RFI 05/2025

NETWORK CARRIER AND INFRASTRUCTURE SERVICES BUSINESS REQUIREMENTS SPECIFICATION

Table of Content

RFI 05/2025

Network Carrier and Infrastructure Services

Business Requirements Specification Bid Bond

This document forms part of the RFI 05/2025 pack. The document sets out SARS's business requirements for the Network Carrier and Infrastructure Services (Data Carrier Network Services Tower; Voice Carrier Services Tower; and the Communication Platform as a Service Tower) and the models under which the Services are to be provided.

1.   USE OF TERMS IN THIS DOCUMENT

1.1.   Glossary Table

The capitalised terms in this document have the meanings given to them in the glossary table below. The Bidder is referred to paragraph 2.2 of the _RFI Main Document_ (SARS RFI 05/2025 1-1 Network Carrier and Infrastructure Services Summary Guidelines Instructions and Conditions) for the use and meaning of capitalised terms generally in the RFI pack.

Term	Meaning
AI	AI stands for "artificial intelligence," which is the simulation of human-intelligence processes by machines, especially computer systems.
Chatbot	A chatbot is an artificial intelligence (AI) software application that simulates a conversation with human users over a messaging interface, such as a website chat window or a messaging app. In the context of procurement tender business requirements, a chatbot could be designed to assist users in navigating the tendering process, provide guidance on documentation requirements, answer frequently asked questions, and provide updates on the status of users' tender submissions. The chatbot could be integrated with other procurement systems and tools to streamline the tendering process and improve the user experience.
CLI	Call-line identity Services
Customer Provisioning Portal	Customer Provisioning Portal is a Service Provider–provided portal which is accessible by SARS via a secure internet connection to provide functionality for SARS to place orders, and review order progress and order history. The detailed functionality required is discussed in the detailed requirements for each Tower in this document.
COT	Contract Obligation Tracker supplier-management document for tracking agreed contract deliverables that must be fulfilled for the duration of the contract, manging aspects such as supplier performance, supplier risks, **Spend Visibility, and Cost Saving**.
CPaaS	Communications Platform as a Service is a cloud-based platform that allows developers to embed real-time communication features such as voice, video, and messaging into their applications.
DMZ	Network demilitarised zone.
Least Cost Routing (LCR)	Least Cost Routing (LCR) is a telecommunications technique that allows Service Providers to select the most cost-effective method of routing calls or data transmissions across a network. LCR works by analysing various routing options and selecting the path that provides the lowest cost for the Service Provider, based on factors such as call volume, distance, and carrier rates. This approach can help Service Providers to minimise costs and maximise profits, while also ensuring that high-quality service is maintained for customers. LCR is commonly used in telecommunication networks, such as voice and data networks, to optimise routing paths and reduce operating costs
LLM	LLM stands for "Large Language Model", which is a type of artificial intelligence algorithm used in natural-language processing tasks such as language translation, text summarisation, and speech recognition. Large Language Models are characterised by their large size, complex architectures, and ability to generate human-like responses to user input.
Live chat	Live chat is a web-based communication tool designed to facilitate real-time conversations between taxpayers and tax agents regarding tax-related matters. The live chat feature would be accessible through a website or mobile app and

Term	Meaning
	would allow taxpayers to initiate a conversation with a tax agent who is available to respond in real-time. The goal of the live chat feature is to provide taxpayers with a quick and convenient way to ask questions, receive assistance, and obtain information related to their tax obligations. The live chat feature could be staffed by trained tax agents or supplemented with automated tools, such as chatbots or AI-based systems, to provide additional support.
MPLS	multi-protocol label switching.
MO	Mobile Operator, a mobile telecommunications company that provides wireless internet GSM services for mobile device users.
Monitoring and Reporting Portal	Service Provider–provided portal which is accessible by SARS via a secure internet connection to provide monitoring and reporting functionality. The detailed functionality required is discussed in the detailed requirements for each Tower in this document.
MoS	Opinion Score defined in the ITU-T PESQ P.862 standard.
NaaS	A cloud-based service model where networking resources, such as bandwidth, virtualised network functions, and network infrastructure are provided to organizations on-demand over the internet.
NLP	NLP stands for Natural Language Processing, which is a subfield of artificial intelligence that deals with the interaction between computers and humans using natural language. In legal terms, NLP refers to the technology that enables machines to understand, interpret, and generate human language for various applications, such as chatbots, voice assistants, and automated customer service.
P2P	Point to Point Protocol.
PPS&G	Policy, Procedure Standards, and Guidelines.
SASE	SASE stands for Secure Access Service Edge. It is a networking architecture that combines network-security functions with wide-area networking (WAN) capabilities to support the dynamic and distributed nature of modern digital enterprises.
SDM	Service Delivery Manager.
Service Coverage Period	has the meaning set out in paragraph 5.1.7.
SD-WAN	SD-WAN stands for Software-Defined Wide Area Networking. It is an approach to managing and optimising wide-area networks (WANs) using software-based control and automation.
Service Level Class	has the meaning set out in paragraph 5.1.7.
Service Level Agreement (SLA)	SLA stands for Service Level Agreement. An SLA is a formal contract between a Service Provider and its customers or users that specifies the agreed-upon levels of service that will be provided. It typically includes details such as the scope of the service, expected service levels (as defined by SLOs — see below), performance metrics, remedies, penalties for not meeting the agreed-upon levels of service, and other terms and conditions. SLAs help to establish clear expectations and responsibilities for both the Service Provider and its customers and can help to ensure that service quality is maintained over time.
Service Level Indicator (SLI)	SLI stands for Service Level Indicator. An SLI is a quantitative measure that defines a specific aspect of a service's performance, such as availability, latency, or throughput. It is used to track and measure how well a service is meeting its goals and can be used as a basis for making data-driven decisions to improve service quality.
Service Level Objective (SLO)	SLO stands for Service Level Objective. An SLO is a specific target or goal for a service's performance, usually based on one or more SLIs. It defines the level of performance that a Service Provider aims to achieve and maintain for a particular aspect of the service. SLOs are important for setting expectations with customers or users, and for providing a clear and measurable target for service improvement efforts.
SMPP	Short Message Peer to Peer Protocol.
SMS	Short Message Service as provided by Mobile Operators.
SMSC	Short Message Service Centre.
SPFC	Sender Policy Framework.
Term	The Term of the intended contract between SARS and the Service Provider.
USSD	USSD stands for "Unstructured Supplementary Service Data". In legal terms, it refers to a communication technology used by mobile network operators to send information between a mobile device and an application server, using a specific format and protocol. It is often used for mobile banking, prepaid recharge services,

Term	Meaning
	and other interactive applications.
VRF	Virtual Routing and Forwarding.
VPN	Virtual Private Network.
WASP	Wireless Application Service Provider.
WhatsApp	WhatsApp is a cross-platform instant messaging application that allows users to send text messages, voice messages, make voice and video calls, and share various types of media, such as photos and documents.

1.2. References to Other Documents in the RFI Pack

Underlined and italicised names are references (or short names) to other documents in the RFI Pack. The Bidder is referred to paragraph 3.2 of the _RFI Main Document_ for the table of documents and their shortened names.

1.3. Mandatory and Directory Requirements

Bidders are advised to read the business requirements as set out in this document with care. Where SARS has specified a mandatory requirement, (e.g. where the business requirement, by the context or presence of verbs such as "must", "will", "shall" etc., or by explicit instruction indicates that a requirement is mandatory), the Bidder must build and price its solution accordingly. Directory requirements are optional requirements that may improve a Bidder's score in the evaluation of its Proposal.

2. BACKGROUND

To achieve SARS's Vision 2024 of a smart, modern SARS with unquestionable integrity that is trusted and admired is of paramount importance. Pivotal to the delivery of SARS's vision are our digital platforms and technology infrastructure. To foster Strategic Objective 9, of building public trust and confidence, our technology assets have to demonstrate the highest levels of robustness and security. It is indeed for these reasons, inter alia, that SARS prioritises 99% uptime and zero security breaches from known risks. In support of this, the mandate is executed by partnering with third-party suppliers to provide services and products to achieve organisational objectives.

This tender for the Tower Infrastructure contracts for Towers D, V, and C is aligned with several of SARS's Strategic Objectives, including:

- Objective 1: Clarity and certainty for taxpayers and traders of their obligations.
- Objective 2: Make it easy for taxpayers and traders to comply with their obligations.
- Objective 5: Increase and expand the use of data within a comprehensive knowledge-management framework to ensure integrity, drive insight, and improve outcomes.
- Objective 6: Modernise our systems to provide digital and streamlined services.

The primary objective of this RFI is to provide for the delivery, continuity, and cost-effectiveness of SARS's Data Carrier (WAN), Voice Carrier, and Unified Communication Platform services.

SARS has sought to simplify the definition of the services by specifying the requirements, as far as possible, without specifying the detail of the underlying technologies. This approach puts greater emphasis on the agreed service levels, while allowing the Service Provider a certain freedom to configure the technology solutions in the most cost-effective manner. This approach is particularly evident in the requirements specification in Towers D, V, and C.

SARS's objectives in issuing this RFI do not include contracting for the transformation of the network to newer technologies. However, SARS's objective is to contract for services that will allow for the deployment of newer technologies that will improve quality and value for money in the delivery of the services. During the Term of the _Network Carrier and Infrastructure Services Agreement_, inevitable developments in carrier technologies, and service-based offerings, demand that SARS maintains a flexible approach in engaging Service Providers to ensure SARS can take advantage of such developments. This _Business Requirements Specification_ sets out, to the extent that it has currently been determined, the strategic direction SARS is taking regarding services in the Towers. In certain of the Towers, the strategic direction will affect volumes, distribution, and requirements for underlying technologies. These are presented for reasons of transparency to enable the Service Providers contracted to do so with knowledge of SARS's plans in this regard, although implementation of these plans is subject to approvals, budget, and capacity. The information presented in this document is to the best of the SARS's knowledge at the time of issuing this RFI. Flexibility, however, remains a key principle

regarding the directions presented, which may change during the Term.

3. COMPONENTS OF SCOPE

SARS has divided the scope of the tender into 3 (three) Towers of scope:

Tower D: Data Carrier Network Services.

Tower V: Voice Carrier Services.

Tower C: Unified Communication Platform as a Service.

The scope, as defined in each of the Towers above, may overlap. If an element of scope could be read within the definitions of more than one of the Towers, SARS, in its sole discretion, may choose to source such a common element of scope from any of the Service Providers who have been awarded Towers into which the common element of scope could be read. By electing to source such a common element of scope from a particular Service Provider, SARS is not bound to source such common element of scope from the same Service Provider on future occasions during the Term.

4. TECHNOLOGY SPECIFICATIONS

In defining the requirements in each of the Towers, reference may be made to specific technologies or specific products currently deployed in the SARS network. The Bidder must note the following:

- Where a specific technology has been specified as mandatory in this _Business Requirements Specification_, the Bidder's Proposal must be designed with that specific technology.

- Where no specific technology has been specified, the Bidder may propose any technology. The underlying assumption is, however, that the solutions must be based on the proven industry technologies, which SARS prefers.

In addition, during the Term of the envisaged agreement(s) arising from the award of this RFI, the use of alternative technologies may be proposed by the Service Provider and/or requested by SARS and their implementation will not be considered out of scope of the award, provided that they are cost effective and effectively substitute for technologies contained in the Service Provider's original Proposal. SARS's approval is required to implement alternative technologies during the Term. Where new technologies become available and present opportunities to improve availability, cost, or quality, SARS may request the migration to the newer technology, which will not be considered out of scope. Where SARS is unable to take advantage of newer technologies because of a Service Provider's unwillingness or inability to provide such, SARS will retain the right to substitute such elements of scope with services from a different Service Provider.

5. SERVICES COMMON TO ALL TOWERS

The services described in this paragraph 5 must be performed by Service Providers regardless of the Tower(s) for which they are delivering Services, unless otherwise specified.

5.1. Service Management

The Service Providers appointed in each of the Towers will be required to maintain standards of service management and conform to best practice in IT Service Management in their organisation when dealing with the following processes:

- Incidents management
- Problems management
- Change management
- Configuration management
- Service-level management
- Performance and capacity management
- Service-management reporting

An ISO certification (ISO 20000 — IT Service Management) must be held by the Service Provider or a formal IT Service Management Maturity Assessment report showing an overall organisational Maturity score of 4 (quantitively managed or equivalent) or higher.

The appointed Service Provider must have a well-established IT Service Management system/toolset that is automated to support the efficient and effective delivery of IT services to SARS. The automated system will have a ticketing and incident-management module that allows for the automated creation, assignment, and tracking of tickets, as well as automated notifications and escalation based on pre-defined rules.

The CMDB module should automatically keep track of the configuration items (CIs) in the IT infrastructure. The solution should allow for the automated creation, assessment, and approval of change requests. Furthermore, the automated system will have robust service-management reporting and analytics capabilities. It should generate automated reports and dashboards, providing insights into various ITSM metrics such as ticket volumes, resolution times, SLA compliance, and other performance indicators. This enables data-driven decision-making and helps identify areas for improvement.

The Service Provider must provide a 24x7 external web interface (e.g. a contact or service centre) for the reporting of incidents and problems and to provide status updates. The Service Providers are not required to interface directly with the SARS service-management system, nor are Service Providers required to receive requests, respond to incidents, or generally update records directly from the SARS service-management system.

The Service Provider will be expected to participate, provide information, and perform tasks as may be prescribed by the SARS PPS&G in terms of incident, problem, change, service-level, performance, and capacity management.

A key component of the Services is providing the functionality and access for SARS to monitor the delivery of the Services. The requirements for monitoring and reporting are discussed under the specification in each Tower for a Monitoring and Reporting Portal.

A further key component of the Services is the provision of functionality to enable SARS to place and track orders, access procedures, prices, etc. The detailed requirements for a Customer Provisioning Portal (Part of Services Portal) are discussed under the specification in each Tower.

5.1.2 Training

The Service Provider will be required to provide training, at no additional cost to SARS, on its monitoring systems, Monitoring and Reporting Portal, Services Portal, Customer Provisioning Portal, call logging procedures, etc., and offer any other training required by SARS for the integration of the Services.

5.1.3 Technical Support

As and when required by SARS, the Service Provider will be required to provide *ad hoc* technical support for the roll-out of projects, installations, upgrades, downgrades, moves, changes, and decommissions. The engagement of such technical support must be provided by the Service Provider and charged at the Personnel Rates submitted by the Service Provider in its *Tower x Pricing Response Template (where x is the applicable Tower reference)*.

5.1.4 Consulting

The Service Provider will be required to provide SARS with certain *ad hoc* advisory services related to the Services at no additional cost, including the availability and capabilities of new technologies and offerings by the Service Provider and generally in the market. Formal consulting assignments from Service Providers may be engaged by SARS from time to time. These will be undertaken on written authorisation by SARS and fixed rates as proposed by the Service Provider.

5.1.5 Technical Security Requirements

The Bidder's Proposal for Data Carrier Network Services must comply with best practices for enterprise Information Technology Security and the current SARS PPS&G. ISO certification (ISO 27001 — IT Security) must be held by the Service Provider during the Term.

5.1.6 Processes, Procedures, Schedules, and Work Practices

The Service Provider is required to execute the processes, procedures, schedules, and work practices developed in accordance with the *Network Carrier and Infrastructure Services Agreement*. Throughout the Term of the envisaged agreement, the Service Provider will be required to improve and modify the

processes, procedures, schedules, and work practices as required by SARS.

The Bidder must note the obligations to adhere to SARS PPS&G in _Network Carrier and Infrastructure Services Agreement_.

5.1.7 Service Level Requirements

It is of critical importance to SARS that the Service Provider must provide the Services to meet or exceed the Service Levels that are specified in Schedule C of _Network Carrier and Infrastructure Services Agreement_ and its Appendices. The Service Provider will be required to measure, monitor, and report on the delivery of the Services and the performance in terms of the Service Levels.

The Service Level requirements in each Tower are set out in the Tower-specific requirements specifications in paragraphs 6, 7, and 8 below. The methods of calculation, the Service Level Targets, and the provisions regarding Service Level Credits are set out in detail in Schedule C of the _Network Carrier and Infrastructure Services Agreement_.

Service Level definitions are generally made with reference to the SARS Site(s) to which a particular element of the Service applies. For example, the requirement for the service availability for Data Carrier Network services at a SARS Site will depend on the Service Coverage Period and the Service Level Class assigned to the SARS Site.

The Service Coverage Period assigned to a SARS Site is one of Basic, Standard, Extended, or Premium, and will always have the meaning set out in the following table, regardless of the Tower:

Service Coverage Period	Period Covered
Basic	06:00 to 19:00 on weekdays, regardless of whether the weekday falls on a public holiday.
Standard	06:00 to 21:00 on all days, including Saturdays, Sundays, and public holidays.
Extended	06:00 to 00:00 on all days, including Saturdays, Sundays, and public holidays.
Premium	24/7/365 (at all times).

The Service Level Class will be one of: Gold, Silver, or Bronze. The meaning attached to Gold, Silver, or Bronze is defined specifically for each of the services in the each of the Towers.

5.1.8 Service Provider Personnel

The Service Provider personnel-placement obligations specified in this subparagraph apply to all Towers.

The Service Provider must provide an Account Executive ("**Account Executive**") to maintain overall oversight of commercial and escalated operational issues. The Account Executive must hold a position with sufficient decision-making authority and standing in the Service Provider's organisation to represent any issues at the highest level in the Service Provider's organisation. The Service Provider Account Executive will be a member of the Key Service Provider Personnel (see Schedule A of _Network Carrier and Infrastructure Services Agreement_ for definition).

5.1.8.1 The Service Provider personnel-placement obligations specified in this subparagraph apply only to Towers D and V.

The Service Provider must provide a Service Delivery Manager ("**SDM**") who must maintain a presence online or at SARS's Head Office in Brooklyn, Pretoria. The Service Provider SDM will be a member of the Key Service Provider Personnel (see Schedule A of _Network Carrier and Infrastructure Services Agreement_ for definition).

The Service Provider must provide an Operations Manager ("**Operations Manager**") who must maintain a presence at SARS's Head Office in Brooklyn, Pretoria. SARS will make permanent office space available to the Service Provider Operations Manager. The Service Provider Operations Manager will be a member of the Key Service Provider Personnel (see Schedule A of _Network Carrier and Infrastructure Services Agreement_ for definition).

The Service Provider must provide a detailed scope of the responsibilities for the Operations Manager ("**Operations Manager**") and Service Delivery Manager ("**SDM**") from the Service Provider's perspective and must be maintained monthly as part of COT.

At least one the SDM and Operations Manager must be present on site at SARS during office hours (other than by arrangement with the relevant SARS Executive).

5.1.8.2 SARS requires the availability of Key Service Provider Personnel for regular meetings to be held at SARS's request at SARS premises. SARS may also request the presence of Key Service Provider Personnel at meetings at SARS premises given reasonable notice in the light of the urgency with which the subject matter of the meetings is to be addressed.

5.1.8.3 For Tower V, if awarded separately, then only an Operations Manager ("**Operations Manager**") is required to fulfil both roles of SDM and Operations Manager.

5.1.9 Transition

NB: The following requirements are common across the Towers. For transition timelines, refer to the relevant section for each Tower.

5.1.9.1 **Transition Plan**

The Service Provider is expected to provide a transition plan that contains key elements for a transition project to achieve a successful transition and minimise disruptions and compromised services to SARS. The transition plan for the appointed Service Provider should clearly elaborate on the following aspects of the transition plan:

- **Projects Phases**: Clearly stipulated stages of the transition project (e.g. Initiation, Planning, Execution, Monitoring, Closure).
- **Project Management**: The Project schedule for the transition process with scope, timelines, dependencies, milestones, and deliverables, based on the services provided in Tower D and showing a maximum transition period of 3 months. Recommendations for the Transformation timelines for the network are also required.
- **Defined Roles and Responsibilities:** To be defined between the appointed Service Provider, SARS, and outgoing Service Provider.
- **Risk management:** Management of identified risks and issues associated with the transition process and mitigation strategies.
- **Deployment Approach and Migration**: Clearly outline the deployment approach, implementation, and migration to move services to the appointed Service Provider and specify how downtime and disruptions will be minimised during the transition.
- **Training and Knowledge Transfer**: Outline the training approach and mechanisms of knowledge transfer.
- **Quality Assurance**: Approach and processes to reduce or eliminate errors or defects in the final outcomes of a project, and to establish standards, guidelines, and procedures to prevent quality issues and maintain the integrity of the product or service throughout its development.

5.1.9.2 Experienced Transition team

For the transition process, the appointed Service Provider is required to have a **multidisciplinary** transition team with experience in executing transition projects similar to the size of SARS's project. The different roles in the transition team structure should fulfil the following areas of expertise at a minimum, supported by relevant past experience:

- Transition Management
- Project Management
- Vendor and Contract Management
- IT Service Management
- Technical Subject Matter Experts

6. TOWER D: DATA CARRIER NETWORK SERVICES

6.1. **Scope**

The Data Carrier Network Services scope comprises the provision of a fully managed software-defined network-infrastructure platform that will make up the SARS Network serving all SARS Sites per the _SARS Site Classifications_. The sites to which the Data Carrier Network Services are delivered may be changed during the Term, and the scope may include new sites or may exclude SARS Sites that are currently

defined in the *SARS Site Classifications*. The scope also includes any other network-related links that may be required to any external Third Party, Cloud Provider, or Data Centre.

Out of the scope of this RFI is the responsibility for Campus LAN and Data Centre (SARS Enterprise Data Centres, Co-location Data Centre, and Cloud-based Data Centre) services. All equipment and communications within these services are managed by SARS (or by SARS's Managed Network Services Provider on its behalf). The provision and management of the Customer Premises Equipment ("**CPE**") is included in the Data Carrier Network Services scope to provide the interface between the SARS LAN and the WAN, excluding the physical cabling connection from the CPE to the SARS LAN environment.

The Data Carrier (WAN) Service Provider will be required to work and co-operate with SARS and its Managed Network Services Provider, if so determined by SARS, during transition and during the Term of the agreement.

Traditionally, SARS focused entirely on delivering a functionally efficient network, which meant delivering adequate bandwidth, redundancy, resiliency, and security. With no true disruption in business process or network technology, the network was sufficient to support basic business requirements. However, the introduction of Digital Business and IoT has forced SARS to redefine the role of the network to support the enterprise. The new strategically aligned network must provide a platform that supports agility, growth, flexibility, and speed of any deployed application or service required by SARS.

Concurrently, the enhanced network functionality must operate within an increasingly hostile IT/cybersecurity environment, the risks of which increase in proportion to the value of the data traversing the SARS network. SARS is exploring consumption-based models in the network space, to speed up digital transformation, reduce risk and capital costs, and enhance scalability.

SARS wants to consume network infrastructure through flexible operating-expense (OPEX) subscriptions, inclusive of hardware, software, management tools, licenses, and lifecycle services.

SARS's requirements for Data Carrier Network Services include the following:

- **Network as a Service (NaaS):** Provide SARS with network infrastructure hardware, software, services, management, and licensing components consumed in a subscription-based or flexible consumption model. These services include:

  i.   SD-WAN
  ii.   SASE
  iii. External/Public Network Connectivity
  iv.   Private Network Connectivity

- **Edge Networking Service:** Provide SARS with robust private networks to support data transfer and enable real-time capabilities at specific Border Post sites, airports, and harbours. The solution should combine ultra-low latency, high-bandwidth connections between edge devices and the SARS infrastructure or Cloud.

- **Digital Experience Monitoring:** Provide SARS with a solution to monitor and measure the quality of its digital experience while interacting with various applications, services, and websites. It must track and analyse multiple data points to gain insight into how SARS users perceive and interact with digital assets.

- **Mobile Network Service:** Provide SARS with a corporate or private Access Point Name (APN) solution for SARS's mobile network connectivity requirements.

- **Services Portal:** Provide SARS with an intuitive web-based interface to navigate and explore information and deep insights provided by the capability of the Service Provider's services platform, across the extensive range of services including dynamic-monitoring functionality, and with historical trend reports. The Services Portal must include a Customer Provisioning Portal to facilitate the ordering, upgrading, downgrading, and cancellation of circuits, status-tracking of an order, cost of an order, together with a history reporting of all orders made.

6.2.   **Current Delivery Model**

SARS currently engages a single Service Provider to provide Data Carrier Service which is directly managed by SARS.

The current list of technologies is described in the documents below:

- SDWAN network as listed in *SDWAN Diagram*.
- WAN as listed in *WAN Inventory and WAN Diagram*.
- Monitoring and reporting portal.
- Customer Provisioning Portal.

6.3. Required Delivery Model

6.3.1 Accountability

SARS requires a single Service Provider to be accountable for its Data Carrier Network Services, including all carrier elements underpinning SARS's WAN. SARS does not require the Service Provider to provide all the Data Carrier Network Services itself and the Service Provider may source different elements of the Data Carrier Network Services from other Service Providers, provided that the Service Provider manages the provision of the individual elements in a seamless manner from SARS's perspective and takes full accountability for all aspects of the services, including meeting the Service Levels. However, the Service Provider must ensure that penalties related to third-party infrastructure are handed down to the sourced Service Provider. Third-Party infrastructure providers must be held accountable for poor service delivery and unstable infrastructure.

The Service Provider must supply all elements of the Data Carrier (NaaS [SD-WAN / SASE] and Edge Networking Service) to SARS in the Service Provider's name. The Bidder must not propose a solution in any part of its Data Carrier Network Services Proposal that is contingent on SARS's granting the Bidder an agency in order for it to procure elements of the solution from a Third Party in SARS's name.

6.3.2 Non-Exclusivity

SARS intends to contract for the different areas of scope with a Service Provider on the following basis:

Service Component	Contracting Basis
SD-WAN SASE	SARS intends to procure all its NaaS service requirements for the network from a single Service Provider to all SARS Sites.
Private IP Network Connectivity	SARS reserves its rights to procure Private IP Network Connectivity circuits, other than such services making up part of its core WAN network, from any Service Provider.
Edge Networking Service	Although SARS intends to procure all its requirements from the Service Provider, SARS reserves its rights to procure alternative, equivalent, or better technologies from other Service Providers.
Satellite circuits	SARS reserves its rights to procure Satellite circuit services from any Service Provider.
Mobile Network Service	SARS reserves its rights to procure Mobile Services from any Service Provider.
Underlying Infrastructure	Although SARS intends to procure all its requirements from the Service Provider, SARS reserves its rights to procure alternative, equivalent, or better technologies from other Service Providers.

In general, SARS will retain the right to source Data Carrier Network Services from other Service Providers during the Term.

6.3.3 Technical Transformation

The Bidder must supply a complete technical transformation plan to migrate SARS's current MPLS and SD-WAN (Cisco Meraki and Secure Connect based) architecture, Third-Party connections, mobile trucks, mobile cases, and VSAT connectivity to the Service Provider's network.

The Bidder must take note that SARS has transformed 58 access sites from the current MPLS network to the SD-WAN platform. The Service Provider will be expected to take over this part of the network during the transition period.

The transformation project is expected to take from 8 to 12 months. The Service Provider must comply

with the following timelines:

- Installation at Brooklyn Head Office, Pretoria, of WAN connectivity to the Service Provider's network, 2 high speed links, 10Gb/s in capacity (3 months). Thereafter, the below services as stated within the time-periods below, with some being executed in parallel:

  o Migration of 58 x SDWAN branches including Cloud Hub Site (12–18 months).
  o Migration of 110 campus sites, branches, and border posts including backup links (8–12 months).
  o Migration of 10 VSAT sites and 19 Mobile Tax Units also on VSAT (3 months).
  o Migration of 2 Metro Ethernet P2P Circuits and Metro Ethernet Circuits (3 Months).
  o Migration of 56 x Third-Party Links (3 months).
  o Migration of 950 Remote WFH Workers (3 months), predominately "Fixed LTE"–based.
  o Migration of 130 Mobile Suitcases (3 months), GSM-based.

The Bidder should note that during the Term of the agreement, SARS will improve its Data Carrier Network Services in terms of reliability, speed, capacity (including bandwidth on demand), and cost. Capacity and footprint (# of sites) are expected to grow further during the term to support SARS's Digital Strategy.

On request by SARS, the Service Provider must implement:

- Connectivity to new sites and temporary locations;

- The upgrading, downgrading, or cancellation of existing circuits;

- Back-up/redundant circuits. Typically, this would be to implement diverse physical routing; enable use of alternative communication media; or engage a different network operator's physical infrastructure; and/or

- Alternative technology-solution proposals that have been made at the Service Provider's initiative with SARS's approval.

6.4. Detailed Requirements for Data Carrier Network Services

The bidders must take note of the following when designing and proposing their solutions:

6.4.1 Network as a Service

SARS has adopted the following characteristics of NaaS to be incorporated in the Service Provider's service offering:

- **On-demand self-service**: Automatically provision network functions and services without any human intervention from the Service Provider.

- **Network agnostic**: Service offerings and service requests must be abstracted, so network implementation can be configured any number of ways, even across multiple providers.

- **High resource availability**: NaaS services must be intent-based, with location-specific performance characteristics such as low latency or the ability to attach to resources such as mobile devices.

- **Measurement**: Network systems must automatically control and optimise resource use through metering and measurement, with transparent reporting to SARS.

- **Assurance**: Network functions and services will be defined with service-level agreements (SLAs) or service performance metrics, as stipulated by SARS.

The following features and requirements must be included in the NaaS solution:

Functional Requirements

- **Network Provisioning:** The solution must enable SARS to provision and manage the network dynamically, with the ability to add or remove network resources as needed.

- **Network Monitoring.** The solution must provide SARS with real-time monitoring and reporting of network performance, including bandwidth utilisation, latency, and packet loss.

- **IT Security:** The solution must provide secure network access through a range of security features, including firewalls, intrusion-detection and prevention, and encryption; the solution must integrate with the SARS QRadar SIEM to provide full visibility to the SARS SOC.

- **Quality of Service:** The solution must provide SARS with the ability to prioritise traffic flows and ensure that network resources are allocated according to SARS's requirements.

- **Integration:** The solution must be easily integrated with other cloud services, such as compute and storage services, to provide a complete cloud solution for SARS.

Non-Functional Requirements

- **Performance:** The solution must be highly scalable, with the ability to handle large volumes of network traffic and support a high number of concurrent users.

- **Availability:** The solution must be highly available, with the ability to provide uninterrupted service to SARS.

- **IT Security:** The solution must meet industry-standard security requirements and be compliant with relevant regulations and standards.

- **Usability:** The solution must be easy to use and manage, with a user-friendly interface and comprehensive documentation.

- **Support:** The solution must provide SARS with 24/7 technical support, including troubleshooting and resolution of any issues that arise.

Technical Requirements

- **Network Infrastructure:** The solution must be built on a robust network infrastructure, with high- speed connectivity, redundancy, and failover capabilities.

- **Software Stack:** The solution must be built on a scalable and flexible software stack that enables easy integration with other cloud services.

- **API Integration:** The solution must provide APIs that enable SARS to easily integrate the service with its existing infrastructure.

- **Platform Compatibility:** The solution must be compatible with a range of platforms, including desktop and mobile devices, and support a range of operating systems.

6.4.1.1 SD-WAN

SARS is in the process to migrate the current MPLS network to a more cost-effective underlay network, which will include internet broadband, fibre, wireless, LTE, and any similar physical network infrastructure. A managed SD-WAN service is then required as a virtual overlay.

It is important to note that SARS has selected Cisco Meraki as the preferred vendor and solution for all SD-WAN components of the network infrastructure. All proposed services and solutions must be based on the mentioned OEM.

The following SD-WAN features must be included as part of the overall NaaS solution and specific requirements by SARS:

- **Scalability:** The solution must be able to scale up or down quickly to accommodate changes in network traffic and business growth.

- **IT Security:** The solution must have robust security features to protect against cyber threats such as malware, ransomware, and phishing attacks. It must also provide encryption for data in transit and must integrate with existing security controls.

- **Reliability:** The solution must provide high availability and reliable connectivity to ensure business continuity.

- **QoS:** The solution must provide Quality of Service (QoS) features to prioritise mission-critical traffic, such as VoIP and video conferencing, over less important traffic.

- **Centralised Management:** The solution must provide a centralised management console to manage the SD-WAN deployment and to monitor and troubleshoot network performance.

- **Flexibility:** The Solution must be flexible enough to support multiple connectivity options, such as MPLS, broadband, LTE, and 5G.

- **Cost Effective:** The solution must provide cost savings over traditional WAN solutions, such as MPLS, while still providing the required performance and reliability

- **Compatibility:** The solution must be compatible with the existing SARS network infrastructure and able to integrate with other networking and security solutions.

- **Analytics and Reporting:** The solution must provide comprehensive analytics and reporting capabilities to monitor network performance and identify trends and issues.

- **Deployment Options:** The solution must provide deployment options, such as cloud-based, on-premises, or hybrid, to suit SARS's specific needs and requirements.

6.4.1.1.1 Satellite Circuits

SARS utilises satellite services for connectivity to remote and temporary mobile sites and for alternative-medium redundancy. The requirement is for the Service Provider to integrate these satellite circuits into the SD-WAN architecture to provide connectivity in remote locations where traditional terrestrial networks may be limited or unavailable. The Service Provider must deliver the required SD-WAN technology as an overlay service, which will allow for intelligent management and routing of network traffic over multiple transport technologies, including satellite links.

The Service Provider must provide a proposal to take over the management of existing satellite circuits, which include circuit management, monitoring, and maintenance. See _VSAT Site List_ and _VSAT Diagrams_ document for further details.

The Service Provider must also provide a workable alternative solution for the existing satellite sites, based on the result of a site survey conducted. This is a requirement, as this technology no longer provides sufficient bandwidth and network speed needed to support SARS's business applications.

6.4.1.1.2 SASE

A well-architected SASE solution is a further important requirement. SARS requires the services of a single-vendor SASE offering to deliver a converged network and security capability to connect and secure distributed users, devices, and locations to resources in the cloud, edge, and on-premises.

The Service Provider must be able to deliver the SASE services via an operational platform that enable API-level integration of all software and physical components, as well as any external Third-Party providers. This platform should expose the integrated service to SARS via an online portal that displays all service aspects as well as offers co-management options, with levels of engagement supported by the Service Provider from fully managed to co-managed.

This technology must fulfil the need to deliver security across the entire SARS network landscape. To secure all elements of the network, the following SASE components must be included:

6.4.1.1.3 Cloud Security (SASE)

i. DNS-layer Security

ii.   Secure-web gateway

iii.   Cloud-delivered firewall

iv.   Cloud access security broker

v.   Data-loss prevention

vi.   Integration with the SARS QRadar SIEM

6.4.1.1.4 Zero Trust Network Access

The following business requirements are important and must be included as part of the SASE solution:

i.   **IT Security:** The solution must provide a comprehensive set of security features to protect SARS against various threats, including malware, ransomware, and phishing attacks. It must also support a wide range of security protocols and standards, such as SSL, IPSec, and DNSSEC, and must integrate with the SARS QRadar SIEM.

ii.   **Performance:** The solution must provide high performance and low latency, enabling fast access to cloud applications and services. It must also support Quality of Service (QoS) mechanisms to ensure that critical applications receive the necessary bandwidth and priority.

iii.   **Scalability:** The solution must be able to scale up or down to meet the changing needs of SARS. It must support a large number of users, devices, and applications, without compromising performance or security.

iv.   **Flexibility:** The solution must be flexible enough to support a variety of deployment models, including public cloud, private cloud, and hybrid cloud. It must also support a variety of endpoints, including laptops, mobile devices, and IoT devices.

v.   **Cost-effectiveness:** The solution must be cost-effective and provide a predictable pricing model that aligns with SARS's usage patterns. It must also provide a low total cost of ownership (TCO) by reducing the need for on-premises hardware and software.

vi.   **Compliance:** The solution must comply with various regulatory and compliance requirements. This will include the POPIA act, the Cybercrimes Act, as well as international acts such as GDPR, and PCI DSS. It must also provide audit trails and reporting capabilities to help demonstrate compliance.

vii.   **Ease of management:** The solution must be easy to manage and maintain, with a centralised management console that enables administrators to configure, monitor, and troubleshoot the network from a single location. It should also provide automated provisioning and self-service capabilities to reduce the burden on SARS IT staff.

viii.   **Support:** The solution must provide comprehensive support, including 24/7 technical support, training, and documentation. It must also provide a community forum where users can share knowledge and best practices.

6.4.1.2 External/Public Network Connectivity

This section deals with the provisioning, management, and support of network services required to connect Third Parties to SARS. The network services should enable SARS to connect to its Third-Party providers, hyper-scalers, cloud providers, and any co-location facility. The network connectivity must include Layer 2 and/or Layer 3 options and not be limited to a specific technology.

6.4.1.2.1 Third-Party Circuits

SARS uses virtual MPLS circuits from the incumbent Service Provider's network for connectivity to Third Parties. These circuits terminate in the DMZ at the Brooklyn Data Centre. Several third-party circuits terminate at the incumbent Service Provider and are then routed via a VRF to SARS Brooklyn. See *Third-Party Circuits* document for

further details.

The requirement is to provide this service via the External/Public Network Connectivity Service.

The External/Public Network Connectivity Service solution must provide:

i.   Cost-effective, stable, and reliable technologies.
ii.   High-speed with low latencies.
iii. Flexible bandwidth options ranging from 1 Mbps to 1 000 Mbps and 10 Gbps
iv.   Synchronous 1:1 contention ratio with no shaping, throttling, or bottlenecks. (backbone network being oversubscribed).
v.   Interoperability with existing technologies and hardware vendors currently being used by SARS.
vi.   E-Line Service (point-to-point) and E-LAN Service (multipoint-to-multipoint) supported technologies.
vii. IEEE 802.1Q support for VLANs.
viii. Copper RJ45 and fibre SFP options available for hand-off.
ix.   Proactive network monitoring with a 24/7 service desk.

6.4.1.2.2 Private Network Connectivity Service

Private network connectivity refers to a specific need and service that SARS requires to establish and maintain private network connections.

SARS uses private network connectivity to establish secure and exclusive network connections for its internal communication and data exchange, which includes:

- Interoffice Connectivity: Communication to large branch and campus locations. This allows for seamless communication, file sharing, and collaboration between different SARS sites.

- Data Centre Connectivity: Communication to data centres to provide dedicated and high-speed connectivity between servers, storage systems, and other critical infrastructure components.

The Service Provider must deliver a Private Network service, based on the following requirements:

i.   IT Security: Ensuring the network connection is highly secure and protected against unauthorised access and data breaches.

ii.   Reliability: Having a reliable and stable network connection that minimizes downtime and ensures uninterrupted operations.

iii. Performance: Requiring high-speed and low-latency connectivity to support bandwidth-intensive applications, real-time communication, and data transfer.

iv.   Scalability: Allowing for flexible network expansion and the ability to accommodate SARS's growing business needs, such as adding new locations or increasing user capacity.

v.   Cost-effectiveness: Optimising network connectivity costs while meeting the desired performance and reliability levels.

vi.   Redundancy: Implementing redundant network connections or backup options to maintain connectivity in case of primary connection failures.

6.4.2 Edge Networking Service

The Service Provider must deliver reliable, real-time experiences through Edge Networking as a Service, which must include:

i.   Reliable, custom-built networks which enable ultra-low latency and ultra-high bandwidth needed for real-time data processing.

ii.   Management of IoT operational aspects to deliver improved productivity while ensuring the environment remains secure.

iii.   Moving data processing and storage closer to the connected edge to enable real-time decision-making and automation.

iv.   Management of underlying infrastructure along with managed services to optimise performance.

6.4.2.1   Private 5G

The Service Provider must provide a reliable, high-bandwidth, and low-latency private 5G solution, with the ability to support multiple enterprise use-cases on a single network. SARS requires the Service Provider to comply with the following minimum requirements:

- **Reliability:** Must provide Ultra Reliable Low Latency Communication (URLLC), capacity, adequate network coverage, and robust handover functionality to improve reliability in transmitting data traffic in terms of fixed duration and volume.

- **High Availability:** Must ensure maximum availability to SARS applications through a robust solution.

- **Security:** Must ensure complete end-to-end security and privacy for infrastructure, data, and SARS endpoints from any threats.

- **Interworking/interoperability:** Integration with SARS corporate network to ensure service continuity for mission-critical applications.

6.4.3   Mobile Network Service

SARS requires the Service Provider to provide a mobile network to connect devices to the Internet. This mobile capability must be delivered via a corporate/private APN solution. The APN connectivity must support 5G and LTE as a minimum.

The following business requirements must be addressed as part of the Mobile APN solution:

i.   **Secure Connectivity:** The APN must provide a secure connection between SARS mobile devices and the corporate network or the internet. This may involve implementing encryption protocols and firewall protection to safeguard data transmission.

ii.   **Reliability:** The APN must offer reliable and consistent connectivity, ensuring that SARS mobile devices can access the internet or corporate resources without frequent disruptions or downtime.

iii.   **Quality of Service (QoS):** Depending on SARS's business needs, the APN may need to prioritise certain types of traffic, such as video conferencing or real-time data transmission, to ensure a consistent and high-quality user experience.

iv.   **Scalability:** The APN must be scalable to accommodate the growing number of SARS mobile devices and the increasing data-traffic demands of SARS. It must support the addition of new devices without compromising performance.

v.   **Cost-effectiveness:** The APN solution must be cost-effective, providing a balance between the required functionality and the associated expenses.

vi.   **Mobile Device Management (MDM) Integration:** SARS requires centralised management of its mobile devices. The APN solution must be compatible with Mobile Device Management solutions, allowing SARS IT administrators to control device settings, enforce policies, and ensure security.

vii.   **Roaming Capabilities:** The APN must support roaming capabilities, enabling seamless connectivity across different mobile networks, especially in areas with limited network coverage.

viii. **Compliance and Regulatory Requirements:** The APN must comply with relevant regulations and industry standards regarding data privacy, security, and network usage in the South African context.

ix. **Monitoring and Analytics:** The APN must provide monitoring and analytics capabilities to track network performance, usage patterns, and troubleshoot any connectivity issues.

x. **Support and Maintenance:** The APN solution must include adequate technical support and maintenance services to resolve any issues promptly and ensure the smooth operation of the network.

6.4.4 Digital Experience Monitoring (DES)

SARS requires the Service Provider to provide a digital experience and intelligence platform that provides real-time insight into the performance of the network infrastructure, applications, and services. Its capabilities must include network, internet and cloud-monitoring, and insight into the state of the underlying internet infrastructure. Services must include BGP Monitoring, Path Visualisation, Network Metrics, HTTP Server tests, and App Experience tests.

The following requirements must be met:

i. **Network Performance Monitoring**: Real-time visibility into network performance, including latency, packet loss, and bandwidth utilisation. Identify the specific metrics and insights required to monitor and troubleshoot network issues proactively.

ii. **Cloud and Internet Monitoring**: Monitor the performance and connectivity of cloud-based applications and services, as well as the ability to monitor internet Service Providers (ISPs) and external network paths.

iii. **Alerting and Reporting**: Automated alerts and notifications based on predefined thresholds or events. Consider the types of reports and analytics that are needed to gain insights into network performance trends, troubleshoot issues, and make data-driven decisions.

iv. **Integration and Scalability**: Compatibility and integration requirements with existing network infrastructure, management systems, or other monitoring tools.

v. **Training and Support**: Training and support services to ensure effective implementation and ongoing management of the DES solution.

vi. **Compliance and Regulatory Requirements**: Specific compliance or regulatory requirements that must be fulfilled, such as data privacy, industry-specific regulations, or audit trails.

6.4.5 Network Services Portal

The Network Services Portal must be a web-based platform designed to provide network-related services to SARS. The platform must offer a range of services, including network design, installation, configuration, monitoring, and maintenance. The portal must be accessible and user-friendly, with a simple and intuitive interface.

The Network Services Portal must provide the following services:

i. **Network design:** The platform must provide SARS with access to a team of expert network designers who must help them design a customised network solution based on their requirements and budget.

ii. **Installation and configuration:** The platform must offer SARS installation and configuration services for network hardware and software, including routers, switches, firewalls, and other devices.

iii. **Monitoring and maintenance:** The platform must provide SARS with real-time monitoring of its network performance and offer maintenance services to ensure the network is running smoothly and efficiently.

iv. **Support:** The platform must offer SARS 24/7 support from a team of expert network professionals.

The Network Services Portal must have the following functional requirements:

i. **User registration and authentication:** SARS users must be able to create an account on the platform and authenticate themselves to access the services.

ii. **Network design:** SARS users must be able to submit their requirements for network design and receive a customised network solution.

iii. **Installation and configuration:** SARS users must be able to request installation and configuration services for their network devices.

iv. **Monitoring and maintenance:** The platform must provide real-time monitoring of network performance and offer maintenance services.

v. **Support:** The platform must provide 24/7 support to SARS technical staff via phone, email, or chat.

vi. **Payment:** The platform must allow SARS authorised staff to make payments for services rendered.

The Network Services Portal must have the following non-functional requirements:

i. **IT Security:** The platform must ensure the confidentiality, integrity, and availability of user data and transactions.

ii. **Scalability:** The platform must be able to handle many users and provide services without any performance degradation.

iii. **Reliability:** The platform must be available 24/7 and provide reliable services to SARS.

iv. **Usability:** The platform must be user-friendly and provide a simple and intuitive interface.

v. **Compatibility:** The platform must be compatible with a wide range of devices and web browsers.

The following assumptions and dependencies must be considered:

i. The platform must be hosted on a cloud-based infrastructure.

ii. The platform must use industry-standard security protocols to ensure data confidentiality and integrity.

iii. The platform must be compatible with a wide range of devices and web browsers.

6.4.6 Customer Provisioning Portal

The Bidder's Proposal should include a Customer Provisioning Portal which provides the following functionality and information to SARS through a secure internet portal:

- Pricing of new installations, upgrades, downgrades and transfers of circuits.
- Ability to request a new installation, upgrade, downgrade, transfer, or cancellation of a circuit.
- Request a change in the assignments of Service Levels or service-coverage periods to SARS sites.
- List of active Projects and up-to-date status.
- Decommissioning/cancellation.
- Order tracking (including Third-Party orders).

Reporting on a full order history for all orders placed during the Term including the following information:

- Date of placement of order
- Date of fulfilment of order
- Details of order
- Price of order
- Price of component increase/decrease
- Tracking and reporting on variances from the original Proposal configuration

The Bidder is required to provide details of its current capability to deliver the requirements as set out above as well as details of its plan, including timelines, to which the Bidder is prepared to commit to implement the full functionality as set out above. Although it is not a requirement that the Bidder must currently possess the capability to provide all the specified functionality, it is a mandatory requirement

that the Customer Provisioning Portal is operational before the Commencement Date.

6.4.7 Service Levels Required

The Data Carrier Service Provider must provide a highly available wide-area network with solutions as described above. SARS's requirement is for network services to be provided at all SARS Sites at the bandwidth as specified in *SARS Site Classifications*.

SARS prefers to hold the Service Provider accountable for the availability of the Data Carrier Network service to a SARS site as opposed to accountability at an individual circuit level. Because SARS's network requirements span centrally located sites in metropolitan areas to remote border posts, the differences between the technologies that are available in these extremes mean that SARS has had to adopt an approach that is appropriate and reasonable under the different circumstances.

For sites ("Platinum sites") where reliable technologies are abundantly available such as in metropolitan areas, SARS requires that the Service Provider take responsibility for fully redundant connectivity. The redundant circuits must actively participate in the connectivity, even under normal conditions, and failover must be seamless in the event of an incident. There must be no single point of failure in the carrier design (**underlay**) and the service (**overlay**) level at Platinum sites must anticipate that there is never any carrier downtime. For any SD-WAN site, "Platinum Service Level" will apply by default unless otherwise directed by SARS.

For sites not classified as Platinum, SARS still requires that circuit level redundancy (a primary and a secondary circuit) be provided, but the secondary link need not actively participate in the network at all times. The secondary circuit must be tested regularly, at least monthly, and failover to the backup link must be made near-real-time through an automated process. The service levels (defined below for each of the technologies) will apply to the individual circuits (Gold, Silver, or Bronze). Failover must occur in the event that the primary link is unavailable, unreliable, or is experiencing issues such as poor quality, response problems, when error rates exceed specified thresholds, or generally any condition limiting the WAN service to less than that which is expected, including not meeting service levels.

The list of SARS Sites in *SARS Site Classifications* indicates whether a Platinum service level is required for a site. During the term, SARS may convert a SARS Site for which only circuit-level Service Levels have been specified to a Platinum Service Level as the base technologies become available. On request by SARS, the pricing for a site-level Service Level must be proposed by the Service Provider to SARS, who may accept or reject the proposal.

SARS's standard for networking equipment is CISCO and SARS's preference is to maintain this standard for all equipment interfacing directly with SARS's onsite equipment.

6.4.7.1 Platinum Service Level

Given the requirement that a Platinum SARS Site has active redundant WAN circuits and that the core network is highly available, the requirement for availability of a Platinum site is 24/7. The WAN availability must be measured to the CPE router and excludes any period of WAN unavailability due to site environmental factors (e.g. power). The Service Provider is responsible for configuring WAN circuits to the site to meet the Platinum Service Levels for sites.

Service Level Class	Maximum Cumulative WAN Unscheduled Unavailability at the Site
Platinum	0 hours

6.4.7.2 Non-Platinum Site Service Level

The requirements set out for individual circuit technologies define the service levels for circuits at non-Platinum sites. Where a Platinum service level has been specified for a SARS Site, the individual WAN circuits to that site are not subject to service-level availability measures. Circuits providing connectivity from Platinum sites to non-Platinum sites will be subject to service levels at the circuit level.

6.4.7.3 Network as a Service (NaaS) Service Level

6.4.7.3.1 SD-WAN (Current MPLS)

The Service Level Class and Service Coverage Period assigned to the proposed SD-WAN circuits must be the Service Level Class and Service Coverage Periods assigned to the SARS Site. If a circuit connects two SARS sites, the Service Level Class and Service Coverage Period that apply to the circuit will be the lower (less strict) of the two SARS sites it connects. The required availability of the SD-WAN circuits will be measured only during the Service Coverage Period.

Service Level Class	Cumulative Monthly Site Unavailability
Bronze	8 hours
Silver	4 hours
Gold	2 hours
Platinum	0 hours

6.4.7.4   External/Public Network Connectivity Service

The Service Level Class and Service Coverage Period assigned to an External/Public Network Connectivity Service will be the Service Level Class and Service Coverage Periods assigned to the SARS Site. The required availability of the circuits will be measured only during the Service Coverage Period.

Service Level Class	Maximum Cumulative Monthly Circuit Unscheduled Unavailability
Bronze	8 hours
Silver	4 hours
Gold	2 hours

6.4.7.5   Private Network Connectivity Service

The Service Level Class and Service Coverage Period assigned to a Private Network Connectivity Service will be the Service Level Class and Service Coverage Periods assigned to the SARS Site. The required availability of the circuits will be measured only during the Service Coverage Period.

Service Level Class	Maximum Cumulative Monthly Circuit Unscheduled Unavailability
Bronze	8 hours
Silver	4 hours
Gold	2 hours

6.4.8   **Monitoring**

The Service Provider must actively monitor the status of all components of the Data Carrier Network Services. If an incident affects, or is likely to affect, any component of the Data Carrier Network Services, the Service Provider must proactively ensure that the event is logged in the SARS service-management system, diagnose the event, establish the necessary actions to restore Services, and begin and complete restoration activities. The Service Provider must proactively inform SARS or a party nominated by SARS and keep such party up to date regarding the progress in the detection, diagnosis, and repair events.

For SARS's monitoring purposes, SARS requires the SNMP community strings (read-only access) within the Service Provider's network related to the SARS network. For clarity, SARS requires read access to all Service Provider equipment (routers) that deliver connectivity to SARS Sites to verify that the services are being delivered in accordance with the Agreement, in terms of availability, performance, and capacity.

The Service Provider will be required, at SARS's discretion, to maintain a presence in the SARS Network Operations Centre. The Service Provider's personnel will form part of the SARS monitoring team and (a) will be required to help identify, diagnose, and resolve incidents involving, or related to, the Tower D services, including logging and updating incident and problem records on SARS's service management-system. (b) The Service Provider must be the interface point for communication and escalation. This will not be required as part of the base services and will be separately priced as an optional service.

6.4.9 Integration with the Tower V (Voice Carrier) Service Provider(s)

Internal voice traffic (see Tower V) includes the carriage of internal traffic and external traffic to and from centralised break-out points at the Alberton Campus and the Doringkloof Campus over VoIP. The data network (underlay) for the carriage of internal voice traffic must and will be provided by the Tower D provider.

6.5. Transition

6.5.1 Timelines

The Service Provider(s) appointed in Tower D must complete the Transition Services within a **3-month period** from the time of the award and finalisation of the contract. By this time, the Service Provider must have assumed full management responsibility for the full scope of Data Carrier Network Services. In addition to any other commitment required in the *Network Carrier and Infrastructure Services Agreement*, the Service Provider must have:

- Fully designed, developed, and implemented the processes, procedures, schedules, and work practices detailed in *Network Carrier and Infrastructure Services Agreement*, especially those detailed in Schedule B-D and its attachments.

- Committed to reporting and meeting Service Levels as set out in Schedule C-D.

- Developed and established the necessary interfaces with other SARS Service Providers required to deliver Data Carrier Network Services.

- Taken over the management of Data Carrier Network Services that are sourced through Third Parties.

- Attended any training specified by SARS to understand the SARS environment, systems, and operating procedures.

- Developed and implemented the Services Portal, which includes the Customer Provisioning Portal.

6.5.2 Transition Expectations and Constraints

Pricing for transition must include all activities the successful Service Provider will need to undertake to meet all the requirements of this Business Requirements Specification, including the activities to take over from the incumbent Service Provider. The current Service Provider is contracted to perform handover activities to the Service Provider.

7. TOWER V: VOICE CARRIER SERVICES

7.1. Scope

The Voice Carrier Services scope comprises the provision of the following:

- Underlying communication technologies that enable SARS's inbound and outbound voice communications at an acceptable quality at the lowest possible cost.

Functional Requirements

- Hosted voice services, such as hosted phones or VaaS (Voice as a Service).

Sars has currently provisioned 13500 users on the MS Teams Phone Platform. The winning Bidder must be able to provide a Hosted Direct Routing solution which will be SBC's. Microsoft Teams licences are out of scope because SARS is already licenced with E5 licences that include Microsoft Teams Phone.
- The Bidders in Tower V must supply a proposal for a Contact Centre as a Service that will support 1 000 agents with integration into Microsoft Teams.

Monitoring and Reporting Portal

- Onsite Voice Services (IP or IP-enabled PABXs and Cisco Call Manager), IP telephony, cabling, handsets, headsets, teleconferencing equipment) are out of the Tower V scope. These onsite voice services are managed by SARS, or the Managed Network Services provider on behalf of SARS.

- If determined by SARS, the Service Provider(s) in Tower V will be required to work with SARS's Network Service provider during transition and during the Term.

- The Tower V scope includes the responsibility for connecting the Service Provider's onsite termination equipment to the onsite voice gateways.

7.2. Current Delivery Model

7.2.1 Outbound Calls from SARS Sites

SARS currently routes all its outbound calls to fixed-line and mobile operators via two Service Providers' external VoIP network, depending on least-cost routing, volumes, and voice quality.

The physical infrastructure to carry the calls is over SIP trunks via Alberton Campus and Doringkloof for all branches and border posts, and via Brooklyn for QA and Contact Centre application testing. There are currently 2 CLIs that go out via outbound dialling, a 012 number from DRK, and 010 number from Alberton.

For all the other SARS branches, voice communications are provisioned in a separate VRF on the same last miles as data communications, except for the new SDWAN sites.

7.2.2 Inbound Calls to SARS Sites

Inbound voice calls to SARS's numbers are carried over SIP Trunks at Alberton Campus and Doringkloof. All calls from SARS's toll-free number are routed inbound via these SIP Trunks. The SIP Trunk solution design is based on a peering Session Initiated Protocol–Network to Network Interface (SIP:NNI). The SIP Trunk solution provides for the connection of an IP PBX telephony system to the third-party network over a managed IP-access link. A single SIP Trunk supports a minimum of 30 concurrent voice SIP sessions (voice channels) for the origination and termination of voice calls.

The current SIP Trunks support the following features:

- Telephony services (using a G.729 codec)
- G2, G3, and G4 Fax (T.38)
- Direct dialling inward (DDI)
- Direct dialling outward (DDO)
- Caller line identification presentation (CLIP)
- Caller line identification restriction (CLIR)
- Call forward
- Number barring

The bandwidth required across the access link is determined by the number of concurrent voice and fax calls. The provisioned bandwidth per session (or channel) for voice calls is 20 kbps

The VoIP Connect SIP Trunk solution at Alberton and Doringkloof is fully redundant with Premium support 24/7/365. Two standalone production sites with identical configuration are at Alberton and Doringkloof, with 1 860 concurrent SIP-session capacity per site and support for the G.729 Codec.

Two standalone test sites with identical configuration are in Brooklyn, with 30 concurrent SIP-session capacity per site, also supporting the G.729 Codec.

Each SBC has its own set of IP addresses and routing. The virtual ASR SBC is configured to the Third-Party SBC.

The SIP Trunk solution comes with its own SBC load balancer that balances the voice calls. There was a need to add an additional load balancer (F5) that handles the failover of agents and calls between the 2 stacks.

7.3. Required Delivery Model

7.3.1 Requirement Overview

SARS's objective is to award the scope of Tower V to separate Service Providers subject to ongoing achievement of the lowest cost for calls at acceptable quality. SARS therefore retains the right to award certain parts of the scope (e.g. certain outbound call types and certain call destinations) to other voice-carrier providers. On an annual basis, Preferred Inbound Carrier Provider and the Preferred Outbound Carrier Provider(s) must provide pricing for all SARS's inbound and outbound call destination classes (e.g. international, national, local, mobile operator). SARS will update its call-routing strategy to the Service Provider's specifications based on the best pricing per destination.

The VoIP Connect SIP Trunk solution for Inbound at Alberton and Doringkloof must be fully redundant, with Premium support of 24/7/365. Alberton and Doringkloof will be two standalone production sites with identical configuration with minimum 1 860 concurrent SIP-session capacity per site and with support for the G.729 Codec. The architecture at each of these 2 sites must support a user base of ±10 000 users.

Sars has currently provisioned 13500 users on the MS Teams Phone Platform. The winning Bidder must be able to provide a Hosted Direct Routing solution which will be SBC's. All number ranges must be able to be ported from existing vendor to the new vendor. Microsoft Teams licences are out of scope because SARS is already licenced with E5 licences that include Microsoft Teams Phone. The bidder must be a Direct Routing certified telco provider for Microsoft Teams, to provide voice trunks or to switch and port numbers between them.
Interoperability with third-party systems: the solution with direct routing allows clients with users on the Microsoft cloud to continue using third-party systems such as an existing
PBX, call centres, and/or existing analogue telephony adaptors (ATA), helping preserve existing investments and provides the flexibility to have a phased, tested migration onto
this platform. This interoperability option is crucial from a migration and transition perspective as it helps with a smooth, low risk migration from one platform to another.
The Microsoft Teams users will be enabled and solved for via the Bidder's Hosted Direct Routing service, this service will function autonomously with the Call Ingress and Egress routed via the Bidder's PSTN network.
The providers SBC's will communicate with the Microsoft tenant on one interface, and the PSTN cloud on the other.
Create the billing account on Soft Switch and SBC breakouts and allocate numbers as well as rate cards.
Create Subdomain for use on the customers tenant and configure this on SBC for peering using TLS and SIP options for Tenant Tracking and statistics.
Route number ranges across SBC towards the Subdomain on the Tenant, this is done via Azure for signalling.
Perform UAT with customer on various functionality and interactions on both Test and production environments.

7.3.3 Preferred Outbound Voice Carrier Provider

In line with the centralised break-out strategy set out in paragraph 7.3.1, a Preferred Outbound Voice Carrier Provider must carry calls over its own SIP Trunking infrastructure for break out at both Alberton and Doringkloof, and no other sites. During the term of the contract, SARS may require additional break-out points, for example from SARS's Brooklyn head office. The charges related to additional break-out points will be treated on a project basis as may be defined in a separate work order.

The Preferred Outbound Voice Carrier Provider must carry calls to all destinations (international, national, local, and mobile calls to all South African mobile operators) and therefore must provide the price (per second) for calls to each.

7.3.4 Preferred Inbound Voice Carrier Provider

The required SIP Trunk solution should provide for the connection of an IP PBX telephony system to the preferred inbound voice carrier over a managed IP-access link. A single SIP Trunk should support a minimum of 30 concurrent voice SIP sessions (voice channels) for the origination and termination of voice calls which should not be fewer than 1 860 SIP sessions.

The SIP Trunk must be delivered with an associated geographical number range consisting of at least 300 publicly routable numbers for every 30 SIP sessions.

The Preferred Inbound Voice Carrier should provide interconnectivity for voice calls within and outside South Africa through its established and extensive local and global network reach and peer operator arrangements. The SIP Trunk service must be scalable in increments of 30 sessions, unless specifically stated otherwise.

SIP Trunking solution must be engineered to deliver sustainable high-quality voice services with guaranteed high availability, reliability, and predictable performance. The solution must also ensure the security and integrity of voice communications over its network through the use of robust and proven technology platforms, and best-practice network and security architectures.

7.3.5 Future Technical Transformation

SARS's future strategy includes the routing of all outbound and inbound voice and video calls via Microsoft Teams at the lowest cost at acceptable voice-quality levels through the Preferred Outbound Voice Carrier Provider(s). The solution functionality must also have the ability to record all conversations and integrate into the SARS document store where these voice logs will be kept. There should also be the ability to play back and download these voice logs via Microsoft Teams. The bidder must supply a separate proposal, including voice-rate cards associated with the solution, in free-form format.

For the Preferred Inbound Voice Carrier Provider, a fully redundant cloud-based failover load-balancing solution is required for high availability of incoming calls from the 0800 number. If either one of the internal Data Centres fails (e.g. because of loss of power on premises), the failover solution must still be accessible for the site that is down, so that CC agents and calls can be failed over to the functional backend site.

7.4. Detailed Requirements for Voice Carrier Services

7.4.1 Preferred Inbound and Outbound Provider Requirement

Bidders for the Preferred Inbound and Outbound Voice Carrier Provider scope must submit a Proposal that will provide:

- Inbound and outbound Voice Carrier Services for all SARS Sites; and

- SIP Trunk circuits at Alberton Campus, Doringkloof, and Brooklyn.

Bidders for the Preferred Inbound and Outbound Voice Carrier Provider must complete the pricing templates for **all elements** of the Voice Carrier Services Tower.

- **Existing Number Retention**

The Service Provider must be able to provide the Voice Carrier Services without requiring SARS to change its geographic numbers for inbound calls. The Preferred Inbound and Outbound Voice Carrier Provider will therefore be required to port SARS's existing geographical numbers to meet this condition as part of the Transition.

- **Outbound call-concurrency assumptions**

The outbound call-concurrency value is calculated at design phase of each site based on 1/3 of the actual number of users at the site. For example, if there are 90 actual users at a site, then under this assumption, the design of the site should cater for a maximum of 30 concurrent users.

- **SIP Trunks**

In addition to the immediate requirement for SIP trunking to Alberton, Brooklyn, and Doringkloof, the Service Provider may be requested by SARS, during the Term, to provide SIP Trunking to other major centres. Additionally, the Service Provider may, from time to time, be requested to increase or reduce the number of channels provided over such deployed SIP Trunks.

7.4.2 Preferred Outbound Voice Carrier Provider Requirement

Bidders submitting Proposals for the Preferred Outbound Voice Carrier Provider scope must clearly state the per-second rates to the different destination types outlined in the pricing template *Tower V*

Pricing Response Template.

The Preferred Outbound Voice Carrier Provider solution must carry the outbound calls over a SIP trunk from the Alberton and Doringkloof sites. The charges for the Preferred Outbound Voice Carrier Provider must be only for outbound calls. The cost of the SIP Trunk must not be separately charged and no minimum charges must apply (i.e. the charges for the outbound calls must include the costs associated with the SIP trunking). The outbound CLI from both Alberton and Doringkloof Trunks should be configurable to match the current 0800 Contact Centre Number or any other number that SARS may require it to be changed to during the Term.

7.4.3 Audio Quality

Audio quality will be deemed to be acceptable at a MoS of 3.8 or higher. To achieve acceptable voice quality to mobile phones, the Bidder must propose a solution which takes SARS's outbound calls directly to the cellular network provider's networks via interconnection links and must not rely on "over-the-air" cellular transport to take calls from the SARS site (for example, the Bidder must not propose on-site direct-to-air least-cost routing appliances).

7.4.4 Call Line Identification

All voice services and the pricing proposed must include Call Line Identification functionality to the extent allowed by ICASA regulations.

7.4.5 Volume-based Discounting

SARS disfavours pricing that is based on discounts that are contingent on the actual volume of outbound calls or on the actual spend SARS makes to qualify for such discounts. SARS cannot predict the actual volume of calls in the future and will have no certain method of evaluating such pricing. If the pricing offered by a Bidder in its Proposal includes discounts, such pricing must be expressed using the discount level offered to SARS, irrespective of volumes.

7.4.6 Term-based Discounting

The approach to evaluation of term-based discounting will be based on the intended Term of the contract. The pricing for the Preferred Inbound Voice Carrier Provider service should be based on the assumption of a 5-year minimum term.

7.4.7 Per-second Billing

The Bidder must specify its solution in terms of per-second billing with no minimum durations payable.

7.4.8 Monitoring and Reporting Portal

Monitoring and reporting are critical requirements to be dealt with in the Bidder's Proposal.

SARS requires the Preferred Inbound Voice Carrier and Preferred Outbound Voice Carrier Provider to provide a Monitoring and Reporting Portal that is accessible by SARS or a SARS-designated agent via a secure internet connection. The provision of a Monitoring and Reporting Portal in a Bidder's Proposal for Preferred Outbound Carrier Provider is not mandatory, but will improve such Bidder's evaluation score for this Service. A Monitoring and Reporting Portal must provide the following:

7.4.8.1 Real-time (or near-real-time with no longer than 10 minutes' delayed updating) status of all in-scope elements of the Voice Carrier Services:
- o Up/down availability status (colour-coded).
- o Capacity utilisation (by traffic type).
- o Error rates.
- o Traffic flow.

7.4.8.2 Up-to-date accumulated statistics (or near-real-time with no longer than 10 minutes' delayed updating) of all in-scope elements of the Voice Carrier Services over the Term of the agreement including:
- o Availability.
- o Capacity utilisation (by traffic type).
- o Error rates.
- o Traffic flow.

Detailed time-interval records should be kept for at least 60 (sixty) days.

7.4.8.3 A downloadable electronic record of all details of inbound and outbound calls. The entire detailed history of all call records must be available for the duration of the Term.

7.4.8.4 Reports of all outages affecting the Voice Carrier Services (including one-time outages and special summaries for severe outages). Such outage reports will include at least the following details: date and location of outage; outage hours; root cause of outage; actions taken, impact, timelines, and problem resolution; associated Service Level Credits; and the following cumulative data: total number of outages, average duration of outage, average response time, and average repair time.

7.4.8.5 Reports of all major events affecting or potentially affecting the Voice Carrier Services.

7.4.8.6 Reports of all events that were not repaired within the required time intervals.

7.4.8.7 Reports indicating trends by root cause as determined on trouble-ticket closure. In addition, the record of identified actions the Service Provider is taking to resolve problems.

7.4.8.8 Reports with a historical correlation of trouble tickets affecting the same element of the Services. The correlation parameters (e.g., network elements, number of trouble tickets, and time period of measurement) may be determined by SARS.

7.4.8.9 Inventory data, including the configuration, assignments, parameters, barcodes, SARS location, logical link capacities, and settings applied to all items of equipment implemented to deliver the Voice Carrier Services.

The Monitoring and Reporting Portal must include functionality to:

o Effect role-based access.

o Filter all reports to certain date ranges, and other filters to limit the data selected. Summarisation functionality must allow summarisation of selectable time periods (e.g. per day, week, month, year, etc.).

o Specify recipients of the report and the ability to email reports to the specified recipient email addresses at specified frequencies.

o Send SMS notifications of incidents as defined by SARS.

The Bidder is required to provide details of its current capability to deliver the requirements as set out above as well as details of its plan, including timelines, to which the Bidder is prepared to commit to implement the full functionality as set out above. Although it is not a requirement that the Bidder must currently possess the capability to provide all the specified functionality, it is a mandatory requirement that the Monitoring and Reporting Portal is operational 3 (three) months after the Effective Date and no later than when the first service are taken on by the Service Provider during Transition.

7.4.9 Monitoring

Service Providers appointed, the Preferred Inbound Voice Carrier, and Preferred Outbound Voice Carrier must actively monitor the status of all components of the Voice Carrier Services within the scope awarded. In the event of an incident affecting any component of the Voice Carrier Services, the Service Provider must proactively diagnose, establish the necessary actions to restore Services, and begin and complete restoration activities. The Service Provider must proactively contact SARS or a party nominated by SARS at designated stages in the detection, diagnosis, and repair of events.

The Service Provider will be required, at SARS's discretion, to maintain a presence in the SARS Network Operations Centre. The Service Provider's personnel will form part of the SARS monitoring team and (a) will be required to help identify, diagnose, and resolve incidents involving, or related to, the Tower D services, including logging and updating incident and problem records on SARS's service management-system. (b) The Service Provider must be the interface point for communication and escalation. This will not be required as part of the base services and will be separately priced as an optional service.

7.4.10 Integration with the Tower D Data Carrier (WAN) Service Provider(s)

Bidders submitting a Proposal for both Tower V and D must note that their Proposal for Tower V must propose the carriage of voice traffic over the same physical circuits as that for Tower D. The voice circuits will be logically separated from the data circuit on the same physical circuit, except for SD-WAN sites.

7.4.11 Service Levels

The Service Level Class and Service Coverage Period assigned to the various voice circuits will be the Service Level Class and Service Coverage Period assigned to the SARS Site that the circuit connects. The required availability of the voice circuit will be measured during the Service Coverage Period of the circuit.

SIP Trunking

Service Level Class	Maximum Monthly Cumulative SIP Trunk Unavailability
Bronze	4 hours
Silver	2 hours
Gold	1 hours

7.5. Transition

The current Service Provider is contracted to perform handover activities to the successful Bidder. Pricing for transition must include all activities the successful Bidder will need to undertake to meet all the requirements of the Business Requirements Specification, including the activities to take over from the incumbent Service Provider.

The Service Provider(s) appointed in Tower V must complete the Transition Services within a 3 (three) month period from the time of the effective date and finalisation of the contract. By this time, the Preferred Inbound Voice Carrier and Preferred Outbound Voice Carrier must have assumed full management responsibility for the full scope of Voice Carrier Provider Services. In this regard, the Service Provider must have:

- Fully designed, developed, and implemented the processes, procedures, schedules, and work practices detailed in the *Network Carrier and Infrastructure Services Agreement*, especially those detailed in Schedule B-V and its attachments.

- Attended any training specified by SARS to understand the SARS environment, systems, and operating procedures.

- Where necessary, to have affected the necessary cession and assignment agreements with incumbent Service Providers.

- Deployed the necessary Trunking or taken over responsibility for existing circuits.

- Cut over Voice Carrier Services to the Service Provider's solution while retaining SARS's existing inbound numbers.

If SARS has made such appointment(s), Bidder(s) appointed as Preferred Outbound Voice Carrier Provider(s) must have deployed the necessary infrastructure at Alberton Campus and Doringkloof to carry outbound calls from these sites within a period no longer than 3 (three) months from the time of the award and finalisation of the contract with the Preferred Outbound Voice Carrier Provider(s).

The Bidder must note that there are no transition project charges for the Preferred Outbound Voice Carrier Service Provider to take on the services and that all costs relating to the transition are to be absorbed in the usage charges.

8. TOWER C: UNIFIED COMMUNICATION PLATFORM AS A SERVICE (CPAAS)

8.1. Scope

The provision of the CPaaS comprises the delivery of the following:

Replacement of Existing Messaging Channels: The Service Provider must provide secure (VPN,

encrypted, Patch Policy, Timelines & Communications) channels for existing SMS, USSD, short code messages (eBooking) and short URL (e.g. bit.ly) services. The Service Provider must provide integration into SARS systems and ensure that communication messages are sent and delivered reliably, securely, and in a timely manner, with delivery receipts delivered back to SARS systems.

Provision of New Communication Channels: The Service Provider must be able to support potential future channels, including integration into existing or newer modern trending technologies such as WhatsApp, Bulk Email, and System Generated Letters (communications messages), Facebook, Twitter/X, Telegram, LinkedIn, Webchat, Livechat, and other potential new cloud-based technologies. The provider must have the necessary expertise to integrate new viable channels seamlessly with the existing communications channels and the current SARS systems via acceptable and secure integration technologies.

Service Providers must enable SARS to take advantage of AI/NLP/LLM services such as ChatGPT/Copilot or similar and integrate these into SARS's communications systems (Chatbot, Livechat) to enhance customer experience by leveraging the power of AI/NLP/LLM for more intelligent and personalised interactions.

System Generated Forms are printed output that is processed (folded, collated, and sorted) optionally together with inserts (e.g. booklets, newsletters) and inserted into mailing envelopes. To print the System Generated Forms, data (taxpayer-specific data) are merged with predefined layout and background overlays to produce the final printed output. SARS uses several processes, formats, and methods to transmit data to produce different types of System Generated Forms. SARS is investigating and would want, as part of the Bidder's solution, the ability to perform print streaming directly to the Service Provider. In this respect, the Service Provider should be able to support the processing of AFP (Advanced Function Printing), Postscript, and colour where necessary. The Service Provider should also be able to support "jogging" for sheet layouts and optimised AFP for dynamic image references and TLEs (Tagged Logical Elements). This will need to include preferred AFP configurations.

8.2. Current Delivery Model

SARS currently maintains contracts with two Service Providers to transmit SMS messages and deliver to the taxpayer. A single Service Provider delivers the USSD service integrated with SARS systems. The Chatbot (Lwazi) is an internal SARS system, like the AI Assistant from sars.gov.za, and it may be required in future to integrate this service into the latest AI-based technologies.

The SMS functionality currently used by SARS entails outbound messages that do not require a response from the subscriber. Messages are sent using the SMPP protocol over the internet to the Service Provider's SMSC. Delivery receipts and reporting on undeliverable messages is a requirement.

8.3. Required Delivery Model

8.3.1 Non-Exclusivity

SARS seeks to enter into contracts with up to two Service Providers in Tower C Category A to transmit SMS messages. It is emphasised that the award of such contracts shall not be exclusive to any particular Service Provider. If more than one Service Provider is appointed, SARS will have the discretion to route SMS traffic to a specific Service Provider based on the following criteria:

- Least-cost routing.

- Reliability in terms of Service Reliability Engineering concepts such as SLI, SLO, and SLA offered.

- Availability and performance (if a Service Provider's Service is unavailable or is delivering SMS in times in excess of the Service Level Objective, then the alternative Service Provider may be used by SARS, either on a temporary or on-going basis).

SARS shall, during the term of the contract, periodically update the routing algorithms for its SMS traffic to the Service Providers based on then-trending pricing and reliability as they may apply to different classes of subscribers. Such updates shall occur at least yearly.

8.3.2 Mobile Operator Agreements

The Service Provider must maintain agreements with each of the Mobile Network Operators ,and its SMSC (Short Message Service Centre) must bind securely with each of the Mobile Network Operators directly. The Service Provider must not be reliant on, and must not send traffic via other WASPs, to transmit SMS messages to the MNOs.

The Bidder must supply SARS with any codes of conduct that SARS will be required to agree to as a condition of providing the Services.

8.4. Functional Requirements for CPaaS (Communication Platform as a Service)

8.4.1 SMS Requirements

The Service Provider must provide a solution for SMS-based services that meets the following minimum requirements:

A high volume of local SMS's is delivered daily. A much smaller volume of SMS's is delivered internationally. The solution should be able to deliver SMSs to any handset anywhere in the world.

Scheduled or ad-hoc reminders and messages regarding SARS's services, including reminders to business channels/partners/taxpayers, promotional messages, employee notices, and SARS Exchange-based e-mail-to-SMS.

General transactional notices, including notices about certain filing status, transactional message notifications, and individual reminders.

Transactional (time-sensitive) notices, which must be passed to recipients without delay, such as password resets, One-Time Pin (OTP) and event-triggered operational notifications and alerts.

The solution must provide delivery confirmations that can be interrogated by SARS to determine the delivery status of a message, which may or may not be used by SARS initially. A report or file must be provided to SARS through SFTP on a daily basis that includes the messages that were not delivered and the reasons why, in order for SARS to process through a cleanup exercise. The Bidder must provide details on how this can be accomplished by its solution.

The solution must be capable of restricting transmission of certain types of messages to certain times of the day, which may vary depending on the day of the week, while still sending other types of messages as they are sent from the SARS systems (typically alerts, OTPs, etc.). The solution must provide SARS with the flexibility to change these times periodically.

8.4.2 USSD (Unstructured Supplementary Services Data)

The Service Provider must support SMS-based services that enable session-based transactions for SARS. The functionality must support user-initiated SMS-based queries, allowing subscribers to initiate queries and receive responses from SARS systems through SMS. The Service Provider must also allow taxpayers to request their Personal Income Tax (PIT) registration number and issue the IT150 form, where an email address is available on record. Additionally, the Service Provider must support the ability to view a summarised Auto Assessment (SIM01) and accept the Auto Assessment, thereby filing the taxpayer's Personal Income Tax Return.

Furthermore, the Service Provider must provide account queries, such as balance statements for PIT, and provision of Statement of Account (SOA). The request for "Balance of account" must respond to both Assessed Tax and Administrative Penalties. The Service Provider must also confirm whether or not the taxpayer must submit a tax return (PIT) and initiate a request for a Branch eBooking and Call Back.

For all services on offer, taxpayers will initiate a USSD session by typing a single predefined string of characters, comprising an asterisk (*), followed by several digits and ending with a hash (#), e.g., 1207277#, and pressing *dial*. The predefined string of characters to initiate the USSD session must be accessible via any telecommunications network (e.g., Telkom, MTN, etc.).

The USSD session must be identifiable from other service channels to report on it. Service-specific authentication will be performed by SARS back-end systems, based on the risks associated with the service request. SARS back-end systems must process the request and respond to USSD with the appropriate outcome, supplementing the transaction with SMS messages where applicable.

All USSD message content is in draft wording and will be confirmed with all applicable stakeholders concerned. The exact USSD trigger numbers (7277) must be transferred to the new Service Provider. The channel must be developed to contain further use cases as the need arises. The taxpayer must be able to initiate the USSD session with SARS, regardless of the telecommunication network operator that they use. The following USSD introductory messages are mostly common to all services when the USSD session is initiated, and applicability shall be specified within the detailed designs.

The Service Provider shall provide applicable data to the Enterprise Data Warehouse (EDW) for reporting purposes. The following reporting requirements must be met:

Total number of USSD sessions, including session lengths, per Service Request, per calendar month, and per day.

Total number of rejected USSD sessions, including session lengths, per rejection reason, per calendar month, and per day. Rejection reasons shall include invalid information received, taxpayer not registered or does not exist, attempted use of channel by tax practitioners, authentication failed, status of tax reference number, multiple tax reference numbers, and duplicate service requests for services where duplicates are prohibited.

Total number of processed USSD sessions, including session lengths, per Type and per Outcome Type, per calendar month, and per day.

For all service types, the session timeout before the service request is rejected or finalised must be reported.

For Return Filing Confirmation, differentiate between Current Bulk Year and Prior Bulk Year and report whether the return is not required, required, or submitted.

For TRN request, report whether the TRN was issued or not.

For Balance of the account, report whether the balance is a credit balance, debit balance, or zero balance.

For Simulated Tax Assessments, report whether a SIM01 is available, viewed, accepted, or if the taxpayer chooses to file through an alternative channel. Additionally, report whether the SIM01 was abandoned without action selection or if the session timed out.

Detailed session data shall be made available, including originating phone number, session number, dates and times, and session content.

The same information shall be made available from the Alternative Tax Platforms (ATP) to allow for reconciliation of billing.

The same information shall be made available for SMS messages triggered by this process.

8.4.3 MMS (Multi-media Messaging services)

The Bidder shall demonstrate its capability to enable SARS to send MMS to subscribers of all mobile networks in compliance with applicable laws and regulations. The proposed solution shall enable SARS to send and receive taxpayer documents, branded links, bulk MMS messages, event details, troubleshooting screenshots, instructional product videos, custom map images, and other related content, as required by SARS. The proposed solution shall provide for the ability to troubleshoot problems and guide customers through demos using MMS messages. To ensure compatibility with SARS systems, the solution must support the file extensions shown in Table 1 below. The proposed solution shall meet all security, privacy, and data-protection requirements specified by SARS, and shall be scalable to meet SARS's future needs.

Table 1: MMS File Extensions

Images	.bmp .dib .gif .heic .ico .jpeg .jpg .pjpeg .png .svg .tif .tiff .webp
Media (Audio & Video)	.amr .avi .flac .flv .m1a .m1v .m2a .m4a .m4b .m4p .m4, .m4v .mov .mp1 .mp2 .mp3 .mp4 .mpa .mpeg .mpg .mpv .oga .ogg .ogm .ogv .ogx .qt .spx .wav .wap .webm .wmv
Documents	.csv .pdf .rtf

Calendar and Business Cards	.cal .vcard .vcf
Miscellaneous	css .html .js .json .smil .txt .xml

8.5. Potential Future Cloud-based Communication Services

SARS aims to appoint a panel of qualified and experienced Service Providers from whom we can request these services for the duration of the contract. This panel will be selected based on the criteria outlined in the tender document and will be expected to deliver high-quality services that meet our specific requirements at the time. The panel will consist of a limited number of pre-qualified providers who have demonstrated the ability to deliver a full set or subset of these specialised services that align with our requirements and standards. We will leverage this panel to ensure that we can access the services we need in a timely and cost-effective manner, while maintaining the high level of quality and security that we require.

As part of our future requirements, we are looking for a cloud-based solution that can deliver shortened URLs using services such as bit.ly and integrate with our existing SARS systems. We will base these requirements on Gartner's Communications Platform as a Service (CPaaS) model, which emphasizes the need for Service Providers to offer flexible, scalable, and secure communication solutions, fully integrated into the existing SARS systems. The proposed solution should support multiple communication channels and enable easy integration with our existing systems. We will prioritise providers that can offer high levels of reliability, scalability, and security, as well as those that can demonstrate experience in delivering similar services to other organisations.

Additionally, we will be looking for providers that can offer competitive pricing models and flexible contract terms.

Below are the required services:

- **Messaging Services:** The platform should support the delivery of SMS, MMS, and other messaging services to enable effective communication with customers.

- **WhatsApp:** The platform must enable SARS to engage taxpayers via WhatsApp, Facebook, YouTube, and other feasible communication channels in compliance with applicable laws and regulations. The proposed solution should allow taxpayers to use a dedicated WhatsApp business account number to communicate with SARS securely. The solution should enable taxpayers to opt-in to the service, use natural language to communicate with SARS, and request specific query types or service requests in a structured menu format. General-advice queries must be referred to the existing SARS Chatbot (Lwazi) for first-line response. The proposed solution should integrate with applicable back-end systems to automate the processing of requests and responses and provide operational reporting and data collection on channel usage. The proposed solution should meet all security, privacy, and data-protection requirements specified by SARS and should be scalable to meet SARS's future needs.
- **Chat Services:** The platform should support chat services such as web chat, social media messaging, and chatbots to enable personalised and efficient communication with customers.
- **Shortened URL Services:** The platform should include shortened URL services such as bit.ly to enable the delivery of short, trackable URLs in messaging and chat services.
- **Analytics and Reporting:** The platform should provide analytics and reporting capabilities to enable monitoring and analysis of message and call traffic, user engagement, and other metrics to improve performance.
- **Integration with Existing Systems:** The platform should be able to integrate with existing CRM, ERP, and other business systems to enable seamless communication with customers and enhance productivity.
- **Multichannel Support:** The platform should support multiple channels of communication, including email, SMS, voice, chat, and social media messaging, to provide customers with a choice of communication channels to improve accessibility.
- **Bulk Email requirements:** The platform should support the creation and sending of Bulk Email to taxpayers as part of campaigns or via the integration into SARS systems.
- **Letter processing:** The platform should support the creation and sending of bulk system-generated letters to be printed and posted through integration with the SARS solution.
- **Security and Compliance:** The platform should provide robust security measures such as encryption, multi-factor authentication, and data protection to ensure the privacy and security of customer information, as well as regular patching of the vendor's servers to ensure security risk mitigation. It should also comply with relevant data protection and privacy regulations such as POPIA, GDPR and

CCPA.

- **Scalability and Availability:** The platform should be scalable and highly available to handle increasing traffic and ensure uninterrupted service. SARS has periods during the year in which the volumes increases significantly and the Bidder must be able to scale up to handle increased volumes without impacting delivery times to handsets.

8.6. Non-Functional Requirements for CPaaS (Communication Platform as a Service)

- **Volumes:** While the current volumes of SMS sent by SARS are projected at 240 million per annum, this figure is expected to increase at more than 10% per annum during the Term depending on the acceptance, usage, and enhancement of this channel for taxpayer communications. SARS, however, makes no commitment to volumes of SMSs that will be sent during the Term or, in case of more than one SP, what will be sent to which SP.
- **API Specifications:** The Service Provider must provide well-documented APIs that allow SARS to integrate the communications channel into its existing systems seamlessly. The APIs should support standard protocols, such as REST and SOAP, and allow for easy integration with a wide range of programming languages and platforms.
- **Protocol Support:** The Service Provider must support a range of communication protocols, including SMS, USSD, WhatsApp, Email, and Letters. They must also have the capability to support emerging technologies such as WebChat, Facebook, Twitter, Telegram, LinkedIn, and other cloud-based technologies.
- **Network Connectivity:** The Service Provider must have a robust and reliable network infrastructure that can handle high volumes of messages with low latency. The Service Provider must have multiple points of presence (POPs) across the country to ensure that messages are delivered quickly and reliably.
- **Data Storage:** The Service Provider must provide secure and scalable data storage for messages, delivery reports, and other communication-related data. They must ensure that data is backed up regularly and stored in multiple locations to prevent data loss in the event of any disaster or outage.
- **Backup and Disaster Recovery (DR):** The Service Provider must have a comprehensive backup and disaster recovery plan in place to ensure that the service remains available in the event of any disruption or outage. They must regularly test their backup and DR procedures to ensure that they are effective and can restore service quickly.
- **IT Security:** The Service Provider must have robust IT security measures in place to protect the communications channel and the data transmitted over it. They must use industry-standard encryption and authentication mechanisms to ensure the confidentiality, integrity, and availability of data.
- **Monitoring and Reporting:** The Service Provider must provide comprehensive monitoring and reporting capabilities that allow SARS to track the performance and availability of the communications channel. They must provide real-time alerts and notifications in the event of any issues or outages.
- **Scalability:** The Service Provider must have a scalable infrastructure that can handle large volumes of messages without compromising on the quality of service. The Service Provider must be able to scale the infrastructure up or down based on the changing needs of SARS.
- **Confidentiality:** The CPaaS provider should ensure the confidentiality of all communication data, including voice and messaging traffic. The provider should have appropriate security measures in place to protect against unauthorised access or disclosure of information.
- **Data Encryption:** The provider should offer end-to-end encryption for all communication data transmitted over its platform. Encryption helps to protect the privacy of users and prevents interception or eavesdropping by unauthorised parties.
- **Compliance with POPIA:** The provider should comply with the requirements of POPIA, including the collection, processing, and storage of personal information. The provider should have policies and procedures in place to ensure compliance with POPIA and should provide regular reports on its compliance status.
- **Access Controls:** The provider should have robust access controls in place to ensure that only authorised users can access communication data. Access controls should include user authentication, role-based access controls, and activity monitoring.
- **Data Retention:** The provider should have a clear data retention policy that specifies for how long communication data is stored and how it is securely deleted when no longer needed. The retention period should comply with the requirements of POPIA and other relevant regulations.
- **Incident Response:** The provider should have an incident response plan in place to handle security incidents and data breaches. The plan should include procedures for notifying affected parties and for cooperating with law enforcement and regulatory authorities.

8.7. Monitoring and Reporting Portal

SARS requires that the Bidder's Proposal include a comprehensive plan for monitoring and reporting.

The Service Provider must conduct real-time monitoring of all relevant aspects of the SMS Carrier Service, including circuits to the MOs, capacity utilisation of critical elements, and queue status. Additionally, the Service Provider must provide up-to-date monthly accumulated statistics for all in-scope elements of the SMS Carrier Services over the Term of the agreement, including traffic volumes, incidents, and problems, and a breakdown of volumes per channel, and — within each channel — the relevant department or cost centre. The Bidder must provide monitoring tools to analyse the outbound transactions to detect unusual usage and ensure reconciliation of invoices to SARS data. The reporting provided by the Service Provider must enable SARS to make informed decisions about service improvements and optimisation, and facilitate a productive working relationship between SARS and the Service Provider.

8.8. Transmission of SMSs from SARS

Currently, SARS sends SMSs to its incumbent Service Providers using the internet. The Bidder may propose alternative connection options that may present lower risk and improved reliability. The Service Provider must bear all costs relating to such connections.

8.9. Service Reliability Requirements

SARS understands that no Service Level can be guaranteed for delivery to a mobile device. However, SARS is seeking Proposals that will provide Service Levels across those components in the delivery chain through which performance and reliability undertakings can be offered and that are within the Service Provider's control.

The Bidder will be required to propose such Service Levels which will be incorporated in Schedule C of the Network Carrier and Infrastructure Services Agreement. Any Service Levels proposed by the Bidder must be measurable by the Bidder and those target levels proposed will form the basis for performance management and the payment of Service Credits.

- **Service Reliability Engineering (SRE):** Essential to ensure that the communications channel as a service is reliable and efficient for SARS.
- **Monitoring:** The Service Provider must have a robust monitoring system in place that provides insight into the performance of the communications channel. The monitoring system should be able to track key performance indicators such as latency, uptime, message delivery, and response time. The monitoring system should also detect potential issues before they become critical.

- **Incident Response:** The Service Provider must have a well-defined incident response process (be able to access SARS Remedy ITSM system via the web portal). The incident response process should include clear escalation procedures, communication channels, and resolution times. The Service Provider should also have a team of dedicated incident responders who are available 24/7 to handle any issues.

- **Post-Incident Reviews:** The Service Provider must conduct post-incident reviews to identify the root cause of any issues and take steps to prevent them from happening again. The post-incident review process should be well-documented and include clear action items.

- **Testing/Release:** The Service Provider must have a well-defined testing and release process that ensures that changes to the communications channel are thoroughly tested before they are released to production. The testing process should include both functional and performance testing, and the release process should be well-documented and follow industry best practices.

- **Capacity and Scale:** The Service Provider must have the capacity to scale the communications channel to meet the growing needs of SARS. The Service Provider should have a well-defined capacity planning process that includes regular capacity assessments and the ability to quickly scale up or down based on demand.

- **ITSM Process:** The Service Provider must be able to integrate its ITSM process with SARS's ITSM process to ensure that there is a seamless flow of information and communication between the two organisations. The Service Provider should use Remedy web access to open and track incidents, change requests, and service requests.

- **Integrated View of all Communications:** The Service Provider must be able to provide SARS with an integrated view of all communications done via the communications channel. This view should include data on all transactions and should be reconciled with billing data to ensure accuracy.

In summary, SRE requirements for the communications channel as a service include monitoring, incident response, post-incident reviews, testing/release, capacity, and scale, ITSM process, and an integrated view of all communications. These requirements ensure that the communications channel is reliable, efficient, and meets the needs of SARS and taxpayers.

8.10. Transition

8.10.1 Timelines

The current Service Provider is contracted to perform handover activities to the successful Bidder. Pricing for transition must include all activities the successful Bidder will need to undertake to meet all the requirements of this Business Requirements Specification, including the activities to take over from the incumbent Service Provider.

The Service Provider(s) appointed in Tower C (CPaaS) is required to complete the Transition Services within a 3 (three) month period from the time of the award and finalisation of the contract. By this time, the Service Provider must have assumed full management responsibility for the full scope of the existing Carrier Services for SMS, Short Message, USSD, WhatsApp, Bulk SMS/Bulk email, and letter flattening and printing, including potential future requirements awarded to the SP. In this regard the Service Provider must have:

- Fully designed, developed, and implemented the processes, procedures, schedules, and work practices detailed in Network Carrier and Infrastructure Services Agreement, especially those detailed in Schedule B-S and its attachments.

- Attended any training specified by SARS to understand the SARS environment, systems, and operating procedures.