, all government departments must "procure all information technology goods and services through" SITA. The Act contemplates two routes to such procurement. Either the department will acquire the goods and services *from* SITA, or the department will procure it *through* SITA, if the latter indicates that it is unable to provide the service itself. All organs of state other than departments have a discretion whether to procure ICT from or through SITA or whether to procure independently of SITA.

4.7.1 GAP Analysis

The policy review (see ***Addendum A at 9.1.8***) identified the following gaps.

Policy Area	Gap Identified	Implication
Procurement Alignment	SITA regulations focus on traditional procurement; limited guidance on cloud service procurement.	May delay cloud deployment; unclear approval process for SaaS/PaaS/IaaS vendors.
SITA Mandate and Capacity	SITA has limited in-house cloud technical expertise, high vacancy rate. Leadership churn, board litigation/reinstatement, ministerial interventions; high vacancies.	Reliance on external vendors; risk of insufficient oversight and compliance monitoring.
Procurement Methods for Cloud Services	Regulations do not define frameworks for global vendors or multi-tenant services.	Potential for legal and contractual challenges with international cloud providers.
Data Classification and Interoperability	Regulations high-level; do not define detailed requirements for data location, classification, and cross-system interoperability.	Risk of non-compliance with POPIA, inefficient data integration, and security vulnerabilities. Tension with other data classification frameworks such as under DPSA policies.
Competition and Vendor Lock-In	Centralised procurement can limit competition. deviation now possible but process-bound.	Risk of over-reliance on a single vendor, reduced bargaining power, and inflated costs.
Regulatory Coherence	Policies reference general IT standards but do not integrate modern cloud compliance frameworks.	Lack of alignment with ISO/FedRAMP/SOC2; may hinder government adoption of international cloud solutions.
Enforcement and Accountability	Weak enforcement mechanisms; oversight largely procedural.	Delayed compliance audits, unclear responsibility for breaches or service failures.

International Benchmarking	No direct reference to international best practices for public sector cloud adoption.	Government may lag in efficiency, security, and innovation compared to international counterparts.
Funding & Resource Mobilisation	Budgeting and funding for cloud projects not clearly defined.	Potential underfunding or resource misalignment for large-scale cloud initiatives.
Legal Effect	SITA regulations are largely administrative; limited statutory force for modern cloud architectures.	Ambiguity around legal authority to approve or regulate hybrid/public cloud; risk of compliance gaps.

4.7.2 Findings

The SITA Act and regulations provide a strong legal foundation for centralised IT governance but do not sufficiently address modern cloud deployment requirements. Key gaps include procurement methods for cloud services, detailed data classification and security standards, international vendor engagement, and agile project execution. Alignment with other data classification policies, such as those contained in DPSA determinations and directives, is not evident. Collaborative capacity building with SITA will be critical to ensure smooth deployment and long-term sustainability.

SITA has recently been under harsh critique by the Auditor-General (AGSA) and Parliament's Standing Committee on Public Accounts (SCOPA) for their lack of ability to service their legislated mandates taking up to 123 days to turn around procurement requests and only providing 37% of government ICT services. There exists a high vacancy rate (60%) in the agency, inadequacies in their supply chain management and internal capabilities resulting in operational instability, governance challenges and reputational damage.

In June 2025, regulation 17.8 of the SITA Regulations was amended to permit government departments to procure IT services outside of SITA if SITA fails to meet stipulated price, quality or turnaround time thresholds. Departments are to issue a deviation request, and SITA has a fixed 10 working-day response window. If SITA does not meet the criteria, the department may legally proceed with external vendors such as hyperscalers. The service delivery failures viewed alongside the revised regulation materially undermine the effective centralisation of ICT procurement under SITA. In reality, there is no longer an exclusive mandate to procure ICTs for government departments in South Africa.

4.8 Data Protection, Information Governance and Cloud-specific norms

South Africa's data protection and information governance regime forms the legal environment within which cloud services may be adopted, accessed and managed by public institutions. Unlike procurement legislation, these instruments regulate the substantive treatment of information itself, including the conditions under which personal and classified data may be processed, stored, transferred and safeguarded. POPIA, MISS and related governance directives therefore operate as threshold requirements that determine whether particular datasets may lawfully be migrated to cloud environments, the security measures required for such migration and the institutional responsibilities linked to data stewardship across the state.

For the purposes of this paper, these instruments are significant because they provide the normative and regulatory constraints that cloud procurement must satisfy. Yet they are characterised by fragmentation, uneven legal force and substantial gaps in their applicability to modern digital architectures. POPIA

establishes binding conditions for personal information processing but does not supply cloud-specific security baselines. MISS remains the only government-wide classification framework but predates digital systems and provides no mechanism for mapping classification tiers to cloud controls. The DPSA Cloud Computing Determination offers policy direction but lacks binding effect, technical detail and enforceability. Taken together, these instruments shape the legal boundaries of cloud adoption but do not constitute a coherent, cloud-aligned data governance framework. Their limitations therefore reinforce the broader structural challenges that inhibit the lawful and consistent procurement of cloud services in South Africa's public sector.

4.8.1 Protection of Personal Information Act 2013

POPIA constitutes the primary legal framework governing the processing of personal information in South Africa and applies in full to public-sector cloud adoption. The Act imposes binding conditions relating to security safeguards, purpose limitation, data minimisation, cross-border transfers and accountability, and requires responsible parties to ensure that personal information is stored and processed in a manner that upholds these conditions. While POPIA establishes the foundational legal constraints for cloud migration, it does not provide cloud-specific security baselines, residency rules, encryption standards or guidance on multi-tenant environments. As a result, compliance assessments for cloud procurement remain fragmented and department-specific, with no authoritative mechanism for determining whether particular cloud architectures meet POPIA's requirements. POPIA therefore serves as a critical constraint on cloud adoption but does not supply the technical or governance standards needed to operationalise compliant cloud procurement across government.

4.8.1.1 GAP Analysis

The policy review (see ***Addendum A at 9.1.9***) identified the following gaps.

Policy Area	Gap Identified	Implication
Procurement Alignment	Lack of standard POPIA-compliant data-processing clauses in public cloud tenders.	Inconsistent application across departments increases breach risk and vendor uncertainty.
SITA Mandate & Capacity	SITA lacks privacy engineering capacity and clear alignment with the Information Regulator.	Weak oversight and enforcement of POPIA in state-managed cloud projects.
Procurement Methods for Cloud Services	POPIA's s 72 lacks clear adequacy mechanisms for multi-region cloud operations.	Restricts international vendor participation and complicates data-flow compliance.
Data Classification & Interoperability	No unified framework for classifying "personal," "sensitive," and "sovereign" data across departments.	Misclassification risks unlawful transfer or over-restriction of harmless datasets.
Competition & Vendor Lock-In	Data-portability rights are not fully operationalised.	Potential entrenchment of dominant vendors; limits citizen control over data.
Regulatory Coherence	Overlaps between POPIA, National Data and Cloud Policy, and the Cybercrimes Act 2020.	Ambiguity over breach reporting and investigatory authority.
Enforcement & Accountability	Information Regulator under-resourced; limited fines and slow enforcement.	Diminished deterrence; compliance treated as administrative formality.

International Benchmarking	Limited convergence with GDPR adequacy frameworks.	Cross-border data exchanges remain legally uncertain.
Funding & Resource Mobilisation	POPIA compliance relies on self-funding entities; no ring-fenced state budget.	Implementation gaps in small municipalities and SOEs.
Inclusion & Access	POPIA silent on exclusion caused by digital-only identity ecosystems.	Risk of discrimination against rural and elderly citizens; violates fairness principles.

4.8.1.2 Findings

POPIA provides a robust constitutional and regulatory foundation for privacy in South Africa but requires significant reinforcement to remain effective within a cloud-based digital ID ecosystem. While its alignment with global norms facilitates international cloud participation (e.g., AWS Africa Region), institutional fragmentation, limited enforcement capacity, and absence of clear cross-border adequacy mechanisms create uncertainty. For a national Digital ID to maintain public trust and inclusivity, POPIA's principles, lawfulness, minimality, purpose limitation, and human oversight, must be translated into concrete technical and contractual safeguards. Hybrid access, paper-based alternatives, and human-in-the-loop review mechanisms are essential to balance efficiency with the constitutional right to privacy and equality.

4.8.2 Minimum Information Security Standard (MISS)

MISS is the Cabinet-approved national security directive that establishes the classification system governing the protection of state information. Although binding on all organs of state, MISS predates modern digital systems and provides no framework for applying its classification categories to cloud environments. It lacks guidance on encryption, logical segmentation, key management, access federation and cloud-specific security controls. Because MISS remains the only government-wide classification instrument, its analogue formulation leaves departments without an authoritative basis for determining whether classified information may be stored or processed in cloud environments. MISS therefore represents a foundational governance gap: it defines the obligation to protect classified information but offers no mechanism for aligning those obligations with contemporary cloud architectures, leading to inconsistent departmental interpretations and heightened security and compliance risk.

4.8.2.1 GAP Analysis

The policy review (see ***Addendum A at 9.1.10***) identified the following gaps.

Policy Area	Gap Identified	Implication
System Architecture & Timelines	MISS does not address digital or cloud architectures and sets no timelines for modernisation.	Departments migrate - or avoid migrating - without authoritative guidance, producing fragmented implementation.
Standards & Interoperability	No cloud-aligned standards for encryption, identity, APIs or secure data exchange.	The government cannot ensure consistent or interoperable cloud deployments.
Data Classification & Publication	No mapping between classification levels and cloud controls or residency rules.	Departments cannot determine which datasets may lawfully move to cloud environments.

Identity, Access, Audit	MISS lacks standards for digital identity, access federation or cloud-native audit logging.	Access-control practices are inconsistent and weaken POPIA and security compliance.
Municipal Adoption	No guidance for municipalities on applying classification obligations in digital systems.	Municipal cloud adoption is inconsistent and often under-secured.
Method Support in the System	MISS does not provide procurement-aligned criteria for evaluating cloud security.	Bid specifications and evaluations lack a legal or technical foundation.
Readiness & Legacy Migration	No migration protocols for moving classified data into cloud environments.	Departments improvise high-risk or overly restrictive migration strategies.
Hosting & Sovereignty	MISS assumes physical control and does not define cloud sovereignty safeguards.	Departments cannot assess sovereignty compliance in hosted or multi-tenant environments.
Transparency vs Confidentiality	MISS emphasises secrecy but provides no guidance on balancing transparency obligations in cloud contexts.	Record-keeping and accountability practices vary unpredictably.
Funding & Capacity	MISS imposes obligations without resourcing or capacity-building mechanisms.	Departments lack expertise to operationalise classification duties in cloud systems.

4.8.2.2 Findings

MISS remains the state's only formal classification framework, but its analogue-era design makes it incompatible with digital and cloud environments. It offers no cloud-specific security controls, no mapping between classification levels and cloud architectures, and no guidance on residency, encryption or access management. As a result, departments cannot reliably determine whether classified data may be migrated to cloud services, leading to inconsistent interpretation and generally risk-averse avoidance of cloud adoption. The absence of an institution mandated to modernise MISS further reinforces fragmented governance. MISS therefore constitutes a foundational gap in South Africa's cloud-governance ecosystem: it imposes security obligations but provides no mechanism to fulfil them in modern digital systems.

4.9 Sector-specific ICT and procurement governance instruments

In this sub-section a sample of implementation instruments that are currently employed across the South African public sector, relevant to the procurement of cloud solutions, are analysed. This analysis provides some insight into policy and regulatory instruments at a lower level than those analysed above and closer to the implementation level.

The first instrument analysed below is a rare example of a dedicated cloud standard adopted by a South African organ of state, namely Eskom. This instrument is thus within the overall category of cloud policies. The second set of instruments analysed falls within the public procurement policy category. Here a sample of different SCM Policies of various public entities (at all three levels of government) are compared.

4.9.1 Eskom Cloud Standard Policy

4.9.1.1 Gap Analysis:

The policy review (see ***Addendum A at 9.1.11***) identified the following gaps.

Policy Area	Gap Identified	Implication
Procurement Alignment	No direct link to PFMA or PPA; vendor selection processes undefined.	Potential non-compliance with Treasury oversight; risk of opaque contracting.
Data Localisation Flexibility	Mandates full data localisation.	Limits interoperability with international clouds; raises cost and resilience risks.
Incident Response Framework	No detailed cyber-incident escalation or coordination plan.	Slower response to breaches; unclear accountability.
Performance Monitoring & Audit	No SLA enforcement metrics or integration with Eskom's audit trail system.	Weak service-delivery oversight; vendor lock-in risk.
Cloud Broker Governance	Broker role defined conceptually but lacks procurement, licensing, or accountability framework.	Unclear liability and conflict-of-interest controls.
Inter-agency Integration	No coordination mechanism with SITA/DCDT for national cloud strategy alignment.	Duplication of effort; fragmented public-sector cloud ecosystem.
Digital Skills & Capacity	Requires advanced in-house expertise not currently widespread.	Delayed rollout and increased dependency on third-party consultants.
Compliance Automation	Manual audit and risk-assessment processes.	Inconsistent regulatory compliance and high administrative overhead.

4.9.1.2 Findings:

Eskom's Cloud Standard (240-150139783) demonstrates a mature internal framework built on NIST and GWEA principles, ensuring security, sovereignty, and structured adoption. However, it remains internally focused and lacks integration with national procurement and digital-transformation frameworks. To align with the PPA and broader cloud-governance reforms, Eskom should introduce digital procurement mechanisms, centralised audit integration, and interoperability standards shared with SITA and NT. Strengthening SLA enforcement, incident management, and transparent vendor evaluation would transform the policy from a technical reference model into a national benchmark for sovereign cloud governance.

4.9.2 SCM Policies Sample

Comparative and normative analysis of samples of existing and model SCM policies in South Africa from the perspective of cloud procurement.

4.9.2.1 Review

Dimension	What good SCM policy should cover (in cloud era)	Traditional / low cloud attention example: municipal SCM	Emerging / cloud-aware SCM policy example	Assessment / observations
Legal & Statutory Fit	Should comply with MFMA, PPPFA, NT SCM regulations, and also align with cloud-specific regulation (data sovereignty, offshoring, cross-border, security)	Example: Sample Municipality SCM Policy 2025/26 — includes a clause on "Procurement of IT related goods or services" but treats them similarly to physical goods	A policy that references national Data & Cloud Policy and integrates cloud procurement parameters (e.g. specifying cloud hosting, data location, SLAs) — less common in municipal SCM policies but appearing in draft SCM policies in some departments.	Many existing SCM policies do not differentiate cloud services with special treatment; this gap leads to risk of misalignment with the newer National Data & Cloud Policy.
Process & Procedures	Needs to define cloud-specific procurement pathways: how to do RFPs for cloud, usage billing, trial/proof of concept, exit/portability, scalability.	The sample municipal SCM policy defines acquisition management, competitive bidding, deviations, committees etc. but does not elaborate on consumption billing or cloud exit	In more modern departments, SCM proposals are starting to include "procurement of digital and cloud services" as a separate category with specific evaluation criteria	Traditional SCM frameworks are rigid, focusing on capital procurement and fixed assets; cloud introduces Opex, scaling, elasticity, which many policies are not yet structured for.
Risk, Security & Compliance	Policy should require compliance with POPIA, cybersecurity, encryption, audits, data classification, service continuity, exit rights	Traditional SCM policies often include general contract terms, but do not explicitly demand or assess cloud risk dimensions (e.g. cross-border data flow, encryption, vendor audit rights)	Emerging SCM proposals may embed clauses referencing compliance standards (e.g. ISO 27001, technical security controls).	Without explicit risk clauses, cloud contracts may slip through problematic terms; SCM must raise the bar on contractual risk management
Vendor & Market Access / Competition	Should encourage open competition, prevent vendor lock-in, require interoperability and portability, mandate transparency in pricing.	Municipal SCM tends to focus on lowest bidder or preferential procurement; cloud competition considerations (e.g. egress costs, switching penalties) rarely accounted for	A cloud-aware policy could require vendors to disclose exit costs and interoperability standards as part of evaluation scoring	The lack of vendor lock-in safeguards is a material risk when contracting cloud services under traditional SCM regimes.
Deviation & Exceptions	Must allow special deviations or agile procurement routes for cloud where conventional cycles are too slow, with clear approval thresholds	Traditional policies provide for deviations / ratification of minor breaches but not necessarily for emergent ICT needs. E.g. Sample municipal SCM policy includes "Deviation	More mature SCM policies may have a "cloud exception" route, with an expedited approval path and accountability	Given slow SCM cycles, a cloud-exception or deviation route is essential to avoid stalling projects.

		from and ratification of minor breaches" clause		
Contract Management & Performance	Post-award monitoring must include cloud-specific metrics (uptime, latency, data integrity, SLAs, usage, billing review, audits).	Traditional SCM focuses on supplier performance (delivery, quality, timeliness), contract registers, supplier evaluation. E.g. municipal policies include contract performance monitoring	Cloud-aware SCM policies will include technical performance indicators and periodic audits of cloud service compliance.	Incorporating technical SLAs and audit rights is critical; otherwise oversight remains superficial.
Funding / Budgeting Model	Must enable Opex / consumption funding (not just CapEx), include budgeting for scaling, variable usage, FinOps awareness.	Most SCM policies focus on predetermined budgets and fixed cost procurement. Cloud's variable cost model is poorly accommodated.	Some department IT procurement frameworks are beginning to include scalable budget envelopes or contingency for usage growth.	Without budgeting flexibility, cloud usage may be constrained or cause overruns.
Policy Governance / Oversight	SCM oversight should include cloud units in audit, periodic review, stakeholder representation (IT, cybersecurity)	SCM oversight is generally financial and procurement committees; IT/tech is a stakeholder but often secondary.	In updated SCM or ICT procurement policies, oversight committees include IT/security representation.	To manage cloud risk and alignment, committees must include technology and security expertise.

4.9.2.2 Illustrative Example Comparison

Aspect	Sample Municipal SCM	Cloud-aware Department (hypothetical + actual emerging practices)
"Procurement of IT goods / services" clause	Exists but treated as generic procurement (no differentiation)	Has a separate section for cloud & digital services, with special criteria (security, portability, scalability)
Deviation pathways	Has general deviation / ratification clauses for minor breaches (small value or urgent)	Includes "expedited cloud procurement deviation" with defined thresholds & responsibilities
Contract performance	Supplier performance reviews (on delivery, quality) and regular contract register updates	Also monitors technical performance (uptime, response time, data integrity, security audits)
Risk & compliance	Typical legal/contract terms, but little on cloud-specific security, cross-border data, encryption	Explicit clauses for POPIA, encryption at rest/in transit, audit rights, data residency, exit/egress terms
Budgeting / funding	Fixed budgets per financial year, procurement plans embedded in budgets	Includes flexible reserve or scalable funding model to allow variable usage growth

4.9.2.3 Findings

South Africa's current Supply Chain Management (SCM) policies across municipalities, departments, and public entities remain largely grounded in a traditional procurement mindset that prioritises tangible goods and fixed-cost services. While this framework supports compliance and accountability, it is poorly suited to the dynamic, usage-based nature of cloud computing. There is an urgent need to reframe SCM

policies to explicitly recognise cloud and digital services as a distinct procurement category governed by tailored evaluation criteria—such as data security, resilience, interoperability, and exit strategies. The inclusion of an expedited deviation mechanism, modelled on SITA Regulation 17.8, would allow agile procurement of cloud services without undermining transparency or competition.

Future SCM reforms should also embed technical and contractual safeguards, including enforceable SLAs, vendor audit rights, and disclosure of egress or switching costs, to mitigate risks of vendor lock-in and ensure continuous performance oversight. Budgeting frameworks must evolve to accommodate the operational expenditure (Opex) model of cloud services and integrate FinOps practices that monitor consumption and cost optimisation. Oversight mechanisms need to become more multidisciplinary—bringing together procurement, IT, and cybersecurity expertise—to ensure alignment between financial compliance and technological risk management. Lastly, all SCM frameworks should be harmonised with the National Data and Cloud Policy (2024) to ensure consistency with national goals on data sovereignty, open standards, and secure digital transformation. Collectively, these adjustments would modernise SCM's legal and operational capacity to support cloud-based procurement in a transparent, secure, and innovation-friendly manner.

4.10 Conclusion

South Africa's digital public procurement ecosystem is undergoing rapid conceptual reform but remains legally fragmented and procedurally immature. Across the reviewed frameworks, the National Data and Cloud Policy (2024), DGPF (2024), Digital Transformation Roadmap (2025), PPA (2024), Eskom Cloud Standard, SITA regulations, and SCM policies, there is a shared ambition to digitise government systems, expand cloud adoption, and promote interoperability. Yet, the legal and institutional instruments that should operationalise this vision remain in a transitional phase, leaving government departments and public entities without consistent guidance on how to lawfully and competitively procure digital services.

Closest to the fire in regulating South Afrifa's digital transformation is the DSU in the Presidency who are supported, somewhat ambiguously it seems, by the DCDT and NT. The Digital Transformation Roadmap is explicitly "spearheaded by the newly created Digital Service Unit in the Presidency". However institutional overlaps persist between the DSU, SITA, DCDT, DPSA and NT, particularly regarding ICT procurement, data classification, and infrastructure regulation. The DCDT remains the policy custodian for digital communications and infrastructure (as seen in the Communications & Digital Technology Infrastructure Roadmap 2024) while the NT governs public procurement and fiscal oversight (through the PFMA/MFMA/PPA) and DPSA seems to primarily responsible for data classification, at least as used in the public service.

4.10.1 Legal Clarity and Procurement Pathways

The PPA introduces, for the first time, a statutory basis for e-procurement through a centralised digital platform under the PPO. The Act mandates interoperable open data, digital tendering, and a future e-marketplace, but defers the technical and procedural details, such as APIs, data standards, and identity

controls, to forthcoming regulations. This means that while the "what" of digital procurement is clear (a unified ICT-based system), the "how" remains undefined.

Other policy instruments, like the DGPF and National Data and Cloud Policy, are non-binding and primarily aspirational. They lack the legislative teeth to compel departments to adopt cloud-first procurement or to harmonise their processes with the new PPA system. The SITA Act and its practice notes remain the main operational mechanism for ICT procurement, yet SITA's administrative inefficiencies and recent legislative reform (SITA Regulation 17.8) now permit departments to (readily) deviate from SITA if turnaround times or cost benchmarks are not met. This regulatory shift represents the most material opening for direct digital procurement by departments, allowing competitive sourcing from the broader market, including hyperscalers, provided that value-for-money and compliance tests are satisfied.

While entities like Eskom have adopted internal cloud standards consistent with NIST and the Government-Wide Enterprise Architecture (GWEA), these standards operate in isolation from national procurement law. They illustrate a maturity in technical governance but highlight the absence of a unified legal bridge between operational cloud governance and Treasury-regulated procurement obligations.

4.10.2 Market Access and Competition

Across all frameworks, market access principles are acknowledged but inconsistently applied. The Data and Cloud Policy recognises risks of market concentration but lacks procurement tools, such as modular contracting, data portability requirements, or innovation sandboxes, to mitigate vendor lock-in. The DGPF calls for private-sector partnerships but provides no mechanism to guarantee competitive neutrality or SME participation. Similarly, SCM policies at departmental and municipal levels treat digital services like physical goods, overlooking consumption-based pricing, scalability, and portability criteria that are central to fair competition among cloud providers.

The introduction of deviation rights under SITA Regulation 17.8 partially addresses this issue by enabling direct competition among service providers when SITA underperforms. This reform, together with the PPA's future e-marketplace, could level the playing field between traditional integrators and hyperscalers, provided implementation ensures transparent evaluation criteria and uniform digital procurement templates. Without such harmonisation, departments risk inconsistent interpretations of cloud procurement obligations and further fragmentation in vendor access.

4.10.3 Digital Sovereignty and Privacy

Data sovereignty remains the dominant policy lens across all reviewed documents. The National Data and Cloud Policy and Eskom Cloud Standard mandate that sensitive government data be hosted within South Africa, subject to POPIA and national cybersecurity directives. While these measures protect state information and align with global data-protection norms, they can inadvertently restrict cross-border innovation and multi-region resilience.

POPIA provides the constitutional anchor for privacy and sets binding rules on lawful processing, cross-border transfer, and security safeguards. However, enforcement capacity within the Information Regulator and alignment between POPIA, the Cloud Policy, and SITA oversight remain weak. The absence

of a unified data-classification framework across government creates uncertainty over which datasets may be hosted offshore or shared across agencies.

Sovereign-cloud principles are therefore asserted but not yet operationalised: no instrument defines compliance benchmarks, key-management standards, or encryption requirements for cloud-based procurement. A harmonised approach, combining POPIA-aligned controls with cloud-neutral technical standards, would allow hyperscalers to compete on equal footing while maintaining lawful data residency and auditability.

4.10.4 Data Classification and Interoperability

Subsequent engagements with industry experts indicate that interoperability between hyperscalers no longer presents a significant technical constraint, as migration tools and common API standards have made data and workload transfer relatively seamless. The greater challenge lies in data classification and governance, where the absence of a uniform, enforceable schema across departments continues to create compliance uncertainty under POPIA and inconsistent access protocols for shared systems. As digital transformation accelerates, future regulatory focus should shift from solving interoperability to standardising data classification and access controls, ensuring secure, lawful, and efficient data sharing across all levels of government.

While several institutions currently play fragmented roles in South Africa's data governance landscape, the Information Regulator, established under POPIA, is best positioned to serve as the central authority on public-sector data classification. As an independent body reporting to Parliament and already empowered to regulate the processing and transfer of personal information, the Regulator has both the legitimacy and mandate to enforce privacy rights and ensure compliance across public institutions. Its current remit, however, focuses narrowly on personal data, and does not extend to the broader classification of public sector information, such as internal-use, open data, restricted administrative data, and confidential interdepartmental records. In this context, its legislative mandate should be expanded to include the development and enforcement of a unified, tiered classification framework that can guide all organs of state in determining data sensitivity, accessibility, and processing standards.

The fragmented, unaligned institutional landscape consists of at least the following key roles in data classification:

DPSA: Issues directives to departments under the Public Service Act, including the Cloud Directive that mandates data classification via MISS. However, it lacks direct authority over data law or enforcement. Supports Information Regulator with implementation directives under the Regulator's schemas.

State Security Agency: Custodian of MISS, the classification system for state security information (e.g. Secret, Top Secret). It is historically the authority on national security-related information, but its focus is narrow.

Information Regulator: Enforces POPIA and PAIA, and oversees personal data processing, privacy, and transparency. Has regulatory powers, including enforcement, but not yet a formal mandate for comprehensive public data classification (e.g. open vs confidential vs internal). Independent and accountable to Parliament. Governs data subject rights, cross-border transfers and privacy impact

assessments, all of which overlap with classification. With slight legislative expansion, it could assume a broader public-sector data governance role, including classification schemes for open, sensitive, and restricted data, beyond just personal information.

SITA: Technical implementer of government ICT solutions. May advise or host infrastructure but not empowered to set legal standards.

The Presidency / DCDT / National Data & Cloud Policy: Through the Presidential Commission on 4IR and DCDT policies, the Presidency has championed digital reform but without specifying institutional mandates for data classification itself. The Presidency should drive the whole-of-government strategy, but delegate execution to the Information Regulator.

An efficient approach would be to capacitate the Information Regulator, in coordination with the DPSA for implementation and the SSA for state security classifications, to assume this function through regulations or ministerial directive, thereby ensuring coherence, enforceability, and whole-of-government adoption of a digital-era data governance framework. This centralised binding data classification framework would be developed by the Information Regulator, mandated by Parliament or cabinet, and implemented across departments via DPSA directives, with SSA guidance only on "Secret/Top Secret" security clearance classifications, and possibly reviewed annually through an independent Data Governance Council, possibly similar to the Gauteng Data Centre of Excellence.

4.10.5 Overall Assessment

South Africa's current framework for digital public procurement is policy-rich but execution-poor. The legal direction is clear: move toward cloud-enabled, transparent, and data-driven procurement. Yet institutional inertia, overlapping mandates, and the lack of codified procurement standards for digital services impede real progress. For hyperscalers and other technology providers, opportunity lies in the transitional space between SITA reform and full PPA implementation where departments seek compliant yet agile procurement solutions.

> **"South Africa's current framework for digital public procurement is policy-rich but execution-poor"**

The medium-term reform challenge is to translate digital-sovereignty aspirations into operational procurement law that guarantees fair competition, open standards, and privacy by design. Until then, government buyers must navigate an evolving patchwork of policies, balancing innovation with compliance in one of the most ambitious but complex public-sector digital transformations on the continent.

5 ANALYSIS OF POLICY GAPS AND PROCUREMENT BARRIERS

South Africa's emerging digital government agenda is characterised by ambitious policy commitments that encourage departments to pursue cloud-first strategies, enable data-driven service delivery and modernise legacy systems. However, these policy intentions are confronted by a procurement framework and institutional architecture that were designed for an earlier era of ICT acquisition. The misalignment between the nature of cloud services and the rules, processes and institutional mandates governing procurement creates structural barriers that hinder the realisation of digital transformation objectives. This section examines these barriers in detail by analysing the disconnect between policy and procurement, the constraints on competition and innovation inherent in the current regulatory design, and the institutional architecture that shapes ICT procurement across government.

5.1 Misalignment between policy objectives and procurement rules

While the National Data and Cloud Policy is highly ambitious in terms of cloud-first adoption, data-sharing, and digital trust, it fails to provide policy guidance on implementation through contracting mechanisms. This is problematic because:

- *Cloud adoption depends on procurement.*
  "Cloud-first" cannot be achieved without:
  - Market-responsive procurement methods
  - CSP onboarding frameworks
  - Flexible, fast procurement processes
  - Budget clarity and legal certainty for departments
- *Treasury rules, GCCs, and SITA procurement regulations still apply*
  The National Data and Cloud Policy assumes that standard procurement rules can facilitate appropriate public cloud services procurement.
- *Departments are left in a legal void*
  The National Data and Cloud Policy states: "Government departments and entities shall prioritise cloud services as the primary option for new ICT procurement." However, there is no accompanying guidance on *how* to do this within the existing procurement rules.

A practical problem

Imagine a department wants to procure an AI-enabled public service chatbot hosted in a secure cloud (SaaS + PaaS model). Under current rules:

SITA may not have pre-approved CSPs.

Budgeting is tricky because cloud is often usage-based, not fixed-cost.

The PFMA/Treasury prescripts may require competitive bidding with strict price/value evaluation upfront.

There is no flexibility for pay-as-you-go models, trial runs, or rapid iteration.

Despite the National Data and Cloud Policy telling departments to go "cloud-first," the procurement framework makes it difficult, legally risky, or even impossible to do so within compliance rules.

The National Data and Cloud Policy articulates a decisive shift towards cloud-first adoption, emphasising the use of cloud services as a primary option for new ICT procurement. Yet it offers little guidance on how departments are expected to procure these services within the constraints of existing regulatory instruments. The policy assumes that traditional procurement rules - Treasury Regulations, GCC and SITA procurement requirements - can accommodate cloud services without adaptation. This assumption is flawed. Cloud procurement relies on pricing and contractual arrangements that differ fundamentally from those associated with conventional goods or static ICT systems. Cloud services are typically consumption-based, scalable on demand and subject to frequent updates. These characteristics are incompatible with procurement rules that favour fixed specifications, fixed pricing and long, single-cycle tender processes.

Moreover, cloud providers operate commercial models built around integrated terms and conditions that are designed to reflect the technical realities of their platforms, including the shared-responsibility model. Attempting to incorporate only selected clauses into South Africa's standard-form contracts - while disregarding core CSP terms - creates legal incoherence, duplication of obligations, uncertain order-of-precedence and may exclude customer protections embedded in the CSP's own contractual framework.

Without a procurement approach capable of reconciling these differences - both in pricing logic and contractual structure - departments will continue to face uncertainty when attempting to acquire cloud services under instruments designed for materially different technologies.

Departments are thus confronted with a legal void. Although they are directed to prioritise cloud solutions, there is no corresponding modification of procurement rules that would legally permit agile contract structures, flexible payment models or multi-vendor interoperability arrangements. For example, procurement rules do not readily accommodate pay-as-you-go pricing or rapid iteration through proof-of-concept deployments. Similarly, existing frameworks discourage the ongoing competition needed to

optimise cost and performance throughout the contract lifecycle, because once a contract is awarded, competitive tension is effectively suspended for extended periods. Departmental attempts to comply simultaneously with cloud-first policy instructions and traditional procurement prescripts create procedural uncertainty, compliance risks and delays that frustrate digital transformation efforts.

5.2 Barriers to competition and innovation

South Africa's public cloud procurement framework suffers from fundamental structural deficiencies that systematically obstruct market competition and technological innovation. Whilst policy documents articulate ambitious digital transformation objectives, the absence of operationalised procurement pathways creates a regulatory vacuum wherein government entities lack clear legal authority to acquire cloud services through methods suited to their consumption-based, scalable nature.

The most significant barrier emerges from the profound mismatch between traditional supply chain management frameworks and cloud service delivery models. Existing SCM policies, designed for capital asset acquisition, cannot accommodate operational expenditure patterns, variable usage billing, or rapid provisioning cycles characteristic of cloud computing. Procurement processes requiring six-month tender cycles for services that should be provisioned within days fundamentally negate the speed and flexibility advantages that justify cloud adoption. This temporal misalignment forces departments into extended evaluation procedures ill-suited to rapidly evolving technology markets, by which time the competitive landscape has materially shifted.

Competition suffers particularly from the complete absence of vendor diversity safeguards across all reviewed instruments. No framework addresses interoperability requirements, data portability mandates, or switching cost disclosure obligations that would mitigate vendor lock-in risks. The extensive governance and compliance requirements mandated by directives from the DPSA create de facto advantages for large established vendors capable of navigating complex bureaucratic processes, whilst effectively excluding innovative smaller providers and local technology firms. This regulatory barrier directly contradicts South Africa's developmental procurement objectives around broad-based economic empowerment and technology transfer, concentrating market power amongst a handful of multinational hyperscalers and incumbent integrators.

Institutional fragmentation compounds these difficulties through overlapping and often conflicting mandates between SITA, NT, DCDT, the DSU, and the DPSA (as elaborated in the next section). The absence of coordinated procurement authority creates fundamental uncertainty about whether departments must procure through SITA's transversal contracts or may engage directly with cloud providers. Whilst recent amendments to SITA regulations permit deviation when performance thresholds are unmet, this reform paradoxically increases rather than resolves uncertainty, as departments now navigate multiple regulatory regimes without clear hierarchy or conflict-resolution mechanisms.

Perhaps most critically, the governance-first implementation sequencing mandated across policy instruments creates systematic delay through bureaucratic "wait states". Requirements that departments establish comprehensive committee structures, develop extensive policies, obtain multiple approvals, and complete detailed business cases before technology procurement can proceed directly conflict with agile,

iterative approaches essential for cloud innovation. The DPSA Cloud Circular's requirement for prior approval, comprehensive total cost of ownership analysis, and six-month compliance deadlines exemplifies this anti-innovation posture, transforming what should be rapid proof-of-concept deployments into prolonged approval marathons.

Data sovereignty requirements, whilst legitimate from a security perspective, lack the technical specificity necessary for competitive implementation. The absence of a unified data classification framework means providers cannot design compliant solutions without entity-specific interpretation of vague localisation mandates. This uncertainty increases entry costs and compliance risk, deterring innovative providers whilst advantaging incumbents with established government relationships and risk tolerance.

The PPA offers potential remediation through its mandate for digital procurement infrastructure, but substantive reform remains deferred to unwritten regulations, leaving the market in extended transition without clear compliance pathways or competitive evaluation standards.

5.3 Institutional constraints

South Africa's digital procurement transformation confronts paralysing institutional fragmentation that renders even well-intentioned policy reforms largely unenforceable. The fundamental constraint lies not in policy vision but in the absence of coherent institutional architecture to operationalise digital procurement at scale across government.

SITA occupies the centre of this institutional dysfunction. Legally mandated under section 7(3) of the SITA Act to serve as the exclusive procurement gateway for all government departmental ICT acquisitions, SITA simultaneously suffers catastrophic capacity deficits that undermine this centralised model. Parliamentary oversight bodies, particularly SCOPA, have characterised SITA as a "horror show" and "cash cow", citing procurement turnaround times exceeding 123 days against service-level expectations of mere weeks, alongside providing merely 37 per cent of required government ICT services. Staff vacancy rates approaching 60 per cent, persistent governance crises involving board removals and reinstatements, and endemic irregular expenditure have destroyed institutional credibility. The 2025 amendment to SITA Regulation 17.8, permitting departments to bypass SITA when performance thresholds are unmet, represents tacit acknowledgement of systemic institutional failure rather than genuine reform, creating parallel procurement pathways without resolving underlying capacity constraints.

This SITA crisis intersects destructively with overlapping mandates across multiple institutions lacking defined coordination protocols. The newly established DSU within the Presidency ostensibly spearheads the Digital Transformation Roadmap, yet its relationship with the DCDT, which maintains policy custody over digital infrastructure through its Communications and Digital Technology Infrastructure Roadmap, remains formally undefined. Simultaneously, the DPSA issues binding directives on cloud computing and data governance for the public service, whilst NT retains fiscal oversight and procurement regulation through the PFMA and emerging PPA framework. The future PPO, mandated to develop centralised digital procurement infrastructure, adds another institutional layer without clarifying interfaces with SITA's statutory ICT procurement monopoly or the DSU's transformation coordination role. This fragmentation

is furthermore exacerbated by unresolved institutional questions arising from the recent introduction of the proposed State Digital Infrastructure Company (SDIC) under the National Data and Cloud Policy. The SDIC's mandate to "manage digital infrastructure" remains undefined, creating uncertainty about whether sovereign data-centre and cloud-infrastructure functions will reside with SITA, the SDIC or a hybrid governance model.

These overlapping authorities generate what the reviewed documents characterise as "coordination risk" and "mandate confusion", wherein departments face conflicting obligations without legal mechanisms for resolution. A department seeking cloud services must theoretically satisfy SITA Act requirements, comply with DPSA cloud directives requiring comprehensive business cases and departmental approval, align with NT supply chain management regulations, obtain PPO endorsement once operational, and coordinate with the DSU's transformation priorities. No instrument establishes hierarchy amongst these requirements or designates a single accountable authority.

Provincial and municipal tiers compound this fragmentation. The PPA's instructions bind national departments but operate only as non-mandatory guidelines for municipalities, requiring individual council adoption. Provincial government coordination remains entirely absent from reviewed frameworks, creating three-tier implementation variance that fundamentally undermines the "single system" objective articulated in digital transformation policies.

Capacity constraints pervade all institutions involved. The Information Regulator, constitutionally mandated to enforce the POPIA, operates with insufficient resources to provide timely guidance or enforcement for cloud-specific data-processing arrangements. The DPSA mandates extensive governance structures, Data Governance Committees, Knowledge Management Committees, Chief Data Officers, without providing staffing budgets, training programmes, or technical assistance, assuming departments can establish sophisticated capabilities from existing constrained resources. This unfunded mandate approach creates implementation paralysis, particularly in smaller departments and municipalities lacking baseline digital literacy.

A further institutional constraint lies in the government's inability to reconcile standard public-sector contractual instruments, such as the GCC, NT's standard bidding documents and SITA's contractual templates, with the integrated commercial and technical terms used by cloud providers. Cloud contracts operationalise critical aspects of platform architecture, including the shared-responsibility model. Fragmented or selective incorporation of CSP terms creates duplication, conflicting obligations and uncertain order-of-precedence, exposing departments to legal and operational risk. At the same time, wholescale adoption of CSP commercial terms may undermine public-interest and sovereignty considerations that government is constitutionally bound to embed in its commercial arrangements. At present, no institution has the mandate or capacity to develop harmonised cloud-specific contracting frameworks or to manage their consistent application across organs of state.

Additionally, while cloud procurement frequently occurs through partner ecosystems, including resellers and managed-service providers, South Africa lacks clear institutional guidelines on how such indirect procurement models interact with PFMA/MFMA rules, SITA prescripts and socio-economic obligations—

such as SITA's requirement that 40 per cent of certain ICT spend flow to black-owned SMMEs. Without explicit institutional guidance, these partner-based procurement routes risk inconsistent application or non-compliance.

Finally, hybrid and multi-cloud architectures cannot be effectively or lawfully deployed without a binding national data-classification framework defining which workloads may reside in which environments. The absence of such a framework creates a systemic governance vacuum. Agencies are left to interpret sensitivity and risk without central authority, leading to inconsistent procurement decisions, misaligned security controls and avoidable compliance failures.

In sum, South Africa's institutional arrangements lack the clarity, authority and alignment required for cloud procurement. Until a centralised governance function is established—with explicit mandates for architectural oversight, contracting frameworks, data-classification rules and partner-ecosystem regulation—cloud adoption will remain fragmented and legally uncertain.

5.4 Conclusion

In combination, these institutional constraints shape a procurement environment in which departments must choose between strict adherence to outdated processes and the practical necessity of bypassing them to enable cloud adoption. The prevalence of deviation mechanisms is therefore symptomatic of a broader structural problem: the institutional design of ICT governance has not been modernised to accommodate cloud technologies. The result is a system that perpetuates inefficiency, increases procurement risk and undermines the coherence of the government's digital transformation agenda. These constraints reinforce the need for a centralised authority capable of reconciling digital policy, data governance and procurement law within a unified and legally binding framework.

6 COMPARATIVE REVIEW OF INTERNATIONAL BEST PRACTICES

6.1 Comparative Perspectives on Procuring Cloud and Digital Infrastructure

South Africa's comparatively slow public-sector cloud adoption provides an opportunity to draw on the regulatory and institutional experiments of other jurisdictions. Countries such as the United Kingdom, Canada, Australia, France, Estonia, Chile, Kenya, Brazil, New Zealand, Singapore and India have all had to reconcile traditional procurement law with service-based, rapidly evolving ICT and cloud models. Their experiences show that cloud procurement is not simply a technical issue, but a problem of administrative law, institutional design and market regulation. The brief case studies below focus on four elements in each jurisdiction: the regulatory framework for ICT procurement, the mechanisms actually used to contract for cloud and other XaaS services, the resulting supplier landscape, and the way data classification and privacy are translated into cloud-appropriate controls. Each ends with a short legal critique and lessons for South Africa.

6.1.1 United Kingdom

The UK has pursued an explicitly market-oriented digital-government strategy, underpinned by central standards and a highly developed e-procurement ecosystem.

Regulatory framework

Cloud procurement sits within the general public procurement regulations, supplemented by central Cabinet Office policies and a digital service standard that governs how technology is specified, designed and delivered. A central security classification policy sets the baseline for handling official information.

Procurement mechanisms for ICT

The G-Cloud framework and associated digital marketplace are the primary tools for procuring cloud services. They function as centrally-led framework agreements with regular refresh cycles, from which contracting authorities draw down via call-off contracts. Alongside the standard G-Cloud pricing catalogue, many cloud providers also offer optional commercial models, such as commitment-based discounts or savings-plan structures, that can be negotiated separately where consistent with procurement rules. These models introduce additional flexibility in cost optimisation but require careful alignment with framework terms, call-off procedures and public-sector contracting constraints.

Supplier landscape

The marketplace features both hyperscalers and a large number of domestic SMEs, particularly in niche services and managed support. However, scale and branding still give hyperscalers a significant competitive advantage.

Data classification and governance

The security classifications policy links information sensitivity to procedural and technical controls, including how and where data may be hosted. This provides a relatively clear legal bridge between classification and cloud deployment.

UK: Critical legal observations and lessons for South Africa

Legally, G-Cloud shows how a centrally managed framework can maintain competition, transparency and equal treatment while accommodating rapid technological change. But there are also risks: the complexity of listing requirements may still exclude smaller suppliers; frequent refreshes demand significant central capacity; and the model presupposes a relatively high level of procurement and digital maturity in contracting authorities. The presence of alternative cloud-provider pricing structures further underscores the need for procurement officers to reconcile provider-specific commercial features with the mandatory terms of public-sector call-off contracts. For South Africa, the lesson is not to copy G-Cloud mechanically, but to recognise that a lawful, dynamic marketplace requires strong central capability, clear listing criteria and proactive support for SMEs, or it simply entrenches the position of the largest providers.

6.1.2 Canada

Canada's approach illustrates how security and data protection can be built directly into procurement eligibility for cloud services.

Regulatory framework

Cloud procurement is governed by the general federal procurement framework and by central policies on cloud adoption and security. Treasury-level policies and standards set mandatory requirements for departments, particularly around information security and privacy.

Procurement mechanisms for ICT

Canada uses centrally managed supply arrangements and standing offers for cloud. Providers must undergo a security and capability assessment before becoming eligible to offer services to the government under these arrangements.

Supplier landscape

Infrastructure services are dominated by global providers, while Canadian firms play a larger role in integration, analytics and managed services. The pre-qualification system provides a predictable route to market for those who can meet the criteria.

Data classification and governance

A tiered classification system is directly linked to technical and contractual controls and to the level of certification a provider must hold to serve a given tier.

Canada: Critical legal observations and lessons for South Africa

From a legal perspective, Canada's model reduces discretionary risk by making security and classification a condition of eligibility rather than something assessed ad hoc in each procurement. The downside is that certification schemes can become rigid and resource-intensive, potentially excluding innovative smaller providers who cannot bear the cost of compliance. The lesson for South Africa is that central certification can greatly improve legality and consistency in cloud procurement, but only if it is proportionate, transparent and accompanied by support mechanisms that prevent it from becoming a de facto barrier to entry.

6.1.3 Australia

Australia combines strong central guidance with panel-based procurement of cloud and ICT services.

Regulatory framework

The Commonwealth Procurement Rules govern all federal procurement. They are supplemented by detailed information-security and protective-security frameworks, and by guidance from a central digital-transformation body.

Procurement mechanisms for ICT

Whole-of-government panels and standing offers are widely used for cloud and related ICT services. Agencies call off these arrangements rather than running fully bespoke cloud tenders.

Supplier landscape

There is a mix of hyperscalers and Australian-owned providers, including sovereign-cloud offerings aligned with national-security requirements.

Data classification and governance

Classification regimes are integrated with information-security manuals that specify the controls required for different sensitivity levels, including hosting and personnel requirements for cloud providers.

Australia: Critical legal observations and lessons for South Africa

Panels provide legal certainty and economies of scale, but they also carry a risk of market closure if refresh cycles are slow or entry criteria are poorly designed. Once panels are in place, new or smaller suppliers may find it hard to gain access, and agencies may default to panel use even when more competitive options exist. For South Africa, the key lesson is that panel-based cloud procurement can be lawful and efficient, but it must be accompanied by clear rules on panel refresh, review and competition, or it risks ossifying the supplier base.

6.1.4 France

France has placed questions of sovereignty and jurisdiction at the centre of its cloud strategy.

Regulatory framework

ICT procurement sits within the general public procurement code, but is heavily influenced by cybersecurity and sovereign-cloud policies and by certification regimes run by a central security agency.

Procurement mechanisms for ICT

Complex cloud and digital-infrastructure projects often use more flexible procedures that allow technical dialogue before final bids. Eligibility for these procedures may be limited to providers that meet sovereign-cloud criteria.

Supplier landscape

The supplier mix is shaped deliberately: domestic sovereign-cloud operators and "trusted" local entities of global providers are favoured for sensitive workloads.

Data classification and governance

Data classification is tied to sovereignty controls: certain categories must be hosted in environments that satisfy specified legal and technical conditions, including jurisdictional insulation from foreign law.

France: Critical legal observations and lessons for South Africa

France's approach underscores the legitimacy of using procurement as a tool to protect constitutional and security interests. However, it also carries a competition risk: strict sovereignty criteria can narrow the supplier base and raise costs, and may be challenged if they are not clearly linked to objective, proportionate security needs. For South Africa, the lesson is that sovereignty-driven cloud procurement must be articulated in clear legal terms, supported by risk assessments, and balanced against competition and value-for-money principles.

6.1.5 Estonia

Estonia is often presented as a digital exemplar, but its model is rooted in a particular scale and institutional context.

Regulatory framework

Digital government is governed by a mix of information-law statutes and specific regulations around interoperability and digital infrastructure. These instruments collectively create a strong normative framework for data exchange and system integration.

Procurement mechanisms for ICT

Rather than a single cloud marketplace, Estonia relies on modular, often agile, procurement of digital components that must connect to a centrally governed interoperability layer.

Supplier landscape

The market is dominated by domestic SMEs that build services on top of the state-provided digital backbone.

Data classification and governance

Classification and access rules are embedded in information-law statutes and technical regulations governing the interoperability framework, which define who may access what data and under what conditions.

Estonia: Critical legal observations and lessons for South Africa

Legally, Estonia demonstrates the power of architecture-driven regulation: procurement is constrained by mandatory interoperability and security standards, which reduces arbitrary system choice by agencies. The potential weakness is that such a model depends on strong central technical capacity and on sustained investment in the core backbone. For South Africa, the lesson is that setting architectural and interoperability obligations in law can guide ICT procurement decisions, but this only works if the central state can actually maintain the backbone and enforce the standards.

6.1.6 Chile

Chile provides an example of incremental digitalisation through a central procurement platform rather than a fully-fledged cloud-governance regime.

Regulatory framework

General procurement law, a central e-procurement system and a national digital-government strategy form the backbone of ICT procurement.

Procurement mechanisms for ICT

Cloud-capable solutions are bought primarily via a central procurement platform that supports catalogue purchasing and modular contracting.

Supplier landscape

Hyperscalers offer infrastructure services, but much of the value is captured by local firms that provide applications and integration.

Data classification and governance

Data governance rests largely on privacy law and sector-specific rules; cloud-specific classification and security standards are still evolving.

Chile: Critical legal observations and lessons for South Africa

Chile shows that central e-procurement tools can lower administrative costs and enable iterative digital procurement even before cloud-specific law is fully developed. The risk is that, without clear cloud and data-classification norms, agencies may take inconsistent approaches, potentially undermining legality and equality of treatment. For South Africa, the lesson is that e-procurement platforms are useful, but they cannot substitute for clear, binding cloud-security and data-classification frameworks.

6.1.7 Kenya

Kenya's model is particularly instructive as a middle-income African country coupling general procurement law with cloud-specific standards.

Regulatory framework

Cloud procurement is governed by general procurement legislation, a dedicated data-protection statute and technical standards issued by a central ICT authority.

Procurement mechanisms for ICT

Agencies procure cloud services through standard procedures but must apply central cloud standards when specifying and evaluating solutions.

Supplier landscape

Infrastructure is often provided by global players, while Kenyan firms play a significant role as integrators and managed-service providers.

Data classification and governance

A tiered data-classification approach is linked to cloud-hosting rules in the technical standard, giving agencies concrete parameters for deciding where and how data may be hosted.

Kenya: Critical legal observations and lessons for South Africa

Kenya demonstrates that administrative standards can be used to regulate cloud procurement without waiting for primary legislative reform. This is legally attractive but comes with rule-of-law risks if standards are not clearly authorised, consulted on and consistently enforced. For South Africa, the lesson is that interim cloud-governance standards could be issued under existing powers, but they should be transparently developed and linked to an eventual statutory framework to avoid legitimacy challenges.

6.1.8 Brazil

Brazil has pursued parallel reforms in procurement law and digital-government policy.

Regulatory framework

Recent procurement-law reform and a dedicated digital-government statute together provide the legal basis for digital and cloud procurement.

Procurement mechanisms for ICT

Flexible procedures are used for complex ICT and cloud projects, including mechanisms that allow dialogue with bidders. Standardised contracting and a central e-procurement portal are used for more routine cloud services.

Supplier landscape

Again, hyperscalers tend to supply infrastructure, with Brazilian firms active in integration, migration and managed services.

Data classification and governance

Privacy and data-protection rules inform contract design, but classification and cloud-specific obligations are still maturing and are not uniformly applied across all entities.

Brazil: Critical legal observations and lessons for South Africa

Brazil shows that modernising procurement procedures (for example by adding more flexible methods for complex ICT) can make a real difference in cloud projects, even before all substantive standards are fully settled. The risk is that greater procedural flexibility, if not bound by clear guidance, can increase the scope for arbitrary or poorly justified decisions. For South Africa, the lesson is that introducing more flexible procedures for complex ICT procurement should be accompanied by strong guidance on when and how they are used, to preserve legality and accountability.

6.1.9 New Zealand

New Zealand offers a relatively compact, high-trust example of framework-based cloud procurement.

Regulatory framework

General procurement rules, a cloud-first policy and central digital-government guidance together establish the framework within which agencies procure cloud services.

Procurement mechanisms for ICT

All-of-government framework agreements for cloud allow agencies to procure under pre-negotiated terms without running separate tenders.

Supplier landscape

Both global and domestic cloud providers are covered by these frameworks, with some agreements designed specifically to support local providers.

Data classification and governance

Privacy and information-access laws require structured risk assessments; central guidance provides templates for cloud-specific risk and classification decisions.

New Zealand: Critical legal observations and lessons for South Africa

Legally, New Zealand's framework-agreement model reduces transaction costs and supports compliance by embedding risk-management and classification into standard terms. The vulnerability is dependency on central capacity: if frameworks are poorly managed or not updated, agencies have limited lawful alternatives. The lesson for South Africa is that framework agreements can be powerful tools for cloud procurement, but they require ongoing stewardship, not a once-off design effort.

6.1.10 Singapore

Singapore represents a highly centralised, state-driven model of digital-government and cloud procurement.

Regulatory framework

General procurement rules operate alongside dedicated digital-government legislation and detailed ICT and security policies set by a central digital authority.

Procurement mechanisms for ICT

Cloud services are often procured centrally, with a central technology agency negotiating bulk contracts and making them available to agencies under standard conditions.

Supplier landscape

Global providers are prominent but operate within a tightly controlled architecture and governance model.

Data classification and governance

A multi-tier data-classification scheme is backed by detailed ICT and security policies, including explicit rules about when different classes of data may be hosted in public cloud.

Singapore: Critical legal observations and lessons for South Africa

Singapore's model shows how far centralisation can go: both architecture and procurement are tightly governed from the centre. This promotes legal certainty and coherence, but may concentrate power and reduce space for local experimentation or alternative providers. For South Africa, the lesson is that increasing central cloud-governance capacity is essential, but it should be balanced with mechanisms that preserve competition and allow context-sensitive innovation.

6.1.11 India

India offers an example of centralised empanelment in a very large and diverse system.

Regulatory framework

General financial and procurement rules are supplemented by central digital-government policies and cloud-governance arrangements.

Procurement mechanisms for ICT

A central list of pre-approved cloud providers is maintained, and public entities procure from this list through a central e-marketplace or other standard procedures.

Supplier landscape

Both hyperscalers and major domestic technology firms appear on the central list; smaller providers tend to participate through partnership or as SaaS application developers.

Data classification and governance

Data-protection and sectoral norms inform which providers may host which types of workloads, with central guidance issued for cloud deployments.

India: Critical legal observations and lessons for South Africa

India's empanelment approach reduces legal uncertainty by making provider eligibility a national-level decision. The trade-off is that the empanelment process itself becomes a powerful gatekeeper; if criteria or processes are opaque, it can entrench incumbents and undermine equal treatment. For South Africa, the lesson is that central provider lists or frameworks must be governed by clear, contestable criteria and accessible processes, or they risk becoming legally and politically vulnerable.

6.1.12 Lessons for South Africa

Looking across these jurisdictions, three legal themes stand out.

First, legality in cloud procurement improves when security, data-classification and architectural rules are fixed centrally and made binding, whether through legislation, regulation or clearly authorised standards. Where these are absent, ICT procurement tends to become fragmented and discretionary, which is precisely South Africa's current risk.

Second, procurement mechanisms matter as much as substantive standards. Frameworks, panels, certified supplier lists, marketplaces and flexible procedures each carry distinct legal risks and benefits. They can reduce transaction costs and improve consistency, but if poorly designed or managed, they can entrench incumbents, exclude SMEs or undermine competition. South Africa must therefore choose and design these mechanisms consciously, rather than treating them as neutral administrative tools.

Third, the institutional location of cloud-governance authority is crucial. All of the comparator jurisdictions have some form of central body or function that links digital policy, security standards and procurement practice. Without a comparable institutional anchor, South Africa's cloud-related reforms risk being diffused across multiple departments and regulators, making coherent, lawful ICT procurement much harder to achieve.

For South Africa, the implication is unequivocal: without centrally legislated data-classification standards, centrally procured cloud frameworks and institutional authority for cloud governance, cloud adoption will remain fragmented, legally uncertain and operationally constrained.

6.2 Principles of agile and cloud-friendly procurement

Apart from country-specific examples that South Africa can draw on, principles of cloud-friendly procurement have emerged at the international level that also serve as important comparative pointers. Notably principles include:

- Public buyers should specify outcomes and controls rather than brands or box-level configurations;
- use multi-supplier framework agreements to keep competition "always on";

- require portability and reversibility to avoid lock-in; and
- align security and privacy to statutory duties

Procurement patterns to embed:

- Framework agreements with mini-competitions - keep price/performance pressure over time and enable rapid call-offs as needs evolve.
- Portability and switching by design - require adherence to a recognised code for data portability and switching (for example, SWIPO for infrastructure services) and insist on a tested exit plan.
- Include export formats, assisted migration, and verified data deletion.
- Shared-responsibility clarity - vendors must document which security and compliance duties sit with the provider and which with the department, and provide tooling to evidence this split.
- Live technical evaluation - score real service behaviour (identity, logging, encryption, automation) rather than paper promises.

6.2.1 CISPE Framework

The Cloud Infrastructure Services Providers in Europe (CISPE) framework represents a set of industry-led principles governing the provision of cloud infrastructure services within the European Union. The framework is significant as an articulation of internationally recognised norms relating to cloud service provision, particularly in relation to data protection, interoperability, portability and fair competition. It operates within a mature regulatory environment shaped by the General Data Protection Regulation (GDPR), EU competition law and established digital governance institutions, and therefore reflects a high degree of alignment between legal regulation, procurement practice and technological development.

The CISPE framework provides a useful comparative benchmark against which to assess the extent to which South Africa's procurement and governance systems accommodate the operational realities of cloud computing. Unlike domestic policy instruments, which are predominantly governance-oriented, the CISPE principles engage directly with the contractual and operational dimensions of cloud service provision. These include commitments relating to data control, transparency in service provision, avoidance of vendor lock-in, and the facilitation of switching between cloud providers.

However, the direct application of CISPE principles within the South African context is neither straightforward nor entirely appropriate. The European cloud ecosystem is characterised by a higher degree of regulatory harmonisation, institutional capacity and market maturity, including the presence of regionally anchored infrastructure providers and established competition frameworks. By contrast, South Africa's cloud market is more concentrated and more dependent on global hyperscale providers, with comparatively limited domestic infrastructure capacity. As such, the transplantation of CISPE principles without adaptation may give rise to unintended constraints, particularly in relation to localisation, market participation and industrial policy objectives.

Notwithstanding these contextual differences, the CISPE framework highlights several areas in which South Africa's current approach to cloud procurement is underdeveloped. In particular, it underscores the importance of integrating procurement methodology with governance frameworks, ensuring interoperability and portability across platforms, and promoting competitive and diverse supplier

ecosystems. These dimensions are only partially reflected in South African policy instruments and remain largely absent from procurement rules.

A policy review of the CISPE framework (see ***Addendum A at 9.1.12***) using the same review framework applied to South African instruments in section 4 above shows an overwhelming strong qualitative rating in relation to procurement of cloud solutions. Only two categories, Institutional Mandates and Implementation Feasibility, scored a moderate rating, with none rated as weak.

The CISPE framework is clear in its subject matter, setting out concrete principles on data protection, switching, portability, transparency, and fair competition in cloud infrastructure services. Internally, CISPE is more coherent than the South African framework, integrating data protection, customer control, switching, and anti-lock-in principles into a unified cloud governance logic, whereas comparable concerns in South Africa are distributed across procurement law, POPIA, MISS, and departmental directives.

From a procurement perspective, CISPE is highly relevant because it engages directly with the contractual and operational issues that arise in cloud procurement, including switching processes, data portability, and avoidance of lock-in. Its value lies in informing procurement design rather than prescribing procurement methods, particularly in relation to framework agreements, exit rights, and cloud-specific contract terms.

On competition, CISPE explicitly resists vendor lock-in and supports customer choice, making it a useful benchmark for South Africa, where current instruments do not adequately embed portability and interoperability into procurement design. On sovereignty, its Digital Sovereignty Principles and Data Protection Code of Conduct are relevant to localisation and customer assurance, though its European conception of sovereignty cannot be straightforwardly transplanted into the South African context.

As an industry association framework supported by codes and declarations rather than a public governance architecture, CISPE does not allocate institutional mandates and cannot resolve the South African questions relating to the roles of NT, DPSA, DCDT, SITA, or the Information Regulator, a significant limitation given the fragmented institutional competence that characterises the current public procurement system. On implementation, CISPE is operationally useful as a benchmark because it is grounded in practical cloud service issues, with its switching framework being particularly valuable for translating principle into operational detail. However, direct application in South Africa would require substantial adaptation to local procurement law, budgeting rules, public sector capacity constraints, and domestic regulatory institutions, making it a viable influence rather than a ready-made template.

Overall, CISPE aligns strongly with global best practice on cloud market design and contract governance and serves as a valuable comparative reference for South Africa, even if it does not constitute a complete model for public procurement reform.

6.2.2 Data Strategies and Data classification

6.2.2.1 What "good" looks like

A department-wide data strategy should include:

- inventory of datasets;
- classification rules mapping to controls (encryption at rest/in transit; key ownership; logging/retention);
- access policies tied to roles; and
- standards for interoperability.

The system should adopt the principle of privacy-by-design:

- default minimisation, purpose limitation, and auditability;
- vendor attestation of processing locations and sub-processors;
- lawful cross-border transfer logic where relevant.

Reversibility must be incorporated into contractual arrangements:

- contractually require structured export (open formats),
- assisted migration windows, and
- certified deletion, tested during the term (not only at exit).

6.2.3 Cloud deployment model and cloud migration

6.2.3.1 Definitions to anchor procurement

Rather than relying on the service-model taxonomy developed by the United States National Institute of Standards and Technology, public procurement in South Africa should anchor its cloud terminology and standards in the European Union's rights-based framework. The EU model, built on the GDPR, the CISPE Data Protection Code of Conduct, and the SWIPO Code of Conduct for Switching and Porting, defines cloud environments through the nature of the data processed, the legal responsibilities of the processor and controller, and the guarantees for portability, reversibility, and sovereignty. This approach prioritises compliance, transparency, and privacy over purely technical deployment labels. Under the CISPE Code, validated by the European Data Protection Board, providers must demonstrate full alignment with GDPR principles such as privacy-by-design, data minimisation, and lawful processing. The complementary SWIPO Code sets enforceable rules for migration and exit, ensuring that public entities can retrieve, transfer, and delete data in structured and interoperable formats without dependency on a single provider. Adopting this EU-aligned definitional model in South Africa would harmonise procurement with the objectives of POPIA and the National Data and Cloud Policy, embedding portability, accountability, and data sovereignty as the foundation for all government cloud deployments and migrations.

The classifications of cloud services should focus on data categories (personal, sensitive, non-personal, critical infrastructure data) and related compliance duties under GDPR and the Free Flow of Non-Personal Data Regulation, whereas the NIST (USA) focusses on service models (XaaS) and deployment models (public, private, community, hybrid).

Cloud deployment decisions under GDPR are driven by data sensitivity and sovereignty needs whereas under NIST deployment is determined mainly by operational and cost factors and mapped through standardised model definitions.

In terms of migration and exit, GDPR provides for explicit rights to portability and reversibility under SWIPO, and providers must give structured, interoperable export formats and deletion certificates. Contrastingly with NIST, migration is treated as a technical transition exercise, with no embedded legal rights to portability.

Regarding security and compliance, the GDPR approach is anchored in privacy by design, lawful processing, accountability and continuous certification whereas under the NIST it is anchored in US standards (FedRAMP, NIST SP 800-53) with voluntary adoption outside the US context.

6.2.3.2 Selecting the deployment model (privacy and sovereignty first)

Deployment choices should be determined by data classification and risk, not by infrastructure convenience. Personal and sensitive data, such as health, biometric, or citizen-registry information - should be hosted in environments certified under a GDPR-aligned code (for example, the CISPE Code) and located within sovereign or jurisdictionally-controlled regions. Non-personal or anonymised datasets may be processed in federated or public-cloud environments, provided that contractual and technical safeguards preserve compliance with POPIA sections 19 and 72.

Government-critical workloads may require community or "trusted-cloud" models under sovereign-cloud conditions similar to those developed within the EU's GAIA-X initiative, ensuring that data remain under South African legal jurisdiction while leveraging international hyperscaler infrastructure. This model links data sensitivity to legal control, mirroring the European principle that data protection follows the data, irrespective of location or service provider.

6.2.3.3 Migration and portability requirements

Cloud migration must operationalise the GDPR principles of accountability and data subject rights. The SWIPO Code of Conduct, endorsed by the European Commission under the Free Flow of Non-Personal Data Regulation, provides a practical blueprint for this. It obliges providers to: Disclose migration procedures in advance, detailing data formats, dependencies, and expected timelines. Provide structured, interoperable export formats and APIs so that departments can re-host workloads or repatriate data without loss of integrity.

Offer assisted migration and certified deletion after exit, ensuring full reversibility. Document sub-processor chains and security controls during migration to preserve POPIA and GDPR compliance.

South African framework contracts should incorporate these obligations directly, requiring suppliers to demonstrate tested exit procedures, data portability, and evidence of deletion certificates as a contractual condition.

6.2.3.4 Contractual and technical controls for migration

A GDPR-aligned procurement template should embed:

- Shared-responsibility matrices defining processor versus controller duties, aligned to GDPR Article 28 and POPIA section 21.

- Breach-response clauses reflecting GDPR Articles 33–34 and POPIA section 22, requiring notification to the Information Regulator and data subjects "as soon as reasonably possible."
- Lawful transfer mechanisms, referencing EU Model Clauses or equivalent local adequacy frameworks for cross-border data flows.
- Continuous certification to recognised standards such as ISO 27001, ISO 27018, or the CISPE Data Protection Code of Conduct, with annual third-party audits and publication of results.

These controls transform migration from a one-off event into a life-cycle compliance obligation.

6.2.3.5 Implementation for South Africa

Embedding the GDPR model into South Africa's cloud procurement policy would:

- Provide legal symmetry between POPIA and international best practice, enhancing interoperability with EU partners.
- Strengthen data sovereignty, ensuring that state data remain under national law even when processed by multinational providers.
- Guarantee reversibility and competition, lowering switching costs and enabling small and medium local providers to participate on equal terms.
- Support the National Data and Cloud Policy's 2024 objective of "secure, inclusive and locally-governed cloud infrastructure."

By reframing cloud deployment and migration through the GDPR's legal and ethical lens, South Africa can move from a purely technical conception of cloud adoption to a rights-driven, accountable, and sovereign digital environment that balances innovation with the constitutional protection of privacy and access to information.

6.2.4 Tech infrastructure for SMMEs and start-ups.

6.2.4.1 From compliance to capability building

A rights-based cloud and data ecosystem should not only safeguard personal information but also empower inclusive economic participation. Under the European Union's GDPR framework, digital markets are structured around fairness, accountability, and user control - principles equally relevant to South Africa's developmental priorities. Applying these concepts locally means ensuring that SMMEs and start-ups can access compliant, affordable, and interoperable infrastructure without being locked into proprietary ecosystems. Data protection becomes an enabler of innovation: by guaranteeing trust, transparency, and lawful processing, it lowers barriers for emerging enterprises to handle personal data responsibly and to participate in public-sector value chains.

6.2.4.2 Data governance and trust as market foundations

The GDPR approach demonstrates that a strong data-governance culture - anchored in privacy-by-design and data-minimisation - creates a predictable environment for smaller firms. For South Africa, this aligns with POPIA and with the DPSA's Directive on Public Service Information Security (2022). Government procurement frameworks can extend this trust infrastructure by:

- Embedding privacy-by-design standards into all public digital projects, requiring suppliers and subcontractors (including SMMEs) to adopt the same compliance obligations as primary vendors.
- Creating "compliance-as-a-service" toolkits within national cloud platforms so that local start-ups can automatically inherit encryption, access-logging, and breach-notification mechanisms aligned to POPIA and GDPR.
- Developing a national data-trust framework, overseen by the Information Regulator and NT, that certifies SMME data processors and provides assurance to contracting authorities similar to the CISPE or SWIPO registers in the EU.

6.2.4.3 Infrastructure access and digital inclusion

To translate compliance into opportunity, South Africa's public cloud initiatives should directly support equitable infrastructure access. Government-backed regional cloud hubs, such as Dube iConnect within the Dube TradePort SEZ, can serve as secure, POPIA-compliant hosting zones offering subsidised compute resources and local-data residency for small innovators. These hubs can mirror the EU's Digital Innovation Hub model, linking connectivity, mentorship, and GDPR-grade compliance services. Open APIs and interoperability standards should be mandated in government systems so that start-ups can build complementary applications without discriminatory licensing or data-access restrictions. This mirrors GDPR's portability principle and supports the Competition Commission's digital-platform reform agenda.

Cloud credits and digital-skills programmes, jointly funded by NT, the Small Enterprise Development Agency (SEDA), and hyperscaler partners, can ensure that small suppliers achieve technical competence and compliance simultaneously.

6.2.4.4 Procurement as an economic policy instrument

The PPA explicitly requires socio-economic and environmental considerations in procurement planning. By embedding GDPR-inspired transparency and POPIA-compliant data safeguards into tender requirements, the state can use procurement to catalyse a trusted local digital-services market. Examples include:

- Reserved work-packages for small cloud integrators or data-analytics start-ups that demonstrate POPIA compliance certifications.
- Scoring criteria rewarding open-source and interoperable solutions that enhance data portability and citizen control.
- Knowledge-transfer obligations requiring large vendors to mentor or subcontract to local SMMEs on privacy engineering and cybersecurity practices.

This transforms compliance from a cost centre into a lever for inclusion and domestic capability growth.

6.2.4.5 Institutional support and alignment with policy objectives

The GDPR's ecosystem of supervisory authorities offers a model for institutional cooperation. In South Africa, a similar network should connect the Information Regulator, DCDT, and NT's OCPO (and future PPO). Their joint mandate would be to: maintain a registry of trusted cloud service providers compliant

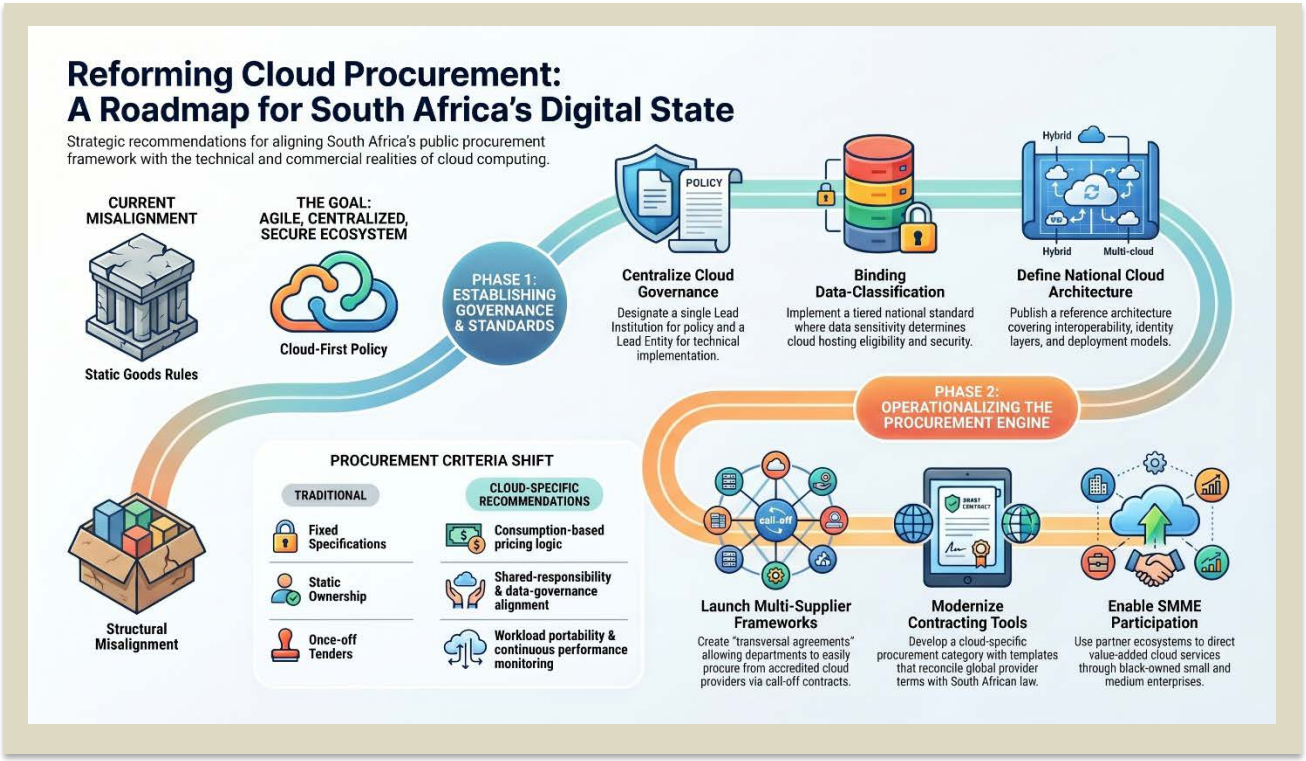
with POPIA and aligned to EU-level safeguards; coordinate training and certification for public-sector buyers to evaluate data-protection clauses in RFPs; and ensure that government data strategies actively promote local innovation and sovereignty, as set out in the National Data and Cloud Policy.

6.2.4.6 Outcome

A GDPR-aligned and POPIA-anchored infrastructure model ensures that digital transformation uplifts rather than excludes. It positions South Africa's SMMEs and start-ups within a trusted, rights-respecting data economy, where lawful processing, privacy assurance, and open standards become preconditions for market participation. This approach fuses the EU's rigor on data protection with South Africa's developmental imperatives, building an inclusive digital ecosystem that is both globally interoperable and locally sovereign.

7 RECOMMENDATIONS

South Africa's transition to cloud-enabled public administration requires a coherent regulatory and institutional framework that aligns procurement rules, data governance, contract structures and architectural choices. The comparative analysis in Section 6 demonstrates that successful cloud procurement depends on three pillars: (i) centrally governed classification and security standards; (ii) centrally procured or accredited cloud frameworks enabling lawful, competition-compatible access to multiple cloud providers; and (iii) cloud-appropriate procurement mechanisms, including contracting structures capable of accommodating dynamic pricing, shared-responsibility arrangements and rapid technological evolution. The recommendations below translate these principles into a set of actionable reforms suited to the South African context.



7.1 Establish Central Cloud-Governance Authority and Framework

South Africa's fragmented institutional landscape requires immediate structural intervention to establish clear accountability and eliminate overlapping mandates. South Africa requires a single, authoritative institutional locus for cloud governance, a central, authoritative and capacitated lead implementation entity and explicit rules governing the relationship between these central entities and all other organs of

state. The overlapping mandates of SITA, National Treasury, DPSA, DCDT and the Information Regulator must be rationalised into a coherent governance framework.

7.1.1 Designate a Lead Institution for Cloud Governance

Government should formally assign cloud governance, including explicit coordination authority over all digital transformation procurement, to a single lead institution. The DSU within the Presidency can potentially fulfil this role supported by an Inter-Ministerial Committee with binding decision-making power. Governance of distinct elements of cloud procurement, such as setting data standards and formulating standard contract terms, can be assigned to particular institutions, such as the Information Regulator and PPO respectively, but with explicit linkages to DSU ensuring oversight and coordination. This coordination mechanism must operate through formal memoranda of understanding establishing decision hierarchies, escalation protocols, and dispute resolution procedures.

7.1.2 Designate an Institutional Lead Entity for Cloud Implementation

Parallel to the centralised governance architecture, a single entity must be designated as the institutional lead entity for implementation of public cloud services. In this respect, SITA's institutional future demands definitive resolution. Either SITA transitions to a competitive service provider without procurement gatekeeping authority, competing on merit alongside private vendors under uniform evaluation criteria, or SITA dissolves entirely with residual implementation functions transferring to a cloud procurement unit within the PPO or potentially the proposed SDIC. The current ambiguous position, wherein SITA retains statutory authority whilst departments increasingly bypass it through regulatory deviations, creates compliance uncertainty and market confusion.

7.2 Develop a National Cloud Reference Architecture

The lead institution should publish an authoritative reference architecture defining interoperability standards, identity layers, audit requirements, deployment models (public, private, hybrid, multi-cloud), and cross-government integration patterns. Without this architectural baseline, individual procurement processes will continue to produce inconsistent and incompatible solutions.

The key step in developing the cloud reference architecture is to reform public procurement instruments for cloud services. Current procurement instruments, such as GCC, Treasury Regulations, SITA prescripts, PFMA/MFMA rules, PPPFA regulations, are designed for static goods or traditional ICT systems. Cloud procurement requires new instruments. It is accordingly imperative that fit-for-purpose instruments be created as set out below.

7.2.1 Create a Cloud-Specific Procurement Category

Government should establish a dedicated “Digital Services and Cloud Procurement” category within the procurement system, with evaluation criteria tailored to cloud services, including:

- consumption-based pricing logic
- architectural interoperability

- shared-responsibility alignment
- data-classification compliance
- resilience, availability and portability considerations
- partner-ecosystem participation and SMME development

This category should guide specification design, evaluation models, and contracting terms for all cloud-related procurement. The PPA provides clear statutory authority for the creation of different categories of procurement and the differentiated governance of such distinct categories.

7.2.2 Establish a Multi-CSP Framework Contract / Transversal Agreement

South Africa should adopt a multi-cloud, multi-CSP transversal framework agreement, administered by the Institutional Lead Entity, that accredits all cloud providers meeting centrally defined security, data-classification and architectural standards. This framework should:

- allow all organs of state to procure cloud services via call-off contracts
- maintain competition between providers and partners
- prevent lock-in by enabling workload portability where technically feasible
- allow accredited CSPs to offer commitment-based pricing or savings models within a lawful public-sector contractual structure
- enable SMME participation through partner and reseller channels
- provide predictable, pre-negotiated contractual terms compatible with PPA, PFMA, MFMA and Treasury delegations.

This framework mirrors the successful architectures used in the UK (G-Cloud), Australia, New Zealand and Canada while remaining aligned with South African procurement law. Implicit in this recommendation is the creation of a clear regulatory regime for framework procurement, which is currently absent in South African law.

7.2.3 Develop Harmonised Cloud Contracting Templates

Government must design cloud-specific contracting instruments that reconcile:

- CSP integrated Ts&Cs (security, shared responsibility, data handling specifics)
- South African GCC/Treasury frameworks
- PPA/PFMA/MFMA compliance
- data-classification rules
- liability, indemnity and escalation clauses
- comprehensive exit provisions

Partial incorporation or “cherry-picking” of CSP clauses should be avoided, as this produces duplication, conflicting obligations and uncertain order-of-precedence. Regulatory reform should mandate interoperability and data portability as standard contractual requirements for all cloud procurements above specified thresholds, preventing vendor lock-in through statutory obligation rather than voluntary best practice.

7.2.4 Introduce flexible procedures for complex cloud procurement

Procurement mechanisms such as competitive dialogue, negotiated procedures and phased evaluation should be authorised for complex ICT procurement. These procedures allow deeper technical engagement and reduce the risk of ill-fitting specifications in fast-evolving digital markets.

7.3 Implement binding data-classification and security

A unified, binding data-classification framework is the precondition for lawful deployment of hybrid, multi-cloud or sovereign-cloud architectures. It is recommended that the Information Regulator take the lead in creating such a framework.

7.3.1 Publish a national data-classification standard

Government should implement a statutory or regulatory classification model defining which categories of information may be stored or processed in:

- public cloud
- hybrid and multi-cloud environments
- private or sovereign cloud
- offshore vs onshore facilities

This standard should be mandatory for all organs of state.

7.3.2 Link classification tiers to cloud-provider eligibility

Cloud-provider accreditation under the multi-CSP framework should be tiered according to classification requirements, mirroring Canada's Protected A/B/C tiers. Eligibility to handle sensitive workloads should require certification against centrally defined security controls.

7.3.3 Balance security concerns and operational flexibility

Whilst legitimate security concerns justify data localisation for classified information, blanket residency requirements impose unnecessary cost and resilience constraints. Risk mitigation should follow data classification principles, mandating South African hosting only for sensitive categories whilst permitting multi-region deployments for public or low-sensitivity administrative data. The data-classification standard should thus allow for balancing these competing interests in contractual terms.

7.4 Strengthen Institutional Capacity and SMME Participation

7.4.1 Build Cloud-Procurement Competencies

Government must invest in skills: cloud architecture, pricing analysis, contract governance, identity and security management. Substantial capacity investment is a precondition for successful public cloud

procurement, potentially done through partnerships with CSPs providing technical training, architecture guidance, and managed service capabilities to government ICT teams.

7.4.2 Enable SMME Participation through partner ecosystems

Clear prescripts should define how reseller and managed-service partners may participate in cloud procurement under prevailing preferential procurement frameworks (PPA/PPPFA). The preferential procurement framework should be calibrated to accommodate global cloud providers' operational realities, potentially through mandatory local partnering requirements, substantive subcontracting obligations to qualifying enterprises, or economic value-add commitments including skills transfer and research investment. SMME obligations should be operationalised by directing value-added cloud-service components through accredited black-owned SMMEs.

7.5 Clarify Governance of Sovereign Cloud Infrastructure

South Africa must resolve the institutional ambiguity between SITA's Government Private Cloud and the proposed SDIC. Clarification is needed on:

- who operates sovereign data centres
- who governs sovereign cloud certification
- whether SDIC's "digital infrastructure" mandate extends to cloud
- how private providers may partner in sovereign-cloud configurations

Without this clarity, sovereign-cloud policy cannot be operationalised.

7.6 Introduce continuous monitoring, transparency and auditability

Real-time monitoring, audit trails, and transparent consumption reporting should be mandated for all cloud deployments to strengthen accountability, cost management and oversight under PPA/PFMA/MFMA. Contracts must incorporate audit rights enabling government verification of storage locations, encryption key custody arrangements ensuring South African jurisdiction over cryptographic materials, government-conducted penetration testing rights, and breach notification protocols aligned with POPIA requirements.

8 CONCLUSION

South Africa's digital transformation agenda has reached a decisive moment where ambition must translate into institutional capability and legal certainty. The strategic shifts required are neither incremental nor optional, but rather foundational to realising the vision articulated across multiple policy frameworks. Three core transformations emerge as essential.

First, the transition from aspirational policy to binding regulatory architecture must be completed. The PPA presents a unique legislative opportunity to codify cloud-specific procurement methods, establish enforceable interoperability standards, and harmonise conflicting mandates across SITA, NT, and sectoral digital authorities. Without this legal consolidation, departments will continue navigating an unworkable tension between cloud-first directives and procurement frameworks designed for an analogue era.

Second, South Africa must establish unified, enforceable data classification and governance frameworks as the foundational infrastructure for all cloud procurement decisions. The Information Regulator's mandate should be expanded to encompass comprehensive public-sector data classification, working in coordination with the DPSA and the SSA. This framework must directly determine permissible cloud deployment models, data residency requirements, and security controls, providing legal certainty under POPIA whilst enabling interoperability across government.

Third, institutional coordination requires structural intervention through DSU, supported by binding Inter-Ministerial Committee oversight, and a lead implementation entity, either SITA or a dedicated Digital Procurement and Data Governance Centre of Excellence/Unit within the PPO (once the PPA has come into operation). The lead implementation entity must reconcile fragmented mandates, develop standardised procurement templates, provide technical advisory capacity, and establish the market infrastructure, including multi-supplier frameworks and dynamic purchasing systems, that enables competitive, innovation-friendly cloud acquisition whilst mitigating vendor lock-in risks.

These shifts represent a move from procurement compliance to procurement enablement, from institutional fragmentation to coordinated authority, and from regulatory ambiguity to legal certainty. Without decisive action reconciling digital policy objectives with procurement law, South Africa risks perpetuating a system where transformative vision remains confined to policy documents whilst implementation falters under the weight of incompatible regulations, inadequate institutional capacity, and market structures that entrench rather than challenge concentration. The opportunity exists; the imperative is execution.

ADDENDUM A: POLICY REVIEW TABLES

9.1.1 Public Procurement Act 28 of 2024

Category	Assessment Summary
1. Legal Clarity	The PPA gives a directional mandate for e-procurement: the Public Procurement Office (PPO) "must develop" an ICT-based procurement system to enhance efficiency, transparency and integrity, including a single platform for officials, bidders, suppliers and the public, plus open/interoperable data, an e-marketplace, and reporting/hosting for analytics and oversight. The Act also obliges procuring institutions to use technology and, when available, to use the components of this national system. However, the Act defers key technical details (standards, APIs, security baselines, identity frameworks, timelines and migration rules) to future regulations/instructions and the PPO's design process.
2. Policy Coherence	The digitisation mandate must align with the national e-strategy/ICT norms under ECTA and with POPIA when publishing or handling procurement data (the Act expressly contemplates publication/access but allows confidentiality carve-outs). This creates a workable spine but requires downstream rules so POPIA minimality and transparency can co-exist in the e-procurement data model.
3. Procurement Compatibility	The PPA centralises architecture decisions in the PPO and anticipates method frameworks (to be prescribed by the Minister); the ICT system must support those methods once set. The PPA creates broad scope for design and implementation of dedicated procurement methods appropriate for cloud procurement. Until regulations are made, departments must digitise within a transitional vacuum, existing PFMA/MFMA practice continues.
4. Market Access & Competition	The single platform + e-marketplace can lower entry costs and standardise documents; publication and open data can reduce information asymmetry. But without prescribed interoperability/Open Data schemas, smaller vendors may face integration burdens with bespoke formats.
5. Digital Sovereignty & Security	The Act mandates a national system with public access to information but leaves hosting model, data residency, identity & access management, audit, and crypto choices to later rules. Those choices must be harmonised with POPIA security safeguards and any national cybersecurity guidance.
6. Institutional Mandates	PPO is the design/owner of the national system; it can issue binding instructions for most institutions and guidelines/circulars for municipalities (which can adopt them). Procuring institutions must adopt tech "to the extent possible" and consume PPO system components when available. Clear escalation lines for standards-setting sit with PPO; municipal uptake needs council adoption. Institutional alignment with SITA is not clear.

7. Implementation Feasibility	The Act requires a prior ICT due-diligence and readiness assessments, and then a progressive rollout of components for e-procurement. But it sets no statutory timeline, leaving sequencing to PPO instructions—useful for flexibility, risky for drift. Feasibility depends on funding, standards decisions, migration toolkits, and capacity at PPO/provincial treasuries/municipalities.
8. Global Best Practice Alignment	The Act's direction (single portal, open/interoperable data, analytics/publication, e-marketplace) aligns with UNCITRAL/e-GP and Open Contracting norms; adopting OCDS (data model + publication guidance) would operationalise "interoperable open data" and accelerate analytics/civil-society oversight.

9.1.2 General Conditions of Contract

Category	Assessment Summary
1. Legal Clarity	The GCC is meant to be non-amendable in the "general" part (so that all public contracts share baseline terms) and is supplemented by Special Conditions of Contract (SCC) for project-specific deviations. The GCC defines foundational contract mechanics (delivery, payments, termination, warranties, force majeure, etc.). However, GCC does not anticipate or explicitly provide for digital or cloud procurement modes or how digital contract execution, auditing, or system integration should be done. In that sense, it's neutral on "how the infrastructure works."
2. Policy Coherence	GCC is broadly coherent with procurement law (PFMA, SCM frameworks) and with the requirement that government tenders use uniform conditions. It dovetails with the idea of standardisation in supply chain and procurement. But when overlaid with a digital procurement infrastructure (e-procurement, smart contracts, APIs, audit logs), there is little built-in guidance. The GCC assumes paper/deliverable flows and manual processes.
3. Procurement Compatibility	GCC is widely accepted and used in government tendering, so any digital procurement engine must be able to enforce and incorporate GCC clauses (or reference them) in digital bid contracts. The platform should allow "SCC overrides" where project-specific deviations are inputted. Because GCC is standard, digital systems can reference clause IDs and track compliance. But GCC does not define digital amendment rules, electronic signatures, or automated variation workflows.
4. Market Access & Competition	The standardisation of terms under GCC helps bidders by providing predictability. A digital procurement platform could further that by providing machine-readable contract terms, clause checkers, and automated compliance alerts for bidders. GCC's uniformity is an enabler to digitisation, but the reference text needs adaptation to allow dynamic digital enforcement (e.g., automated penalty computation, milestone checks).
5. Digital Sovereignty & Security	Because GCC assumes physical documentation, there's no built-in clause for digital security, key management, identity verification, audit trails, or data retention in cloud systems. If a contract is executed or monitored via a digital system, additional SCC or rider clauses will be needed to specify data jurisdiction, audit logs, encryption, non-repudiation, electronic signature, etc. The digital procurement system must ensure that GCC obligations (delivery, acceptance, penalty, warranties) are traceable and logged in a tamper-resistant system.

6. Institutional Mandates	GCC places contracting obligations on "supplier" and "purchaser" under the standard public procurement architecture. But it does not designate which party is responsible for ensuring digital compliance (platform, tool). In a digital system, there should be clarity whether PPO, SITA, or procuring institution must ensure contract enforcement, system availability, versioning of contract templates, and audit logs. The digital engine will need to act as the "agent" for contract execution (issuing notices, tracking delivery, triggering penalties) under GCC semantics.
7. Implementation Feasibility	Since GCC is stable and well understood, digital systems can codify its clauses into modules (e.g., delivery module, forfeiture module, termination module). The challenge is mapping human, legal text clauses into executable logic reliably, especially in edge cases. SCC variations will need a digital overrides layer. Feasibility increases if the digital procurement tool is built to reference clause IDs and allow logic branching (e.g. if "force majeure" then suspend penalty, etc.).
8. Global Best Practice Alignment	Globally, contract templates are evolving to support smart contracts, digital contract lifecycle management, auditability, and data traceability. GCC's baseline approach is conservative and manual. To align with "contract as code" paradigms, the digital implementation of GCC would need to embed modular, versioned contract templates, immutable audit trails, digital signature support, event triggers, and API hooks for performance verification. Integrating GCC into the e-procurement platform is consistent with best practice, but GCC itself needs augmentation for a fully digital ecosystem.

9.1.3 National Data and Cloud Policy

Category	Assessment Summary
1. Legal Clarity	The policy articulates clear objectives, definitions (e.g., SaaS/PaaS/IaaS), and institutional roles (e.g., SITA). However, it sometimes blends policy ambition with operational statements without legal binding authority. It is a *policy* document, not a legislative instrument, and lacks enforceability unless backed by regulation. There is potential confusion between aspirational goals and mandated duties. Clarity around procurement obligations for departments is implied but not codified.
2. Policy Coherence	The policy acknowledges and references several existing laws (POPIA, ECTA, Cybercrimes Act, SDIA, etc.) and strategies (e.g., e-Government Roadmap), but some institutional overlaps (e.g., between DPSA, SITA, DCDT, and sector regulators) may generate confusion. The paper tries to harmonise these regimes, but the framework for coordination is still underdeveloped. It integrates national priorities and continental ambitions (AfCFTA, Smart Africa) but offers few mechanisms to resolve policy tensions or misalignment.
3. Procurement Compatibility	While the policy encourages cloud-first approaches and unified government data centres, it stops short of specifying **how procurement rules should adapt**. There's no mention of modern procurement principles (e.g., agile contracting, framework agreements), nor guidance on aligning SITA rules or Treasury procurement reforms. Procurement is seen through the lens of infrastructure provision, not as a strategic enabler. CSP onboarding processes, evaluation criteria, or procurement flexibility for innovation are not addressed.

4. Market Access & Competition	The document acknowledges market concentration by multinationals and encourages SMME participation. However, it offers limited concrete proposals to reduce entry barriers or implement fair vendor evaluation. It defers competition issues to the Competition Commission and recognises anti-competitive risks but does not integrate procurement tools (like sandboxing or modular contracting) to address them. Guidelines for open competition in cloud service contracts are absent. The policy states that CSPs shall ensure transparency regarding data portability and interoperability costs and technical implications at the point of contracting.
5. Digital Sovereignty & Security	Strong emphasis on data sovereignty, localisation (esp. for sensitive government data), and cross-border controls. The document aligns with POPIA and proposes restrictions on hosting government-critical data offshore. It also encourages treaty alignment and robust national cybersecurity. However, the security provisions rely heavily on outdated instruments like MISS and anticipate revisions that have not yet occurred, creating potential legal uncertainty. The Policy proposes a basic data classification framework, but provides little detail on the implementation of the framework.
6. Institutional Mandates	SITA is presented as the central node for sourcing infrastructure and managing SLAs, but its current underperformance and capacity limitations are acknowledged. There is tension between centralisation (SITA) and operational autonomy (departments managing their own applications). The policy proposes an Advisory Council and interdepartmental teams but does not yet clarify reporting lines or accountability frameworks. Coordination between National Treasury, DCDT, SSA, and DPSA is implied but structurally unclear.
7. Implementation Feasibility	The policy is comprehensive in vision, but ambitious in its execution. It requires significant investment in broadband, skills, security, and institutional reform, most pertinently capacitation of SITA. The reliance on under-resourced bodies like SITA and DPSA creates implementation risks. Proposals to mandate cloud services for all new ICT procurement may face resistance without corresponding budget reforms or procurement flexibility. The absence of a costed implementation plan weakens its feasibility. Absence of details on core implementation tools, like a data classification framework and mechanism, undermines feasibility.
8. Alignment with Global Best Practices	The policy reflects alignment with global principles: cloud-first strategy, open data, privacy protection (GDPR-like), and inclusion of cross-border considerations. It references international trends and aims to harmonise with AU digital frameworks. However, it does not incorporate agile procurement models or digital service standards (e.g., UK's GDS, Estonia's X-Road, or EU's NIS2 compliance models). No strong benchmarking to model jurisdictions like Kenya, Australia, or Chile is provided.

9.1.4 Government Digital Strategy

Category	Assessment Summary
1. Legal Clarity	The DGPF is a *framework*, not a statutory instrument and it is currently only a draft. A final version has not been published. It provides policy guidance but lacks legislative force. Its implementation will depend on coordination through the Public Service Act, PAM Act, SITA Act, and PPA (once implemented). It calls for the eventual creation of a *Digital Government Act* to codify digital principles into law.

2. Policy Coherence	The DGPF consolidates scattered ICT policies (2001 e-Government Policy, 2016 Integrated ICT Policy White Paper) under a single vision aligned with the NDP 2030 and 4IR Strategy. However, overlaps remain with the DCDT, SITA, and NT mandates, risking fragmentation. The "whole-of-government" principle is sound but lacks an enforceable coordination structure.
3. Procurement Compatibility	The framework recognises procurement as a critical enabler of digital transformation. It highlights the need for eProcurement, framework agreements, agile contracting, and cloud pay-per-use models. However, it does not yet align these mechanisms with the PPA or NT regulations. It also fails to outline clear procedures for procuring cloud services or AI-driven systems.
4. Market Access & Competition	Encourages PPPs and private-sector partnerships but lacks detailed mechanisms for ensuring open competition, SME participation, and vendor-neutral procurement. It acknowledges SITA's role but provides limited guidance on addressing vendor lock-in or building local digital industry capacity.
5. Digital Sovereignty & Security	The DGPF emphasises data governance, cybersecurity, and data localisation, referencing POPIA and the Cybercrimes Act. It calls for a Whole-of-Government Data Management Framework and investment in a Government Private Cloud, data centres, and shared infrastructure. However, there is no defined national framework for data classification, cross-border storage, or sovereign cloud compliance.
6. Institutional Mandates	The framework allocates coordination to DPSA, but SITA, DCDT, and sector departments retain overlapping mandates. It calls for a new digital transformation component, potentially within or alongside SITA — similar to the UK's Government Digital Service (GDS) or Australia's Digital Transformation Agency. However, this new body's legal status and budget are undefined.
7. Implementation Feasibility	Implementation faces typical cross-government barriers: legacy systems, low digital skills, limited funding, and fragmented ICT budgets. The DGPF's call for centralised ICT budgeting and skills audits is practical but requires strong NT and DCDT cooperation.
8. Global Best Practice Alignment	Aligns with the OECD Digital Government Policy Framework and World Bank's GovTech approach, emphasising "digital by design," "data-driven government," and "citizen centricity." It also draws comparative lessons from Estonia, Spain, Rwanda, and Mauritius. However, the DGPF's reliance on policy rather than enforceable digital law limits its capacity to emulate these international exemplars.

9.1.5 South Africa's Communications & Digital Technology Infrastructure Roadmap

Category	Assessment Summary
1. Legal Clarity	The C&DTI Roadmap sits under DCDT's mandate to plan and coordinate national digital infrastructure; it aligns with existing e-Government and digital strategies but is a ministerial policy direction rather than a statute or formal policy document. It signals priorities (broadband, spectrum use, DPI, cloud-ready infrastructure) while relying on existing laws (PFMA/MFMA, ICASA Act, Electronic Communications Act) and departmental plans for execution.

2. Policy Coherence	It dovetails with ongoing DCDT work (e.g., SA Connect, spectrum, digital skills, the proposed State Digital Infrastructure Company (SDIC)) and the national medium-term planning cycle, but coherence depends on interlocks with NT/SCM rules and SITA's evolving role. Parliamentary briefings in late-Oct 2024 underscore SDIC delays—an immediate coherence risk.
3. Procurement Compatibility	The C&DTI Roadmap's infrastructure and DPI ambitions must transact through existing SCM frameworks (PFMA/MFMA, Treasury Regulations, PPPFA, and in future, PPA) and ICT procurement pathways (including SITA or permitted deviations/alternatives). Without explicit "cloud/XaaS" procurement guidance, departments must map C&DTI Roadmap projects to general SCM instruments
4. Market Access & Competition	It gestures toward open, investment-friendly infrastructure (broadband rollout, shared networks) in step with global digital economy practice; competitive neutrality and tech-agnostic standards are needed to avoid single-vendor dependency in DPI/cloud.
5. Digital Sovereignty & Security	Strong emphasis on data sovereignty, localisation (esp. for sensitive data). C&DTI Roadmap momentum implies data-protection, cybersecurity, and resilience baselines across public infrastructure and cloud-adjacent systems. Execution must align to POPIA, national cyber norms and sectoral security controls referenced in DCDT planning.
6. Institutional Mandates	DCDT leads; portfolio entities (SITA, Sentech, BBI, .ZADNA, SABC, ICASA) are implicated. Institutional risk persists where SDIC establishment is delayed and where SITA capacity/governance constraints affect digital infrastructure and cloud projects linked to the C&DTI Roadmap.
7. Implementation Feasibility	Feasibility hinges on budget availability, procurement agility, spectrum and rights-of-way (rapid deployment), municipal wayleaves, and programme management capacity. DCDT APP/Annual Reports highlight resource and coordination constraints that the C&DTI Roadmap must overcome.
8. Alignment with Global Best Practices	Themes in the C&DTI Roadmap (interoperable DPI, scalable/secure tech, ecosystem enablement) reflect international guidance (e.g., ITU/GSMA). To fully align, South Africa should codify cloud/DPI reference architectures, open standards, and assurance frameworks in procurement and operating models.

9.1.6 South Africa's Roadmap for the Digital Transformation of Government

Category	Assessment Summary
1. Legal Clarity	The Digital Transformation Roadmap provides strategic direction but lacks legal enforceability. It is a policy framework, not a legislative instrument, meaning its implementation depends on coordination with existing laws such as the PFMA, MFMA, PPPFA and PPA (once implemented). It outlines intent (e.g., cloud-first adoption, interoperability) but stops short of prescribing binding rules or regulations, although the Roadmap suggests the creation of such rules.

2. Policy Coherence	The document is conceptually coherent and aligns with the National Development Plan (NDP) and Fourth Industrial Revolution (4IR) Strategy. However, overlaps exist with the SITA Act, Digital Skills Strategy, and National Cloud and Data Policy, leading to potential duplication of mandates and fragmented implementation.
3. Procurement Compatibility	The Digital Transformation Roadmap lacks a clear framework for cloud contracting, data sovereignty clauses, and POPIA compliance within procurement processes. It relies by implication on future harmonisation with NT and the PPA to translate principles into enforceable procurement practice without providing any guidance on how the high levels of procurement centralisation and coordination that will be required to realise the Roadmap's objectives, are to be achieved. Given the Roadmap's considerable reliance on the IFMS as an enabling tool, and the material procurement challenges experienced in relation to the IFMS to date (noted in the Roadmap's supplementary documents), serious concerns arise pertaining to procurement compatibility. While addressing regulatory barriers is identified as a milestone among the M&E indicators and metrics, it is of significant concern that no activity, indicator, or data source are identified in the M&E framework.
4. Market Access & Competition	The policy promotes private-sector participation and PPPs, especially for cloud infrastructure and digital service delivery. However, it provides limited detail on ensuring competitive neutrality or SME participation, which may allow dominant hyperscalers to capture public-sector cloud demand. There is little indication of an appreciation of differentiated market access and competition tensions and opportunities across different layers and initiatives of the overall strategy.
5. Digital Sovereignty & Security	The policy emphasises local data hosting, interoperability, and secure government clouds, aligning with digital sovereignty principles. Envisages creation of data standards by DPSA and creation of a National Data Governance Authority. Strong emphasis on the key role of data standards.
6. Institutional Mandates	Mandates several implementation and coordination structures, such as an Inter-Ministerial Committee (IMC), Inter-Departmental Working Group (IDWG), DSU, GITOC and DSTI GovTech Centre, with strong indication of the lead to be taken by IDWG and DSU. However, the relationship with SITA, DPSA and NT (especially OCPO and future PPO) in relation to procurement is not formally defined nor is procurement coordination noted as a distinct and critical cross-cutting enabler.
7. Implementation Feasibility	Implementation depends on interdepartmental cooperation, skills development, and funding availability. Many departments still operate in silos with legacy systems. The DSU could drive progress, but its operationalisation and budget are uncertain, as is a strategy to address SITA capacity challenges (that are noted).
8. Global Best Practice Alignment	The Digital Transformation Roadmap is aligned with international frameworks like the UN e-Government Survey, OECD Digital Government Principles, and the AU Digital Transformation Strategy (2020–2030) and draws on several international best-practice case studies. However, global best practice would require stronger legal and institutional integration between digital policy and public procurement law - an area still underdeveloped.

9.1.7 DPSA Determinations and Directives under the Public Service Act

Category	Assessment Summary
1. Legal Clarity	Overall, the legally binding instruments provide clear frameworks, but coordination between advisory and mandatory instruments requires clarification and there is some ambiguity around enforceability versus SITA mandates.
2. Policy Coherence	All five instruments explicitly reference overlapping legislation (POPIA, PAIA, MISS, Public Service Act, Constitution) and position themselves as implementation mechanisms rather than creating new requirements. The Data Governance Directive effectively consolidates by repealing the previous conflated "Knowledge and Data Management" directive. However, significant coordination gaps exist: no clarification of interfaces between DPSA, SITA, NT, and DCDT; potential tensions between cloud procurement autonomy and centralised approval requirements; risk of duplicated governance structures (separate Data and Knowledge Management (KM) committees). The frameworks acknowledge interdependencies conceptually but lack operational integration mechanisms.
3. Procurement Compatibility	Critical weakness across all instruments. The Cloud Circular mandates extensive pre-procurement requirements (business cases, total cost of ownership (TCO) analysis, risk assessments, DPSA approval) that conflict with agile cloud procurement principles. The Digital Services Standard is silent on procurement despite requiring cloud platforms. The Data Governance instruments treat procurement peripherally with governance-first sequencing that may create "wait states". The KM Directive provides no procurement guidance beyond requiring database establishment. None address: modular contracting, consumption-based pricing, rapid prototyping, cloud marketplaces, or iterative procurement. The governance-heavy, approval-centric approach fundamentally misaligns with cloud procurement best practices requiring speed, flexibility, and experimentation.
4. Market Access and Competition	Systematic failure across all instruments. None address vendor diversity, SME participation, competitive dynamics, or measures to prevent vendor lock-in. The Cloud Circular shows preference for "private government cloud where capability exists" without competition provisions. Extensive compliance requirements (SLAs, security protocols, governance structures) create de facto advantages for large established vendors. Database-centric KM approach implicitly favours enterprise platform vendors. No provisions for: open standards, interoperability requirements, simplified processes for smaller providers, preferences for emerging/innovative suppliers, or support for South African technology providers. This represents a critical gap given South Africa's developmental procurement objectives and the sensitivity to avoid single hyperscaler monopolies in cloud markets.
5. Digital Sovereignty & Security	Highly variable performance. The Cloud Circular provides exceptionally strong provisions: mandatory data classification per MISS, prohibition on moving classified data to public clouds, explicit data residency requirements within South African borders, clear data ownership provisions, and restrictions on data processing/mining. Data Governance instruments strengthen security governance through binding POPIA/MISS compliance but lack technical specifications for cloud environments (no data localisation rules, cross-border transfer protocols, or residency specifications). The Digital Services Standard and KM Directive address security only at high governance levels without operational detail. The instruments are notably silent on provisions for government access to data by foreign cloud providers, sovereign cloud requirements, and emergency data repatriation protocols. Security is acknowledged but sovereignty is underspecified, which is particularly concerning given foreign hyperscaler dominance.

6. Institutional Mandates	Strong intra-departmental clarity but weak inter-institutional coordination. All instruments clearly define Head of Department accountabilities and establish governance structures (committees, offices, designated officials). Matrices and reporting hierarchies are comprehensive for departmental implementation. However, systematic failure to address cross-government coordination emerge in the absence of clarity on SITA's technology provision role, NT's approval requirements, DPSA's support functions, and DCDT's digital transformation authority. The requirement for separate Data Governance and Knowledge Management committees without integration mechanisms risks duplication. No protocols for inter-departmental data/knowledge sharing or resolution of conflicting mandates. Provincial government coordination entirely absent. This fragmentation creates significant implementation risks for shared cloud platforms and cross-cutting digital services.
7. Implementation Feasibility	Ambitious requirements with inadequate support mechanisms. Strengths include: binding timeframes (6 months for cloud compliance, 12-24 months for governance structures), phased approaches using recognised methodologies (COBIT, CMMI maturity models), detailed deliverables specifications, and enforcement mechanisms via Public Service Act. However, critical gaps undermine feasibility: no budget allocations or funding guidance; no staffing provisions (new roles mostly designated from existing staff); no capacity-building programmes or technical assistance from DPSA; no differentiation by department size/capability; simultaneous implementation across all departments. The Cloud Circular's 6-month deadline for existing solutions is particularly unrealistic given documentation requirements. The assumption that departments can establish governance offices, appoint CDOs/CKOs, develop comprehensive policies, implement tools, and conduct training without additional resources is highly optimistic. Potential bottleneck at DPSA review stages with no specified turnaround times.
8. Alignment with Global Best Practice	Strong conceptual alignment but implementation divergences. Positive elements include explicit adoption of international standards (NIST cloud definitions, DAMA DMBOK, ISO 30401 for KM, ISO 25010 for digital services, COBIT/CMMI for governance); user-centred design principles; lifecycle approaches; emphasis on TCO analysis and security by design. References to UK GDS, Australian frameworks, and ITU guidelines demonstrate awareness of international practice. However, significant gaps in contemporary cloud-era practices with no recognition of API-first architecture, microservices, DevOps/DataOps, data mesh, serverless computing, or consumption-based models; database-centric KM approach is dated (modern practice emphasises social platforms, wikis, AI-powered discovery); extensive pre-procurement documentation contrasts with iterative, test-and-learn approaches; centralised approval mechanisms contradict devolved, agile models. The frameworks adopt 2010s cloud governance thinking rather than 2020s platform and ecosystem approaches. Strong on traditional governance, weak on enabling innovation.

9.1.8 SITA Rules and Procurement Policy

Category	Assessment Summary
1. Legal Clarity	SITA Act provides clear legal authority for centralised IT management across government. Mandates SITA to approve and manage ICT projects in departments. Some ambiguity exists regarding outsourcing, multi-tenant cloud use, and international cloud service providers. New Regulation 17.8 allows departments, from 1 June 2025, to bypass SITA when SITA cannot meet a department's time/cost requirements — a material legal/practical shift departments can leverage for cloud procurements.

2. Policy Coherence	SITA regulations align with broader government ICT policies and digital transformation objectives. Fragmentation exists across departmental interpretations of approval processes for cloud deployments. Parliament and AGSA proceedings have highlighted inconsistent execution across portfolios, with SCOPA questioning SITA's viability and oversight.
3. Procurement Compatibility	Regulations require departmental projects to be approved via SITA, including procurement of IT services. However, SITA as an agency is under serious scrutiny regarding their fitness to hold office with allegations of cadre deployment and ineptness. The framework is traditional, geared to in-house or local vendors, with limited guidance for cloud SaaS, PaaS, or IaaS solutions. Regulation 17.8 now requires SITA to respond within defined windows (reported as 10 working days) or departments may proceed externally - enabling competitive routes to hyperscalers where SITA timelines/costs underperform. SCOPA labelled SITA a "horror show"/"cash cow"; multiple reports on irregular spend, leadership churn, and ministerial probes.
4. Market Access & Competition	SITA centralisation can limit direct market access to international providers. Potential for vendor lock-in if centralised contracts favour a single provider however, working exclusively with hyperscalers crowds out smaller and local suppliers. Cabinet-level reform now forces SITA to compete; departments can procure outside SITA if they show better value/speed, which directly opens market access for hyperscalers.
5. Digital Sovereignty & Security	Strong focus on government control of data. Security standards exist, but detailed technical requirements for multi-tenant cloud and hybrid deployments are absent. Persistent audit and governance regressions (incl. procurement/controls) increase the premium on provable security baselines (encryption, logging, residency, access governance) and POPIA-aligned designs in any cloud footprint.
6. Institutional Mandates	SITA's mandate includes oversight, standards-setting, procurement, and operational management of government IT. Capacity to manage large-scale cloud projects may be limited; reliance on external vendors may be necessary. SITA's legislative mandate to be an ICT supplier creates potential conflicts with municipal SCM autonomy and the PPA's aim for uniform procurement. Revised regulations of 2025 now allow government departments to procure top-shelf services without being forced to use SITA if SITA cannot satisfy their requirements, greatly reducing SITA's exclusive mandate and expanding departments' mandate to procure independently. SITA leadership churn and governance disputes (board removals/reinstatements; ministerial interventions) have impaired mandate execution; departments report SITA as a performance bottleneck in mission systems (e.g. e-courts, Home Affairs, SAPS).
7. Implementation Feasibility	Approval and governance processes are formal and may be slow, impacting agile cloud deployments. Departments may lack cloud readiness, requiring extensive capacity building. High vacancy rates and capacity constraints (reported ~57% staff vacancies; even portfolio-specific vacancies above 50% mentioned in AG briefings) make delivery riskier unless a project includes enablement/managed services.

8. Global Best Practice Alignment	Policies do not yet reflect cloud-first strategies, hybrid models, or global compliance frameworks (ISO, FedRAMP, SOC2). Opportunity to integrate hyerscaler best practices for secure, compliant, and scalable government cloud adoption.

9.1.9 Data Protection, Information Governance and Cloud-specific norms

Category	Assessment Summary
1. Legal Clarity	POPIA establishes the statutory foundation for privacy and personal data protection in South Africa, operationalising section 14 of the Constitution (right to privacy). It defines eight lawful processing conditions (accountability, processing limitation, purpose specification, further processing limitation, information quality, openness, security safeguards, and data subject participation) and empowers the Information Regulator to enforce them. The Act clearly delineates roles for "responsible parties" and "operators," binding both public and private entities.
2. Policy Coherence	POPIA aligns conceptually with global data protection regimes like the GDPR and African Union Convention on Cybersecurity and Data Protection but diverges in institutional maturity and enforcement consistency. It complements the Electronic Communications and Transactions Act (ECTA) but overlaps with the National Data and Cloud Policy on issues of data residency and localisation—necessitating coherent application between sectoral regulators (e.g., Information Regulator, DCDT, and SITA).
3. Procurement Compatibility	POPIA's s 19–22 security obligations and s 72 cross-border data transfer rules require that any cloud procurement ensures contractual clauses and technical controls that meet these standards. Section 71 (automated decision-making) demands human review mechanisms in cloud-based AI identity verification processes. Compliance must be written into SLAs, data-processing agreements, and sub-processor terms.
4. Market Access & Competition	POPIA applies uniformly to all service providers, but local interpretations of s 72 may hinder international cloud vendors if adequacy decisions are not standardised. Certainty around cross-border transfer mechanisms (binding corporate rules, standard contractual clauses) could enhance fair competition and market entry for global cloud providers while protecting sovereignty.
5. Digital Sovereignty & Security	POPIA's security safeguards (Condition 7) align with sovereign-data mandates under the National Data and Cloud Policy, requiring encryption, access control, and breach notification. Section 72 indirectly enforces data localisation by restricting offshore transfers absent adequate protection.
6. Institutional Mandates	The Information Regulator holds primary oversight but coordination with SITA, DHA, and the State Security Agency is essential for coherent implementation in national cloud programmes. Institutional fragmentation currently causes ambiguity in accountability—whether breaches in a hybrid cloud are investigated by SITA, DHA, or the Regulator.

7. Implementation Feasibility	Technically feasible through existing hyperscalers' control sets (encryption at rest/in transit, IAM, CloudTrail auditing). Practically constrained by skills shortages in government, lack of standardised DPIA templates, and limited capacity of the Regulator. Hybrid architecture (local sovereign zone + global redundancy) provides a pragmatic path to compliance.
8. Global Best Practice Alignment	Largely aligned with GDPR principles (lawfulness, fairness, transparency, minimality) and ID4D principles on inclusion and governance. Gaps remain in data-portability rights, algorithmic transparency, and interoperability with verifiable credential frameworks like eIDAS 2.0. Incorporation of privacy-by-design and privacy impact assessments (DPIAs) into hyperscalers' architectures would close these gaps.

9.1.10 Minimum Information Security Standard (MISS)

Category	Assessment Summary
1. Legal Clarity	MISS is a Cabinet-approved security directive that establishes the state's classification system. While binding on organs of state, it was drafted for analogue environments and provides no clarity on how classification duties apply to digital or cloud systems, creating uncertainty in modern contexts.
2. Policy Coherence	MISS predates POPIA, the Cybercrimes Act and all modern digital-government policies. It is not harmonised with cloud-first strategies or interoperability initiatives, resulting in conceptual tension between its custodial security model and the distributed architecture of cloud computing.
3. Procurement Compatibility	MISS contains no cloud-specific standards, offering no basis for translating classification levels into technical controls. Procurement teams cannot rely on MISS when drafting specifications, evaluating cloud providers or ensuring compliant contractual arrangements.
4. Market Access & Competition	The absence of defined cloud-security standards creates an uneven playing field: hyperscalers rely on international certifications, while domestic SMEs lack an authoritative compliance pathway. This uncertainty suppresses competitive participation in government cloud tenders.
5. Digital Sovereignty & Security	MISS reflects a physical-control paradigm and does not address data residency, jurisdiction, encryption-key ownership or tenant isolation. Without updated standards, the state lacks a clear framework for maintaining sovereignty over classified data in cloud environments.
6. Institutional Mandates	MISS does not assign responsibility for updating classification rules for digital systems. No institution - SSA, DPSA, DCDT, NT or SITA - has a clear mandate to modernise or operationalise classification standards for cloud contexts, reinforcing institutional fragmentation.
7. Implementation Feasibility	MISS offers no tools, templates or operational guidance for applying its requirements to digital or cloud systems. Departments must interpret classification duties independently, leading to inconsistent practices and risk-averse avoidance of cloud migration.

8. Global Best Practice Alignment	MISS is misaligned with modern classification regimes used internationally, which integrate cloud-security baselines and technical standards. Its analogue orientation places South Africa behind global norms for secure, cloud-enabled public-sector information management.

9.1.11 Sector-specific ICT and procurement governance instruments

Category	Assessment Summary
1. Legal Clarity	Eskom's Cloud Standard (Rev 1) establishes a cloud-first IT strategy anchored in compliance with the National Cybersecurity Policy Framework, Critical Infrastructure Protection Act, and POPIA. It clearly defines the roles of Cloud Consumer (Eskom), Cloud Provider, Cloud Carrier, Cloud Broker, and Cloud Auditor, consistent with the NIST framework. The document provides extensive clarity on cloud service models (IaaS, PaaS, SaaS) and deployment options (Private, Public, Hybrid, Community). It emphasises that Eskom may only adopt cloud services that are lawful, feasible, secure, and aligned with local data-sovereignty rules.
2. Policy Coherence	The policy aligns with government-wide ICT frameworks, especially the Government-Wide Enterprise Architecture (GWEA), promoting security, interoperability, and cost efficiency. It supports the national "Cloud-First" posture while maintaining Eskom's statutory duties as a National Key Point. However, it does not explicitly integrate with National Treasury procurement regulations or the Public Procurement Act 28 of 2024, which govern contracting for cloud services across SOCs. It aligns well with international cloud frameworks (NIST, COBIT, ITIL, ISO standards). Internally coherent, but not harmonised with broader government cloud policies, including the National Data and Cloud Policy or DPSA Digital Government Strategy. Lacks cross-reference to Treasury or regulatory requirements.
3. Procurement Compatibility	Eskom's standard defines a structured approach to evaluating cloud feasibility through the GIT RMO (Group Information Technology Resource Management Office) process, requiring a business case and Benefits Realisation Plan. This ensures internal accountability but lacks an open-market procurement framework for cloud vendors. There is no direct alignment with PFMA section 51 or Treasury digital-procurement standards. Stronger integration with competitive sourcing, SLA monitoring, and contract transparency would improve compliance.
4. Market Access & Competition	The architecture allows Eskom to engage multiple providers via brokers, encouraging interoperability and preventing vendor lock-in. Yet, the standard still favours on-premise or South African-hosted clouds, limiting cross-border flexibility and potential cost efficiency. There are no criteria for evaluating competing providers' security certifications (e.g., ISO 27017, SOC 2)
5. Digital Sovereignty & Security	The document makes data sovereignty and localisation a binding requirement: all personal or sensitive data must remain within South Africa, with preference for providers whose data centres are locally situated. It integrates cybersecurity requirements and mandates compliance with POPIA, GDPR standards, and SSA oversight. However, while it outlines robust security layers (authentication, authorisation, auditing, encryption), it lacks procedural detail for incident reporting and real-time monitoring integration.

6. Institutional Mandates	The roles of Group IT, GIT Information Security, and the RMO are defined but oversight responsibility (e.g., DCDT or Treasury interface) remains unclear. The inclusion of Cloud Auditor and Cloud Broker roles adds governance rigour, but implementation depends on Eskom's internal capacity. Cross-entity accountability between IT, Legal, and Compliance units needs clearer delineation.
7. Implementation Feasibility	The framework is technically comprehensive and aligned to NIST standards, offering reference architectures and orchestration models. However, feasibility depends on internal digital-skills capacity, service orchestration maturity, and integration with national infrastructure (SITA, GWEA - Government-Wide Enterprise Architecture). The "cloud-first" approach may be slowed by procurement and budgetary red-tape.
8. Global Best Practice Alignment	Eskom's adoption of the NIST Cloud Reference Architecture and GWEA alignment reflects strong adherence to global standards. It mirrors EU "Cloud for Europe" and U.S. FedRAMP frameworks by defining trust boundaries and shared-responsibility models. Yet it stops short of mandating continuous compliance audits, zero-trust frameworks, and automated threat-detection protocols now common in advanced utilities

9.1.12 CISPE Framework Policy

Category	Assessment Summary
1. Legal Clarity	The CISPE framework is comparatively clear in its subject matter and purpose. It sets out concrete principles relating to data protection, switching, portability, transparency and fair competition in cloud infrastructure services. However, it is not legislation and does not operate as a binding public law instrument in South Africa. Its legal force is contextual and derivative, depending in Europe on surrounding instruments such as the GDPR and EU data and competition law. In the South African context, it therefore has persuasive rather than normative force..
2. Policy Coherence	The CISPE framework is internally coherent because it links data protection, customer control, switching, and anti-lock-in principles into a single cloud governance logic. It is more integrated than the South African framework, where comparable issues are distributed across procurement law, POPIA, MISS and departmental directives. Its coherence is strengthened by the fact that it sits within a broader European digital policy environment oriented toward portability, interoperability and fair market access.
3. Procurement Compatibility	CISPE is highly relevant to procurement compatibility because it engages directly with contractual and operational issues that matter in cloud procurement, including switching processes, data portability, transparency of service conditions and avoidance of lock-in. Unlike many South African policy instruments, it is attentive to how cloud services are actually acquired and exited. However, it is not itself a procurement framework and does not prescribe public procurement methods in the manner a national procurement regulation would. Its value lies in informing procurement design, especially in relation to framework agreements, exit rights and cloud-specific contract terms.

4. Market Access & Competition	The CISPE framework strongly emphasises an open and competitive cloud environment and explicitly resists vendor lock-in and restrictive commercial practices. It supports customer choice and switching, and its policy vision is clearly oriented toward reducing dependency on dominant providers. This makes it particularly useful as a benchmark for South Africa, where current instruments do not adequately embed portability and interoperability into procurement design. That said, CISPE arises in a market with more mature competition regulation and a stronger regional policy architecture than South Africa presently has.
5. Digital Sovereignty & Security	CISPE places significant emphasis on customer control over data, processor compliance, and transparency regarding where and how services operate. Its Digital Sovereignty Principles and Data Protection Code of Conduct are particularly relevant to questions of lawful processing, localisation expectations, and customer assurance. However, its conception of sovereignty is shaped by the European regulatory environment and cannot simply be transplanted into South Africa, where sovereignty concerns intersect differently with localisation policy, state security instruments and public sector procurement mandates.
6. Institutional Mandates	CISPE does not allocate public institutional mandates in the way a state framework does. It is an industry association framework supported by codes and declarations rather than a public governance architecture. As such, it cannot answer the South African questions relating to the roles of National Treasury, DPSA, DCDT, SITA or the Information Regulator. Its limitation here is significant: it offers principles, but not a model for resolving fragmented institutional competence in a public procurement system.
7. Implementation Feasibility	As a benchmark, CISPE is operationally useful because it is grounded in practical cloud service issues such as switching timelines, portability processes, transparency of service conditions and contractual commitments. Its switching framework is particularly valuable because it translates principle into operational detail. However, implementation in South Africa would require adaptation to local procurement law, local budgeting rules, public sector capacity constraints and domestic regulatory institutions. It is therefore feasible as an influence, but not as a direct template.
8. Global Best Practice Alignment	CISPE aligns strongly with contemporary global concerns around data protection, switching, portability, interoperability and fair competition in cloud markets. Its frameworks anticipate or respond to leading regulatory developments in Europe, especially around GDPR compliance and the EU Data Act. For South Africa, it represents a valuable comparative benchmark on cloud market design and cloud contract governance, even if it is not a complete model for public procurement reform.