

Request for Tender

for

**APPOINTING A SERVICE PROVIDER WITH NATIONAL ACCREDITATION ON
THE SITA RFB1183/2013 CONTRACT TO PROVIDE INFORMATION,
COMMUNICATION AND TECHNOLOGY (ICT) SUPPORT SERVICES TO THE
SOUTH AFRICAN NATIONAL BIODIVERSITY INSTITUTE FOR A PERIOD OF
THIRTY-SIX (36) MONTHS**

**The South African National Biodiversity Institute (SANBI)
Private Bag X101
Silverton
Gauteng
0184**

Tender No: SANBI: IT355/2019

Contents

1. Introduction and Background.....	3
2. Purpose.....	4
3. Scope of Work	4
3.1 Responses submitted by prospective Service Providers should include the following:.....	4
3.2 Managed Support Services Profile.....	5
3.3 Delivery Approach and Value Proposition	6
4. Key Personnel and Competencies of the Service Provider	7
5. Mandatory Documents Required	7
5.1 Mandatory Requirements / Documents	7
5.2 Other Documentation Required (failure to submit these documents will result in disqualification)	8
6. Occupation Health, Safety and Environmental Requirements	8
7. Communication and Statement of Good Faith	9
8. Compulsory Briefing Session.....	9
9. Submission of Tender.....	9
10. Evaluation Criteria.....	10
11. Contract Period	11
12. Availability of tender.....	11
13. General	11
13.1 Non-Disclosure Agreement	11
13.2 Costs	11
13.3 Intellectual Property	11
13.4 Liability	12
14. Annexures A to R.....	13
Annexure A: User Base	13
Annexure B: Infrastructure and Applications	14
Annexure C: Costing Model.....	17
Annexure D: ICT Asset Management.....	18
Annexure E: Backup Management.....	19
Annexure F: Directory Services.....	23
Annexure G: Desktop Support.....	26
Annexure H: Messaging	27
Annexure I: Network Management.....	29
Annexure J: Patch Management	33
Annexure K: Perimeter Security	35
Annexure L: Service Desk	38
Annexure M: System Development and Test Platforms	40
Annexure N: Security.....	41
Annexure O: Software Distribution Services	42
Annexure P: Virtualization	44
Annexure Q: Hosting (Disaster Recovery)	46
Annexure R: Storage	48

1. Introduction and Background

The South African National Biodiversity Institute (hereafter referred to as SANBI) is a public entity which is mandated by the National Environmental Management: Biodiversity Act (NEMBA), Act No. 10 of 2004. SANBI's mission is to champion the exploration, conservation, sustainable use, appreciation and enjoyment of South Africa's exceptionally rich biodiversity for all people. The Institute provides biodiversity knowledge and information through research and communication and gives biodiversity planning and policy advice and pilots best practice biodiversity management models in partnership with a wide range of stakeholders. In addition, it manages botanical and the zoological gardens.

SANBI currently utilises an Information, Communication and Technology (ICT) Support Services contract to provide a comprehensive managed support service to meet the strategic goals and objectives of the Institution. The support services of an ICT Service Provider ensure that the required ICT capacity and capability are provided to enable and support the organisational mandate. The new model to be adopted will be service based to address gaps identified within the current model and based on strategic intent and objectives to address the increased demands. By the adoption of a new service model SANBI will benefit from a broad range of technological experts and services.

SANBI has **two (2)** main ICT operational centers namely at the SANBI Head Office situated in the Pretoria National Botanical Garden (PNBG) which includes the National Zoological Garden in Pretoria and at the Kirstenbosch National Botanical Garden in Cape Town. Both these centers and the National Zoological Garden in Pretoria together service approximately 832 users and hosts the major ICT infrastructure. SANBI also has smaller operational centers with connectivity and ICT needs in the provinces indicated below with a user count collectively of 245.

See Annexure A: User Base and distribution

- **Eastern Cape** (Kwelera National Botanical Garden and the Biodiversity Monitoring Assessment Office in East London)
- **Free State** (Free State National Botanical Garden in Bloemfontein)
- **Gauteng** (Walter Sisulu National Botanical Garden in Roodepoort)
- **KwaZulu-Natal** (KwaZulu-Natal National Botanical Garden in Pietermaritzburg the KwaZulu-Natal Herbarium and the Biodiversity Monitoring Assessment Office in Durban)
- **Limpopo** (Thohoyandou Botanical Garden and the Mokopane Biodiversity Conservation Centre, Mokopane)
- **Mpumalanga** (Lowveld National Botanical Garden in Mbombela)
- **Northern Cape** (Hantam National Botanical Garden in Nieuwoudtville)
- **Western Cape** (Harold Porter National Botanical Garden in Betty's Bay and the Karoo Desert National Botanical Garden in Worcester)

****NB** Expansion to the North West Province is anticipated within 2-3 years.**

2. Purpose

SANBI requires a Service Provider to provide comprehensive ICT Managed Support Services to meet the strategic goals and objectives of the Institute.

The purpose of this Request for Tender (RFT) is to consider tender responses from suitability qualified, experienced and professional Service Providers with the flexibility to offer both in-house and remote support, and to submit a proposal to supply SANBI with a Managed Services solution to their ICT outsourcing requirements.

The RFT serves to provide potential Service Providers with directives of the relevant ICT managed support services required by SANBI.

3. Scope of Work

SANBI currently employs an outsourcing model for much of its ICT functions and as such relies primarily on the support services of ICT Service Providers to ensure that the ICT capacity and capability enables and supports the Institution's mandate.

SANBI requires a comprehensive ICT managed support service and solution across the Institute's major and minor operational centers that includes all functional areas, but are not limited to operational, administrative, performance and infrastructure management.

The ideal Service Provider will be required to have an in depth understanding of ICT (best practice standards and frameworks i.e. Microsoft, Prince2) and be able to support the Institutional requirements at strategic and operational levels within the ICT Directorate. The required support services by the successful Service Provider includes but is not limited to activities related to ICT strategic and operational planning, reporting, monitoring, projects, systems analysis, security and regulatory compliance.

3.1 Responses submitted by prospective Service Providers should include the following:

- The proposed outsourcing model(s) for services required by SANBI ICT to provide to its internal clients, formal partners and stakeholders
- The proposed transitioning process and cost
- The increase/expansion clause/terms within the model proposed
- The exit clause/terms within the model proposed
- Any recommendations or considerations within the model proposed that would enhance the management of ICT services in SANBI
- Explicit reference to past successful managed support service rendered and a minimum of three (3) references of large enterprise (in excess of 1500 users) where managed ICT support outsource services were rendered on company letterheads
- The names and contact details of a minimum of three (3) clients/former clients where such a managed support service had been implemented successfully. (SANBI reserves the right to request the named clients to verify such implementations)

All Service Providers must complete a cost breakdown of their outsourced service for SANBI as described in this RFT, detailing the required ICT roles and their costs (Only to be included in envelope one (1) (See section 9))

All proposals are to include VAT and SANBI will assume that all pricing received is VAT inclusive and in South African Rand (ZAR).

Any work undertaken outside of the scope of services outlined in this RFT, or requiring additional resources to be completed, shall be viewed as a project, which will require a scoping session and a quotation, upon request by SANBI's ICT Management. This will not form part of the agreed fulltime resources within this RFT.

All pricing supplied in the Request for Tender (responses) shall remain valid for a period of four (4) calendar months (120 days).

3.2 Managed Support Services Profile

The scope of the managed support service is reflected in Table 1 below.

Table 1: ICT Support Services

1	Service Delivery Management	Overall responsibility for the delivery of all aspects of the Managed Support Services via a Service Level Agreement (SLA) management process
2	Change Control Install, move, add, change and decommission/dispose standards is applicable (IMACD)	Overall responsibility for the change control processes, end-to-end in the environment following Information Technology Infrastructure Library (ITIL) framework for managing Information Technology support services
3	Service Desk	Manage the lifecycle of calls logged at the service desk from creation to resolution Provide technical information and support to all computer users of SANBI and its tenants
4	Project and Programme Management	Manage and execute the full life-cycle of projects pertaining to ICT support services requirements
5	Desktop Management	Manage, support, install, configure and update systems software continually
6	Network Administration	Manage and support internal networks and provide as required e.g. Virtual Local Area Network (VLAN) for other services Manage hardware, software and security ensuring that our network is functioning and available at all times Manage internal networks and provide networks as required e.g. VLAN for other services e.g. tenants, QOS (quality of service for Video conferencing), WAN/LAN/Wi-Fi
7	Server Administration	Perform patch management and Anti-Virus deployment on all infrastructure Perform Operating System Updates Perform File Server and Data Management Storage of data lifecycle in adherence to policies and relative legislation ensuring compliance thereof
8	E-mail and Intranet Management	Manage the high volumes of inbound and outbound electronic mail within the Institution, ensuring e-mail backup services are in place to ensure continuity of this service within the environment Manage and support an intranet service on a SharePoint platform for collaboration and sharing of internal content
9	Hosting	Enable and provide hosting/cloud services within the environment for technology and applications which can be

		served by this internet based service or the development and implementation of a hybrid model where not sustainable for the Institute Oversee and manage all services hosted with third party Service Providers e.g. firewall security, website hosting, etc.
10	Security	Monitor and report on cyber security and conduct security reviews, access controls and processes and report on it
11	Backup Management	Refine, review and test the data backup policy and procedures to ensure compliance with relative legislation and this includes the retention of data as required
12	Disaster Recovery (DR) and Business Continuity Plan (BCP)	Review and amend DR and BCP policies and tools and ensure procedures are continually updated and tested to enable the recovery of SANBI's technology infrastructure and systems following a natural or human disaster where ICT is concerned
13	Infrastructure	Network Policy enforcements & Data Centre Operations Manage the Institute's entire ICT infrastructure including the monitoring and performance management of all hardware, software, and network in use Ensure procedures and guidelines to enforce, manage, monitor and maintain the network are implemented
14	Database	Perform database administration and Upgrades and monitor and report on it as indicated in SLA
15	ICT Asset Inventory and Lifecycle Management	Manage and support the lifecycle of ICT assets within the Institution which includes hardware and software (Excluding the sourcing of hardware and software)

3.3 Delivery Approach and Value Proposition

The ideal Service Provider is required in their response to provide an overview of the proposed delivery approach should they be awarded this contract for the provision of ICT support services, and how they will proceed with the integration, implementation and overall delivery of the service requirements.

The ideal Service Provider should provide a description of the services model support proposed and how it will benefit the ICT support capability should they be awarded the tender.

Service Providers are expected to price their services according to two phases. The time duration of each phase is at the discretion of the Service Provider. These phases are:

- **Inception Phase** – migration from incumbent and existing model to a new Service Provider for all services as they are currently deployed, followed by the ongoing operation and maintenance of these systems. The transitioning process should be managed as projects with agreed timeframes and deliverables by all parties. Service Providers are required to include the following transitioning requirements:
 - Operating systems (servers/desktops) to the latest version
 - SQL Servers to the latest version
 - VMWare servers from HYPER-V (ESX to Microsoft)
 - Virtual machines to be migrated from secondary sites (NZG, PTA and Data Centre) to primary data center

- **Strategic Phase** – implementation of upgraded or replacement systems and upgraded or replacement architectures to realize cost savings and/or additional value to SANBI for the longer term while improving the user experience, security and governance of the overall environment.

Service Providers should identify and indicate the cost of transitioning to a technology landscape that will mitigate any business risk. Refer to Annexure B for a full list of current infrastructure and applications.

(Both phases also refer to Annexure C: Costing Model: Transition Management)

All Service Providers shall be held liable to deliver the support services contained in their proposals. All Service Providers must respond with the services they will deliver in accordance with the specified requirements rather than what could be implemented. SANBI reserves the right to audit Service Providers delivering the support services. All services metrics will be managed via an agreed Service Level Agreement (SLA).

4. Key Personnel and Competencies of the Service Provider

The Service Provider will be responsible for providing the personnel for the listed support services. Should it become necessary to replace any personnel for any of the listed services during the course of this tender they may only be with individuals that have similar or better qualifications or experience.

The Successful Service Provider's team must possess the following competencies:

- Ability to work independently and deliver efficiently on high quality service deliverables
- Ability to work in a team and manage processes that require inputs within specific and across support service domains
- Excellent analytical, conceptual and organisational abilities
- Demonstrable experience of issues and processes within the relevant support service domain

5. Mandatory Documents Required

5.1 Mandatory Requirements / Documents

Tenders must include the following documentation (**Failure to submit this required documentation WILL lead to disqualification**):

- Pre-Qualification criteria for preferential procurement:
Section 4(1) a: A tenderer having a stipulated minimum Broad-Based Black Economic Empowerment (B-BBEE) Status Level Contributor, level 2. A valid original or certified copy of a B-BBEE Status Level Certificate or sworn affidavit must be submitted.
- Duly completed and signed **SBD forms**
- Compulsory briefing session certificate of attendance
- A copy of the Company Central Supplier Database (CSD) registration report

- Fee/cost structure to be submitted with the “ORIGINAL” tender document only (Refer to point 9)
- Proposals must include all completed Service Specifications (Annexures **D to R**)
- A valid copy of the **Unemployment Insurance Fund (UIF)** letter of compliance issued by the Department of Labour
- A certified copy of Liability Insurance Cover for the company and the total cover available per claim to the value of R2.5 million
- Letter of Good Standing from the office of the **Compensation Commissioner** as required by the Compensation for occupational Injuries and Diseases Act (COIDA). The letter should be issued by the Department of Labour
- A copy of the latest Audited Financial Statements

5.2 Other Documentation Required to Verify Competency (failure to submit documented evidence / certificates for all the competencies listed will result in disqualification):

- Certified competency for the full Microsoft Office technology stack (tenderer to have Microsoft Accreditation with no partnering allowed)
- Certified competency for CA Service Desk and IT Asset Management
- Certified competency for Cisco Networking Administration
- Certified competency for HP Networking Administration
- Certified competency and capacity for DELL Server Administration
- Certified competency and capacity in VEEAM and Hyper-V Backup Management

Proposals must include all completed Service Specifications (Annexures D to R)

All documents must be neatly bound, clearly labelled and include a Table of Contents.

6. Occupation Health, Safety and Environmental Requirements

Service Providers will be expected to have the ability to deliver and implement the Occupation Health and Safety Act (OHSA) and its regulations and the Compensation for Occupational Injuries and Diseases Act (COIDA) relating to health, safety and the environment.

It will be expected of potential Service Providers to execute ICT work in a manner that complies with all the requirements of the Acts and regulations and in doing so, minimise the risk of incidents/accidents occurring.

It will be expected of the potential Service Provider to supply an occupational health, safety and environmental file before signing the contract. This file will have to be approved by the SANBI Deputy Director for Health, Safety and the Environment before commencement of the contract. The Health, Safety and Environmental File will become SANBI property at the end of the contract.

7. Communication and Statement of Good Faith

All information provided by SANBI in this RFT is offered in good faith. Individual items are subject to change at any time. SANBI makes no certification that any item is without error.

Formal communications may include, but are not be limited to:

- Recommendations to SANBI in writing, regarding any discrepancies, errors or omissions which may exist within this RFT
- Recommendations to SANBI in writing, regarding any enhancements which might be in SANBI's best interests
- SANBI will make a good faith effort to provide a written response to each question or request for clarification that requires addenda within 5 calendar days. All questions and answers will be shared with all bidders registered at the compulsory briefing session.

All technical information in this RFT should be directed to: ITTender@sanbi.org.za.

All bid related queries shall be e-mailed to: sanbi.tenders@sanbi.org.za

SANBI will not respond to any questions or request for clarification which requires addenda if received after **28 October 2019**.

8. Compulsory Briefing Session

A compulsory briefing session will be held on:

Date: 23 October 2019 at 13:00

Venue: Administration Building, Kirstenbosch National Botanical Garden, Rhodes Drive, Newlands, Cape Town.

Failure to attend the compulsory Briefing Session will disqualify a potential bidder's proposal.

9. Submission of Tender

Service Providers are to submit one pack of the original proposal marked "ORIGINAL" in envelope #1 and 3 copies marked "COPY" in envelope #2.

Financial or pricing details should only be included in the pack marked "ORIGINAL".

Financial information included in the documents in the pack marked "Copy" will lead to your bid being disqualified.

Failure to submit 1 pack of original and 3 packs of copies, will lead to the bid being disqualified.

Closing date and time for enquiries/responses: 11:00 on 1 November 2019

Tenders can be submitted in the following manner:

Physical Delivery

Drop off in the Tender Box located in the Biodiversity Building at the Pretoria National Botanical Garden, 2 Cussonia Avenue, Brummeria, Pretoria, Gauteng during office hours or on the closing date **1 November 2019 by 11:00**. Normal office hours: 08:00–16:00 (See street address above).

Via Courier, addressed to:

The Deputy Director: Supply Chain Management

Biodiversity Building

Pretoria National Botanical Garden, 2 Cussonia Avenue, Brummeria, Pretoria, Gauteng during the hours 9:00–16:00 or on the closing date **1 November 2019 by 11:00**.

NB. E-mailed and faxed submissions will not be accepted. Late submissions will not be considered.

10. Evaluation Criteria

In accordance with the National Treasury Instruction Note on the Amended Guidelines in Respect of Bids that include Functionality as Criterion for Evaluation (issued 3 September 2010), this bid will be evaluated in the following stages:

The **first stage** will evaluate functionality according to the criteria listed in the table below:

CRITERIA FOR EVALUATING FUNCTIONALITY		WEIGHT / POINTS
Proposal Accuracy, quality and completeness.	5	5
Past Experience This refers to the experience of the Service Provider to undertake the scope of the work as defined in this tender		45
Experience and partnerships in multi-vendor environments	15	
Portfolio of Managed Services	15	
Provide at least three (3) traceable reference (The names and contact details of any past or present clients where similar managed support services have been supplied over the past three years, a brief description of these support services and success metrics	15	
Managed Service Model This refers to how the Service Provider proposes to improve processes and functions to improve operations and create value		10
Approach to implement optimized ICT Operations and Management	5	
Time to transition to an efficient Service Provider Managed Model	5	
Industry experience Proven experience and insight in aligning to industry best practices and standards		15
Application of best practices in transitioning to Service Provider Model	5	
Approach to supporting multi-vendor technologies	5	
Approach to Knowledge Management	5	
Team Capacity & Capability of the Service Provider The tenderer should indicate the following for the team members to be utilised in the execution of the contract by supplying CVs for each member with the following information (CV not more than three (3) pages in total): • Qualifications, experience, skills and expertise for relevant service support domain (Refer to section 4) • A brief description of individual's experience of similar work in the past five (5) years • Name of previous employer/s and position held in enterprise		25

• Proposed role in the services to be provided for this tender	
TOTAL	100

Bids that fail to score a minimum of 70 points out of a possible 100 points for functionality will not be eligible for further consideration.

The second stage will evaluate the price and preference points of those bids that meet the minimum threshold for functionality. In accordance with the Preferential Procurement Regulations, 2017 pertaining to the Preferential Procurement Policy Framework Act (No.5 of 2000), the 80/20-point system will be applied in evaluating proposals that qualify for further consideration, where price constitutes 80 points and a maximum of 20 points will be awarded on the bidder's B-BBEE Status Level Certificate.

Sufficient information must be provided to allow the evaluation panel to evaluate proposals against these criteria.

11. Contract Period

The duration of the proposed outsourcing service agreement shall be for a period of three (3) years, which will be reviewed every twelve (12) months based on performance against an agreed Service Level Agreement (SLA). Penalties related to non-performance will be detailed in the SLA.

12. Availability of tender

No tender documents will be issued at the briefing session. Potential Service Providers are requested to download the tender documents from the SANBI website: www.sanbi.org

13. General

Unless specifically requested, all documentation submitted to SANBI will not be returned to the bidder. All received information will be treated with confidentiality by SANBI.

13.1 Non-Disclosure Agreement

SANBI reserves the right to require the successful bidder to enter into a non-disclosure agreement.

13.2 Costs

The RFT does not obligate SANBI to pay for any costs of any kind whatsoever that may be incurred by the potential Service Provider or any third parties, in connection with the tender.

13.3 Intellectual Property

All submitted tenders should not use any intellectual property of SANBI including, but not limited to: All logos, registered trademarks, or trade names of SANBI, at any time without the prior written approval of SANBI, as appropriate.

All documentation, software customisation and/or any intellectual property developed by the appointed Service Provider during the duration and as part of this contract shall become the property of SANBI.

13.4 Liability

SANBI shall not be liable to any bidder, person, or entity for any losses, expenses, costs, claims, or damages of any kind:

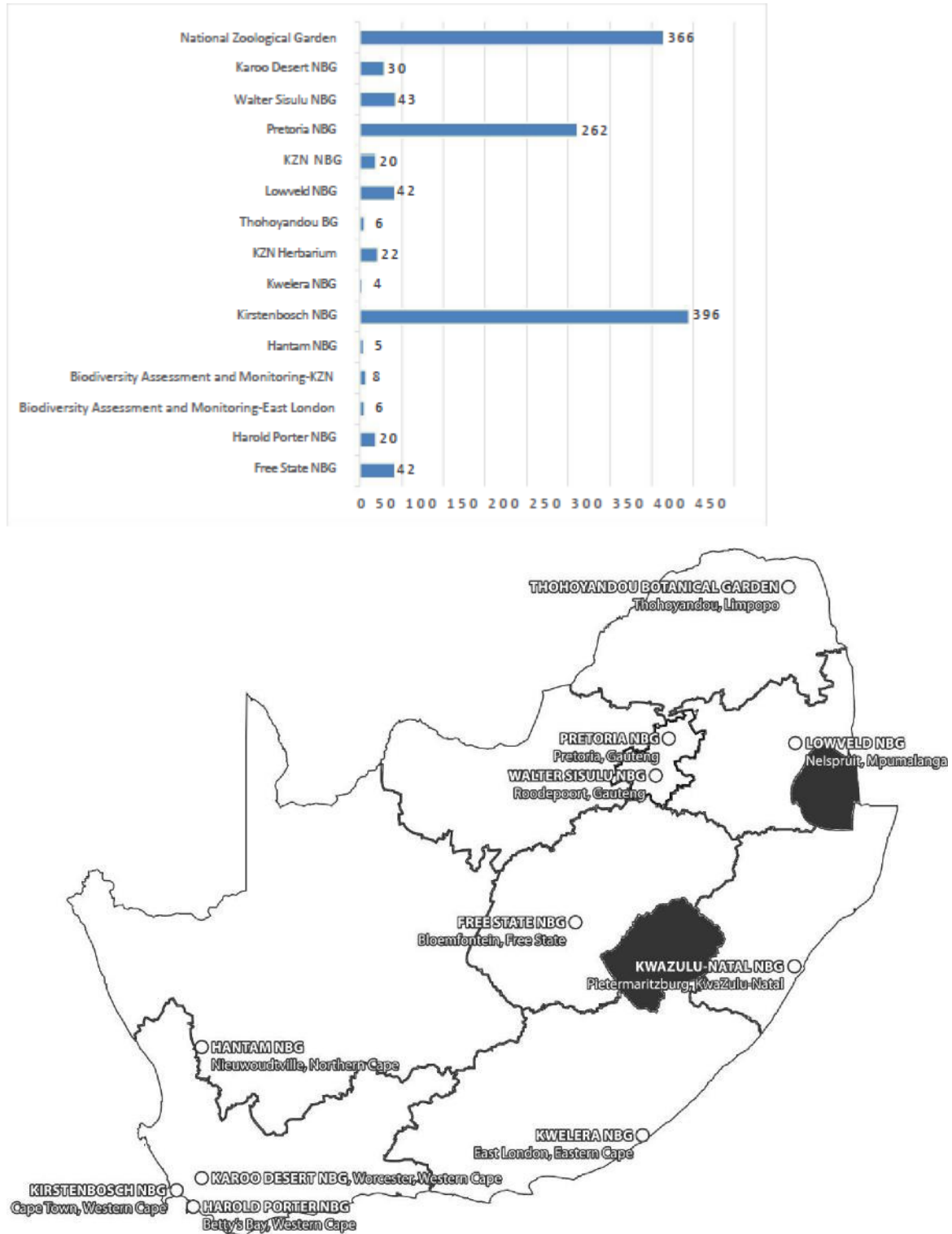
- Arising out of, by reason of, or attributable to, the bidder responding to this RFT, or
- As a result of the use of any information, error, or omission contained in this RFT document or provided during the RFT process

14. Annexures A to R

Annexure A: User Base

The existing user count per region is reflected in Figure 1 below.

Figure 1: User count per region



Annexure B: Infrastructure and Applications

Server Environment

SANBI Server environment includes the following services:

- DNS
- DHCP
- File Services
- Microsoft Windows Server 2003/2008/2008R2/2012/2012R2
- Microsoft Hyper V Environment 2012 R2
- Fortigate Firewall
- Active Directory
- Platform for directory services (Active Directory 2008/ r2)
- SQL Platform (SQL server 2008 SP1 /2012)
- Web proxy (TMG)
- Backup Exec 2012 and Veeam 9.5
- Exchange Online 2016 / Office 365

Other Services include:

- Web Services (IIS)
- Terminal Services
- MS SQL Server
- Platform for financial management application (ACCPAC)
- Nedbank banking system
- Platform for PRECIS / BRAHMS /Specify (in-house application, uses Interbase)
- Amlib Library Database
- Barnowl (Risk Management)
- Microsoft SharePoint 2016
- Pastel
- IQual (Procurement)
- FBA (Financial)
- BIT Defender (Security)
- LYNC 2010
- Microsoft Teams

Desktop Environment

The following desktop platforms are the standard deployed within SANBI:

- Microsoft Windows 7 Enterprise (standard)
- Microsoft Windows 10 Enterprise (standard)

Office Applications

- Microsoft Office 2016 Professional
- Microsoft Project 2016 Professional
- Microsoft Publisher 2016 and above
- Microsoft Visio 2016 and above
- Microsoft Outlook 2016

Other Software Applications supported within SANBI Environment include:

- Adobe Acrobat Reader 11.2 and above
- Adobe Acrobat 6 and above
- Adobe Illustrator 9 and above
- Adobe InDesign 3 and above
- Adobe Photoshop 5 and above
- Adobe Photoshop Elements 2 and above
- Adobe Premier 6
- Ahead Software Nero 6 and above
- Apple QuickTime 7 and above
- CorelDraw Suite 8 and above
- Cyberlink PowerDVD 5 and above
- ESRI ArcView 3.3 and above
- FileZilla 2 and above
- IrfanView 4 and above
- Macromedia Dreamweaver Macromedia Fireworks
- Macromedia Flash 10 and above
- Macromedia Freehand 10
- Microsoft EndNote 5.0 and above
- Microsoft FrontPage 97 and above
- Microsoft Visual Basic 2005 and above
- Microsoft Works 7 and above
- Mozilla Firefox 3 and above
- PuTTY 1.0 and above
- RealVNC Viewer 4 and above
- Roxio Easy CD Creator 10 and above
- Skype 5.0 and above
- Sun JRE 6 and above
- 7 Zip 3 and above
- Refman 10.0
- VLC Media 1.8 and above
- Unistat
- Precis
- Daemon Lite 4.0
- Google Earth 5 and above
- Miracle PERSAL
- Personnel Manager
- CutePDF 2 and above
- CA Service Desk

Virtualization platforms

- Microsoft Windows 2012 (R2) Server

Virtualization software

- Hyper V

Directory Services

- Microsoft Active Directory

E-mail System

- Microsoft Exchange 2016
- IIS 7
- Microsoft SQL Server 2008 and 2012 Standard Edition

Systems Monitoring

- HP Procurve Manager
- SCOM
- Solar Winds
- SSCM
- IMC

Internet Access Management

- Fortigate Proxy

Server Hardware

- Dell PowerEdge R710 and R410

Storage Area Networks (SAN) Hardware

- Dell MD3200i / IBM Storewiz 5000

Bandwidth Management Appliances

- Riverbed

Network Switches (incl. CORE)

- HP ProCurve
- CISCO

Wireless Bridging

- Fortinet AP / CISCO AP

Enterprise Database

- SQL Server (2008 / 2012)

Intranet Technology

- SharePoint 2016

Extranet Technology

- WordPress

Mail Environment

- Exchange 2016
- Hybrid Exchange (Office 365)

Annexure C: Costing Model

Service Element	Monthly Cost	Annual Cost	Baseline Volume and Remarks	Duration
Transition Management (Inception and Strategic Phases refer point 3.3)				
IT Asset Management				
Backup Management				
Directory Services				
Desktop Support				
Messaging				
Network Management				
Patch Management				
Perimeter Security				
Service Desk				
Systems Development Lifecycle and Testing (SDLC)				
Security				
Software Distribution Services				
Virtualization, Platforms				
Hosting (Disaster Recovery)				
Telephone Management				
Software Licencing Management				
Storage Management				
Total Cost (Vat) Inclusive				

Annexure D: ICT Asset Management

ICT Asset Management	Ability to Deliver (Y/N)	Supplier Motivation where response is no	Comment /
Deliverable Specification • Involvement at other organizations in the last three years where you have provided the services and key activities • Asset Management processes you may have documented and vested use to support this service • Quality management practices for which you may be certified • ITAM methodologies used and certification • How would you ensure SLA compliance in the event of the use of sub-contractor organisation • Your view of the short to medium term trends and developments in the Asset Management space and how may add value to SANBI regarding SANBI objectives of standardisation, consolidation, continuous service improvement and cost reduction			

Annexure E: Backup Management

Backup Management	Ability to deliver (Y/N)	Supplier Motivation where response is no	Comment /
Deliverable Specification At a minimum the following deliverables will be required: • Perform In-scope services backups and rotation of media as per client's backup policy • Test backup media to ensure that incremental and full recovery of data is possible and ensure In-scope services backup integrity, capability and compatibility • Manage backups and backup schedules to ensure that services and users are not adversely affected • Check that restores complete outside of backup windows • Label all media with client supplied barcodes • Schedule backups of all IT service configurations on Daily, weekly, monthly and yearly schedules • Configure data retention rules according to client policy • Select the business-critical data as per the approved data selection list • Schedule the backups in the approved time window • Apply client approved file type and directory exclusions to backup jobs • Install and remove backup agents on devices as required • Configure backup selection lists on agents • Restore requested data to specified location • Supply daily, monthly and yearly success/failure reporting • Develop, document and maintain Backup and Recovery schedules and procedures that adhere to Clients requirements and policies			

• Continually recommend best practices for Backup and Recovery Services, strategies, policies and procedures • Test backup media to ensure that incremental and full recovery of data is possible and ensure In-scope services backup integrity, capability and compatibility		
Reporting Requirement Frequency: Daily Format: Microsoft Word or Excel By when: 06:00 Mon - Fri every week including public holidays. Content: Exception list highlighting • each server which failed to backup successfully • details on which selections failed • reasons for the failure Frequency: Daily Format: Microsoft Word or Excel By When: 10:00 Mon-Fri every week including public holidays. Content: Exception list highlighting • Each server which failed to backup successfully • Confirmation of communication with the relevant system administrator of the servers for which the backups failed • Service Administrators decision i.e. rerun the backup during business hours, rerun the backup after business hours or take no action • Actions taken on incidents where backup has failed to run		
Frequency: Weekly Format: Microsoft Word or Excel By when: 10:00 Monday of every week including public holidays. Content: Complete overview of previous week's daily backups highlighting for each server • Daily successes • Daily failures		

• Indicating where backups failed but were successfully rerun before the next backup window Frequency: Weekly Format: Microsoft Word or Excel By when: 16:00 Monday of every week including public holidays.		
Content: Exception list for weekly backup highlighting • Servers which failed to backup successfully • Details on which selections failed • Reasons for the failure • Confirmation of communication with the relevant system administrator of the servers for which the backups failed • Service Administrators decision i.e. rerun the backup during business hours, rerun the backup after business hours or take no action • Actions taken on incidents where backup has failed to run		
Frequency: Monthly Format: Microsoft Word or Excel By when: within 5 working days of the end of the calendar month Content: Exception list for monthly backup highlighting • Servers which failed to backup successfully • Details on which selections failed • Reasons for the failure • Confirmation of communication with the relevant system administrator of the servers for which the backups failed • Service Administrators decision i.e. rerun the backup during business hours, rerun the backup after business hours or take no action • Actions taken on incidents where backup has failed to run Frequency: Annually Format: Microsoft Word or Excel By when: within 2 working weeks of the end of the calendar year Content: Exception list for annual backup highlighting		

• Servers which failed to backup successfully • Details on which selections failed • Reasons for the failure • Confirmation of communication with the relevant system administrator of the servers for which the backups failed		
• Service Administrators decision i.e. rerun the backup during business hours, rerun the backup after business hours or take no action • Actions taken on incidents where backup has failed to run		
Service Level Agreement • 100% compliance with documented and signed off backup selections • No more than 3 consecutive daily backup failures per server per week • No more than a total of 5 daily backup failures per 30-day rolling period per server • No more than 1 weekly backup failure per rolling 5-week period • No failures for any monthly or annual backup per server		

Annexure F: Directory Services

Directory Services	Ability to deliver (Y/N)	Supplier Motivation where response is no	Comment /
Deliverable Specification Active Directory • Manage access to the directory servers (domain controllers) • Manage, create and remove Client user and computer objects in accordance with Client • Policies • Manage, create and remove organizational units and related logon scripts • Manage directory replication between Sites • Manage directory server health through the monitoring system • Manage directory Sites and Services • Manage Flexible Single Master Operation (FMSO) role management • Investigate and resolve directory server related issues; • Liaise and log a support ticket with vendor until service is restored whenever required • Implement measures to ensure that unauthorized personnel cannot gain access to the equipment • Update directory server as-built/configuration document • Update operating processes and procedures			
DHCP Services • Manage DHCP server access • Manage DHCP clients and leases • Manage DHCP reservations and reserved clients • Manage the DHCP database • Manage DHCP server scopes, super scopes and multicast scopes; • Configure security dynamic updates • Investigate and resolve DHCP related issues • Update DHCP configuration document			

• Update DHCP operating processes and procedures		
DNS Services • Manage DNS server access • Manage the internal DNS records Manage the DNS database • Review database and remove old records on a regular basis • Manage disk space for DNS logs and database • Manage service performance statistics provided by the monitoring solution • Capture usage performance statistics provided by the monitoring solution • Investigate and resolve DNS-related issues • Liaise and log a support ticket with vendor until service is restored whenever necessary • Liaise and log a call to the Service Provider hosting public DNS records for changes required • Update DNS configuration document • Update DNS operating processes and procedures		
Group Policy Services • Manage Group Policy objects • Create, modify and update Group Policy objects as required by the Client • Reports on resultant set of policy (RSOP) data • Back up, restore, import and copy of Group Policy objects • Manage and perform changes as requested to login scripts • Manage the Group Policy compliancy in line with the Client Policies		
Radius • Manage and maintain radius authentication for Fortinet firewalls • Manage and maintain radius authentication for wireless infrastructures • General day to day operational changes as may be required from time to time		
Reporting Requirements: Frequency: Monthly		

Format: Microsoft Word or Excel When: By 5th working day of the end of the calendar month Content: • Overall health status of the directory services infrastructure per office or geographic region • List of any additions, deletions or modifications to any of the service elements described		
• List of all unused User Objects • List of all unused Computer Objects • List of unused distribution groups • List of all User Objects with elevated (administrative) privileges • List of all service accounts • Detail and describe functionality of any new or changed Group Policies		
Service Level Agreement The minimum acceptable service level is as follows: • 99% uptime of the AD, DNS, DHCP and Group Policy services availability across all regions • Where uptime is defined to exclude planned or maintenance downtime as detailed in the RFC document • Excused Unscheduled "Down Time" will be excluded from the calculation as provided for in the calculation formula • All authorised emergency changes and/or changes made during business hours that affect availability are excluded		

Annexure G: Desktop Support

Desktop Support	Ability to deliver (Y/N)	Supplier Motivation where response is no	Comment /
Deliverable Specification End User Desktop comprises support for workstation devices, including • Laptops • Desktops • Printers • Mobile Devices • This includes hardware support, Operating system upgrades, software support and interface support. • Support will be provided exclusively via telephonic and remote access methods • Software support will be limited to the Operating System, Microsoft office suites and standard software packages for which a Standard Operating Procedure (SOP) is available • Support will include basic troubleshooting and configuration for all aspects of day-to-day user activities including but not limited to, printing, internet access, server access via client software, anti-virus, package updates, access to shared resources etc.			
Reporting Requirements Frequency: Quarterly Format: Microsoft Word or Excel By when: within 5 working days of the end of the month or as agreed Content: • Comparison of deployed Operating Systems across the Group • Comparison of deployed office suites across the Group			
Service Level Agreement Standard operating mean time to respond and mean time to repair metrics as agreed for priority 1,2 and 3 service desk calls during operating hours only (SLA)			

Annexure H: Messaging

Messaging	Ability to deliver (Y/N)	Supplier Motivation where response is no	Comment /
Deliverable Specification: - Secure the Messaging Environment as per Microsoft best practice guidelines - Report, investigate and resolve degraded Messaging services - Report, investigate and resolve performance related issues - Liaise with internal stakeholders and third parties for related issues - Investigate and resolve capacity related issues - Liaise and log a support ticket with external vendor/s as may be required until service is restored whenever required - Implement measures to ensure that unauthorized personnel cannot gain access to the equipment - Update Messaging server as-built/configuration document - Update operating processes and procedures			
Reporting Requirements Frequency: Monthly Format: Microsoft Word or Excel By when: within 5 working days of the end of the calendar month Content: A report containing the following information: - Number of active mailboxes i.e. those that have sent email within the previous 90 days - Number of inactive mailboxes i.e. those which have not sent or received email within the previous 90 days - List of mailbox sizes ordered from largest to smallest compared with permitted mailbox size - Uptime report of the cluster components for the previous month - Uptime report of the service for the previous month			

Service Level Agreement The minimum acceptable service level is as follows:		
• 90% uptime for the mail transport service • Where uptime is defined to exclude planned or maintenance downtime as detailed in the RFI document • Excused Unscheduled “Down Time” will be excluded from the calculation as provided for in the calculation formula. • All authorised emergency changes and/or changes made during business hours that affect availability are excluded		

Annexure I: Network Management

Network Management	Ability to deliver (Y/N)	Supplier Motivation where response is no	Comment /
Deliverable Specification: Architecture and Design • Review architecture and ensure compliance with vendor and international best practice • Review architecture and ensure compliance with Group standards • Provide architecture recommendations for any changes or additions with due care • Provide architecture recommendations for any changes or additions similar or better Quality of Service on all links as current • Monitoring of infrastructure for events and alarms • Provide level 1,2 and 3 technical support for environment • Escalate to vendors where required to address problems and incidents • Manage the last mile service providers transparently to Group IT			
Manage Service Failures • Facilitate and manage the process of replacing failed equipment where necessary • Attempt to resolve problems on hardware or software not currently under maintenance using publicly accessible information when necessary • Interface with other providers of services to resolve problems where necessary			
Services Maintenance • Maintain software at version n-1 where n is the latest version release • Upgrade software as and when recommended by vendor to mitigate identified performance or vulnerability issues on systems			

Perform backups of the installed configurations of all devices		
IP Address Management - Review IP address infrastructure in accordance with best practice standards - Manage IP address structure across the LAN and WAN and update design documentation Capacity Management - Respond to any overutilization of bandwidth by identifying the root cause and mitigating or resolving the problem - Strict control of QoS configurations as per Client policy to guarantee no utilization of bandwidth by unauthorized traffic Access Management - Manage access to environment to support governance and compliance requirements of the business - Ensure devices Ability to deliver with access management policy - Report on access when required Break/Fix - Hardware break-fix 24 hours / 7 days a week support - Onsite services to remediate when all remote support efforts have been exhausted - Strict control of QoS configurations as per Client policy to guarantee no utilization of bandwidth by unauthorized traffic Other - The provision of uncontended (1:1) internet access service to the production data centre of a minimum of 5Mbit/s - The provision of uncontended (1:1) internet access service to office locations with greater than 50 staff of a minimum of 5Mbit/s The provision of internet access via IP Transit with no distinction between local and national browsing		
Reporting Requirements:		

Frequency: Monthly

Format: Microsoft Word or Excel

By when: Within 5 working days from the end of the calendar month

Content:

A report containing the following information:

- Uptime reports on all managed devices.
- Comparative report on installed and available IOS versions
- Updated upgrade path for all managed devices not at software version n-1
- Backup status report of all managed devices

Frequency: Quarterly

Format: Microsoft Visio

By when: At agreed quarterly intervals

Content:

- Updated accurate diagrams of all managed LAN's, WAN's and data centre network infrastructure

Frequency: Near Real-time

Format: Online Web

By when: **Daily, Weekly, Monthly and Annually**

Content:

Usage statistics of all the last mile links and any other links which may form part of the WAN including:

- Total bandwidth consumption inbound and outbound
- Per QoS band
- Combined bands (sum total)
- Top 50 bandwidth consumption by:
- Inbound IP address
- Outbound IP address
- Inbound Port
- Outbound Port
- Uptime

Frequency: Monthly

Format: Microsoft Word or Excel

By when: within 5 working days of the end of the calendar month

Content:

Average monthly usage statistics of all the last mile links and any other links which may form part of the WAN including:

Total bandwidth consumption inbound and outbound • Per QoS band • Combined bands (sum total) Uptime		
Service Level Agreement The minimum acceptable service level is as follows: • 90% uptime on any managed, non-redundant equipment • 90% uptime on any managed, redundant equipment • Where uptime is defined to exclude planned or maintenance downtime as detailed in the RFI document • All authorised emergency changes and/or changes made during business hours that affect availability are excluded		

Annexure J: Patch Management

Patch Management	Ability to deliver (Y/N)	Supplier Motivation where response is no	Comment /
Deliverable Specification At a minimum the following deliverables will be required: • Management and maintenance of the System Centre Software deployed on all server instances • Monthly patch cycle including downloading and distribution of all Microsoft Security and Critical patches. • Development Server deployment, implementation and testing • Development Workstation deployment, implementation and testing • Production Server deployment, implementation and testing • Production Workstation deployment, implementation and testing • Maintenance of Development Server list • Maintenance of Development Workstation list • Maintenance of Production Server list • Maintenance of Production Workstation list			
Reporting Requirements Frequency: Monthly Format: Microsoft Word or Excel By when: the 6th working day following implementation of production patching Content: Percentage compliance/noncompliance displayed both graphically and in tabular form for different systems groups as may be defined from time to time but typically: • Servers managed by the Outsource Service Provider • Servers managed by Internal Group IT • Servers managed by internal system administrators • Workstations			

• Exceptions list, detailing each server that is not patched along with reasons for the failure. Detailed description of any exceptions due to the technical issues, actions being taken and expected date of resolution		
Service Level Agreement Definitions • T0: Microsoft Critical & Security patch released • T+x : x days post patch release date • The service will be deemed successful on the following basis: • Patch distribution by T+7 • Communication of patch release and distribution to Group IT by T+7 • Rolling 3-month average of 98% compliance of all servers managed by the Outsource Service Provider • Rolling 3-month average of 90% compliance of all workstations which have connected to the domain within the last 30 days • Distribution of reporting requirements within stipulated time frames		

Annexure K: Perimeter Security

Perimeter Security	Ability to deliver (Y/N)	Supplier Motivation where response is no	Comment /
Deliverable Specification Policy and configuration management a. Installation, maintenance, and configuration of new and existing hardware and software. • Firewall updates and security patch management • Configuration backup management • Firewall system administration and troubleshooting • Testing failover and other resiliency systems • Log monitoring and analysis of firewall events • Integration of firewall services into monitoring and alerting systems • Firewall policy change requests of approved change control requests • Firewall security, availability, and performance monitoring. • Rule-set validation, verification, tuning, and optimization • Review of firewall policy and firewall security posture assessments • Comprehensive reporting upon written request • Incident response related to disruptions of service from firewall • Reporting errors and connectivity or performance problems between systems with traffic traversing the firewall			
Proxy Configuration Agreement • Installation, maintenance, and configuration of new and existing hardware and software • Proxy service updates and security patch management • Provide access for auditors and assist auditors where required • Configuration backup management • Proxy system administration and troubleshooting			

• Testing failover and other resiliency systems		
• Log monitoring and analysis of proxy events • Integration of proxy services into monitoring and alerting systems • Proxy policy change requests of approved change control requests • Proxy availability, bandwidth and performance monitoring • Integration and configuration of URL filtering in line with Clients policies • Rule-set validation, verification, tuning, and optimization • Review of proxy rules in alignment with clients Acceptable Usage Policy • Weekly and Monthly usage reports of users and websites • Comprehensive reporting upon written request • Incident response related to disruptions of service from users to proxy service • Reporting errors and connectivity or performance problems between clients traversing through the proxy		
VPN services • Configuration and maintenance of secure VPN access into the corporate network • Assist end user with troubleshooting of VPN access clients		
Reporting Requirements Frequency: Ad-hoc Format: Microsoft Word or Excel By when: As agreed with Client Content: General reports as follows: • Top users by bandwidth consumed • Top users by time spent • Top allowed web sites • Top denied websites • Top website categories		
Service Level Agreement The minimum acceptable service level is as follows: • 90% uptime on any managed, non-redundant firewall asset		

• 90% uptime on any managed, redundant firewall asset • Where uptime is defined to exclude planned or maintenance downtime as detailed in the RFI document • Excused Unscheduled “Down Time” will be excluded from the calculation as provided for in the calculation formula • All authorised emergency changes and/or changes made during business hours that affect availability are excluded		
---	--	--

Annexure L: Service Desk

Service Desk	Ability to deliver (Y/N)	Supplier Motivation where response is no Comment /
Deliverable Specification Availability • 7:00- 17:00 Mon - Fri Local time in each office for Desktop and user call management services • 24 hours / 7 days a week for Back Office Server Services (or as stipulated in each service item) • First call resolution • Perform initial troubleshooting and attempt to resolve call telephonically • Single point of contact. Log a call via the following methods • Email • Telephone • Web Interface (optional) • Group IT access to service desk system • ITIL aligned management of service calls including • Incident management • Request management • Problem management • Classification of calls according to priority (P1, P2, P3) • P1 -An incident that has a major impact on the Customer's service and which cannot be circumvented. A complete loss of the Customer's service or the impacted business function is halted. If a Customer has multiple VPNs at a site, then if one of the VPNs fails then it is considered a severity one fault as the Customer business function running over that VPN is halted • P2 -An incident that has a large impact on a portion of the Customer's service and cannot be circumvented, causing a significant loss of the Customer's service, but the impacted business function is not halted		

P3 -An incident that has a small impact on the Customer's service or where a single user or component are affected and it causes some impact to Customer's business, but the incident can be circumvented • Third party incident management if sub-contractors are utilized to provide service • Call tracking • Pro-actively manage incidents and escalation of calls with pre-defined thresholds • Updates to end users & Close service calls when resolved		
Reporting Requirements Frequency: Weekly Format: Microsoft Word or Excel When: By 12:00 every Monday Content : A report containing the following information: • Total Number of calls logged in the previous week by type (incident/Service request) • Total Number of calls logged in the previous week by type (incident/Service request) and only by AA staff • Total Number of P1, P2 and P3 incidents logged in the previous week with a short description of each including time to respond and time to repair		
Service Level Agreement • Less than 3% (of a minimum of 100) of inbound calls to the IT Service Desk abandoned after 60 seconds • Inbound Call Response Rates, 98% call are answered within 60 seconds • 98% of inbound e-mails to the Service Centre responded to within 20 minutes • Longest 5% of all calls wait time averaged over total number of calls in the longest 5% will not exceed 5 min • Resolve access rights incidents /requests within 60 minutes (1hr) • Resolve compliance violations within 5 minutes		

Annexure M: System Development and Test Platforms

Test ICT Platforms	Ability to deliver (Y/N)	Supplier Motivation where response is no	Comment /
Deliverable Specification The Service Provider shall deliver, install, and configure the ITSM product and include the set-up of roles, profiles, workflows, templates, screen designs, and reports in the test environment as defined by the SANBI to support its Development, Test and Production Environments.			
Reporting Requirements Frequency: Weekly/Monthly Format: Microsoft Word or Excel or PDF - Detailed list of defects, organized by severity level, including a short description, the person responsible for resolution and the planned method for resolution - List of all tests completed that executed successfully - List of all tests completed that executed and failed			

Annexure N: Security

Security	Ability to deliver (Y/N)	Supplier Motivation where response is no	Comment /
Deliverable Specification • Manage endpoint infrastructures • Keep of endpoint signatures up to date • Infrastructure assessments • Daily tasks to ensure coverage over infrastructure • Monthly visibility reports			
Reporting Requirements Frequency: Weekly Format: Microsoft Word or Excel When: COB every Friday Content: A report containing the following information: • Comparison of endpoint deployment with single source of authority (AD)			
Service Level Agreement Servers: • 100% of active servers deployed with signature at current release, as of date of measurement			

Annexure O: Software Distribution Services

Software Distribution Services	Ability to deliver (Y/N)	Supplier Motivation where response is no	Comment /
Deliverable Specification Availability 7:00 to 17:00 Monday to Friday Local time in each office for Desktop and user call management services 24 hours daily, 7 days per week for Back Office Server Services (or as stipulated in each service item) • First call resolution • Perform initial troubleshooting and attempt to resolve call telephonically • Single point of contact. Log a call via the following methods • Email • Telephone • Web Interface (optional) • Group IT access to service desk system • ITIL aligned management of service calls including • Incident management • Request management • Problem management • Classification of calls according to priority (P1, P2, P3) • P1: An incident that has a major impact on the Customer's service and which cannot be circumvented. A complete loss of the Customer's service or the impacted business function is halted. If a Customer has multiple VPNs at a site, then if one of the VPNs fails then it is considered a severity one fault as the Customer business function running over that VPN is halted • P2: An incident that has a large impact on a portion of the Customer's service and cannot be circumvented, causing a significant loss of the Customer's service, but the impacted business function is not halted			

P3: An incident that has a small impact on the Customer's service or where a single user or component are affected, and it causes some impact to Customer's business, but the incident can be circumvented • Third party incident management if sub-contractors are utilized to provide service • Call tracking • Pro-actively manage incidents and escalation of calls with pre-defined thresholds • Updates to end users & Close service calls when resolved		
Reporting Requirements Frequency: Weekly Format: Microsoft Word or Excel When: By 12:00 every Monday Content : A report containing the following information: • Total Number of calls logged in the previous week by type (incident/Service request) • Total Number of calls logged in the previous week by type (incident/Service request) and only by AA staff • Total Number of P1, P2 and P3 incidents logged in the previous week with a short description of each including time to respond and time to repair		
Service Level Agreement • Less than 3% (of a minimum of 100) of inbound calls to the Service Centre abandoned after 30 seconds • Inbound Call Response Rates, 98% call are answered within 30 seconds • 98% of inbound e-mails to the Service Centre responded to within 20 minutes • Longest 5% of all calls wait time averaged over total number of calls in the longest 5% will not exceed 2 min		

Annexure P: Virtualization

Virtualization, Platforms and Storage	Ability to deliver (Y/N)	Supplier Comment / Motivation where response is no
Deliverable Specification • Maintain and manage the Client specific virtualization software with the latest agreed software patches and agreed version of virtualization software • Ensure virtualization software is maintained on the agreed Patch level in adherence to Patch policy and in accordance with vendor recommendation • Upgrade virtualization software with minor version upgrades • Perform system administration and configuration • Provide host and host cluster configuration • Host high availability configuration • Provide host storage administration and configuration • Provide Virtual Network Configuration • Perform VM template management • Provide user role administration • Provide performance monitoring with corrective action for resource optimization • Provide VM self-service configuration • Implement measures to ensure that unauthorized personnel cannot gain access to the equipment • Investigate and resolve performance related issues • Liaise and log a support ticket with vendor until service is restored when necessary • Update design documentation to reflect the environment changes • Update configuration details for VMs • Update operating processes and procedures		
Reporting Requirements Frequency: Monthly Format: Microsoft Word or Excel		

When: 5 Working Days at the end of the calendar month or as agreed :		
Content: Uptime reports for the previous month for virtualization infrastructure including Underlying virtual base hosts Supporting switching infrastructure Supporting management infrastructure Capacity reports including: RAM – available, used, reserved CPU – available, used, reserved HDD – available, used, Reserved		
Service Level Agreement The minimum acceptable service level is as follows: • 95% uptime on virtual server platform • All authorised emergency changes and/or • changes made during business hours		

Annexure Q: Hosting (Disaster Recovery)

Hosting (DRP)	Ability to deliver (Y/N)	Supplier Motivation where response is no	Comment /
Deliverable Specification • Co-location facilities to match those currently being consumed • Minimum of 25km physical distance between primary and disaster recovery data centres • Production and disaster recovery data centres to be located in the “logical centre” of the network i.e. providing the best possible access (on average) to all the WAN connected offices • 24 hours / 7 days a week, 365 days per year (24 x 7x 365) access to the data centres for authorized personnel • Provide level 1,2 and 3 technical support for environment • Report, investigate and resolve degraded access to the hosting environment • Report, investigate and resolve performance related issues • Liaise with internal stakeholders and third parties for related issues • Liaise and log a support ticket with vendor until service is restored whenever required • Implement measures to ensure that unauthorized personnel cannot gain access to the hosted equipment • Update data centre as-built/configuration document • Update operating processes and procedures			
Reporting Requirements Frequency: Monthly Format: Microsoft Word or Excel By When: within 5 working days of the end of the calendar month Content: • Uptime of the facility for the previous month			

• Availability of facility for the previous month • Any relevant data centre metrics such as power consumption, data		
Service Level Agreement The minimum acceptable service level is as follows: • 95% uptime on storage platforms • 95% uptime of all facilities power • 95% uptime of all facilities cooling systems • 95% uptime of all facilities fire suppression systems • 95% uptime on any managed, non-redundant hosting equipment • 95% uptime on any managed, redundant hosting equipment • Where uptime is defined to exclude planned or maintenance downtime as detailed in the RFI document • Excused Unscheduled “Down Time” will be excluded from the calculation as provided for in the calculation formula		
• All authorised emergency changes and/or changes made during business hours that affect availability are excluded • Compliance to business continuity plan recovery time objectives		

Annexure R: Storage

Storage	Ability to deliver (Y/N)	Supplier Motivation where response is no	Comment /
Deliverable Specification • Provide level 1,2 and 3 technical support for environment • Installation of hardware as per vendor specific best practices • Configuration of hardware as per vendor specific best practices • Monitor and manage the storage components via appropriate technologies or management packs • Report on any failed storage device • Liaise with vendor until failed device or component is replacement • Investigate and report degraded storage hardware • Investigate and resolve performance related issues on the storage hardware • Liaise with storage vendor on performance related issues until resolved			
Reporting Requirements Frequency: Monthly Format: Microsoft Word or Excel By When: within 5 working days of the end of the calendar month Content: • Uptime reports for the previous month • for storage infrastructure including: • Number of failed disks/replaced disks • Number of online disks • Number of standby disks Performance Reports Including: • Disk IOPS • Disk Read IO Rates			
Service Level Agreement The minimum acceptable service level is as follows: • 95% uptime on storage platforms			