



|  |  |
| --- | --- |
| **RFx No:** | **RFP 3086/2025** |
| **Description** | **REQUEST FOR PROPOSAL FOR THE PROVISON, INSTALLATION, CONFIGURATION INCLUDING, MAINTENANCE AND SUPPORT OF INTERNET BANDWIDTH SOLUTION TO SITA AND ITS CLIENTS FOR A PERIOD OF FIVE (05) YEARS** **REVISED BID SPECIFICATION** **RFP3086-2025\_Rev01** |
| **Virtual** | **Non-Compulsory Briefing Session will be held as follows:****Date: 11 April 2025****Time: 11:00am**[**Join the meeting now**](https://teams.microsoft.com/l/meetup-join/19%3Ameeting_NDc0NWYxMmEtZTVlYS00ODhmLWJmMGEtYTZjYjljZGQwOTVm%40thread.v2/0?context=%7b%22Tid%22%3a%2248cd5724-88c7-48c3-a665-945436edd7fc%22%2c%22Oid%22%3a%22ecc35aa4-150f-4a78-a045-3b0070db33fa%22%7d)**Meeting ID: 351 612 714 272** **Passcode: wj36Q4Ex**  |
| **Closing Date for questions / queries** | **02 May 2025 at 16:30pm** |
| **Bid Response Submission Address**  | Tender Office459 Tsitsa Street, Erasmuskloof, Pretoria, 0105 |
| **RFx Closing Details and Time** | **Date:**  **16 May 2025** **Time:** 11:00 (South African Time) |
| **RFx Validity Period** | 200 Days from the Closing Date  |

Contents

[1. Introduction and background 4](#_Toc195465653)

[1.1 Purpose 4](#_Toc195465654)

[1.2 Background 4](#_Toc195465655)

[2. Scope of Bid 5](#_Toc195465656)

[2.1 Scope of Work 5](#_Toc195465657)

[2.2 Delivery address 6](#_Toc195465658)

[2.3 Current Customer Infrastructure 7](#_Toc195465659)

[3. Requirements 8](#_Toc195465660)

[3.1 Product / Service / Solution Requirements 8](#_Toc195465661)

[3.1.1 Installation and Configuration, Technical and Solution Requirements 8](#_Toc195465662)

[3.1.2 Performance Requirements 12](#_Toc195465663)

[3.1.3 Administration and Reporting Requirements 12](#_Toc195465664)

[3.1.4 Internet service solution requirement components 15](#_Toc195465665)

[3.2 Service Elements 16](#_Toc195465666)

[3.2.1 Full-Service Agreement 16](#_Toc195465667)

[4. Bid Evaluation Stages 18](#_Toc195465668)

[4.1 Mandatory Administrative responsiveness (Stage 1) 18](#_Toc195465669)

[4.1.1 Attendance of briefing session 18](#_Toc195465670)

[4.1.2 Registered Supplier 18](#_Toc195465671)

[4.1.3 Bid Submission Instructions 18](#_Toc195465672)

[4.2 Technical returnable documents 19](#_Toc195465673)

[4.2.1 Instruction and evaluation criteria 19](#_Toc195465674)

[4.2.2 Technical mandatory requirements (Stage 2) 19](#_Toc195465675)

[4.3 Technical Functionality evaluation Requirements (Stage 3) 26](#_Toc195465676)

[4.4 Special Conditions of Contract Verification (Stage 4) 30](#_Toc195465677)

[4.4.1 Special Conditions of Contract 30](#_Toc195465678)

[4.4.2 Contracting Conditions 30](#_Toc195465679)

[4.4.3 Delivery Address 30](#_Toc195465680)

[4.4.4 Losses 30](#_Toc195465681)

[4.4.5 Penalties 31](#_Toc195465682)

[4.4.6 Delivery timeframes 31](#_Toc195465683)

[4.4.7 Scope of work changes 31](#_Toc195465684)

[4.4.8 Benchmarking 31](#_Toc195465685)

[4.4.9 Performance Benchmarking: 32](#_Toc195465686)

[4.4.10 Price Benchmarking: 32](#_Toc195465687)

[4.4.11 Supplier performance reporting 33](#_Toc195465688)

[4.4.12 Certification, Expertise and Qualification 33](#_Toc195465689)

[4.4.13 Logistical Conditions 34](#_Toc195465690)

[4.4.14 Skills transfer and training 35](#_Toc195465691)

[4.4.15 Regulatory, Quality and Standards 35](#_Toc195465692)

[4.4.16 Security clearance requirements 36](#_Toc195465693)

[4.4.17 Confidentiality and non-disclosure conditions 36](#_Toc195465694)

[4.4.18 Guarantee and warranties 37](#_Toc195465695)

[4.4.19 Intellectual Property Rights 39](#_Toc195465696)

[4.4.20 Counter Conditions 39](#_Toc195465697)

[4.4.21 Fronting 39](#_Toc195465698)

[4.4.22 Business Continuity and Disaster Recovery Plans 40](#_Toc195465699)

[4.4.23 Supplier Due Diligence 40](#_Toc195465700)

[4.4.24 Sub-contracting as a condition of tender 40](#_Toc195465701)

[4.4.25 Preference Goal Requirements conditions 40](#_Toc195465702)

[4.4.26 Declaration of compliance and acceptance SCC 41](#_Toc195465703)

[5.1.1 INSTRUCTION AND POINT ALLOCATION 46](#_Toc195465704)

[Annex A: Bidder substantiating evidence 51](#_Toc195465705)

[6. Technical Mandatory Requirement Evidence 51](#_Toc195465706)

[6.1 Bidder Certification / Affiliation Requirements 51](#_Toc195465707)

[6.1.1 (a) Independent Communication Authority 51](#_Toc195465708)

[6.1.2 (b) Internet Service Coverage Requirements (ISP/POPs) 51](#_Toc195465709)

[6.1.3 (c) Internet Service Coverage Requirements (ISP) 51](#_Toc195465710)

[6.1.4 (d) Internet Routing Requirements 51](#_Toc195465711)

[6.1.5 (e) International Connectivity Requirements (ASN/BGP) 51](#_Toc195465712)

[6.1.6 (f) Internet Routing Requirements 52](#_Toc195465713)

[6.1.7 (g) International Connectivity Requirements 52](#_Toc195465714)

[6.1.8 (h) International Peering Connectivity Requirements 52](#_Toc195465715)

[6.2 Bidder Experience and Capability Requirements 52](#_Toc195465716)

[6.3 Special Conditions of Contract 53](#_Toc195465717)

[6.4 Third Party Risk Management Assessment 54](#_Toc195465718)

[6.6 Technical Functionality Requirements 54](#_Toc195465719)

[6.7 Preference Points Preferential Goals Evidence 54](#_Toc195465720)

[Annex B: THIRD-PARTY RISK MANAGEMENT (TPRM) ASSESSMENT 56](#_Toc195465721)

[7. Instructions 56](#_Toc195465722)

[7.1 Evaluation Criteria 56](#_Toc195465723)

[7.1.1 Company risk 56](#_Toc195465724)

[7.1.2 All questions for all other risk elements: 57](#_Toc195465725)

[7.2 Third Party Risk Assessment 57](#_Toc195465726)

[7.3 Third Party Risk Management Declaration 60](#_Toc195465727)

[7.3.1 Declaration of Acceptance 60](#_Toc195465728)

[Annex C: Product/Service Functional Requirements ADDENDUM 1 62](#_Toc195465729)

# Introduction and background

## Purpose

The purpose of this **RFP (Request for Proposal)** to invite Suppliers (hereafter referred to as “bidders”) to submit proposals for the design, installation, configuration, provision including, maintenance and technical support of Internet bandwidth solution to SITA and its clients for a period of **five (05) years**.

## Background

The Internet and Security team within NTSS plays a pivotal role in facilitating Internet and extranet connectivity services for various NGN clients, including SITA. These services are integral for accessing the wider Internet landscape and facilitating external email communications. The contract replacement is requested by SITA to deliver on the Internet and Internet related services required for SITA clients and Government as a whole.

The services offered by the I&S team are foundational in supporting the broader platform. The NGN core, responsible for Wide Area Networking (WAN) connectivity between departmental sites, synergizes with I&S services to enable seamless communication via email and the Internet. This communication spans intra-departmental, inter-departmental, and external third-party interactions, thereby facilitating comprehensive external communication and e-Government initiatives. The I&S services augment the NGN core's capabilities, enhancing the overall offering and ensuring a robust communication infrastructure.

The Internet and Security Services team within Network Technology and Strategy Service is responsible for providing Internet and extranet connectivity services to SITA itself, all the NGN clients and the SAPS client.

* 1. It is of critical importance that SITA has the internet contract in place to ensure that:
		1. Internet services at large is provided to SITA itself, all the NGN clients and the SAPS client.
		2. Inbound and outbound flow of all external e-mail for clients that do not make use of the general upstream mail cleansing service provided by SITA.
		3. To ensure SITA can continue supporting and honouring currently contracted Internet and Security Service Level deliverables.
		4. To accommodate growth - The growth in demand for Internet based and bandwidth intensive services has increased dramatically over the past few years and the client base require more, faster and cheaper connectivity. In addition to the regular upgrading required to accommodate growth in existing services, SITA needs to be able to provide Internet bandwidth to other services that are accessed via the Internet – such as the Cloud services – or other services that clients (or SITA) develop for market or in support of Government initiatives such as SA Connect and Broadband network connectivity.
		5. SITA also must ensure the service provider for the contract and the contract itself are able to cater for rapid deployment of large amounts of bandwidth. An example of this type of requirement which is addressed in this contract is the Broadband Network.
	2. In addition, this bid will need to accommodate the below Internet Services URGENT requirements:
		1. Provision of fully redundant, protected and secure breakout points to the three SITA Internet breakout points located at SITA centurion, SITA Cape town and SITA Pietermaritzburg.
		2. Provision of fully redundant, protected connectivity links from the three DMZs (SITA Centurion, SITA Cape town and SITA Pietermaritzburg) to TERACO (NAPAFRICA) in each individual TERACO data centre in Cape Town, Johannesburg and Durban, that will be used for the Internet peering purpose and failover access to tenants located at the Internet Exchange at these locations.
		3. Full upstream Redundancy with backup links that are triangulated between three SITA which are located at SITA Cape town, SITA Centurion and SITA Pietermaritzburg.
		4. A fully protected layer 2 service that is provisioned over a fibre network that utilizes geographically diverse fibre routes to ensure the maximum uptime of the underlay network in each of the SITA DMZ locations.
		5. SITA requires the Internet Service to include DDOS mitigation for all DDOS traffic that may transit via the Service Providers network to the SITA.
		6. Migrate and configure the existing Internet Connectivity and Internet Services to the new high-bandwidth Internet Connectivity and Services.
		7. Addressing the current datacentre relocation from SITA Observatory to the new tier 3 Africa Data Centre while ensuring seamlessly delivery of the Internet service to the client base if not completed by the time the current contract is replaced.
		8. Provide, maintain and technical support Internet Services at contracted Service Level Agreement (SLA) and Service Performance Metrics for a period of five (05) years, which include the security SLA.

# Scope of Bid

## Scope of Work

The scope of work for the bidders is as follow:

* 1. Supply, install and provision of high-capacity bandwidth internet connectivity that offers complete, fully redundant and secure Internet architecture with the below requirements.
		1. Provision of fully redundant, protected and secure breakout points to the three SITA Internet breakout points located at **SITA centurion**, **SITA Cape town** and **SITA Pietermaritzburg**. Network Diagram **see section 3.1 table 2.**
		2. Provision of three point to point links triangulated between **SITA Centurion**, **SITA Cape town** and **SITA Pietermaritzburg.**
		3. Provision of fully redundant, protected connectivity links from the three DMZs (**SITA Centurion, SITA Cape town** and **SITA Pietermaritzburg**) to **TERACO (NAPAFRICA**) in each individual TERACO data centre in Cape Town, Johannesburg and Durban, that will be used for the Internet peering purpose and failover access to tenants located at the Internet Exchange at these locations.
		4. A **fully protected layer 2 service** that is provisioned over a fibre network that utilizes **geographically diverse fibre routes** to ensure the maximum uptime of the underlay network in each of the SITA DMZ locations.
		5. Full upstream ISP internal redundancy within the ISP's and SITA's own ASN space with backup links that are triangulated between three SITA sites which are located at **SITA Cape town**, **SITA Centurion** and **SITA Pietermaritzburg**.
		6. **DDOS mitigation** for all DDOS traffic that may transit via the Service Providers network.
	2. Maintenance and Technical Support:
		1. Annual Maintenance and technical support for a period of **five (5) years** must be included in the offering.
		2. The bidder must be accredited or certified to do maintenance and technical support of the high-capacity internet bandwidth Solutions.
		3. The service provider will be responsible to manage the solution throughout the duration of the contract.
	3. Provide Professional Services:
		1. Design of required high-capacity Internet architecture solution and integration of the requirements.
		2. Project management for the installation and configuration of the Internet architecture solution.
		3. Transfer of skills to SITA NTSS technical support resources.
		4. Develop the handover documentation where necessary.
		5. Implementation plan for the solution with timelines.

## Delivery address

The services must be supplied or provided at the following physical address(es).

Table 1: Delivery address

| **No** | **SITA** | **Physical Address** |
| --- | --- | --- |
| 1 | SITA Centurion | 1 John Vorster Road, Pretoria |
| 2 | SITA Pietermaritzburg | Natalia Building, 330 Langalibalele (former Longmarket) Street, Pietermaritzburg, 3201 |
| 2 | SITA Cape Town | Black River Park, Fir StreetObservatory, CAPE TOWN**(Note: The Cape Town site address is subject to confirmation at time of contract)**New Address**108 De Waal Street, Elfindale, Diep River CPT** |

## Current Customer Infrastructure

Internet traffic enters the SITA-managed perimeter network from the Internet Service Provider (ISP) via an ISP router located on site at each of the two current SITA Points of Presence, PoPs, located in Centurion and Cape Town.

Traffic is distributed from the Government Internet Exchange (or GIX) within the SITA perimeter network to a few Client VPNs each allocated their own unique IP address space as a sub allocation of the provider-independent IP address space allocated to the South African Government.

The SITA-operated network infrastructure for Government employs a core network with MPLS-based VPNs, providing segregation of traffic for departments. The departments create their own security policies for their VPNs and the DMZ of each VPN is architected to give effect to these policies.

SITA currently has two Internet breakout points in Centurion and Cape Town, configured in active-active mode, with a triangulation setup via the ISP’s backbone.

Internet bandwidth capacity is as follows:

* Centurion Internet Breakout - 30Gbps
* Cape Town Internet Breakout - 40Gbps
* Cape Town - Centurion ISP triangulation setup - 30Gbps

**Figure 1:** Internet breakout points



# Requirements

## Product / Service / Solution Requirements

SITA is a service provider and, for the most part, acts as the sole Internet Service Provider for the Government. Its clients are various national and provincial government departments which have a degree of autonomy in the establishment and operation of their IT systems and use a variety of internet services.

The requirement in the **RFP** is for the provision of high-bandwidth Internet services with maintenance and technical support to SITA and its clients and it must cater for underlay network to be **100 Gbps capable**, with the capability to commence the Internet service with **40Gbps** of provisioned internet bandwidth, with the capability to scale the Internet service to **100 Gbps** in all three of SITA’s POPs.

During the period of the contract the upstream bandwidth described above will need to be increased on an ad hoc basis according to SITA and its customer requirements while still staying within the bounds of the contract.

**Although this bandwidth will be allocated between the PoPs based on demand at each centre, the solution must provide the bandwidth as a total bandwidth pool available at each SITA PoP so that SITA need not specify the split to the provider and that reallocation to a single PoP should be automatic and seamless in the event of a failover scenario.**

The supplier must provide layer 2 connectivity between the SITA PoPs in Cape Town, Centurion and Pietermaritzburg for SITA DMZ triangulation at 100G in order to facilitate backhauling of traffic to provide additional redundancy and SITYA internal DMZ failover scenario.

The solution must be complete and functional according to minimum performance standards and statement of work set out below in this document. Any rectification of shortcomings in the proposed solution requiring any additional expenditure will be for the supplier's account.

### Installation and Configuration, Technical and Solution Requirements

* 1. Supply and install high bandwidth internet connectivity that offers complete and fully redundant Internet architecture with the following below requirements:
		1. Provision of fully redundant, protected and secure breakout points to the three SITA Internet breakout points located at **SITA Centurion**, **SITA Cape town** and **SITA Pietermaritzburg**. Network Diagram **see section 3.1 table 2.**
		2. Three point to point links triangulated between **SITA Centurion**, **SITA Cape town** and **SITA Pietermaritzburg.**
		3. Provision of fully redundant, protected connectivity links from the three DMZs (**SITA Centurion, SITA Cape town** and **SITA Pietermaritzburg**) to **TERACO (NAPAFRICA**) in each individual TERACO data centre in Cape Town, Johannesburg and Durban, that will be used for the Internet peering purpose and failover access to tenants located at the Internet Exchange at these locations.
		4. A **fully protected layer 2 service** that is provisioned over a fibre network that utilizes **geographically diverse fibre routes** to ensure the maximum uptime of the underlay network in each of the SITA DMZ locations.
		5. Full upstream ISP internal redundancy within the ISP's and SITA's own ASN space with backup links that are triangulated between three SITA sites which are located at **SITA Cape town**, **SITA Centurion** and **SITA Pietermaritzburg**.
		6. **DDOS mitigation** for all DDOS traffic that may transit via the Service Providers network

**Figure 2:** Internet connectivity



* 1. All links and network infrastructure indicated in blue above must be provided by the bidder as described below:
		1. SITA requires the service provider to establish on-site presence in **Centurion**, **Cape** Town and Pietermaritzburg locations.
		2. SITA requires a fully protected layer 2 service to be provided between the following locations:

|  |  |
| --- | --- |
| **Between:** | **Speed:** |
|  Centurion and Cape Town |  100Gbps |
|  Centurion and Pietermaritzburg  |  100Gbps |
|  Cape Town and Pietermaritzburg |  100Gbps |

* + 1. SITA requires the capability to be able to connect 6 x 100 Gbps network devices to the providers on site nodes in the follow locations meaning in each POP the provider must deploy a device with 6 x 100gbps ports:

| **Location** | **Speed:** |
| --- | --- |
|  Centurion and Cape Town |  6 X 100Gbps |
|  Centurion and Pietermaritzburg  |  6 X 100Gbps |
|  Cape Town and Pietermaritzburg | 6 X 100Gbps |

* + 1. SITA requires a protected layer 2 service for Internet IP transit to be provided in the following locations:

|  |  |  |
| --- | --- | --- |
| **Location** | **Provisioned speed** | **Speed:** |
|  Centurion  | 40Gbs | 100Gbps |
|  Cape Town  | 40Gbs | 100Gbps |
|  Pietermaritzburg | 40Gbs | 100Gbps |

* + 1. Provider needs to provide a network architecture diagram demonstrating the use of diverse fibre routes and diverse fibre providers to ensure maximum uptime of the underlay network.
		2. SITA requires the underlay network to be 100 Gbps capable, with the capability to commence the Internet service with 40Gbps of provisioned internet bandwidth and with the capability to scale the Internet service to 100 Gbps in all three of SITA’s POPs.
		3. SITA additionally requires dedicated 20 Mbps links from the service providers network to Centurion, Cape Town and Pietermaritzburg and these links must carry permanently allocated static IP addresses from the Service Providers ASN to allow out-of-band management of the SITA environment by the SITA staff.
		4. The provider must accept /28 prefixes and propagate those prefixes across their network, to allow SITA to selectively advertise /28 prefixes to the ISP out of any one of their POPs. The ISP may however aggregate these according to Internet standards to the rest of the world.
		5. SITA requires the Internet Service to include DDOS mitigation for any and ALL DDOS traffic that may transit via the Service Providers network to the SITA ASN 37130
		6. SITA requires BGP peering with the ISP’s Internet service transit edges to the SITA BGP peering links to allow SITA to use BGP flow spec to advertise traffic limits and traffic filters to prevent traffic from transiting across from the provider’s ASN to the SITA ASN 37130 to prevent DDOS type of traffic from over utilising the transit peering links and effecting SITA NGN client service with upstream illegitimate traffic.
		7. Full upstream Redundancy with backup links that are triangulated between three SITA DMZs which are located at SITA Cape town, SITA Centurion and SITA Pietermaritzburg.
		8. Ensure that each breakout point can carry and provide Internet connectivity for the full bandwidth procured at any point in time.
		9. The equipment deployed on SITA at the SITA POPs, must be capable of establishing connectivity to Huawei networking equipment.
		10. The provider is responsible for managing the fault life cycle of all layer 1 protected service links. SITA will not interact with any third parties that the bidder contracts in to provide the service, this is entirely the bidder’s responsibility.
		11. To provide continuous service quality evaluation for the full duration of the contract. Failure to deliver the service in accordance with the contract service parameters and required uptime metrics will result in penalties.
		12. Provide individual connectivity between the three DMZs (SITA Centurion, SITA Cape town and SITA Pietermaritzburg to TERACO (NAPAFRICA) that is used for Microsoft peering, other internet exchange providers and failover access to TERACO.
	1. Migrate and configure the existing Internet Connectivity and Internet Services to the new high-bandwidth Internet Connectivity and Services.
	2. Addressing the current datacentre relocation from SITA Observatory to the new tier 3 Africa Data Centre while ensuring seamlessly delivery of the Internet service to the client base if not completed by the time the current contract is replaced.
	3. Provide, maintain and technical support Internet Services at contracted Service Level Agreement (SLA) and Service Performance Metrics for a period of five (5) years as follows:

**Hardware and Network Extension to SITA PoPs**

* + 1. The supplier must extend its network to the designated SITA PoPs (Centurion, Cape Town and Pietermaritzburg).
		2. This includes the installation of the supplier's own managed routers, switches, network infrastructure, and fibre, or any necessary equipment to deliver the required solution.
		3. All infrastructure and cabling upstream of SITA’s owned and managed routers/switches is the responsibility of the service provider.
		4. The service must be provided on hardware owned by the service provider.
		5. The service provider will be bound by a Service Level Agreement (SLA) to provide and maintain sufficient hardware to meet the required mail delivery times.
		6. These requirements must include, but are not limited to, floor/rack space, power requirements including consumption, and thermal emissions in BTUs.
		7. The supplier will be liable for SITA-imposed charges at applicable rates for hosting such a cabinet/rack.
		8. Installation of infrastructure must adhere to SITA-approved Switching Centre standards.
		9. The service provider will be responsible for the insurance of their own equipment.

**Service Termination**

* + 1. The service must be supplied to and terminated on the designated network ports on SITA infrastructure at each SITA premises.
		2. The connectivity requirement: 100G fibre hand off will be required.

**Architectural Restrictions and Protocols**

* + 1. Supplier must note that all documents and designs created for SITA will be owned by SITA.

### Performance Requirements

1. **Solution Architecture and Network Design**
	* 1. The solution architecture and network design must ensure continuous operation between the three Points of Presence (PoPs), maintaining full load handling in a redundant or fail-over configuration. SITA will supply public address spaces in this regard.
2. **Bandwidth and Capacity Management**
	* 1. The supplier must ensure sufficient bandwidth is always provided in both upstream and downstream directions and upgrade the bandwidth when necessary.
		2. Capacity management of all service aspects is the responsibility of the service provider.

### Administration and Reporting Requirements

* + 1. The supplier must provide an on-line reporting portal for SITA to access real-time as well as historical information in the form of graphs, statistics and reports.
		2. Reporting must use a sampling/averaging window of no greater than 5 minutes.
		3. All service data must be available on-line for the full-service contract period at the required 5-minute granularity. No roll-up /summarizing / re-averaging of data is permitted.
		4. The reporting tool must be able to preserve peaks within any reporting window.
		5. Data from the portal/s must be available in XML or CSV format on demand.
		6. The portal required for this service must provide reports on at least, but not limited to, the following elements: Total bandwidth utilization:
	+ Total bandwidth utilization
	+ Excess traffic
	+ Dropped traffic
	+ Latency
	+ Reachability
	+ Availability
	+ DDOS traffic reporting ie traffic passed and traffic blocked
	+ BGP flow spec injection reporting (What dropped/null routed)
	+ NETFLOW reporting (web interface)

All the above information must be available on the total solution as well as on a per PoP basis.

* + 1. Access to the portal must be restricted to SITA Support staff.
		2. SITA will require monthly Service Management meetings with full reporting on all aspects of the service at each meeting. The reports must be supplied in hard copy at the meetings.
		3. SITA will require electronic reports on the SLA metrics and the link utilization by close of business on the 3rd day of the month following the reporting period.
		4. SITA will require all RCA reports to be submitted to SITA within 3 working days of the associated fault / incident having been resolved.

**Benchmarking:**

* + 1. SITA will have the right, not more than once per annum, and not commencing prior to the second year of the contract, to benchmark the service provider’s performance on some or all of the services and/or some or all of the charges, as designated by SITA.
		2. Benchmarking will be conducted by an independent industry-recognised benchmarking service provider (Benchmarker) designated by SITA and approved by the partner and such approval shall not be unreasonably withheld.
		3. When engaging the Benchmarker, the Benchmarker will be directed to:
		4. Make all commercially reasonable efforts to complete its analysis within 90 days after its engagement, to the extent practical;
		5. Select a representative sample of organisations, which shall be of a sufficient number as determined by the Benchmarker in its sole discretion and may include some services for which the partner is also the service provider; and
		6. Perform any normalisation that is reasonably required.
		7. SITA on the one hand, and the partner on the other hand, will each bear their own costs incurred in connection with the benchmarking and will share equally the Benchmarker’s fees and expenses. The Parties will cooperate with the Benchmarker as reasonably requested by the Benchmarker, including, as appropriate, making available knowledgeable personnel and pertinent documents and records. The Benchmarker will enter into a confidentiality agreement with SITA prior to being provided with confidential information of either Party.
		8. Each Party will be provided a reasonable opportunity to review, comment on, and request changes in the Benchmarker’s proposed findings. The Benchmarker will have sole discretion as to how it addresses such requests. Following such review and comment, the Benchmarker will issue a final report of its findings and conclusions.

**Performance Benchmarking:**

* + 1. The Benchmarker will review the partner’s performance of the services for which there are service levels, comparing the partner’s achieved levels to the service level target.
		2. The ‘service level target’ shall mean that each service level under this agreement for any service element subject to the benchmarking is at least as good as the service levels in the highest (i.e., ‘most favourable to SITA’ quartile of the service levels for similar services by other organisations.
		3. If the Benchmarker concludes that the service provider’s performance of the services is below the service level target, the service provider shall, within 30 days after the Benchmarker’s decision, develop for SITA review and approval, a plan to bring the performance up to the service level target as soon as practically possible and in all events within 90 days after the approval of such plan. The service levels will be adjusted accordingly effective 90 days after SITA approves the plan. The partner will bear the costs of the implementation of the plan.

**Price Benchmarking:**

* + 1. The Benchmarker will review the partner’s pricing of the services provided under the service contract to SITA, comparing the pricing to the market sector for services that are essentially the same in terms of committed service levels and volumes.
		2. The ‘price level target’ shall mean that each service price under this agreement for any service element subject to the benchmarking, is at least as good as the price levels in the highest (i.e., ‘most favourable to SITA’ quartile of the service levels for similar services by other organisations.
		3. If the Benchmarker concludes that the service provider’s pricing of the services is above the price level target, the service provider shall, within 30 days after the Benchmarker’s decision, develop for SITA review and approval, a revised pricing plan to bring the pricing in line with the Benchmarker’s findings as soon as practically possible and in all events backdated to the date of the findings. The partner will bear the costs of the implementation of the plan.

###  Internet service solution requirement components

**Table 2:** Bill OF Material components

| **Item** | **Requirement**  |
| --- | --- |
| Supply, install and provision of high-capacity bandwidth internet connectivity that offers complete, fully redundant and secure Internet architecture with the below requirements. | * + 1. Provision of fully redundant, protected and secure breakout points to the three SITA Internet breakout points located at **SITA centurion**, **SITA Cape town** and **SITA Pietermaritzburg**. Network Diagram **see section 3.1 table 2.**
		2. Provision of three point to point links triangulated between **SITA Centurion**, **SITA Cape town** and **SITA Pietermaritzburg.**
		3. Provision of fully redundant, protected connectivity links from the three DMZs (**SITA Centurion, SITA Cape town** and **SITA Pietermaritzburg**) to **TERACO (NAPAFRICA**) in each individual TERACO data centre in Cape Town, Johannesburg and Durban, that will be used for the Internet peering purpose and failover access to tenants located at the Internet Exchange at these locations.
		4. A **fully protected layer 2 service** that is provisioned over a fibre network that utilizes **geographically diverse fibre routes** to ensure the maximum uptime of the underlay network in each of the SITA DMZ locations.
		5. Full upstream ISP internal redundancy within the ISP's and SITA's own ASN space with backup links that are triangulated between three SITA sites which are located at **SITA Cape town**, **SITA Centurion** and **SITA Pietermaritzburg**.
		6. **DDOS mitigation** for all DDOS traffic that may transit via the Service Providers network.
 |
| Maintenance and Technical Support. | * + 1. Annual Maintenance and technical support for a period of five (5) years must be included in the offering.
		2. The bidder must be accredited or certified to do maintenance and support of the proposed Solutions.
		3. The service provider will be responsible to manage the solution throughout the duration of the contract.
 |
| Provide Professional Services: | * + 1. Design of required Internet architecture solution and integration requirements.
		2. Project management for the installation and configuration of the Internet architecture solution.
		3. Transfer of skills to SITA NTSS technical support resources.
		4. Develop the handover documentation where necessary.
		5. Implementation plan for the solution with timelines
 |

## Service Elements

### Full-Service Agreement

Incident Priorities are defined as follows –

* 1. **Priority 1 (Critical)** - An Incident will be assigned a “Priority Level 1” if the Incident has the potential of having a high business impact on SITA Client e.g. an outage affecting a large and substantial number of SITA Client users performing critical functions.
	2. **Priority 2 (High)** - An Incident will be assigned as “Priority Level 2” if it has the potential of a noticeable impact on SITA Client but does not rise to the level of a Priority 1 incident. Without limiting the generality of the foregoing, examples of Priority 2 incidents include outages that affect multiple SITA Client users performing non-critical functions.
	3. **Priority 3 (Medium)** - An Incident will be assigned as “Priority Level 3” if the incident has the potential to have minimal impact on SITA Client or a significant impact on a single user. Without limiting the generality of the foregoing, examples of Priority 3 incidents include outages affecting a single SITA Client user.
	4. **Priority 4 (Low)** -An Incident will be assigned as “Priority Level 4” if the incident is a trivial incident with little or no impact to SITA Client or a user that does not rise to the level of a Priority 1, Priority 2 or Priority 3 incident.

**3.2.2 Response time and distance**

The below are committed Incidents Resolution Service Level per priority

**Table 3:** Response time and distance

| **Priority** | **Response Time** | **Resolution Time** |
| --- | --- | --- |
| P 1  | 15 minutes (24/7/365) | 4 Hour (24/7/365) |
| P 2  | 30 minutes (24/7/365) | 6 Hours (24/7/365) |

* + 1. **Fault logging management**

**Table 4:** Fault logging management

| **Respond** | **Service Measure** | **Service Level** |
| --- | --- | --- |
| **Incident Management** | Number of Incidents responded to within the target time. | 99% of Incidents responded to within the target time. 100% of Incidents will be responded to within the target time + 25% |
| **Method** | The Service Levels are measured and reported on individually from the time that the Incident is logged by Client at the Service Provider's Service Desk until the time that the Incident is accepted on the Service Provider's Service Desk. |
| **Formula** | Number of Incident tickets responded to within Service Level Target / Total number of Incident tickets responded to \* 100 (Calculation - each incident is measured, Met=1, Miss = 0, If 10 incidents and 9 is met calculation is (9/10)\*100=90%) |
| **Exclusions** | Incidents with respect to Infrastructure not architected for the specific priority response time, shall be reported on as KPIs. |
| **Measurement Interval** | Measured and Reported Monthly |
| **Measurement Tool** | To be done via the SITA service management tool ("**ITSM**") |
| **Resolve** | **Service Measure** | **Service Level** |
| **Incident Management** | Number of Incidents responded to within the target time. | 99% of Incidents responded to within the target time. 100% of Incidents will be responded to within the target time + 25% |
| **Method** | The Service Levels are measured and reported on individually from the time that the Incident is logged by Client at the Service Provider's Service Desk until the time that the Incident is resolved on the Service Provider's Service Desk. In year one the Service Provider is responsible for the SITA cloud support group until the call is resolved by the SITA group including the Service Provider internal performance |
| **Formula** | Number of Incident tickets responded to within Service Level Target / Total number of Incident tickets responded to \* 100 (Calculation - each incident is measured, Met=1, Miss = 0, If 10 incidents and 9 is met calculation is (9/10)\*100=90%) |
| **Exclusions** | Incidents with respect to Infrastructure not architected for the specific priority response time, shall be reported on as KPIs. |
| **Measurement Interval** | Measured and Reported Monthly |
| **Measurement Tool** | To be done via the SITA service management tool ("**ITSM**") |

# Bid Evaluation Stages

* 1. The bid evaluation process consists of **the following stages**, according to the nature of the bid.
	2. A Bidder must qualify for each stage to be eligible to proceed to the next stage of the evaluation. The stages are:

Table 5: Bid Evaluation Stages

|  |  |  |
| --- | --- | --- |
| **Stage** | **Description** | **Applicable for this bid YES/NO** |
| Stage 1  | Mandatory Administrative requirements | YES |
| Stage 2  | Technical Mandatory requirement | YES |
| Stage 3 | Technical Functional Requirements | YES |
| Stage 4 | Special Conditions of Contract verification | YES |
| Stage 5 | Price and Preference points | YES |

## Mandatory Administrative responsiveness (Stage 1)

### Attendance of briefing session

1. **A Non-Compulsory Virtual briefing session will be held**. The bidder must sign the briefing session attendance register using the same information (bidder company name, bidder representative person name and contact details) as submitted in the bidder’s response document.
2. Bidders need to complete **all the SBD documents** which needs to be submitted as stated in the Invitation to Bid Document.

### Registered Supplier

1. Only responses from bidders who are registered as a Supplier on National Treasury’s Central Supplier Database (CSD) in terms of National Treasury’s Instruction Note 4A of 2016/17 will be considered for award on this **RFP**.
2. In the case of joint ventures or consortiums the bidder must demonstrate that at least one of the parties to the bid response attended the briefing session.

### Bid Submission Instructions

**Note that a Two Envelope process will be followed and therefore bidders must submit as follows:**

1. **One (1) original file excluding pricing** which must be submitted in **a separate envelope**.
2. **One (1) hard copy excluding pricing** which must be submitted in **a separate envelope**.
3. **One (1) electronic copies on USB memory stick/ flash drive** in Portable Document Format (**PDF) of the RFP Document and Technical / Functionality Response**.
4. **One (1) electronic copies on USB memory stick/ flash drive** in Portable Document Format **(PDF)** **of pricing only**.
5. It is the Bidder’s responsibility to ensure that the information and contents on the electronic copies is the same as in the hard copies.
6. To ensure that the electronic copies are not damaged, the bidder must submit the USB’s (memory stick/ flash drive) in a sealed padded envelop and be clearly marked.
7. Bidders shall submit proposal responses in accordance with the prescribed manner of submission as specified above. **Failure to comply with the above instructions on submitting a proposal will lead to disqualification.**
8. The **RFP** Responses (hard and electronic copies) must be clearly marked as follows: Bidder’s Name & Contact Details, **RFP** Number, **RFP** Description, and Closing Date.
9. All Bids in this regard shall only be accepted if they have been placed in the tender box before or on the closing date and stipulated time.
10. Late bids shall not be considered.
11. The proposal must be signed by an authorised employee, agent or representative of the bidder. The proposal must bear the initials of the signatory at the bottom of every page as an indication that the bidder has familiarised itself with the terms and conditions of this **RFP** document.
12. Faxed or e-mailed bids will not be accepted.
13. Bidders shall submit proposal responses in accordance with the prescribed manner of submission as specified in this document. **Failure to comply with the bid submission requirements will lead to disqualification.**
14. Bidders are required to submit all returnable documents/information together with their Bids/proposals on or before the closing time and date of the Bids/proposals.
15. All services supplied in accordance with the bidder’s proposal must be in accordance with all applicable legal requirements in terms of South African law, policies and regulations.

## Technical returnable documents

### Instruction and evaluation criteria

1. The bidder must comply with ALL the requirements as per the Technical Mandatory Requirements below by providing substantiating evidence in the form of documentation or information, failing which it will be regarded as “NOT COMPLY”.
2. The bidder must provide a unique reference number (e.g. binder/folio, chapter, section, page) to locate substantiating evidence in the bid response.
3. The bidder must comply with ALL the TECHNICAL MANDATORY REQUIREMENTS for the bid response to proceed to the next stage of the evaluation.

### Technical mandatory requirements (Stage 2)

Table 6: Technical Mandatory Requirements

| **Mandatory Requirements** | **Substantiating evidence of compliance (used to evaluate bid)** | **Evidence reference (to be completed by bidder)** |
| --- | --- | --- |
| 1. **BIDDERS CERTIFICATION/AFFILIATION REQUIREMENTS**
 |
| 1. **Independent Communication Authority**

The Bidder must be licensed by the Independent Communication Authority of South Africa (ICASA) for the following:1. Individual Electronic Communication Network Service (IECNS); and
2. Individual Electronic Communications Service (IECS) operator.
 | Attach to **ANNEX A** a copy of valid documentation (letter/certificate/license) as proof that the Bidder is licensed by the Independent Communication Authority of South Africa (ICASA) for the following:1. Individual Electronic Communication Network Service (IECNS); and
2. Individual Electronic Communications Service (IECS) operator.

**NOTE (1):** SITA reserves the right to verify information provided. | <provide unique reference to locate substantiating evidence in the bid response – see **Annex A,** **paragraph 6.1 (a)** > |
| 1. **Internet Service Coverage Requirements (ISP/POPs)**

The Bidder must be an Internet Service Provider (ISP) who operates a national core backbone with Points of Presence (POPs) within the Cape Town, Pietermaritzburg and Tshwane Metro areas. | Attach to **ANNEX A** a copy of valid documentation (Map Coverage) as proof that the Bidder has presence (POPs) across South Africa, including POPs in Cape Town, Pietermaritzburg and Tshwane Metro.**NOTE (1):** SITA reserves the right to verify information provided. | <provide unique reference to locate substantiating evidence in the bid response – see **Annex A paragraph 6.1 (b) >** |
| 1. **Internet Service Coverage Requirements (ISP)**

The Bidder must be an Internet Service Provider (ISP) who obtains international capacity directly from undersea cable operators. | .Attach to **ANNEX A** a copy of valid documentation (letter/certificate/license) as proof that the Bidder is an Internet Service Provider (ISP) who obtains international capacity directly from undersea cable operators.**NOTE (1):** SITA reserves the right to verify information provided. | <provide unique reference to locate substantiating evidence in the bid response – **see Annex A, paragraph 6.1 (c) >** |
| 1. **Internet Service Coverage Requirements**

The Bidder must be an Internet Service Provider (ISP) who owns and operates network infrastructure at international points of presence and has negotiated its own transit and peering with International Internet providers. | Attach to **ANNEX A** a copy of valid documentation (letter/certificate/license/affidavit) as proof that the Bidder is an Internet Service Provider (ISP) who owns and operates network infrastructure at international points of presence and has negotiated its own transit and peering with International Internet providers. The evidence documentation must indicate the following:1. Individual Electronic Communication Network Service (IECNS); and
2. Individual Electronic Communications Service (IECS) operator.

**NOTE (1):** SITA reserves the right to verify information provided. | <provide unique reference to locate substantiating evidence in the bid response – **see Annex A, paragraph 6.1 (d) >**  |
| 1. **Internet Peering Requirements (ASN/BGP)**

The Bidder must have a public Autonomous System Number(s) (ASN) to peer with SITA using Border Gateway Protocol (BGP) without stripping or altering SITA’s ASN in any way and must be able to support the 4-byte ASN format. | The Bidder **must** provide a valid documentation (letter or a sworn affidavit) indicating a valid registrar-assigned, non-private Autonomous System Number(s) (ASN).**NOTE (1):** All documentation (letter or a sworn affidavit) must be dated and signed.**NOTE (2):** SITA reserves the right to verify information provided. | <provide unique reference to locate substantiating evidence in the bid response – **see Annex A, paragraph 6.1 (e) >** |
| 1. **Internet Routing Requirements**

SITA requires the ability to advertise individual /28 routing prefixes and for the service provider to accept and advertise these within the providers network to ensure the shortage routing path from the Providers ASN to the closest of the 3 SITA POPs where these individual /28 subnets may migrate between dynamically.**NOTE (1):** These individual /28 routing prefixes may be summarised to peers or transit providers.  **NOTE (2):**  This is a critical requirement and forms part of SITA’s Business Continuity planning in order to support per client fail over should the need arise. | The Bidder **must** provide a valid documentation (letter or a sworn affidavit) indicating they have the ability to accept and advertise individual /28 routing prefixes within the provider’s network.**NOTE (1):** All letters must be dated and signed.**NOTE (2):** SITA reserves the right to verify information provided. | <provide unique reference to locate substantiating evidence in the bid response – **see Annex A, paragraph 6.1 (f) >** |
| 1. **International Connectivity Requirements**

The Bidder **must** have continuously supplied transit bandwidth to its customer/s for a minimum period of five (05) years via international landing points on at least two (02) of the following continents: Europe, Asia or North America in the past five (05) from the publication of this bid.  | The Bidder **must** provide the following documentation for International Connectivity Requirements:1. Valid peering agreements between the bidder and international connectivity providers or a sworn affidavit, attesting that the bidder has international landing points on at least two (02) of the following continents: Europe, Asia or North America.
2. The Bidder must provide documentation (Letter, Agreement or Sworn Affidavit) as proof that the bidders has supplied transit bandwidth to its customer/s for a minimum period of five (5) years via international landing points on at least two (2) of the following continents: Europe, Asia or North America in the past five (05) from the publication of this bid.

**NOTE (1):** SITA reserves the right to verify information provided. | <provide unique reference to locate substantiating evidence in the bid response – **see Annex A, paragraph 6.1 (g) >** |
| 1. **International Peering Connectivity Requirements**

The supplier must peer with or obtain transit from multiple partners/suppliers at each of the landing points. | Attach to **ANNEX A** a copy of valid transit/peering agreements at each of the landing points must be in the company’s name (or a registered subsidiary / parent).**NOTE (1):** SITA reserves the right to verify information provided. | <provide unique reference to locate substantiating evidence in the bid response – **see Annex A, paragraph 6.1 (h) >** |
| 1. **Bidders Experience and Capability Requirements**
 |
| The Bidder must have provided, or be providing a total bandwidth of at least 100 Gbps to at least one (1) customer over a continuous period of a minimum of one (1) year in the past five (5) years from the publication date of this bid.**NOTE (1):** The Service provided must include the following:Installation; **and**Configuration; **and**Maintenance; **and**Support. | The Bidder must provide reference details by completing **table 12** from at least one (1) customer to whom a total bandwidth of at least 100 Gbps was provided over a continuous period of a minimum of one (1) year in the past five (5) years from the publication date of this bid.**NOTE (1):** The Service provided must include the following:Installation; **and**Configuration; **and**Maintenance; **and**Support.**NOTE (2):**The Bidder must provide the following information when completing **table 12**:* 1. Company name; **and**
	2. Reference Person Name, Tel and/or email; **and**
	3. Project Scope of Work; **and**
	4. Project Start and End-date.

**NOTE (3):** Failure to complete **table 12** fully as indicated above will result in disqualification.**NOTE (4):** **SITA reserves the right to verify information provided.** | <provide unique reference to locate substantiating evidence in the bid response – see **Annex A paragraph 6.2>**  |
| 1. **Special Conditions of Contract Acceptance**
 |
| The Bidder must accept the following:All the Special Conditions of Contract (SCC) as stated in **section 4.3**. | The Bidder **must** acknowledgethe Special Conditions of Contract (SCC) as stated in **section 4.3** by signing in the declaration of compliance and acceptance of SCC in **section 4.3.26.****NOTE (1):**Failure to complete and sign the SCC in **section 4.3.22** will result in disqualification. | <provide unique reference to locate substantiating evidence in the bid response – **see ANNEX A, paragraph 6.3>** |
| 1. **Third Party Risk Assessment**
 |
| The Bidder must confirm compliance to Third-Party Risk Management Assessment. | The Bidder must comply to the Third-Party Risk Management Assessment requirement by completing All the questions in **Annex B**. **NOTE 1:** SITA reserves the right to verify information provided.**NOTE (2):**Failing to complete all the questions, or not Accepting the Declaration of Acceptance above will result in disqualification. | <Provide unique reference to locate substantiating evidence in the bid response – **see Annex A, paragraph 6.4, and Annex B>** |
| 1. **Product/Service Functional Requirements**
 |
| **The Bidder must confirm compliance to the Product/Service Functional requirements.** | The Bidder must confirm that they comply with the **Product/Service Functional Requirements** by completing **Annex C: Addendum 1**.**NOTE (1):**Failure to comply fully to the requirements as indicated above will result in disqualification.**NOTE (2):** SITA reserves the right to verify information provided. | <provide unique reference to locate substantiating evidence in the bid response – **see Annex A, paragraph 6.5 and Annex C: Addendum 1>** |

## Technical Functionality evaluation Requirements (Stage 3)

1. The Bidder must complete in full all the TECHNICAL FUNCTIONALITY requirements.
2. The Bidder **must provide a unique reference number** (e.g. binder/folio, chapter, section, page) to locate substantiating evidence in the bid response. During evaluation, SITA reserves the right to treat substantiation evidence that cannot be located in the bid response, as “NOT COMPLY”.
3. The evaluation (scoring) of bidders’ responses to the requirements will be determined by the completeness, relevance and accuracy of substantiating evidence
4. Weighting of requirements: The score for the desktop evaluation of TECHNICAL FUNCTIONALITY REQUIREMENTS will be calculated as follows:
5. Each Bidder will be evaluated on each individual requirement as indicated in **table 6 and 7** below. The value scored for each requirement will be multiplied with the specified weighting for the relevant requirement to obtain the percentage achieved for each requirement.
6. SITA reserves the right to verify information / evidence provided by the Bidder.

**Table 6:** Technical Functionality Evaluation Rating Scale

| **Evaluation criteria**  | **Score** |
| --- | --- |
| **(Irrelevant)** (No information provided) | 0 |
| **Good** (Meets minimum requirements) | 3 |
| **Exceeds** (Significantly Exceeds minimum requirements) | 5 |

1. **Weighting of requirements:** The score for the desktop evaluation of TECHNICAL FUNCTIONALITY REQUIREMENTS will be calculated as follows:

**Table 7:** Technical Functionality Weighting Requirements

| **No.** | **Technical Functionality Requirements** | **Weighting** |
| --- | --- | --- |
| 1. | Period for the Full Functionality and Roll Out of the New Internet Architecture solution. | 50% |
| 2. | Installation and Configuration of the fully redundant Internet Architecture (Fully protected layer 2). | 50% |
| **TOTAL** |  **100%** |

1. **Minimum threshold**. To be eligible to proceed to the next stage of the evaluation the bid must achieve a minimum threshold score of **60%**.

**NOTE (1):**

The Bidder must achieve at least **60%** for each of the technical Functional requirement sections indicated in table above, failing which will result in disqualification.

**NOTE (2):**

SITA reserves the right to verify All the information provided.

**NOTE (3):**

Bidders should take note of the Minimum Requirements as well as the Minimum Threshold.

Should the bidder not meet the Minimum Requirements, or the Minimum Threshold the Bidder will be disqualified.

**Table 8:** Technical Functionality Requirements

| ***TECHNICAL FUNCTIONALITY REQUIREMENTS*** | ***Substantiating evidence and evaluation criteria****(used to evaluate bid)* | ***Weighting*** | ***Substantiation reference****(to be completed by bidder)* |
| --- | --- | --- | --- |
| 1. **Period for the Full Functionality and Roll Out of the New Internet Architecture solution**

The Bidder toclearly indicate how the project will be completed for the duration for the full functionality and rollout of the New Internet Architecture solution from contract effective date.(a) 100% rollout completed in **less than** three (03) months. (b) 100% rollout **completed within** three (03) months.(c) 100% rollout **completed in** **more than** three (03) months.**Minimum Requirement:**(b) 100% rollout **completed within** three (03) months. | **Evidence**The Bidder toprovide a Project plan clearly indicating how the project will be completed for the duration to roll out for the full functionality and Roll out of the New Internet Architecture solution.**Evaluation**0= **Does not meet minimum requirements:** No project plan provided ,or (c) project rollout is more than three (03) months.3= **Meets minimum requirements:** Project plan submitted indicates that 100% roll out to be completed within three (03) months (b).5= **Exceeds minimum requirements:** Project plan submitted indicates that 100% roll out to be completed in less than three (03) months (a).**NOTE (1):** SITA reserves the right to verify the information provided. | 50% | <provide unique reference to locate substantiating evidence in the bid response – **Annex A, section 6.6**> |
| **2. Installation and Configuration of the fully redundant Internet Architecture (Fully protected layer 2)**The Bidder toclearly indicate how the Installation and Configuration of the fully redundant internet architecture will be Installed and configured for the duration of the project.(a) Architecture only capable to address a **single route (non-diverse)** for layer 2 connectivity. (b) Architecture capable to address **redundant** layer 2 connectivity per Points-of Presence (POP) as defined in Section 3.1.(c) Architecture capable to address a **geographically diverse redundant** layer 2 connectivity per Points-of Presence (POP) as defined in Section 3.1.**Minimum Requirement:**(b) Architecture capable to address **redundant** layer 2 connectivity per Points-of Presence (POP) as defined in Section 3.1. | **Evidence**The Bidder toprovide an architecture diagram clearly indicating how the Installation and Configuration of the fully redundant internet architecture will be Installed and configured for the layer 2 connectivity solution. **Evaluation**0= **Does not meet minimum requirements:** No architecture diagram provided and, or does not comply with the minimum Requirement (b). 3= **Meets minimum requirements:** Architectural Diagram clearly explains the capability to address the **redundant** layer 2 connectivity per Points-of Presence (POP) as defined in Section 3.1.5= **Exceeds minimum requirements:** Architectural Diagram clearly explains the capability to address the **geographically diverse redundant** layer 2 connectivity per Points-of Presence (POP) as defined in Section 3.1.**NOTE (1):** SITA reserves the right to verify the information provided. | 50% | <provide unique reference to locate substantiating evidence in the bid response – **Annex A, section 6.6**> |

## Special Conditions of Contract Verification (Stage 4)

* 1. The successful supplier will be bound by Government Procurement: General Conditions of Contract (GCC) as well as this Special Conditions of Contract (SCC), which will form part of the signed contract with the successful Supplier. However, SITA reserves the right to include or waive the condition in the signed contract.
	2. **SITA reserve**s the right to –
	3. Negotiate the conditions, **or**
	4. Automatically disqualify a bidder for not accepting these conditions; **or**
	5. Award to multiple bidders; **or**
	6. Not to award; **or**
	7. To do a partial award.
1. In the event that the bidder qualifies the proposal with own conditions and does not specifically withdraw such own conditions when called upon to do so, SITA will invoke the rights reserved in accordance with subsection 4.4. (b) above.

### Special Conditions of Contract

### Contracting Conditions

1. **Formal Contract** - The supplier must enter a formal written contract (agreement) with SITA.
2. **Right to Audit** - SITA reserves the right, before entering a contract, to conduct or commission an external service provider to conduct a financial audit or probity to ascertain whether a qualifying bidder has the financial wherewithal or technical capability to provide the goods and services as required by this tender.
3. **Right of Award -** SITA reserves the right to award the contract for required goods or services to multiple Suppliers.

### Delivery Address

1. The supplier must deliver the required products or services at as indicated in **Section 2.2**, Delivery Address

### Losses

* 1. The bidder shall be held responsible for any losses caused to SITA due to the bidder’s or his sub bidder’s actions or absence thereof. Damages shall be recovered from outstanding money’s owed to the bidder. Where outstanding moneys are not sufficient to cover the full loss experienced by SITA, the bidder shall be invoiced for the outstanding moneys.
	2. Losses to SITA shall be determined and be assigned to the maintenance bidder where the balance of probability is more than 50% that the failure or incident was caused by the maintenance bidder’s actions or absence of action.
	3. Examples of losses caused to SITA that shall be recovered from the Contract, could include:
1. Work is being performed by the bidder inside the SITA IT environment and intentionally or unintentionally Network cabling is damaged which causes Network Traffic loss.
2. Damage to property during the execution of work.
	1. The bidder must have the required insurance cover in place within two weeks from contract commencement and of sufficient value to cover these types of incidences. SITA shall not interact with the maintenance bidder’s underwriter and shall deduct moneys directly as indicated above.

### Penalties

* 1. Should the maintenance bidder not adhere to the SLA time frame specified to Respond (MaxTTResp) to an incident, the penalty to the maintenance bidder shall be equal to 20% to 25% of the full value of the Scheduled Maintenance cost for that month for the relevant site (labour and equipment).
	2. Should the maintenance bidder not adhere to the SLA time frame specified to Repair (MaxTTRep) of an incident, the penalty to the maintenance bidder shall be equal to 10% of the full value of the Scheduled Maintenance cost for that month for the relevant site (labour and equipment).
	3. The penalty for late submission of a RCAs or RFO document shall be equal to 3% of the full value of the Scheduled Maintenance cost for that month for the relevant site (labour and equipment).
	4. The above penalties shall be applied at SITA’s discretion, following the breach of a Service Level Agreement. The bidder shall have the opportunity to provide a report, within seven calendar days following the incident or SITA’s notice of penalty, indicating why the bidder deem the penalty not to be applied. SITA shall take this into consideration, but SITA’s decision shall be final and shall deduct penalty values from the monthly invoices for the relevant site(s).
	5. Penalties for not adhering to the specified SLA timelines shall be calculated on a sliding scale, and be as follow:
1. Second time not adhering to, for the same site in a three-month period: two times the initial penalty.
2. Third time not adhering to, for the same site in a three-month period: four times the initial penalty.
3. Fourth time not adhering to, for the same site in a three-month period: six times the initial penalty.
4. Fifth and more times time not adhering to, for the same site in a three-month period: ten times the initial penalty.

### Delivery timeframes

* 1. The full Internet bandwidth solution must be implemented within **6 weeks** days after receipt of an official Purchase Order from SITA.

### Scope of work changes

* 1. SITA reserves the right to add or remove any scope requirements from contract.

### Benchmarking

* 1. SITA will have the right, not more than once per annum, and not commencing prior to the second year of the contract, to benchmark the service provider’s performance on some or all of the services and/or some or all of the charges, as designated by SITA.
	2. Benchmarking will be conducted by an independent industry-recognised benchmarking service provider (Benchmarker) designated by SITA and approved by the partner and such approval shall not be unreasonably withheld.
	3. When engaging the Benchmarker, the Benchmarker will be directed to:
	4. Make all commercially reasonable efforts to complete its analysis within 90 days after its engagement, to the extent practical;
	5. Select a representative sample of organisations, which shall be of a sufficient number as determined by the Benchmarker in its sole discretion and may include some services for which the partner is also the service provider; and
	6. Perform any normalisation that is reasonably required.
	7. SITA on the one hand, and the partner on the other hand, will each bear their own costs incurred in connection with the benchmarking and will share equally the Benchmarker’s fees and expenses. The Parties will cooperate with the Benchmarker as reasonably requested by the Benchmarker, including, as appropriate, making available knowledgeable personnel and pertinent documents and records. The Benchmarker will enter into a confidentiality agreement with SITA prior to being provided with confidential information of either Party.
	8. Each Party will be provided a reasonable opportunity to review, comment on, and request changes in the Benchmarker’s proposed findings. The Benchmarker will have sole discretion as to how it addresses such requests. Following such review and comment, the Benchmarker will issue a final report of its findings and conclusions.

### Performance Benchmarking:

* 1. The Benchmarker will review the partner’s performance of the services for which there are service levels, comparing the partner’s achieved levels to the service level target.
	2. The ‘service level target’ shall mean that each service level under this agreement for any service element subject to the benchmarking is at least as good as the service levels in the highest (i.e., ‘most favourable to SITA’ quartile of the service levels for similar services by other organisations.
	3. If the Benchmarker concludes that the service provider’s performance of the services is below the service level target, the service provider shall, within 30 days after the Benchmarker’s decision, develop for SITA review and approval, a plan to bring the performance up to the service level target as soon as practically possible and in all events within 90 days after the approval of such plan. The service levels will be adjusted accordingly effective 90 days after SITA approves the plan. The partner will bear the costs of the implementation of the plan.

### Price Benchmarking:

* 1. The Benchmarker will review the partner’s pricing of the services provided under the service contract to SITA, comparing the pricing to the market sector for services that are essentially the same in terms of committed service levels and volumes.
	2. The ‘price level target’ shall mean that each service price under this agreement for any service element subject to the benchmarking, is at least as good as the price levels in the highest (i.e., ‘most favourable to SITA’ quartile of the service levels for similar services by other organisations.
	3. If the Benchmarker concludes that the service provider’s pricing of the services is above the price level target, the service provider shall, within 30 days after the Benchmarker’s decision, develop for SITA review and approval, a revised pricing plan to bring the pricing in line with the Benchmarker’s findings as soon as practically possible and in all events backdated to the date of the findings. The partner will bear the costs of the implementation of the plan.

### Supplier performance reporting

* 1. **Monthly meetings to be scheduled between SITA and service provider and ADHOC meetings from both sided.**
	2. **A monthly report must be submitted to SITA on the first business day of the following month, with the following information:**
		1. Status of equipment as per maintenance schedule;
		2. Problems, solutions and risks;
		3. Where any downtime occurred, the following must be shown:
			+ - Reason for Outage;
				- Date of Outage;
				- Time of Outage;
				- Total repair time.
	3. **A formal report must be submitted to the SITA representative after every service, maintenance, or repair; including the relevant job sign-off sheets signed by SITA and the service provider.**
	4. **The service provider must provide a detailed schedule that will be used per site for inspections and maintenance, as well as the processes that will be followed to perform the above-mentioned tasks.**

### Certification, Expertise and Qualification

1. The bidder certifies that:
	* 1. **it has the necessary expertise, skill, qualifications and ability to undertake the work required in terms of the Statement of Work or Service Definition and,**
		2. **it is committed to provide the Products or Services; and**
		3. **perform all obligations detailed herein without any interruption to the Customer.**
		4. **at the time of the contracting the intended personnel who will carry out the maintenance**
		5. **The Supplier must provide the service in a good and workmanlike manner and in accordance with the practices and high professional standards used in well-managed operations performing services like the Services.**
		6. **The Supplier must perform the Services in the most cost-effective manner consistent with the level of quality and performance as defined in Statement of Work or Service Definition.**
		7. **Original Equipment Manufacturer (OEM) or Original Software Manufacturer (OSM) work. The Supplier must ensure that work or service is performed by a person who is certified by Original Equipment Manufacturer or Original Software Manufacturer.**

### Logistical Conditions

* 1. The service provider shall have a 24/7/365 Technical Call Centre.
	2. This Call Centre shall have multiple telecommunication lines and shall have a 100% telecommunication uptime and 100% Information Technology uptime. This Call Centre shall be equipped with backup power sources and shall have a 100% power uptime. The bidder shall have a disaster recovery site to which Call Centre operations can be routed, should the primary Call Centre encounter a disaster. The disaster recovery site shall be operational and functional and be able to manage 25% of the operations within 15 minutes, 50% of the operations within 30 minutes, and able to manage full strength within 60 minutes.
	3. The staff manning the bidder’s Call Centre shall have a technical background and understand the SITA ASN connectivity landscape. This Call Centre shall supervise the actions of the technicians on the call out and ensure that the most suitable technical, safe, and economical action is taken to resolve the incident with no risk to SITA and to prevent a failure in the SITA Infrastructure.
	4. If SITA’s email system is down, the above correspondence shall revert to telephonic correspondence with telephonic updates.
	5. Dedicated service manager to keep SITA updated of all the Internet related issues who will be a communication link between SITA and the ISP.
	6. The service provider shall have a proper incident management process in place to ensure that the best possible levels of service quality and availability are maintained.
	7. The Maintenance Bidder shall have an External Escalation Matrix in place within one week of contract award to manage external escalations against his Call Centre. The Maintenance Bidder shall also have an Internal Escalation Matrix in place within one week of contract award to indicate to SITA how internal escalations within the Call Centre shall run.
	8. Proper problem management needs to be implemented by the bidder to eliminate recurring incidents, and to minimize the impact of incidents that cannot be prevented.
	9. Configuration management needs to be implemented to ensure the infrastructure equipment performance, and operational information can be measured throughout its life.
1. **Tools of Trade**
	1. The bidder is expected to use its own resources (cell phone, laptops etc) to communicate with its own offices or outside of the SITA/Client buildings, including all tools and equipment to render the services effectively.

### Skills transfer and training

* 1. The Bidder must ensure that the SITA technical staff receives the required training to ensure the safe operation of the solution.
	2. The in-post training provided must include the possible primary cause and solutions to all the alarm events that can be encountered on the new solution.
	3. Free In-post training must be provided on an on-going basis to ensure that the responsible SITA technical staff is acquainted with the safe operation of the solution and interpretation of all alarm conditions.
	4. The bidder must provide the required free in-post training material i.e., instruction manual to the responsible SITA technical staff.

### Regulatory, Quality and Standards

1. The Supplier must for the duration of the contract ensure compliance with ISO/IEC General Quality Standards, ISO27001, and Protection of Personal Information Act (POPIA).
2. The Supplier must for the duration of the contract ensure compliance with General Quality Standards, ISO 9001
3. The Supplier must for the duration of the contract ensure compliance with SANS standards (SANS 10222-2)
4. Occupational Health and Safety Act, inclusive of the Regulations contained within this Act, with specific reference to the Lead Regulations, Environmental Regulations, Driven Machinery Regulations, Electrical Machinery Regulations, Electrical Installation Regulations and SANS 10142, and Pressure Equipment Regulations.
5. Registered with Department of Labour as Installation Electrician to oversee changes where changes or extensions are made to the electrical installation and to issue a Certificate of Compliance as prescribed by the Occupational Health and Safety Act.
6. Registered as a SAQCC Gas registered refrigerant gas practitioner for the installation, repair or modification and/or maintenance of a refrigeration system.
7. National Key Points Act 1980 as amended.
8. Environmental Conservation Act 1989 as amended.
9. Any approved new site equipment installations and enhancements of Infrastructure must be quality assured and comply with all applicable SABS standards as well as municipality standards.
10. The safety of SITA personnel and visitors to SITA premises must be placed first, always and great care must be taken not to damage any infrastructure or equipment.
11. The Supplier must for the duration of the contract ensure that the proposed product or solution conform to the list of Government Minimum Interoperability Standards (MIOS).

**Note (1):**

Refer to **Annex D** for the MIOS Certification requirements for this Bid Specification, however it is not limited to these items identified. The requirements will be finalised during the contracting stage. The successful bidder needs to ensure compliance with the SITA requirements for the duration of the contract.

### Security clearance requirements

* 1. Company security screening: The supplier may be required to undergo a company security screening conducted by the State Security Agency (SSA). Should the SSA find the supplier not suitable after the conduct of the security screening, the business relationship will be terminated. The following documentation will be required for the company security screening process to be conducted:
		+ - 1. Copy of company registration documentation.
				2. Copy(ies) of identity documentation of Director(s), Member(s) or Trustee(s);
				3. Copy of valid tax clearance certificate.
	2. Security suitability check for individuals: SITA may, at its own discretion and in line with its policies and procedures, require employees of the supplier to be subjected to a security suitability check before commencement of a project or delivering of a service. The security suitability check is conducted by SITA in order to ensure that individuals meet the minimum security requirements and also to verify personal information. The supplier will be required to replace any employee(s) who is found to be not suitable after the conduct of the security screening. The following documentation will be required for the security suitability check:
		+ - 1. Copy of identity document;
		1. Copy(ies) of qualification(s) if SITA requires verification thereof;
		2. Fingerprints – will be taken electronically;
		3. Signed consent form for the conduct of background checks.
	3. Security clearance: A security clearance, issued by either the SSA or Defence Intelligence (DI) is required if any employee of the supplier will have or may gain access to classified information throughout the duration of the project or in the process of delivering a service. The level of security clearance required – Confidential, Secret or Top Secret, will be determined at the sole discretion of SITA. The supplier will have to replace any employee who do not qualify for a security clearance or is found not suitable by the SSA or DI. The following documentation will be required for the security clearance process:
		+ - 1. Completed Z204 or DD1057 security clearance application form;
		1. Fingerprints;
		2. Personal documentation of the applicant, including but not limited to, identity document, passport, marriage certificate (if applicable), divorce order (if applicable), qualifications, salary advice and bank statements.

### Confidentiality and non-disclosure conditions

1. The Supplier, including its management and staff, must before commencement of the Contract, sign a non-disclosure agreement regarding Confidential Information
2. Confidential Information means any information or data, irrespective of the form or medium in which it may be stored, which is not in the public domain and which becomes available or accessible to a Party as a consequence of this Contract, including information or data which is prohibited from disclosure by virtue of:
	1. the Promotion of Access to Information Act, 2000 (Act no. 2 of 2000),
	2. being clearly marked "Confidential" and which is provided by one Party to another Party in terms of this Contract.
	3. being information or data, which one Party provides to another Party or to which a Party has access because of Services provided in terms of this Contract and in which a Party would have a reasonable expectation of confidentiality.
	4. being information provided by one Party to another Party during contractual or other negotiations, which could reasonably be expected to prejudice the right of the non-disclosing Party.
	5. being information, the disclosure of which could reasonably be expected to endanger a life or physical security of a person.
	6. being technical, scientific, commercial, financial and market-related information, know-how and trade secrets of a Party.
	7. being financial, commercial, scientific or technical information, other than trade secrets, of a Party, the disclosure of which would be likely to cause harm to the commercial or financial interests of a non-disclosing Party; and
	8. being information supplied by a Party in confidence, the disclosure of which could reasonably be expected either to put the Party at a disadvantage in contractual or other negotiations or to prejudice the Party in commercial competition; or
	9. information the disclosure of which would be likely to prejudice or impair the safety and security of a building, structure or system, including, but not limited to, a computer or communication system; a means of transport; or any other property; or a person; methods, systems, plans or procedures for the protection of an individual in accordance with a witness protection scheme; the safety of the public or any part of the public; or the security of property; information the disclosure of which could reasonably be expected to cause prejudice to the defence of the Republic; security of the Republic; or international relations of the Republic; or plans, designs, drawings, functional and technical requirements and specifications of a Party, but must not include information which has been made automatically available, in terms of the Promotion of Access to Information Act, 2000; and information which a Party has a statutory or common law duty to disclose or in respect of which there is no reasonable expectation of privacy or confidentiality;
3. Notwithstanding the provisions of this Contract, no Party is entitled to disclose Confidential Information, except where required to do so in terms of a law, without the prior written consent of any other Party having an interest in the disclosure.
4. Where a Party discloses Confidential Information which materially damages or could materially damage another Party, the disclosing Party must submit all facts related to the disclosure in writing to the other Party, who must submit information related to such actual or potential material damage to be resolved as a dispute.
5. Parties may not, except to the extent that a Party is legally required to make a public statement, make any public statement or issue a press release which could affect another Party, without first submitting a written copy of the proposed public statement or press release to the other Party and obtaining the other Party's prior written approval for such public statement or press release, which consent must not unreasonably be withheld.

### Guarantee and warranties

1. The supplier confirms that:
	1. The warranty of goods supplied under this contract remains valid for the duration of the contract after the goods were delivered, installed and commissioned with a sign off, including the clients signature.
	2. In case infrastructure equipment needs to be replaced all relevant guarantees and warranties must be honoured by the service provider. At expiry of the two-year contract, the service provider will transfer the warranty/guarantee to SITA.
	3. The warranty of goods supplied under this contract remains valid for twelve (12) months after the goods, or any portion thereof as the case may be, have been delivered to and accepted at the destination indicated in the contract, or for eighteen (18) months after the date of shipment from the port or place of loading in the source country, whichever period concludes earlier.
	4. as at Commencement Date, it has the rights, title and interest in and to the Product or Services to deliver such Product or Services in terms of the Contract and that such rights are free from any encumbrances whatsoever.
	5. the Product is in good working order, free from Defects in material and workmanship, and substantially conforms to the Specifications, for the duration of the Warranty period.
	6. during the Warranty period any defective item or part component of the Product be repaired or replaced within 3 (three) days after receiving a written notice from SITA.
	7. the Products is maintained during its Warranty Period at no expense to SITA.
	8. the Product possesses all material functions and features required for SITA’s Operational Requirements.
	9. the Product remains connected or Service is continued during the term of the Contract;
	10. all third-party warranties that the Supplier receives in connection with the Products including the corresponding software and the benefits of all such warranties are ceded to SITA without reducing or limiting the Supplier’s obligations under the Contract.
	11. no actions, suits, or proceedings, pending or threatened against it or any of its third-party suppliers or sub-contractors that have a material adverse effect on the Supplier’s ability to fulfil its obligations under the Contract exist.
	12. SITA is notified immediately if it becomes aware of any action, suit, or proceeding, pending or threatened to have a material adverse effect on the Supplier’s ability to fulfil the obligations under the Contract.
	13. any Product sold to SITA after the Commencement Date of the Contract remains free from any lien, pledge, encumbrance or security interest.
	14. SITA’s use of the Product and Manuals supplied in connection with the Contract does not infringe any Intellectual Property Rights of any third party.
	15. the information disclosed to SITA does not contain any trade secrets of any third party unless disclosure is permitted by such third party.
	16. it is financially capable of fulfilling all requirements of the Contract and that the Supplier is a validly organized entity that has the authority to enter the Contract.
	17. it is not prohibited by any loan, contract, financing arrangement, trade covenant, or similar restriction from entering the Contract.
	18. the prices, charges and fees to SITA as contained in the Contract are at least as favourable as those offered by the Supplier to any of its other customers that are of the same or similar standing and situation as SITA; and
	19. any misrepresentation by the Supplier amounts to a breach of Contract.
	20. Sita will only approve quotes which are market related and the service provider will be required to review the quotation if it’s not market related.

### Intellectual Property Rights

1. SITA retains all Intellectual Property Rights in and to SITA's Intellectual Property. As of the Effective Date, the Supplier is granted a non-exclusive license, for the continued duration of this Contract, to perform any lawful act including the right to use, copy, maintain, modify, enhance and create derivative works of SITA's Intellectual Property for the sole purpose of providing the Products or Services to SITA pursuant to this Contract; provided that the Supplier must not be permitted to use SITA's Intellectual Property for the benefit of any entities other than SITA without the written consent of SITA, which consent may be withheld in SITA's sole and absolute discretion. Except as otherwise requested or approved by SITA, which approval is in SITA's sole and absolute discretion, the Supplier must cease all use of SITA's Intellectual Property, at of the earliest of:
	1. termination or expiration date of this Contract.
	2. the date of completion of the Services; and
	3. the date of rendering of the last of the Deliverables
2. If so, required by SITA, the Supplier must certify in writing to SITA that it has either returned all SITA Intellectual Property to SITA or destroyed or deleted all other SITA Intellectual Property in its possession or under its control
3. SITA, always, owns all Intellectual Property Rights in and to all Bespoke Intellectual Property.
4. Save for the license granted in terms of this Contract, the Supplier retains all Intellectual Property Rights in and to the Supplier’s pre-existing Intellectual Property that is used or supplied in connection with the Products or Services
5. Provide SITA with the compliant Occupational Health and Safety File (required on site for period of installation and proof of compliance).

### Counter Conditions

1. Bidders’ attention is drawn to the fact that amendments to any of the Bid Conditions or setting of counter conditions by bidders may result in the invalidation of such bids.

### Fronting

1. The SITA supports the spirit of Broad Based Black Economic Empowerment and recognizes that real empowerment can only be achieved through individuals and businesses conducting themselves in accordance with the Constitution and in an honest, fair, equitable, transparent and legally compliant manner. Against this background the SITA will not condone any form of fronting.
2. The SITA, in ensuring that bidders conduct themselves in an honest manner will, as part of the bid evaluation processes, conduct or initiate the necessary enquiries/investigations to determine the accuracy of the representation made in bid documents. Should any of the fronting indicators as contained in the Guidelines on Complex Structures and Transactions and Fronting, issued by the Department of Trade and Industry, be established during such enquiry/investigation, the onus will be on the bidder / contractor to prove that fronting does not exist. Failure to do so within a period of 14 days from date of notification may invalidate the bid / contract and may also result in the restriction of the bidder/contractor to conduct business with the public sector for a period not exceeding ten (10) years, in addition to any other remedies SITA may have against the bidder/contractor concerned.

### Business Continuity and Disaster Recovery Plans

1. The bidder confirms that they have written business continuity and disaster recovery plans that define the roles, responsibilities and procedures necessary to ensure that the required services under this bid specification is in place and will be maintained continuously in the event of a disruption to the bidder’s operations, regardless of the cause of the disruption.

### Supplier Due Diligence

1. SITA reserves the right to conduct supplier due diligence prior to final award or at any time during the Contract period and this may include pre-announced / non-announced site visits. During the due diligence process the information submitted by the bidder will be verified and any misrepresentation thereof may disqualify the bid or Contract in whole or parts thereof.

### Sub-contracting as a condition of tender

1. SITA in terms of the SITA Preferential Policy (PPP), has an obligation to advance designated groups which includes black SMMEs (i.e. Exempted Micro Enterprises (EME) and Qualifying Small Enterprises (QSE) for the supply of certain ICT goods or services where feasible to subcontract for a contract above R50m, an organ of state must apply sub-contracting to advance designated groups.
2. The sub-contracting percentage for this bid will be negotiated at contracting stage with the Bidder.
3. SITA reserves the right to accept or reject the proposed percentage subcontracting and further negotiate with the preferred bidder and if not satisfied may not award the tender.

Note (1):

In the case of sub-contracting, the sub-contractors must have valid Tax Clearance Certificates which, upon request by SITA, must be made available to SITA for due diligence purposes.

### Preference Goal Requirements conditions

1. The Bidder’s commitment for the Preference Goal Requirements in this tender will be legally binding and the Bidder needs to perform against their commitment for the duration of the contract which will form part of the Contractual Agreement.
2. The Bidder must sustain, or improve the company’s BBBEE Level for the duration of the contact which will form part of the Contractual Agreement.
3. Performance of Preference Goal Requirements will be determined annually. Bidders must submit their Preference status report indicating progress against the Bidder’s Preferential commitments within 30 days of the yearly anniversary of the contract.
4. Bidders need to keep auditable substantive records / evidence and upon request by SITA must be made available for audit and, or due diligence purposes.
5. **SITA** reserves the right to require from a Bidder, either before a bid is adjudicated or at any time subsequently, to substantiate any claim with regards to preferences, in any manner required by **SITA.**
6. **SITA** reserves the right to verify information / evidence provided by the Bidder.
7. **SITA** reserves the right to introduce a **penalty of 1%** of the overall annual year spent by **SITA** for the prior year if the Bidder fails to comply to **paragraphs (a), (b) and (c) above**.

### Declaration of compliance and acceptance SCC

I (we), the bidder hereby declare that I (we) accept ALL the Special Conditions of Contract as specified in **par 4.3** above and shall comply with all stated obligations:

Name of Bidder:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date:\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. **Price and Preference Points Evaluation (Stage 5)**
	1. **COSTING AND PREFERENCE EVALUATION**
2. In terms of the SITA Preferential Procurement Policy (PPP), the following preference point system is applicable **for this** Bid:
	1. **the 90/10 system (90 Price and 10 Specific Goals) for requirements with a Rand value above R50 000 000 (all applicable taxes included).**
3. Points will be allocated for each of the **Preferential Goal Requirements** for this tender as indicated in **table 9,** dependant on **paragraph 1.**
4. Points for this tender shall be awarded for:
	1. Price; and
	2. Preference points for specific goals.
5. The maximum points for this tender will be allocated as follows, subject to **paragraphs 3** above:

 **Table 9:** Points allocation

| **Description** | **Points****Table 11** |
| --- | --- |
| Price | **90** |
| Preference points for specific goals | **10** |
| Total points for Price and preference points for specific goals | **100** |

* 1. **Costing and Pricing Conditions**
1. **SOUTH AFRICAN PRICING**

The total price **must** be VAT inclusive and be quoted in South African Rand (ZAR).

1. **TOTAL PRICE**
	1. Bidder will be bound by the following general costing and pricing conditions and SITA reserves the right to negotiate the conditions or automatically disqualify the bidder for not accepting these conditions:
	2. **The Bidder must include their Costing Proposal and indicate the reference page(s) in both their proposal and SBD 1 form as part of their bid submission.**
	3. Note: Bidders will complete Bidder’s **Costing Proposal** and include this as part of the hard copy submission documents and on the memory stick.
	4. The Bidder’s **Costing Proposal** should be divided into the following categories and should take account of the following, however is not limited to these categories:

| **REQUEST FOR PROPOSAL FOR THE PROVISON, INSTALLATION, CONFIGURATION INCLUDING, MAINTENANCE AND SUPPORT OF INTERNET BANDWIDTH SOLUTION TO SITA AND ITS CLIENTS FOR A PERIOD OF FIVE (05) YEARS** |
| --- |
| **Item** | **Requirement**  |
| Supply, install and provision of high-capacity bandwidth internet connectivity that offers complete, fully redundant and secure Internet architecture with the below requirements. | * + 1. Provision of fully redundant, protected and secure breakout points to the three SITA Internet breakout points located at **SITA centurion**, **SITA Cape town** and **SITA Pietermaritzburg**. Network Diagram **see section 3.1.**
		2. Provision of three point to point links triangulated between **SITA Centurion**, **SITA Cape town** and **SITA Pietermaritzburg.**
		3. Provision of fully redundant, protected connectivity links from the three DMZs (**SITA Centurion, SITA Cape town** and **SITA Pietermaritzburg**) to **TERACO (NAPAFRICA**) in each individual TERACO data centre in Cape Town, Johannesburg and Durban, that will be used for the Internet peering purpose and failover access to tenants located at the Internet Exchange at these locations.
		4. A **fully protected layer 2 service** that is provisioned over a fibre network that utilizes **geographically diverse fibre routes** to ensure the maximum uptime of the underlay network in each of the SITA DMZ locations.
		5. Full upstream ISP internal redundancy within the ISP's and SITA's own ASN space with backup links that are triangulated between three SITA sites which are located at **SITA Cape town**, **SITA Centurion** and **SITA Pietermaritzburg**.
		6. **DDOS mitigation** for all DDOS traffic that may transit via the Service Providers network.
 |
| Maintenance and Technical Support. | * + 1. Annual Maintenance and technical support for a period of five (5) years must be included in the offering.
		2. The bidder must be accredited or certified to do maintenance and support of the proposed Solutions.
		3. The service provider will be responsible to manage the solution throughout the duration of the contract.
 |
| Provide Professional Services: | * + 1. Design of required Internet architecture solution and integration requirements.
		2. Project management for the installation and configuration of the Internet architecture solution.
		3. Transfer of skills to SITA NTSS technical support resources.
		4. Develop the handover documentation where necessary.
		5. Implementation plan for the solution with timelines
 |

| **Item No** |  **REQUEST FOR PROPOSAL FOR THE PROVISON, INSTALLATION, CONFIGURATION INCLUDING, MAINTENANCE AND SUPPORT OF INTERNET BANDWIDTH SOLUTION TO SITA AND ITS CLIENTS FOR A PERIOD OF FIVE (05) YEARS** |  | **YEAR 1** | **YEAR 2** | **YEAR 3** | **YEAR 4** | **YEAR 5** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Unit of measure** | **Quantity**  | **Quantity**  | **Quantity**  | **Quantity**  | **Quantity**  |
| **1** | **Internet Bandwidth solution** |  |  |  |  |  |  |
| 1.1 | 3X Internet Transit links at 100Gig speed  | Gbps | 3 | 3 | 3 | 3 | 3 |
|  | 40Gbps minimum provisioned BW | Gbps | 3 | 3 | 3 | 3 | 3 |
|  | 60Gbs provisioned Bandwidth | Gbps | 3 | 3 | 3 | 3 | 3 |
|  | 80Gbps provisioned Bandwidth | Gbps | 3 | 3 | 3 | 3 | 3 |
|  | 100Gbps provisioned Bandwidth | Gbps | 3 | 3 | 3 | 3 | 3 |
| 1.2 | 3X 100Gig (CN-CT, CT-PMB, PMB-CN) | Gbps | 3 | 3 | 3 | 3 | 3 |
| 1.3 | 3X20Mbps (CN, PMB,CT) | Gbps | 3 | 3 | 3 | 3 | 3 |
| 1.3 | 3X Dedicated links to Teraco at 100Gig speed | Gbps | 3 | 3 | 3 | 3 | 3 |
| **2** | **maintenance and Technical Support** |  |  |  |  |  |  |
| 2,1 | Maintenance and Technical Support for 5 years | 1 | 1 | 1 | 1 | 1 | 1 |
| **3** | **Professional Services** |  |  |  |  |  |  |
| 3,1 | Professional services, solution implementation  | 1 | 1 |  |  |  |  |

* 1. All quoted prices are the total price for the entire scope of required services and deliverables to be provided by the bidder.
	2. The cost of delivery, labour, S&T, overtime, etc. must be included in this bid.
	3. All additional costs must be clearly specified.
	4. **SITA** reserves the right to negotiate pricing with the successful bidder prior to the award as well as envisaged quantities.
	5. These conditions will form part of the Contract between **SITA** and the bidder. However, **SITA** reserves the right to include or waive the condition in the Contract.
	6. **Bidders must complete and submit their Costing Proposal in Excel spreadsheet format.**
	7. The Bidder must complete the declaration of acceptance as per **section 5.4** below by marking with an “X” either “ACCEPT ALL”, or “DO NOT ACCEPT ALL”, failing which the declaration will be regarded as “DO NOT ACCEPT ALL” and the bid will be disqualified.
	8. **RATE OF EXCHANGE PRICING INFORMATION**

**5.3.1 ROE PRICING INFORMATION**

Provide the TOTAL BID PRICE for the duration of Contract and clearly indicate the Local Price and Foreign Price, where –

* 1. **Local Price** means the portion of the TOTAL price that is NOT dependent on the Foreign Rate of Exchange (ROE) and;
	2. **Foreign Price** means the portion of the TOTAL price that is dependent on the Foreign Rate of Exchange (ROE).
	3. **Exchange Rate** means the ROE (ZA Rand vs foreign currency) as determined at time of bid.

**5.3.2 BID EXCHANGE RATE CONDITIONS**

The bidders must use the exchange rate provided below to enable SITA to compare the prices provided by using the same exchange rate:

|  |  |
| --- | --- |
| **Foreign currency** | **South African Rand (ZAR) exchange rate**  |
| 1 US Dollar | R18,01 |
| 1 Euro | R19,73 |
| 1 Pound | R23,42 |

**NOTE (1):**

The ROE indicated above is to ensure a competitive bidding process.

**NOTE (2):**

The ROE stated above will apply for this tender and Bidder need to indicate the foreign content which will be subjected to ROE fluctuation.

ROE fluctuation will only be applied to the specific foreign component.

The details will be negotiated during the contracting phase.

* 1. **Declaration of Acceptance**

|  | **ACCEPT ALL** | **DO NOT ACCEPT ALL** |
| --- | --- | --- |
| 1. The bidder declares to ACCEPT ALL the Costing and Pricing conditions as specified in **par 5.2** above by indicating with an “X” in the “ACCEPT ALL” column, or
2. The bidder declares to NOT ACCEPT ALL the Costing and Pricing Conditions as specified in **par 5.2** above by -
	1. Indicating with an “X” in the “DO NOT ACCEPT ALL” column, and;
	2. Provide reason and proposal for each of the condition not accepted.
 |  |  |
| **Comments by bidder:**Provide the condition reference, the reasons for not accepting the condition. |

* 1. **PREFERENCE REQUIREMENTS**

### INSTRUCTION AND POINT ALLOCATION

1. **The Bidder must complete in full all the PREFERENCE requirements.**
2. **Allocation of points per requirements:** The points allocation of bidders’ responses to the requirements will be determined by the completeness, relevance and accuracy of substantiating evidence.
3. Points will be allocated for each **PREFERENCE requirement** as per the criteria set in each section in the **table 10** below.
4. **The Bidder must provide a unique reference number** (e.g. binder/folio, chapter, section, page) to locate substantiating evidence in the bid response. During evaluation, SITA reserves the right to treat substantiation evidence that cannot be located in the bid response, as “NOT COMPLY”. The evidence needs to be attached to **ANNEX A**.
5. **Preference Goal Requirements:**
	1. The **Bidder must complete the 90/10 preference point system** and submit proof or documentation required in terms of this tender.
	2. The specific Preferential Goal Requirements for this tender is indicated in **table 10** below.
	3. The Bidder must indicate their commitment to claim points for each of the preference points **by signing at par 4.5 in the Invitation to Bid document.**
	4. Failure on the part of a bidder to submit proof or documentation required or to comply to paragraph (d) above in terms of this tender to claim preference points for the **Preference Goal Requirements** for this tender, will be interpreted to mean that preference points are not claimed.
	5. The Bidder’s **commitment** for the Preference Goal Requirements in this tender will be legally binding and the Bidder needs to perform against their commitment for the duration of the contract which will form part of the Contractual Agreement.
	6. The Bidder must sustain, or improve the company’s B-BBEE Level for the duration of the contact which will form part of the Contractual Agreement.
	7. Performance of Preference Goal Requirements will be determined annually. Bidders must submit their Preference status report to **SITA** indicating progress against the Bidder’s Preferential commitments within 30 days after each quarter from the commencement date of the contract.
	8. Bidders need to keep auditable substantive records / evidence and upon request by **SITA** must be made available for audit and, or due diligence purposes.
	9. **SITA** reserves the right to require from a Bidder, either before a bid is adjudicated or at any time subsequently, to substantiate any claim with regards to preferences, in any manner required by **SITA**.
	10. **SITA** reserves the right to verify information / evidence provided by the Bidder.
	11. **SITA** reserves the right to introduce a penalty of 1% of the overall annual year spent by **SITA** for the prior year if the Bidder fails to comply to paragraphs (e), (f) and (g) above.

**Table 10:** Preference Goal Requirements

| **Preference Goal Requirement #** | **Preferential Goal Requirements** | **Preferential Goal Requirements** **(Specific Goals)** |
| --- | --- | --- |
|  | **Preferential Goal Requirements allocated for this tender** | **Substantiating evidence and evidence reference to be completed by bidder. Evaluation per requirement: Each requirement indicated in the table below must be completed and points will be allocated based on the evidence required below:**  | **Evidence reference for the**  |
|  | **B-BBEE Requirements** |  |
| 1) | **B-BBEE Requirements**Promotion of Transformational Objectives. | **Evidence:**The Bidder must provide a copy of the following relevant evidence for the Preferential Goal points which the Bidder qualifies for:1. **Columns A, B, C and D in table 11:**

Copy of relevant proof of the following to confirm the B-BBEE status of the contributor as defined in the Broad-Based Black Economic Empowerment Act:* + - * 1. ***B-BBEE certificate*** *(from a SANAS Accredited Agency the dtic);*

**or** ***Sworn affidavit*** in the format provided by CIPC - ***Applicable to EMEs and QSEs only;*****and/ or**1. **Column D in table 11:**

Copy of ***South African Identification Document (ID***); **and/ or**1. **Column E in table 11:**

Copy of ***Medical Certificate*** ***clearly indicating the disability in line with the B-BBEE status claimed as defined in the Broad-Based Black Economic Empowerment Act***.**Note:**The CIPC (Companies and Intellectual Property Commission) registration documents will also be used as evidence to confirm compliance to the Preferential procurement requirements as part of the evaluation process.**Points allocation:**Points will be allocated for bidders that meets the requirements as indicated in **table 11 in section 5.5.1**. | <provide unique reference to locate substantiating evidence in the bid response – **Annex A, section 6.7**> |

**Table 11:** B-BBEE Points as part of the Preference Goal requirements (Preferential Goal Requirements for **(90/10) system**)

**Note: Bidder to select the section for points they wish to claim (Mark as Y=Yes) in the table below.**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  | **Ownership**  |  |  |  |
|  | **Reference #** | **Contributor Level as defined in the Broad-Based Black Economic Empowerment Act** | **EME/QSEs** | **Black Owned(BO)(51% or more)** | **Black Woman Owned(BWO)(More than 30%)** | **Youth Owned** | **Owned by People living with disabilities** | **Score** | **Bidder to select the section for points they wish to claim(Mark as Y= Yes)** |  |
|  |  |
|  |   |   | **(A)** | **(B)** | **(C)** | **(D)** | **(E)** | **(F)** |  |  |
|  | **1** | **Level 1** | **3** | **2** | **2** | **2** | **1** | **10** |  |  |
|  | **2** | **Level 1** | **3** | **2** | **2** | **2** | 0 | **9** |  |  |
|  | **3** | **Level 1** | **3** | **2** | **2** | 0 | 0 | **7** |  |  |
|  | **4** | **Level 1** | **3** | **2** | 0 | 0 | 0 | **5** |  |  |
|  | **5** | **Level 2 and 3** | **2** | **1** | **0,5** | **0,5** | **0,5** | **4,5** |  |  |
|  | **6** | **Level 2 and 3** | **2** | **1** | **0,5** | **0,5** | 0 | **4** |  |  |
|  | **7** | **Level 2 and 3** | **2** | **1** | **0,5** | 0 | 0 | **3,5** |  |  |
|  | **8** | **Level 2 and 3** | **2** | **1** | 0 | 0 | 0 | **3** |  |  |
|  | **9** | **Level 4 and 5** | **1** | **0,5** | **0,25** | **0,25** | **0,25** | **2,25** |  |  |
|  | **10** | **Level 4 and 5** | **1** | **0,5** | **0,25** | **0,5** | 0 | **2,25** |  |  |
|  | **11** | **Level 4 and 5** | **1** | **0,5** | **0,25** | 0 | 0 | **1,75** |  |  |
|  | **12** | **Level 4 and 5** | **1** | **0,5** | 0 | 0 | 0 | **1,5** |  |  |
|  | **13** | **Level 6** | 0 |   | 0 | 0 | 0 | **0** |  |  |
|  | **14** | **Level 7** | 0 |   | 0 | 0 | 0 | **0** |  |  |
|  | **15** | **Level 8** | 0 |   | 0 | 0 | 0 | **0** |  |  |
|  | **16** | **Non-Contributor** | 0 |   | 0 | 0 | 0 | **0** |  |  |
|  | **Total Maximum Score Allocation:** | **10** |  |  |  |  |  |  |  |
|  | F= A+B+C+D+E |  |  |

1. Bidder substantiating evidence

# Technical Mandatory Requirement Evidence

## Bidder Certification / Affiliation Requirements

### (a) Independent Communication Authority

**Attach** a copy of valid documentation/s (letter/certificate/license) as proof that the Bidder is licensed by the Independent Communication Authority of South Africa (ICASA) for the following **here:**

* + 1. Individual Electronic Communication Network Service (IECNS); and
		2. Individual Electronic Communications Service (IECS) operator.

**NOTE (1):**

SITA reserves the right to verify information provided.

### (b) Internet Service Coverage Requirements (ISP/POPs)

**Attach** a copy of valid documentation (Map Coverage) as proof that the Bidder has presence (POPs) across South Africa, including POPs in Cape Town, Pietermaritzburg and Tshwane Metro **here.**

**NOTE (1):**

SITA reserves the right to verify information provided.

### (c) Internet Service Coverage Requirements (ISP)

**Attach** a copy of valid documentation (letter/certificate/license) as proof that the Bidder is an Internet Service Provider (ISP) who obtains international capacity directly from undersea cable operators **here.**

**NOTE (1):**

SITA reserves the right to verify information provided.

### (d) Internet Routing Requirements

**Attach** a copy of valid documentation (letter/certificate/license/affidavit) as proof that the Bidder is an Internet Service Provider (ISP) who owns and operates network infrastructure at international points of presence and has negotiated its own transit and peering with International Internet providers. The evidence documentation must indicate the following **here**:

1. Individual Electronic Communication Network Service (IECNS); and
2. Individual Electronic Communications Service (IECS) operator.

**NOTE (1):**

SITA reserves the right to verify information provided.

### (e) International Connectivity Requirements (ASN/BGP)

The bidder must provide a valid documentation (letter or a sworn affidavit) indicating a valid registrar-assigned, non-private Autonomous System Number(s) (ASN) **and attach it here**.

**NOTE (1):**

All documentation (letter or a sworn affidavit) must be dated and signed.

**NOTE (2):**

SITA reserves the right to verify information provided.

### (f) Internet Routing Requirements

The bidder must provide a valid documentation (letter or a sworn affidavit) indicating they have the ability to accept and advertise individual /28 routing prefixes within the provider’s network **and attach it here**.

**NOTE (1):**

All letters must be dated and signed.

**NOTE (2):**

SITA reserves the right to verify information provided.

### (g) International Connectivity Requirements

The Bidder **must** provide the following documentation for International Connectivity Requirements **and attach it here**:

1. Valid peering agreements between the bidder and international connectivity providers or a sworn affidavit, attesting that the bidder has international landing points on at least two (02) of the following continents: Europe, Asia or North America.
2. The Bidder must provide a documentation (Letter, Agreement or Sworn Affidavit) as proof that the bidders has supplied transit bandwidth to its customer/s for a minimum period of five (5) years via international landing points on at least two (2) of the following continents: Europe, Asia or North America in the past five (05) from the publication of this bid.

**NOTE (1):**

SITA reserves the right to verify information provided.

### (h) International Peering Connectivity Requirements

**Attach** a copy of valid transit/peering agreements at each of the landing points must be in the company’s name (or a registered subsidiary / parent) **here**.

**NOTE (1):**

SITA reserves the right to verify information provided.

## Bidder Experience and Capability Requirements

* + - 1. The Bidder must complete **table 12** below, noting that:

The Bidder must provide reference details by completing **table 12** from at least one (1) customer to whom a total bandwidth of at least 100 Gbps was provided over a continuous period of a minimum of one (1) year in the past five (5) years from the publication date of this bid.

**NOTE (1):**

The Service provided must include the following:

Installation; **and**

Configuration; **and**

Maintenance; **and**

Support.

* + - 1. The Scope of work must be related.
			2. The Bidder **must provide** the following information when completing **Table 13** below:

**NOTE 2:**

* 1. Company name; **and**
	2. Contact person, telephone **and/or** e-mail address; **and**
	3. Project scope of Work; **and**
	4. Project start and End date.
		+ 1. Project end-date must be current or not older that six (5) years from the publication date of this bid.

**NOTE (3):**

Failure to comply fully to the requirements as indicated above will result in disqualification.

**NOTE (4):**

SITA reserves the right to verify information provided.

**Table 12:** Reference

| **No** | **Company name** | **Reference Person Name, Tel and/or email** | **Project Scope of work**  | **Project Start and End-date** |
| --- | --- | --- | --- | --- |
| 1 | <Company name> | <Person Name><Tel><email> | < Provide scope details of a project from a customer to whom a total bandwidth of at least 100 Gbps was provided over a continuous period of a minimum of one (1) year in the past five (5) years from the publication date of this bid.> | Start Date:End Date  |

## Special Conditions of Contract

The Bidder **must** acknowledgethe Special Conditions of Contract (SCC) as stated in **section 4.3** by signing in the declaration of compliance and acceptance of SCC in **section 4.3.26.**

**NOTE (1):**

Failure to complete and sign the SCC in **section 4.3.22** will result in disqualification.

## Third Party Risk Management Assessment

The Bidder **must comply** with the Third-Party Risk Management Assessment requirement **by completing** **All the questions** in **ANNEX B** and **attach it here**.

**NOTE (1):**

SITA reserves the right to verify information provided.

**NOTE (2):**

Failing to complete all the questions or not Accepting the Declaration of Acceptance above will result in disqualification.

* 1. **Product/Service Functional Requirements**

The Bidder must confirm that they comply with the Product/ Service Functional Requirements for the **provision, installation, configuration including, maintenance and technical support of internet bandwidth solution to SITA and its clients for a period of five (05) years** by completing and signing **Annex C**: **Addendum 1** and **attach it here**.

**NOTE (1):**

Failure to comply fully to the requirements as indicated above will result in disqualification.

**NOTE (2):**

SITA reserves the right to verify information provided

## Technical Functionality Requirements

The Bidder need to **attach** the required Evidence for the Technical Functional Requirements as indicted in **section 4.3 here.**

## Preference Points Preferential Goals Evidence

The Bidder **must**:

* + 1. **Preference Goal Requirements:**

Bidder to select the section for points they wish to claim (Mark as Y=Yes) in **table 11 in section 5.5.1**, dependant on which preference system the Bidder selects in line with **section 5.5.1; and**

Provide a copy of the following relevant evidence for the Preferential Goal points which the Bidder qualifies for as set out in **table 11** in **section 5.5.1** and **attach it here**:

* + - * 1. **Columns A, B and C in table 11:**

Copy of relevant proof of the following to confirm the B-BBEE status of the contributor as defined in the Broad-Based Black Economic Empowerment Act:

***B-BBEE certificate*** *(from a SANAS Accredited Agency);*

**or**

***Sworn affidavit*** in the format provided by CIPC - ***Applicable to EMEs and QSEs only;***

**and/ or**

* + - * 1. **Column D in table 9:**

Copy of ***South African Identification Document (ID)***;

**and/ or**

* + - * 1. **Column E in table 9:**

Copy of ***Medical Certificate*** ***clearly indicating the disability in line with the B-BBEE status claimed as defined in the Broad-Based Black Economic Empowerment Act***.

**Note:**

The CIPC (Companies and Intellectual Property Commission) registration documents will also be used as evidence to confirm compliance to the Preferential procurement requirements as part of the evaluation process.

* + 1. Indicate their **commitment** to claim points for each of the preference points **by signing at par 4.5 in the Invitation to Bid document**.
1. THIRD-PARTY RISK MANAGEMENT (TPRM) ASSESSMENT

# Instructions

1. In terms of the approved SITA Third-Party Risk Management Framework, all Bidders responding to this bid **must** complete the following section by answering **ALL** the questions.
2. By completing the Third-Party Risk Management Assessment, the Bidder agrees to provide all reasonable supporting documentation when requested to do so, as well as during contract finalisation as this **is a pre-award condition of this bid.**
3. Any risk identified during the assessment process will have to be mitigated and/or remediated before or during the contract finalisation phase. A detailed mitigation plan, that is acceptable to SITA, may also be required.
4. Supplier due diligence, as contained in the Special Conditions of Contract, is also applicable to this Third-Party Risk Management process.
5. The following 6 (six) risk elements will be assessed:
	1. Company risk: 10 questions;
	2. Financial risk: 6 questions;
	3. Operational risk: 8 questions;
	4. Governance and compliance risk: 6 questions;
	5. Information security and privacy risk: 7 questions;
	6. Reputational risk: 6 questions.

## Evaluation Criteria

### Company risk

* 1. Questions 2, 3, 6, 8, 9, 10:

| **Evaluation criteria**  | **Score** |
| --- | --- |
| Yes | 0 |
| Partially meet requirements | 0.5 |
| No  | 1 |

* 1. Questions 1, 4, 5:

| **Evaluation criteria**  | **Score** |
| --- | --- |
| Yes | 1 |
| Partially meet requirements | 0.5 |
| No | 0 |

* 1. Question 7:

| **Evaluation criteria**  | **Score** |
| --- | --- |
| Yes, actively operating for more than 5 years  | 1 |
| 2-5 Years actively operating  | 0.5 |
| No, actively operating for less than 2 years  | 0 |

### All questions for all other risk elements:

| **Evaluation criteria**  | **Score** |
| --- | --- |
| Yes | 1 |
| Partially meet requirements | 0.5 |
| No | 0 |

## Third Party Risk Assessment

* 1. The assessment of bidders’ responses to the questions will be determined by the completeness (i.e. all questions answered), undertaking signed (where required) and accuracy of substantiating evidence, when requested. Please note that SITA reserves the right to verify the information provided.

| **Question to assess each risk element**  | **Bidders response:** **Mark relevant box with an “X”**  |
| --- | --- |
| **Company Risk**  |
| 1. Have you disclosed all interests and relationships as required in **SBD 4**, including whether any of your directors, members, trustees, or shareholders are employed by the state, have relationships with SITA employees, or have interests in other entities (whether they are also bidding for this contract, or not)?
 | Yes | Partially | No |
| 1. Are you currently involved in litigation against SITA – or do you foresee litigation being instituted within the next 6 months?
 | Yes | Partially | No |
| 1. Are there any lawsuits or ongoing litigation that could affect this transaction in any way or the bidder as an ongoing concern?
 | Yes | Partially | No |
| 1. Is customer service delivery or contract performance actively monitored by you?
 | Yes | Partially | No |
| 1. Do you have formal strategic planning processes in place?
 | Yes | Partially | No |
| 1. Are any of your directors or shareholders Prominent Influential People (PIP) or Politically Exposed Persons (PEP)?
 | Yes | Partially | No |
| 1. Has your company been actively operating as a going concern for more than 5 years?
 | Yes | 2-5 Years | Less than 2 years |
| 1. Is the company busy with a re-organisational/restructuring process that may impact this transaction?
 | Yes | Partially | No |
| 1. Are any of your suppliers located in a region where geopolitical risk exposure is high?
 | Yes | Partially | No |
| 1. Has any current director of the bidder ever served as a director of a company during a period where a Government contract was cancelled?
 | Yes | Partially | No |
| **Financial Risk**  |
| 1. Did you have positive revenue growth in the past three years?
 | Yes | Partially | No |
| 1. Is the proposed bid price going to be **less than 40%** of your total annual revenue for the previous financial year?
 | Yes | Partially | No |
| 1. Is the financial health of your company in good standing?
 | Yes | Partially | No |
| 1. Were your Annual Financial Statement (AFS) unqualified in the last financial year?
 | Yes | Partially | No |
| 1. Do you have sufficient cash in the bank (2 or more months’ worth of operating cost) to operate under restricted conditions for at least 2 months?
 | Yes | Partially | No |
| 1. Do you have a clean credit record: No current or pending judgement, adverse listing, business rescue or principal sequestration listing?
 | Yes | Partially | No |
| **Operational Risk**  |
| 1. Do you have operational redundancy (resilience) in terms of technology and energy resources to ensure high availability of services?
 | Yes | Partially | No |
| 1. Are your dependencies for logistics either fully under your own control **or** managed through supplier performance management contracts? (Choose “Yes” if fully under your own control and “No” for supplier contracts)
 | Yes | Partially | No |
| 1. Do you have operational procedure standards in place across the organisation, such as change control, release management, access control, incident management, back-up regimes and restore tests, etc?
 | Yes | Partially | No |
| 1. Do you have human resources management in place, including succession planning and mitigation against key reliance on single individuals?
 | Yes | Partially | No |
| 1. Do you have sound supply chain processes in place?
 | Yes | Partially | No |
| 1. Do you have sound third party risk management processes in place (fourth party for SITA)?
 | Yes | Partially | No |
| 1. Do you have a fully-fledged research and development (R&D) department to ensure continuous improvement?
 | Yes | Partially | No |
| 1. Do you rely on locally manufactured components or have actively managed the risk relating to lead times or delivery delays? (Choose “Yes” is you rely on locally manufactured components or can actively manage lead times and prevent delivery delays where manufacturing is not local i.e. not in South Africa)
 | Yes | Partially | No |
| **Governance and Compliance Risk**  |
| 1. Do you comply with all legislation, including labour, health and safety regulations?
 | Yes | Partially | No |
| 1. Do you have the appropriate governance frameworks (Cobit, ITIL, King) in place with due monitoring against set standards?
 | Yes | Partially | No |
| 1. Do you have an internal audit function compliant with IIA standards (insourced, outsourced or co-sourced) in place?
 | Yes | Partially | No |
| 1. Do you follow formally documented enterprise risk management processes?
 | Yes | Partially | No |
| 1. Are all statutory requirements of the entity up to date? Specifically, the following: CIPC Returns, Tax returns, UIF and COIDA.
 | Yes | Partially | No |
| 1. Do you have comprehensive insurance in place, including cover for assets, business disruption and liability?
 | Yes | Partially | No |
| **Information Security and Privacy Risk** |
| 1. Are your physical security perimeters appropriately safeguarded?
 | Yes | Partially | No |
| 1. Do you have video surveillance of areas that will contain SITA information/products?
 | Yes | Partially | No |
| 1. Do you conduct security and suitability verification of all employees prior to employment?
 | Yes | Partially | No |
| 1. Do you have identification verification controls in place in all your buildings?
 | Yes | Partially | No |
| 1. Are your access control protocols verified to be effective by Internal and/or External Auditors?
 | Yes | Partially | No |
| 1. Do you have Security Information and Events Management (SIEM) processes in place?
 | Yes | Partially | No |
| 1. Do you have sufficient information security and cyber arrangements in place for employees working from home?
 | Yes | Partially | No |
| **Reputational Risk**  |
| 1. Do you have anti-bribery and corruption, anti-money laundering and fraud prevention practices in place?
 | Yes | Partially | No |
| 1. Please confirm that neither the company, nor any of its directors has been named in any corruption scandal (choose “Yes” to confirm **not being named** in a corruption scandal)
 | Yes | Partially | No |
| 1. Do you have a social responsibility programme in place?
 | Yes | Partially | No |
| 1. Do you have an environmental protection policy, including potential harmful emission or hazardous waste management?
 | Yes | Partially | No |
| 1. Do you actively manage your organisation’s energy consumption?
 | Yes | Partially | No |
| 1. Is your employment equity plan up to date and actively managed?
 | Yes | Partially | No |

##  Third Party Risk Management Declaration

* 1. The bidder hereby makes the following declaration and confirm the following information (mark with a “X” in the corresponding column):

| **Statement of Declaration**  | **Accept and Confirm** | **Do not accept and confirm** |
| --- | --- | --- |
| 1. All questions in this assessment were answered accurately.
 |  |  |
| 1. SITA can request additional supporting documentation, within reason, to confirm the accuracy and completeness of the information provided in this self-assessment.
 |  |  |

### Declaration of Acceptance

|  |  |  |
| --- | --- | --- |
|  | **Accept all** | **Do not accept all** |
| 1. The bidder declares that all information provided in this assessment is accurate.
2. The bidder understands that any false information may constitute misrepresentation.
	1. SITA reserves the right to verify the information provided.
3. By completing the Third-Party Risk Management Assessment the Bidder agrees to provide all reasonable supporting documentation when requested to do so, as well as during contract finalisation as this is a **pre-award condition of this bid.**
4. The bidders understand and agrees that this section will form part of the contract and is legally binding.
 |  |  |
| **Any additional comments by bidder pertaining to the third-party risk assessment:** |

**NOTE: Failing to complete all the questions, or not Accepting the Declaration of Acceptance will lead to disqualification.**

1. Product/Service Functional Requirements ADDENDUM 1

.

**NB: The Bidder must confirm that they comply with the following Product / Service Functional requirements as indicated below as this will be legal contractual binding.**

Refer to Section 2 Scope of Work and Section 3 Requirements for the detailed information:

**Product/Service Functional Requirements**

| **Solution Feature** | **Description** |
| --- | --- |
| 1. Supply, install and provision of high-capacity bandwidth internet connectivity that offers complete, fully redundant and secure Internet architecture with the below requirements.
 | * + 1. Provide a comprehensive internet architecture solution, inclusive of a managed service platform.
		2. Provision of fully redundant, protected and secure breakout points to the three SITA Internet breakout points located at **SITA centurion**, **SITA Cape town** and **SITA Pietermaritzburg**. Network Diagram **see section 3.1 table 2.**
		3. Provision of three point to point links triangulated between **SITA Centurion**, **SITA Cape town** and **SITA Pietermaritzburg.**
		4. Provision of fully redundant, protected connectivity links from the three DMZs (**SITA Centurion, SITA Cape town** and **SITA Pietermaritzburg**) to **TERACO (NAPAFRICA**) in each individual TERACO data centre in Cape Town, Johannesburg and Durban, that will be used for the Internet peering purpose and failover access to tenants located at the Internet Exchange at these locations.
		5. A **fully protected layer 2 service** that is provisioned over a fibre network that utilizes **geographically diverse fibre routes** to ensure the maximum uptime of the underlay network in each of the SITA DMZ locations.
		6. Full upstream ISP internal redundancy within the ISP's and SITA's own ASN space with backup links that are triangulated between three SITA sites which are located at **SITA Cape town**, **SITA Centurion** and **SITA Pietermaritzburg**.
		7. **DDOS mitigation** for all DDOS traffic that may transit via the Service Providers network.
 |
| 1. Connectivity and Solution Requirements
 | * + 1. SITA requires the service provider to establish on-site presence in Centurion, Cape Town and Pietermaritzburg locations.
		2. SITA requires a fully protected layer 2 service to be provided between the following locations.

Location: Speed:Centurion and Cape Town 100GbpsCenturion and Pietermaritzburg 100GbpsCape Town and Pietermaritzburg 100Gbps* + 1. SITA requires the capability to be able to connect 6 x 100 Gbps network devices to the providers on site nodes in the follow locations meaning in each POP the provider must deploy a device with 6 x 100gbps ports.

Location: SpeedCenturion and Cape Town 6X100GbpsCenturion and Pietermaritzburg 6X100Gbps Cape Town and Pietermaritzburg 6X100Gbps* + 1. SITA requires a protected layer 2 service for Internet IP transit to be provided in the following locations.

Location: Provisioned speed: Layer 1 speed:Centurion 40 Gbps 100 GbpsCape Town 40 Gbps 100 GbpsPietermaritzburg 40 Gbps 100 Gbps* + 1. Provider needs to provide a network architecture diagram demonstrating the use of diverse fibre routes and diverse fibre providers to ensure maximum uptime of the underlay network.
		2. SITA requires the underlay network to be 100 Gbps capable, with the capability to commence the Internet service with 40Gbps of provisioned internet bandwidth and with the capability to scale the Internet service to 100 Gbps in all three of SITA’s POPs.
		3. SITA additionally requires dedicated 20 Mbps links from the service providers network to Centurion, Cape Town and Pietermaritzburg and these links must carry permanently allocated static IP addresses from the Service Providers ASN to allow out-of-band management of the SITA environment by the SITA staff.
		4. The provider must accept /28 prefixes and propagate those prefixes across their network, to allow SITA to selectively advertise /28 prefixes to the ISP out of any one of their POPs. The ISP may however aggregate these according to Internet standards to the rest of the world.
		5. SITA requires the Internet Service to include DDOS mitigation for any and ALL DDOS traffic that may transit via the Service Providers network to the SITA ASN 37130
		6. SITA requires BGP peering with the ISP’s Internet service transit edges to the SITA BGP peering links to allow SITA to use BGP flow spec to advertise traffic limits and traffic filters to prevent traffic from transiting across from the provider’s ASN to the SITA ASN 37130 to prevent DDOS type of traffic from overutilising the transit peering links and effecting SITA NGN client service with upstream illegitimate traffic.
		7. Full upstream Redundancy with backup links that are triangulated between three SITA DMZs which are located at SITA Cape town, SITA Centurion and SITA Pietermaritzburg.
		8. Ensure that each breakout point can carry and provide Internet connectivity for the full bandwidth procured at any point in time.
		9. The equipment deployed on SITA at the SITA POPs, must be capable of establishing connectivity to Huawei networking equipment.
		10. The provider is responsible for managing the fault life cycle of all layer 1 protected service links. SITA will not interact with any third parties that the bidder contracts in to provide the service, this is entirely the bidder’s responsibility.
		11. To provide continuous service quality evaluation for the full duration of the contract. Failure to deliver the service in accordance with the contract service parameters and required uptime metrics will result in penalties.
		12. Provide individual connectivity between the three DMZs (SITA Centurion, SITA Cape town and SITA Pietermaritzburg to TERACO (NAPAFRICA) that is used for Microsoft peering, other internet exchange providers and failover access to TERACO.
 |
| 1. Hardware and Network Extension to SITA PoPs
 | * + 1. The supplier must extend its network to the designated SITA PoPs (Centurion, Cape Town and Pietermaritzburg).
		2. This includes the installation of the supplier's own managed routers, switches, network infrastructure, and fibre, or any necessary equipment to deliver the required solution.
		3. All infrastructure and cabling upstream of SITA’s owned and managed routers/switches is the responsibility of the service provider.
		4. The service must be provided on hardware owned by the service provider.
		5. The service provider will be bound by a Service Level Agreement (SLA) to provide and maintain sufficient hardware to meet the required mail delivery times.
		6. These requirements must include, but are not limited to, floor/rack space, power requirements including consumption, and thermal emissions in BTUs.
		7. The supplier will be liable for SITA-imposed charges at applicable rates for hosting such a cabinet/rack.
		8. Installation of infrastructure must adhere to SITA-approved Switching Centre standards.
		9. The service provider will be responsible for the insurance of their own equipment.
 |
| 1. Service Termination
 | * + 1. The service must be supplied to and terminated on the designated network ports on SITA infrastructure at each SITA premises.
		2. The connectivity requirement: 100G fibre hand off will be required.
 |
| 1. Hosting Equipment Requirements
 | If there is a need for hosting any equipment, such as a network switch, the requirements must be provided. These must include, but are not limited to, floor/rack space and power requirements including consumption and thermal emissions in BTUs.  |
| 1. Protection DDOS Attacks
 | The solution must be able to provide effective protection against DDOS Attacks. |
| 1. Internet Redundancy Links
 | Provide full redundancy for the three Internet breakout in Centurion, Pietermaritzburg and Cape town |
| 1. Solution Architecture and Network Design
 | The solution architecture and network design must ensure continuous operation between the 3 PoPs, maintaining full load handling in a redundant or fail-over configuration. |
| 1. Bandwidth and Capacity Management
 | * + 1. The supplier must ensure sufficient bandwidth is provisioned in both upstream and downstream directions and upgrade the bandwidth when necessary.
		2. Capacity management of all service aspects is the responsibility of the service provider.
		3. Minimum requirements in terms of bandwidth are that the utilization on each of the links between the service provider and the SITA PoPs in Centurion, Pietermaritzburg and Cape Town may not exceed 70%, averaged over a 5 minute period during business hours (i.e. Normal Working days between 07h00 and 17h00).
		4. This utilisation level applies to each link individually.
		5. This utilisation level applies to inbound and outbound traffic.
		6. Utilisation reports must form part of the monthly reporting
 |
| 1. End-to-End Availability
 | The solution must provide **end-to-end availability of 99.99% or higher** is required, where end-to-end means all aspects of the service, including the downstream bandwidth and the service platform itself |
| 1. Log Retention
 | 1. Retain log files pertaining to SITA’s service for a minimum of six (6) months.
2. Provide log files to SITA monthly to ensure an overall log retention period of two (2) years.
 |
| 1. Service Termination
 | 1. The service must be supplied to and terminated on the designated network ports on SITA infrastructure at each SITA premises.
2. The connectivity requirement: 100G fibre hand off will be required
 |
| 1. Architectural Restrictions and Protocols
 | 1. Supplier must note that all documents and designs created for SITA will be owned by SITA
 |
| 1. SLA and Support
 | The service must be SLA based and must have a **24x7x365 support service** that the SITA engineers can access, with engineers available to provide support. |
| 1. Web Interface
 | 1. The service must have a **web interface** which can be accessed by SITA to manage certain aspects of the service and to monitor traffic flow.
2. This interface must be available **24x7x365.**
 |
| 1. Administration and Reporting Requirements
 | 1. The supplier must provide an on-line reporting portal for SITA to access real-time as well as historical information in the form of graphs, statistics and reports.
2. Reporting must use a sampling/averaging window of no greater than 5 minutes.
3. All service data must be available on-line for the full-service contract period at the required 5-minute granularity. No roll-up /summarizing / re-averaging of data is permitted.
4. The reporting tool must be able to preserve peaks within any reporting window.
5. Data from the portal/s must be available in XML or CSV format on demand.
6. The portal required for this service must provide reports on at least, but not limited to, the following elements: Total bandwidth utilization.
7. Total bandwidth utilization
8. Excess traffic
9. Dropped traffic
10. Latency
11. Reachability
12. Availability
13. DDOS traffic reporting ie traffic passed and traffic blocked
14. BGP flow spec injection reporting (What dropped/null routed)
15. NETFLOW reporting (web interface)

All the above information must be available on the total solution as well as on a per PoP basis.1. Access to the portal must be restricted to SITA Support staff.
2. SITA will require **monthly Service Management meetings** with full reporting on all aspects of the service at each meeting. The reports must be supplied in hard copy at the meetings.
3. SITA will require electronic reports on the SLA metrics and the link utilization by close of business on the **3rd day of the month** following the reporting period.
4. SITA will require all RCA reports to be submitted to SITA within 3 working days of the associated fault / incident having been resolved.
5. Enable access to real-time and historical information through graphs, statistics, and reports.
6. Offer an accessible Audit log to track changes in the management portal.
7. Ensure at least six (6) months of data is available online.
8. Provide the ability to access historical data and request reports on earlier periods.
9. Offer data from the portal in CSV or XML format on request.
10. Present reports in PDF and HTML format.
11. Include an option to save reports in PDF format within the portal.
 |

**I, the bidder (Full names)………………………………………………………….representing (company**

**name)…………………………………………………………….. Hereby confirm that I comply with the above**

**Product/Service Functional Requirements and understand that it will form part of the contract and is legally binding.**

**Thus done and signed at …………………………………….. On this………day of……………..….20….**

**……………………………….**

**Signature**

**Designation**

1. **MIOS Certification Requirements**

**Regulatory, Quality and Standards**

* 1. The Supplier must for the duration of the contract ensure compliance with ISO/IEC General Quality Standards, ISO27001, and Protection of Personal Information Act (POPIA).
	2. The Supplier must for the duration of the contract ensure that the proposed product or solution conform to the list of Government Minimum Interoperability Standards (MIOS).

**NOTE (1):**

Refer to the MIOS Certification requirements for this Bid Specification below, however it is not limited to these items identified. The requirements will be finalised during the contracting stage. The successful bidder needs to ensure compliance with the SITA requirements for the duration of the contract.

MIOS Certification requirements for this Bid Specification: To be updated.

C020101 Hypertext Transfer Protocol (HTTP/1.1) RFC 7230

|  |  |
| --- | --- |
| C020109 Upgrading to TLS within HTTP/1.1 (HTTPS) | RFC 2817 |
| C030101 eXtensible Markup Language (XML 1.0) | XML |
| C050101 Hypertext Markup Language 5 (HTML v5) | HTML 5 |
| C050203 Comma-Separated Value (CSV) | RFC 4180 |
|  C050302 Portable Document Format (PDF v1.7) ISO 32000 |

 C050401 Structured Query Language (SQL) 2011 ISO 9075

|  |  |
| --- | --- |
| C050801 JavaScript (ECMAScript Language Specification) | ECMA 262 |