



4th Floor
Riverwalk Office Park
Block A, 41 Matroosberg Road
Ashlea Gardens
PRETORIA
SOUTH AFRICA
0081

P.O. Box 580, **MENLYN**, 0063
Tel: 012 346 1738, Fax: 086 693 7472
E-Mail: enquiries@pfa.org.za
Website: www.pfa.org.za

BID DESCRIPTION	SUPPLY,DELIVERY, INSTALLATION, COMMISSIONING AND SUPPORT OF ON-PREMISE ICT INFRASTRUCTURE
BID NUMBER	OPFA/ICT/012026
CLOSING DATE	24 MARCH 2026
CLOSING TIME	11:00

Bidder name: _____

Company registration number: _____

CSD number: _____



4th Floor
Riverwalk Office Park
Block A, 41 Matroosberg Road
Ashlea Gardens, Extension 6
PRETORIA
SOUTH AFRICA
0181

P.O. Box 580, **MENLYN**, 0063
Tel: 012 346 1738 / 748 4000
Fax: 086 693 7472
E-Mail: enquiries@pfa.org.za
Website: www.pfa.org.za

1. INTRODUCTION

- 1.1. The Office of the Pension Funds Adjudicator (OPFA) was established in terms of section 30B of the Pension Funds Act No.24 of 1956 ("Act") with effect from 01 January 1998 and is funded in terms of section 30R of the Act.
- 1.2. In terms of section 30D of the Act, the main objective of the Adjudicator is to dispose of complaints lodged in terms of section 30A (3) of the Act, and complaints for which the Adjudicator is designated in terms of section 211 of the Financial Sector Regulation Act.

2. OBJECTIVES OF THE REQUIRED SERVICES

- 2.1. The objective and purpose of this bid is to appoint a qualified service provider to:
 - 2.1.1. Supply and deliver new server and storage infrastructure (as per approved Bill of Materials- Annexure A, Page 42).
 - 2.1.2. Install, configure and commission the infrastructure at OPFA's premises in Pretoria.
 - 2.1.3. Migrate existing workloads to the new server infrastructure.
 - 2.1.4. Provide managed support and professional services for a period of 36 months. This period may be renewed for a further period of 24 months.
- 2.2. This bid represents a capital acquisition (CAPEX) model, the OPFA will own the hardware and associated infrastructure assets.
- 2.3. The solution must integrate seamlessly with OPFA's current infrastructure:
 - 2.3.1. Managed Security Services (PAM360, SIEM).
 - 2.3.2. Backup and Disaster Recovery services.
 - 2.3.3. Connectivity services.
 - 2.3.4. Governance and audit frameworks.

- 2.4. The aim is to enable ICT is a key enabler for OPFA's mission, supporting modernisation, improved service delivery, and business continuity. The existing server infrastructure is reaching its end-of-life and must be refreshed to ensure ongoing reliability, compliance, and reliability.

3. CURRENT ENVIRONMENT OVERVIEW

- 3.1. The OPFA operates a hybrid ICT environment designed to support its mission of resolving pension fund complaints efficiently and securely, servicing approximately 85 users.

- 3.2. The current environment includes:

Total number of users per Active Directory:	81 <i>This number may change due to the growth of the organisation.</i>
Primary Data Centre	One office at Riverwalk Office Park in Ashlea Gardens, Pretoria, which serves as the primary site for business and ICT operations, hosting the core production environment.
Server Infrastructure	Enterprise-grade servers (predominantly Dell), supporting Windows Server 2008 or later, Active Directory, Hyper-V, and SCVMM for virtualisation and management.
Network Connectivity	○ The head office maintains high-availability general internet connectivity via a primary 300 Mbps fibre line provided by Frogfoot, with a secondary 200 Mbps failover line provided by Liquid Technologies in the event of primary link failure. ○ In addition to this general connectivity, a dedicated MTN Cloud Connect link operating at 260 Mbps provides direct connectivity between the head office and the disaster recovery (DR) centre in Isando, enabling secure data replication between the two sites.

- 3.3. The OPFA currently runs Microsoft Hyper-V environment hosting the following servers from three (3) Hosts. The table below indicates the current infrastructure details.

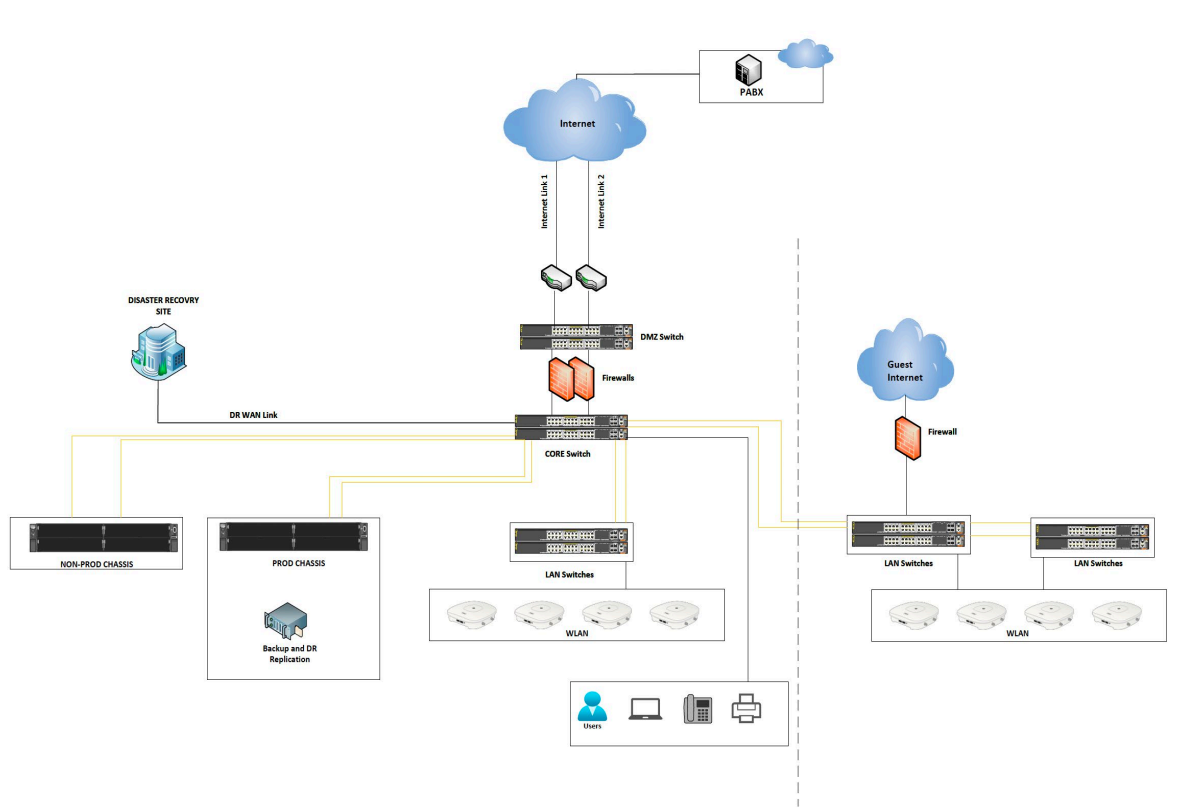
Applications (e.g. SQL)	Operating System	No of CPUs	RAM (GB)	Storage total (GB)	Free Space (GB)	Total Used (GB)
Certificate Authority	Windows Server 2019	2 Virtual processor	8GB	100GB	40GB	60GB
Pastel Evolution	Windows Server 2019	4 Virtual processor	16GB	200GB	130GB	70GB
Exclaim	Windows Server 2019	4 Virtual processor	12GB	400GB	315GB	85GB
File Server	Windows Server 2019	4 Virtual processor	16GB	4.71TB	1.83TB	2.88TB
Inmagic application-Library	Windows Server 2019	2 Virtual processor	8GB	400GB	350GB	50GB
MECM	Windows Server 2019	8 Virtual processor	32GB	1.2TB	610GB	610GB
RDS Server	Windows Server 2019	4 Virtual processor	16GB	200GB	123GB	77GB
Respond Application	Windows Server 2019	4 Virtual processor	16GB	400GB	310GB	90GB
Pastel Partner	Windows Server 2019	4 Virtual processor	16GB	600GB	458GB	142GB
Sage300	Windows Server 2019	8 Virtual processor	16GB	100GB	12GB	78GB
Sage200	Windows Server 2019	8 Virtual processor	24GB	500GB	105GB	385GB
Invgate	Windows Server 2019	4 Virtual processor	16GB	100GB	10GB	90GB
SQL	Windows Server 2019	4 Virtual processor - 3.00GHz	24GB	14TB	7TB	7TB
SQL	Windows Server 2019	4 Virtual processor - 3.00GHz	24GB	14TB	7TB	7TB
Domain Controller (Primary)	Windows Server 2019	2 Virtual processor	8GB	446GB	366GB	80GB

Applications (e.g. SQL)	Operating System	No of CPUs	RAM (GB)	Storage total (GB)	Free Space (GB)	Total Used (GB)
Domain Controller(Se condary)	Windows Server 2019	2 Virtual processor	8GB	100GB	49GB	51GB
Hyper-V Replica	Windows Server 2019	4 Virtual processor	16GB	557GB	462GB	95GB
Website	Windows Server 2019	6 Virtual processor	32GB	600GB	552GB	48GB
Manage Engine Applications	Windows Server 2019	24 Virtual processor	64GB	750GB	646GB	104GB
Antivirus and SIEM servers	Windows Server 2019	8 virtual processors	20GB	600GB	400GB	200GB
Print Server	Windows Server 2019	4 virtual processor	16GB	126GB	78GB	48GB

3.4. Storage and Resources running for Prod

STORAGE		
Total Storage	134,75 TB	
Consumed	63,32 TB	
Free	71,43 TB	
Number of volumes	12	
Servers	4	
Disks	46	
MEMORY AND CPU ON EACH NODE		
Node	CPU	Memory
Node 1	2 X (6 cores and 12 logical processors)	512GB
Node 2	2 X (6 cores and 12 logical processors)	512GB
Node 3	2 X (6 cores and 12 logical processors)	512GB

3.5. Current High-Level Architecture Diagram



3.6. Business Systems

The Technology Stack is hosting the following various core business applications and office automation systems:

Business Applications	
MS Office Cloud Suite	Sage 200 (Finance and SCM)
SharePoint Online	Pastel Partner for Financial Accounting
Respond Case Management System	Invigate IT Solution
Sage 300 (HR and Payroll)	Exclaim Integrated for Risk & Compliance Management

3.7. Telephone Management System

- 3.7.1. The OPFA currently utilises a Voice over IP (VoIP) telephone system powered by 3CX, which is hosted off-premises and managed by a third-party service provider. The 3CX system supports softphone functionality, enabling staff to make and receive calls via desktop or mobile applications.
- 3.7.2. The OPFA plans to integrate Microsoft Teams with the 3CX telephone system in the near future to streamline communication and improve collaboration within the Microsoft 365 environment.
- 3.7.3. The organisation maintains two telephone line carriers, with one serving as the primary link and the other as a redundant secondary link. All OPFA telephone numbers are hosted on the respective service providers' platforms to ensure continuity and portability.

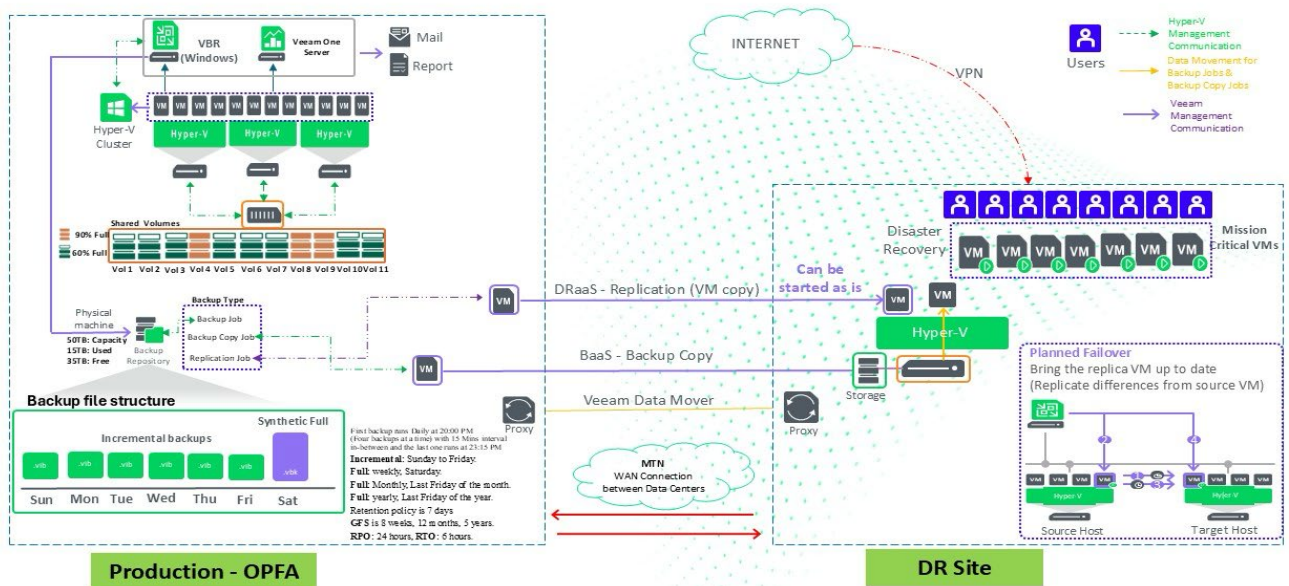
3.8. Desktop Environment

- 3.8.1. The OPFA operates a diverse desktop environment comprising primarily Dell and HP laptops, with a limited number of MacBooks issued to select users based on operational requirements. In addition to laptops, a small number of mobile devices such as iPads are allocated to specific roles that require enhanced mobility and flexibility. The organisation also supports a Bring Your Own Device (BYOD) approach, allowing staff to securely access corporate resources from their personal devices in line with approved security policies.

3.9. Managed Backup and Disaster Recovery

- 3.9.1. **Veeam Backup:** Managed Veeam Backup solution for comprehensive backup and recovery, including daily, weekly, monthly, and yearly schedules.
- 3.9.2. **Disaster Recovery Services:** Data and VMs are replicated between production and DR sites, enabling rapid recovery.
- 3.9.3. **Testing:** Regular backup and restore testing for recoverability and compliance.

Veeam Backup and Replication Low-Level Design OPFA



3.10. OPFA Security Landscape

- 3.10.1. **Managed security services** include endpoint protection, firewall management, intrusion detection/prevention, and regular vulnerability assessments, delivered in collaboration with a third-party provider and in compliance with POPIA.
- 3.10.2. **Firewall:** Fortinet Next-Generation Firewall is deployed to manage perimeter security, prevent intrusions, and enable secure connectivity between networks.
- 3.10.3. **Antivirus:** Symantec Endpoint Protection is used across the organisation to provide comprehensive threat prevention, detection, and response capabilities.
- 3.10.4. **Laptop Disk Encryption:** All OPFA-issued laptops are encrypted using Microsoft BitLocker to ensure data confidentiality and compliance with security policies.
- 3.10.5. **Cybersecurity Awareness Training:** The organisation uses the KnowBe4 platform to deliver ongoing cybersecurity awareness training and simulated phishing campaigns to staff.
- 3.10.6. **Multi-Factor Authentication (MFA):** MFA has been enabled for all users accessing Microsoft 365 services to provide an additional layer of identity verification and reduce the risk of unauthorized access.
- 3.10.7. **Virtual Private Network (VPN):** To ensure secure remote connectivity, the OPFA utilises a Virtual Private Network (VPN) solution powered by Fortinet FortiClient. This allows authorised

users to securely access internal systems and resources from remote locations.

- 3.10.8. **NB:** the platform to be used should be compatible with the existing OPFA security apparatus:
- **Symantec Endpoint Protection:** A comprehensive endpoint security suite for devices.
 - **FortiGate Appliances:** Next-generation firewalls.
 - **KnowBe4:** A security awareness training platform to educate users on best practices for safeguarding organizational assets against phishing and social engineering risks.
 - Vulnerability Management and SIEM: Independently managed by a third-party service provider.

3.11. Support Model and Service providers collaboration

- 3.11.1. Server Infrastructure, Network Support, Database Support, and Advisory Services: This encompasses the provisioning, maintenance, and optimisation of physical and virtual servers; ongoing network monitoring and troubleshooting; database administration including performance tuning, backups, and upgrades; and strategic advisory on ICT architecture to align with business needs.
- 3.11.2. ICT Vulnerability and SIEM: Handled by a specialised third-party service provider, this includes regular vulnerability scanning, assessment, and remediation across the ICT environment, alongside Security Information and Event Management (SIEM) for real-time threat detection, logging, and incident response.
- 3.11.3. Cloud Backup and Disaster Recovery: This service covers automated cloud-based backups of critical data and systems, with robust disaster recovery planning, testing, and failover procedures to ensure business continuity in the event of outages or disasters.
- 3.11.4. Business Application Support: Focusing on the maintenance, troubleshooting, and enhancement of core business applications.
- 3.11.5. Managed MFP (Printer) Services: This involves the deployment, monitoring, and support of multi-function printers.
- 3.11.6. VoIP Telephony: Includes the management of Voice over IP systems, call routing, quality assurance, and integration with collaboration.
- 3.11.7. Data and Links Connectivity: For high-availability data links, including primary fibre connections, failover mechanisms, and dedicated site-to-site links for replication and secure data transfer.
- 3.11.8. **NB:** Bidders must be prepared to work within this model and collaborate openly with OPFA's other service providers, including governance, risk, compliance, and audit teams.

4. BUSINESS DRIVERS

The primary business focus are:

- 4.1. Modernise and future-proof OPFA's ICT infrastructure.
- 4.2. Ensure compliance with POPIA and all relevant South African ICT regulations.
- 4.3. Support scalability and elasticity for future growth.
- 4.4. Improve service delivery to stakeholders.
- 4.5. Facilitate collaboration with governance, risk, compliance, and audit teams.

5. SCOPE OF GOODS AND SERVICES

5.1. The Service Provider shall provide a comprehensive set of Information and Communication Technology (ICT) services to OPFA. The services will be structured into two primary domains:

5.1.1. Supply and implementation of on-premise ICT infrastructure (Capex).

5.1.2. Managed professional services

5.2. In providing the services the appointed Service Provider will be required to comply with OPFA's ICT governance policies, security standards, and applicable South African regulatory requirements. The scope below outlines the minimum requirements expected of the Service Provider.

5.3. PART A: SUPPLY AND IMPLEMENTATION OF ON-PREMISES INFRASTRUCTURE (CAPEX)

#	Scope	Required action
5.3.1	Supply of Hardware and Software	The Service Provider shall: ○ Supply all hardware components in accordance with the approved Bill of Materials (BOM as per Annexure A, Page 42). ○ Ensure all equipment is brand new, enterprise-grade and sourced from authorised OEM channels. ○ Provide full OEM warranties and support agreements. ○ Register all equipment in OPFA's name.
5.3.2	Delivery and Installation	○ The Service Provider shall, through an OEM resource (Professional Deployment) : ○ Deliver all equipment to OPFA's primary site (Pretoria). ○ Install into existing racks or supply additional racks if required. ○ Configure power, cooling and cabling. ○ Ensure compliance with OHS and environmental regulations. ○ Produce a comprehensive Solution Design Document (SDD)

#	Scope	Required action
		covering both the “to-be” (proposed environment) configurations. The SDD must include detailed architecture diagrams (infrastructure, network, storage, security, and logical design), hardware specifications, IP schemas, VLAN segmentation, etc. ○ Upon completion of deployment and configuration, the Service Provider shall conduct a formal handover to OPFA. This must include submission of all configuration files, OEM warranty documentation, and an updated infrastructure topology
5.3.3	Project Management	○ The Service Provider shall appoint a suitably qualified and certified OEM-accredited Project Manager to lead and oversee the full lifecycle of the infrastructure implementation. ○ The appointed Project Manager must: ○ Be directly aligned to the Original Equipment Manufacturer (OEM) of the proposed core infrastructure platform. ○ Be accountable for the successful delivery, commissioning, and formal sign-off of the infrastructure solution.
5.3.4	Configuration and Commissioning	The Service Provider shall: ○ Configure hypervisor environment (Hyper-V or proposed platform). ○ Configure storage pools and redundancy. ○ Implement high availability clustering. ○ Configure VLANs and network segmentation. ○ Implement security hardening in line with CIS benchmarks and OPFA standards.
5.3.5	Migration Services	○ Migrate all existing virtual machines (VMs), applications, and associated data into the new infrastructure. ○ Minimise downtime and operational disruption during migration. ○ Conduct thorough post-migration validation and testing prior to production cut-over. ○ Provide rollback procedures. ○ Validate performance and stability before production sign-off. ○ A minimum of 25 virtual machines (VMs), together with their applications and associated data, shall be migrated into the new infrastructure. ○ All network, storage, and security configurations must conform to OPFA's ICT standards and industry best practices. ○ The solution must deliver operational resilience, redundancy, and integration with OPFA's monitoring and management tools.

#	Scope	Required action
5.3.6	Decommissioning of Existing Infrastructure	The Service Provider shall be responsible for: - the structured and secure decommissioning of all legacy servers and storage infrastructure that is replaced under this project. The decommissioning process must include: - Development of a formal Decommissioning Plan, to be approved by OPFA prior to execution. - Verification that all workloads, applications, data, and dependencies have been successfully migrated and validated before any legacy systems are powered down. - Secure data sanitisation of all storage media in accordance with recognised industry standards (e.g. NIST 800-88 or equivalent), ensuring full compliance with all requirements. - Provision of a Data Sanitisation Report for each device or storage component decommissioned. - Removal of legacy configurations from monitoring systems, backup systems, and security platforms. - No legacy infrastructure may be decommissioned without written approval from OPFA confirming successful migration and operational stability. - The Service Provider shall remain liable for any data breach, loss, or regulatory non-compliance arising from improper decommissioning procedures

Infrastructure components	Equipment compatibility	Warranty and OEM Support
The proposed infrastructure must include: - Enterprise servers - Storage systems - Networking components. - Hypervisor platform licensing - Backup integration compatibility - Redundancy components	All equipment must be compatible with OPFA's existing security stack including: - FortiGate firewalls. - Symantec Endpoint Protection. - Veeam Backup. - Existing SIEM platform.	- All infrastructure must carry a minimum 5-year OEM warranty. - Support contracts must include 24/7 hardware replacement SLA. - The bidder must provide proof of OEM partnership

5.4. Business Continuity and Disaster Recovery (DR) Alignment

- 5.4.1. The organisation currently replicates data for critical and core production workloads to a secondary site to support disaster recovery and backup restoration as part of its existing DR and Backup-as-a-Service capability. Veeam is used as the standard platform to manage replication, synchronization, and recovery processes.
- 5.4.2. The proposed enterprise infrastructure solution must be fully compatible with the existing Veeam backup and replication environment for on-premises workloads.
- 5.4.3. The appointed service provider will be responsible for coordinating with the OPFA disaster recovery and backup teams to plan, execute, and validate the initial data synchronization following implementation of the new solution. This includes ensuring that replication, backup, and restore operations meet agreed performance, integrity, and recovery objectives.
- 5.4.4. The service provider will further be obligated to support and participate in scheduled disaster recovery testing, including test planning, execution, remediation of identified issues, and formal sign-off. In the event of an actual disaster recovery invocation, the service provider will be expected to provide timely support in accordance with agreed service levels to restore services and data.

5.5. PART B: MANAGED PROFESSIONAL SERVICES (ON-PREMISE SUPPORT MODEL)

The Service Provider shall deliver operational support, system management, and advisory services to ensure that OPFA's ICT environment remains robust, secure, and aligned with best practice standards.

Support and Maintenance of the Server Infrastructure which includes the following:

- 5.5.1. Provide comprehensive support and maintenance services for the on-premise server infrastructure deployed under Part A. The objective is to ensure high availability, performance optimisation, security compliance, and operational stability throughout the contract period.

The scope shall include, but not be limited to, the following:

5.5.2. Proactive Infrastructure Monitoring

- 24/7 monitoring of physical servers, virtual hosts, storage systems, and clustering components.
- Real-time alerting for hardware failures, performance degradation, capacity thresholds, and environmental risks.
- Integration with OPFA's existing monitoring and SIEM platforms.

5.5.3. Preventative Maintenance

- Regular health checks of server hardware, storage subsystems, and hypervisor environments.
- Firmware, patches and driver updates in accordance with OEM recommendations.
- Hypervisor patching and updates aligned to OPFA's Change Management process.

5.5.4. Incident and Problem Management

- Second-line and third-line support for all infrastructure-related incidents.
- Root Cause Analysis (RCA) reports for Priority 1 and recurring incidents.
- Coordination with OEM support for hardware-related faults.
- Escalation management in line with agreed SLA response and resolution times.

5.5.5. Performance and Capacity Management

- Ongoing monitoring of CPU, memory, storage IOPS, and network utilisation.
- Trend analysis and capacity forecasting for at least 06 months ahead.
- Recommendations for upgrades or optimisation to prevent performance

bottlenecks.

5.5.6. High Availability and Resilience Management

- Monitoring and management of clustering, failover mechanisms, and redundancy configurations.
- Testing of failover procedures in coordination with OPFA and the DR service provider.
- Ensuring that infrastructure supports defined RTO and RPO targets.

5.5.7. Security and Compliance

- Implementation of security hardening standards.
- Coordination with OPFA's vulnerability management provider for remediation of infrastructure-related findings.
- Enforcement of least privilege access controls on server and hypervisor environments.
- Maintenance of audit logs and configuration baselines.

5.5.8. Configuration and Documentation Management

- Maintenance of up-to-date configuration documentation, including topology diagrams and asset inventories.
- Version-controlled documentation for infrastructure changes.
- Submission of quarterly reports detailing infrastructure health, incidents, SLA adherence, risks, and recommendations.
- The Service Provider shall ensure that all support activities are executed in compliance with OPFA's ICT policies and standards.

5.6. Network Management

- Provide proactive network management in line with agreed-upon uptime service levels and escalation processes.
- Monitor WAN, LAN, VPN, and wireless network performance on a 24/7 basis with automated alerts for outages or degradations.
- Optimise usage through bandwidth tuning, capacity management, and Quality of Service (QoS) configuration.
- Provide rapid fault resolution, including root cause analysis and incident reporting.
- Maintain accurate, version-controlled topology and configuration documentation.
- Apply security patches and firmware updates to network devices in line with best practices.

- Review network capacity frequently and recommend upgrades where appropriate.

5.7. Database Management

- Manage OPFA's SQL Server databases to ensure high availability, security, and performance.
- Monitor 24/7 for anomalies such as blocking queries, deadlocks, and excessive resource usage.
- Conduct recurring maintenance including index management, statistics updates, and integrity validation.
- Perform query tuning and schema optimisation for improved performance.
- Enforce encryption of data at rest and in transit, and apply strict role-based access controls.
- Manage patching, upgrades, and end-of-life (EOL) planning for SQL versions.
- Undertake ongoing growth analysis and capacity forecasting for database resources.

5.8. ICT Support and Advisory Services

5.8.1. Helpdesk and User Support

- OPFA shall retain ownership of all first-line support, including incident logging, basic troubleshooting, and user queries.
- The Service Provider shall provide second-line and above support for escalated issues relating to infrastructure, servers, networks, storage, databases, and operating systems.
- The Service Provider shall establish clear escalation paths from OPFA's internal helpdesk, with SLA-defined response and resolution times.
- The Service Provider shall provide integration with OPFA's ticketing or service desk platform, ensuring visibility across the incident lifecycle.

5.8.2. Change and Release Management

- The Service Provider shall manage ICT changes in line with OPFA's Change Management framework.
- Structured Release Management shall be executed for upgrades, patches, and deployments.

5.9. Service Monitoring and Reporting

- The Service Provider shall maintain centralised monitoring systems.
- The Service Provider shall provide monthly service management reports including incident resolution statistics, SLA adherence, system health, and key performance metrics.

5.9.1. Advisory and Governance Support

- The Service Provider shall provide advisory support in ICT strategy, security, technology trends, and governance compliance.
- The Service Provider shall assist with ICT audits, providing timely documentation and responses to information requests.
- The Service Provider shall support strategic ICT initiatives and projects with solution design and implementation support.

5.9.2. Service Availability

- The Service Provider shall deliver support during standard business hours, with after-hours coverage for critical or high-priority incidents.
- Escalation levels and response times shall be contractually defined in Service Level Agreements.

6. TECHNICAL REQUIREMENTS AND KEY CONSIDERATIONS

The Service Provider shall propose a solution and service model that meets the following technical requirements and key considerations. All bidders must demonstrate compliance in their submissions.

6.1. Integration and Collaboration

- 6.1.1. The proposed solution must integrate seamlessly with OPFA's existing ICT environment without disruption to current operations.
- 6.1.2. The Service Provider shall ensure ongoing collaboration with OPFA's current and future ICT vendors.
- 6.1.3. The Service Provider shall align with OPFA's Disaster Recovery (DR) Service Provider to ensure continuity and resilience within the overall ICT ecosystem.

6.2. Audit , Compliance, and Governance

- 6.2.1. The proposed solution must comply with the Protection of Personal Information Act (POPIA) and all other relevant South African ICT laws, standards, and regulations.
- 6.2.2. Comprehensive documentation of solution design (including infrastructure, storage, network, and security architecture) shall be provided and maintained throughout the contract period.
- 6.2.3. Provide support for the audit.

6.3. Vendor Certification and OEM Partnerships

- 6.3.1. The Service Provider shall hold current and relevant certifications or partnerships with Original Equipment Manufacturers (OEMs), including but not limited to HP, Dell, Microsoft, and VMware.
- 6.3.2. Bidders shall provide documentary proof of such partnerships or certifications within their submissions.

7. SERVICE LEVEL & SUPPORT

- 7.1. The Service Provider shall ensure a minimum infrastructure availability of **99.9% per calendar month**, excluding approved scheduled maintenance windows. Availability shall apply to the core production server infrastructure, including compute hosts, storage platforms, clustering components, and associated virtualisation layers.
- 7.2. Availability shall be calculated using the following formula: **Availability % = (Uptime / (Uptime + Downtime)) × 100**
- 7.3. Where:
 - **Uptime** refers to the total number of hours the infrastructure is fully operational and accessible within the calendar month.
 - **Downtime** refers to the total number of hours of unplanned service interruption affecting production workloads, excluding approved scheduled maintenance.
- 7.4. Partial outages affecting critical production systems shall be considered downtime for the impacted services.
- 7.5. Failure to meet the 99.9% monthly availability target shall trigger SLA penalties as defined in the SLA matrix.
- 7.6. Hardware replacement under the OEM contract.
- 7.7. 24/7 monitoring and support for critical incidents.
- 7.8. Monthly reporting on system health, incidents, and performance.
- 7.9. Penalties for non-compliance with SLAs as per applicable sections in the agreed SLA

Description	Mean Time to Respond	Mean Time to Repair	Target	Penalties
Incidents –Break-fix (Support and Maintenance related incidents)	1 hour	4 hours	95%	3% of the monthly Invoice.
Incidents – Break-fix (threats, security breaches)	1 hour	4 hours	95%	3% of the monthly Invoice.
Service requests (excluding reports)	1 hour	24 hours	95%	3% of the monthly Invoice.
Problem Management (threats, breaches and support and maintenance)	n/a	40 hours	90%	3% of the monthly Invoice.
Problem Management (Root Cause Analysis Report)	n/a	40 hours	100%	3% of the monthly Invoice.
Reports	As per agreed Reporting dates)		100%	5% of the monthly Invoice.

- In cases where service interruptions or failures occur due to circumstances beyond the Service Provider's reasonable control (e.g., natural disasters, national power outages), such incidents must be formally reported to OPFA with supporting documentation and recovery timelines.

8. PENALTIES

- 8.1. Penalties shall apply to delays and SLA breaches as defined in the contract and SLA matrix.
- 8.2. A penalty of 5% of the applicable cost line item will be levied for each week (five working days) of delay, capped at a maximum of 20% per month.
- 8.3. No penalties shall apply where delays are caused by factors outside the Service Provider's control, subject to OPFA's review and approval.
- 8.4. SLA breaches (e.g., uptime, incident response, resolution times) shall attract penalties in line with the agreed SLA matrix.
- 8.5. Penalties may be deducted from invoices or future payments and shall not limit OPFA's right to seek additional remedies if warranted.

9. RETENTION

- 9.1. Upon termination or expiration of the agreement, the Service Provider shall, on demand, immediately hand over to OPFA all documentation, data, information, software, configurations, records, and any other materials related to the services provided.
- 9.2. The Service Provider shall have no right of retention or lien over any OPFA information or property, whether physical or digital, under any circumstances.
- 9.3. All materials must be delivered in a complete, accurate, and usable form to ensure business continuity for OPFA.
- 9.4. Work Product and Intellectual Property: As agreed between the Parties, the OPFA shall own the final deliverables specifically prepared for the OPFA and delivered under this bid and contract if appointed (Final Deliverables), excluding the Service Provider's pre-existing materials, know-how, methodologies, templates (Service Provider Materials).
- 9.5. OPFA Materials: All documents, data and materials provided by the OPFA to the Service Provider (OPFA Materials) remain the property of the OPFA.

10. GENERAL CONDITIONS

10.1. First-Line ICT Support

OPFA will deliver all first-line ICT support internally, in accordance with its adopted IT Service Management (ITSM) framework. The successful bidder's support structure and escalation processes must align with this model, complementing OPFA's existing internal capabilities. The bidder must ensure seamless handover of incident logs, security events, and all relevant audit trails to OPFA, in line with agreed processes and security requirements.

10.2. Onsite Resource Availability

- 10.2.1. The Service Provider shall provide both remote and onsite support services as required to ensure the stability, performance, and security of OPFA's ICT environment. A suitably qualified and authorised technical resource shall be made available onsite at OPFA's primary premises in Pretoria:

- 10.2.2. At least once per week for preventative maintenance, health checks, optimisation, and stakeholder engagement; and
- On an ad hoc basis where operational needs require physical presence.
 - For urgent or high-priority incidents requiring physical intervention, the Service Provider shall ensure that a qualified technical resource is onsite within two (2) hours of formal request by OPFA during business hours. Failure to meet onsite response commitments shall be treated as an SLA breach and managed in accordance with the agreed penalty framework.

11. TRANSITION AND HANDOVER FROM CURRENT ICT TEAM

11.1. The successful bidder will collaborate closely with OPFA's current ICT support team for a period of three months post implementation to ensure a smooth transition and uninterrupted service delivery. This transition period is mandatory and is critical to facilitate effective knowledge transfer and operational stability.

11.2. Collaboration with Other Service Providers

The bidder must demonstrate the capacity and willingness to work collaboratively with other OPFA service providers, including those responsible for backup, disaster recovery, security, and network services. This includes, but is not limited to, participation in joint meetings, coordinated incident response, and support for integrated service delivery models. Such collaboration is both mandatory and essential.

12. SERVICE LEVEL AGREEMENT (SLA)

- 12.1. The service provider will report to the OPFA Senior ICT Manager or delegated personnel.
- 12.2. The service provider will be expected to conclude an SLA with the OPFA and report regularly as proposed by the Senior ICT Manager or delegated personnel with regards to the performance of the SLA.
- 12.3. The service provider will be expected to engage regularly with the OPFA team, as per the schedule and deliverables that will be agreed between the parties.
- 12.4. The service provider will be expected to avail the environment for periodic audits to validate the services being offered.
- 12.5. No penalties will be imposed on the bidder in instances where the agreed SLAs are not met due to reasons that fall outside the bidder's scope.
- 12.6. A maximum of 10% penalty will be levied per month if the cumulative total of SLA breaches per month is more than 10%.

- 12.7. Imposing the penalty does not absolve the bidder from performing the task(s), if repetitive non-compliance continues, the repetitive penalty will be imposed until the task(s) are completed.
- 12.8. If the bidder fails to deliver the goods or services in line with the agreed SLAs, the OPFA reserves the right to deduct any penalty amount, from the next invoice, irrespective of the service to which the penalty applies. The bidder will not accrue service credits for finalising tasks ahead of time; therefore, the bidder will not be able to offset the penalties with the service credits.
- 12.9. Invoices will only be considered for approval once the monthly report has been submitted and accepted by the OPFA. This will take into consideration offsetting the penalties accumulated.
- 12.10. Be responsible for SLA compliance, service reporting, escalation oversight, risk management, and continuous service improvement.
- 12.11. Conduct monthly service review meetings with OPFA and provide consolidated performance reports.

13. CONTINUOUS IMPROVEMENT

- 13.1. The bidder must make a provision of 15% of the total value of the contract for out-of-scope change request or ad-hoc services. This provision will only be used as and when ICT landscape needs to change (e.g relocation). The bidder is not entitled to this amount and will only bill for this amount when the Statement of Work has been signed by the bidder and the OPFA. The request will be initiated by the OPFA representatives.

14. COMPLIANCE WITH RELEVANT LEGISLATION

14.1. In providing the services, bidders will align with the relevant legislation.

Regulation/Law	Relevance to Tender
Protection of Personal Information Act (POPIA), 2013	Governs the processing, storage, and transfer of personal information in ICT environments, including cloud hosting and data replication. Ensures data subject rights, lawful processing, and security safeguards for OPFA's sensitive pension-related data.
National Policy on Data and Cloud Computing, 2024	Mandates secure, interoperable cloud services for public entities, promoting data sovereignty and migration of government IT to compliant clouds. Aligns with OPFA's IaaS hosting and DR replication requirements.
Electronic Communications and Transactions Act (ECTA), 2002	Regulates electronic transactions, cybersecurity, and critical information infrastructure in ICT services, applicable to network management and VoIP telephony support.
Regulation of Interception of Communications and Provision of Communication-related Information Act (RICA), 2002	Controls lawful interception and communication data retention for telecom/ICT services, relevant to VoIP, data links, and monitoring.
Cybercrimes Act, 2020	Addresses cyber threats in ICT infrastructure, including unauthorized access and data interference, critical for managed security and vulnerability management.
Promotion of Access to Information Act (PAIA), 2002	Facilitates access to records while protecting confidential information in public entities like OPFA, applicable to data backups and reporting.
Consumer Protection Act (CPA), 2008	Protects against unfair practices in service contracts, relevant to SLAs, pricing, and support for OPFA as a consumer of ICT services.

15. PRICING AND OFFER

15.1. The below cost model will apply

COST MODEL	
Feature/Requirement	PART A Supply of Hardware and Software, Delivery and Installation, Project Management, Configuration and Commissioning, Migration Services, Decommissioning of Existing Infrastructure, Warranty and OEM Support
Managed Service	Part B Support and Maintenance of the Server Infrastructure, Network Management, Database Management, ICT Support and Advisory Services.
Hardware Ownership	OPFA
Hosting Location	OPFA Premises, Pretoria
Support Model	Managed On-Prem Support
DR Integration	Existing Teraco DR
Migration	Included
SLA/Availability	Defined in proposal
Cost Structure	CAPEX + Monthly Support
Contract Duration	36 months

15.2. FIRM PRICING SCHEDULE

PART A – ONCE OFF (CAPEX)				
	Reference to Scope	Amount Excl		
Supply of Hardware and Software (as per detailed BOM)	5.3.1			
Delivery and Installation	5.3.2			
Project Management	5.3.3			
Configuration and Commissioning	5.3.4			
Migration Services	5.3.5			
Decommissioning	5.3.6			
Grand Total (PART A)				
	Reference to Scope	Year 1	Year 2	Year 3
Support and Maintenance of the server infrastructure	5.5			
Network Management	5.6			
Database Management	5.7			
ICT User Support & Advisory	5.8			
Monitoring & Reporting	5.9			
Total				
Grand Total PART B (Year 1-Year 3)				
Total (A+B)				
PART C – Continuous Improvement 15% of A + B)				

TOTAL PROJECT COST	COST (R)
PART A	
PART B	
PART C	
OTHER(specify items not included)	

TOTAL	
VAT	
TOTAL BID PRICE	
BID PRICE IN WORDS:	

- Bidders may use own template to calculate price, however the price must be mapped to this pricing schedule to ensure completeness and uniformity of pricing. Should the contract be renewed for 24 months the price will be adjusted for CPI
- Pricing: Terms and conditions**

PRICING	COMPLY	DO NOT COMPLY
The bidder confirms that the pricing provided in the response document is an all-inclusive price that takes into consideration all section of this document and all the price adjustments required for the duration of the contract. The bidder confirms that they have reviewed the specification and quantities to ensure that the requirements will meet the OPFA requirements. Any other additional required goods or services that are not specified in the bid document but are absolutely required to make the solution function should be explained in the response (with reasons) and the pricing should be included in the cost model/pricing schedule (under line item <i>“other”</i>). Any omission will be for the bidder's cost.		
WORKING HOURS AND OVERTIME COSTS	COMPLY	DO NOT COMPLY
The bidder accepts that core working hours are as follows: Monday to Friday (excluding public holidays) 07:30 to 17:00. Due to the nature of the ICT services, the bidder accepts that, where required, services may be performed after hours or weekends at no additional cost to the OPFA (e.g., scheduled maintenance, patching, resolutions of major incidents, DR testing, etc.). No overtime for working outside office hours can be claimed by the bidder.		
TRAVELLING, PARKING AND ACCOMODATION AND OVERTIME COSTS	COMPLY	DO NOT COMPLY
The bidders confirm that all travelling, parking and accommodation costs are included in their pricing and will not be charged separately. The OPFA will not accommodate any claims whatsoever for travelling, parking and accommodation. No overtime for working after hours to finish milestones can be claimed by the bidder.		
LOCATIONS	COMPLY	DO NOT COMPLY
The bidder shall be required to deliver the services at locations specified in this document. The bidder accepts that all services will be performed remotely. The bidder accepts that were required, for practical purposes (e.g., data centre visits, conducting DR tests; dealing with major incidents, etc), the bidder resources will be required to work at the OPFA offices or data centres.		

16. EVALUATION OF BID PROPOSAL

16.1. The proposals will be evaluated in four stages outlined below:

- Stage 1 – Administrative compliance.
- Stage 2 – Functionality requirements.
- Stage 3 – Pricing and preference points

16.1.1. Stage 1: Administrative compliance

Document that must be submitted	Non-submission may result in disqualification?	
Master Bid Document	Yes	Provided and bound
Electronic copy (USB /compact disc)	Yes	Same as the master bid document
Invitation to Bid – SBD 1	Yes	Duly completed and signed
CSD Registration	Yes	CSD registration number/Proof of CSD registration. If you are not registered proceed to complete the registration of your company prior to submitting your proposal. Visit https://secure.csd.gov.za/ to obtain your vendor number.
Pricing schedule	Yes	Duly completed.
SBD 4- Bidders Disclosure	Yes	Duly completed and signed.
SBD 6.1 Preference points claim form in terms of Preferential Procurement Regulation 2022	No	Duly completed and signed. Non-submission will lead to a zero (0) score for preference points
Adherence to closing date and time	Yes	Submission by the due date and time.
Confirmation of the Bidder's contribution to Pension/Provident fund	No	Proof of contribution or sworn affidavit must be provided

16.1.2. Stage 2: Functionality requirements

- Bidders must use this checklist to respond to the Technical and functionality evaluation criteria.

Minimum requirement	Information required
Minimum References and Demonstrated Capability	Bidders must provide a minimum of three (3) contactable reference letters for projects of similar scope and complexity relating specifically to Managed Professional Services as outlined in Part B of this bid that have been successfully delivered within the last six (6) years
Required Skills and Knowledge	The bidder must demonstrate that they possess the following critical skills and technical competencies: - Enterprise server infrastructure management (HP or equivalent enterprise platforms). - Virtualisation platform administration (Microsoft Hyper-V and/or VMware). - Storage architecture and high availability clustering. - Advanced SQL Server administration, performance tuning, and optimisation. - Network management including LAN, WAN, VPN, VLAN segmentation, and firewall integration (preferably Fortinet environments). - Incident, Problem, and Change Management aligned to ITIL or recognised ITSM frameworks. - Experience operating within POPIA-compliant and regulated environments. - SLA-driven managed service delivery with measurable performance reporting.
Certified partnerships with relevant OEMs plus experienced Project Manager	The bidder must demonstrate active and current certified partnerships with relevant Original Equipment Manufacturers (OEMs) applicable to the proposed solution, including but not limited to server, storage, virtualisation, and networking platforms.

Minimum requirement	Information required
	○ In addition, the bidder must nominate a suitably qualified and experienced Project Manager who: ○ Holds relevant OEM accreditation or certification aligned to the proposed infrastructure platform. ○ Has a minimum of three (3) years' experience managing enterprise infrastructure. ○ Will be directly accountable for delivery, risk management, stakeholder engagement, and formal project sign-off.
Deployment Plan for Part A	The bidder must submit a detailed and structured Deployment Plan for the implementation of Part A. The Deployment Plan must not exceed a total implementation period of three (3) calendar months from date of contract signature. A detailed project schedule outlining key phases, milestones, deliverables, and dependencies. The plan must include, at minimum: • Estimated Time of Arrival (ETA) for all hardware components, clearly indicating procurement lead times and supply timelines. • Installation and rack deployment schedule. • Configuration and security hardening timeline. • Migration sequencing plan for virtual machines and applications. • Testing and validation milestones. • Production cutover timeline. • Decommissioning schedule for legacy infrastructure. • Risk identification and mitigation strategies. • Resource allocation plan, including OEM technical resources and project management oversight.
PART B	
Provide a methodology for managed professional services (Part B) for the duration of the contract.	All solutions and services must be provided for the full contract period. Willingness to collaborate with other parties, including governance, risk, compliance, and audit teams.
	Qualified Project Team The bidder must propose a suitably qualified and experienced Project Team dedicated to the execution and ongoing management of this contract. The team structure must be clearly defined and supported by CVs and certifications. At a minimum, the team must comprise the following key roles: Service Delivery Manager The Service Delivery Manager shall be the primary point of accountability for operational performance under Part B (Managed Professional Services). The individual must: • Have a minimum of three (3) years' experience managing ICT

Minimum requirement	Information required
	managed service contracts of similar size and complexity. • Demonstrate proven experience in SLA management, vendor coordination, and client engagement within regulated or public sector environments. • Possess recognised IT Service Management certification (e.g. ITIL Foundation or higher).
Support Team Experience & Demonstration	• Bidders must provide clear evidence of an experienced support team, including: ○ Team structure and roles (project manager, systems engineer, support lead, etc.) ○ CVs/resumes of key team members, showing relevant certifications and a minimum of three years' experience in similar projects. • Evidence of previous project assignments at the corporate level (client name, project scope, duration, contactable references). • Organisational chart showing escalation paths for support. • Shortlisted bidders may be required to deliver a presentation to the OPFA evaluation panel, introducing the support team, demonstrating experience, and walking through support processes, escalation procedures, and SLA management • The OPFA reserves the right to verify qualifications and work experience.

16.1.3. Compliance checklist:

Description	Compliance (Yes/No)	Reference to the response and relevant section.
PART A		
1. Hardware Supply & OEM Compliance		
- Supply of hardware aligned to approved BOM		
- All equipment brand new and enterprise-grade		
- OEM warranties (minimum 5 years)		
- OEM hardware replacement SLA		
- Proof of authorised OEM partnership		
- Compatibility with FortiGate, Symantec, Veeam, SIEM		
2. Delivery & Installation		
- Formal handover documentation and sign-off		
- Rack installation and cabling		
- Power and cooling configuration		
- Detailed Solution Design Document (to-be architecture)		
3. Project Management (OEM-led)		
- Appointment of OEM-accredited Project Manager		
- Defined implementation plan (max 3 months)		
- Risk and issue management process		
- Formal project closure and sign-off		
4. Configuration & Commissioning		
- Hypervisor configuration		
- Storage pools and redundancy		
- High availability clustering		
- VLAN segmentation		
- Security hardening (CIS or equivalent)		
5. Migration Services		
- Migrate all existing VMs, applications, and associated data into the new infrastructure.		
- Rollback and contingency plan		
- Conduct thorough post-migration validation and testing prior to production cutover.		
- Performance validation before sign-off		
6. Decommissioning		
- Approved decommissioning plan		
- Secure data sanitisation (industry standard)		
- Removal of legacy monitoring/security configs		

- Migration validation prior to shutdown		
7. DR Alignment		
- Alignment with existing DR provider		
- Infrastructure-level redundancy		
- Participation in DR testing		
PART B		
1. Support & Maintenance of Server Infrastructure		
- 24/7 infrastructure monitoring		
- Preventative maintenance schedule		
- Incident & problem management		
- Capacity monitoring & forecasting		
- HA and clustering management		
- Security hardening & vulnerability remediation		
- Updated documentation and reporting		
2. Network Management		
- Provide proactive network management in line with agreed uptime service levels and escalation processes.		
- Monitor WAN, LAN, VPN, and wireless network performance on a 24/7 basis with automated alerts for outages or degradations.		
- Optimise usage through bandwidth tuning, capacity management, and QoS configuration.		
- Provide rapid fault resolution, including root cause analysis and incident reporting.		
- Maintain accurate, version-controlled topology and configuration documentation.		
- Apply security patches and firmware updates to network devices in line with best practices.		
- Review network capacity frequently and recommend upgrades where appropriate.		
3. Database Management		
- Manage OPFA's SQL Server databases to ensure high availability, security, and performance.		
- Monitor 24/7 for anomalies such as blocking queries, deadlocks, and excessive resource usage.		
- Conduct recurring maintenance including index management, statistics updates, and integrity validation.		
- Perform query tuning and schema optimisation for improved performance.		

- Enforce encryption of data at rest and in transit, and apply strict role-based access controls.		
- Manage patching, upgrades, and EOL planning for SQL versions.		
- Undertake ongoing growth analysis and capacity forecasting for database resources.		
4. ICT Support and Advisory Services		
- OPFA retains ownership of all first-line support, including incident logging, basic troubleshooting, and user queries.		
- Provide second-line and above support for escalated issues relating to infrastructure, servers, networks, storage, databases, and operating systems.		
- Establish clear escalation paths from OPFA's internal helpdesk, with SLA-defined response and resolution times.		
- Provide integration with OPFA's ticketing or service desk platform, ensuring visibility across the incident lifecycle.		
5. Change and Release Management		
- Manage ICT changes in line with OPFA's Change Management framework.		
- Execute structured Release Management for upgrades, patches, and deployments.		
6. Service Monitoring and Reporting		
- Maintain centralised monitoring systems.		
- Provide monthly service management reports including incident resolution statistics, SLA adherence, system health, and key performance metrics.		
7. Advisory and Governance Support		
- Provide advisory support in ICT strategy, security, technology trends, and governance compliance.		
- Assist with ICT audits, providing timely documentation and responses to information requests.		

- Support strategic ICT initiatives and projects with solution design and implementation support.		
8. Service Availability		
- 99.9% availability commitment		
- Deliver support during standard business hours, with after-hours coverage for critical or high-priority incidents.		
- Escalation levels and response times shall be contractually defined in SLAs.		
- Monthly availability reporting		

16.1.4. Stage 3: Functionality Evaluation

- The functionality criteria and technical requirements below will be evaluated and scored. In responding to each criteria the bidder must incorporate the checklist above and respond to the direct requirement.
- Bidders are expected to substantiate each aspect of their response. Bidders must clearly reference their bid response in specific terms. As a minimum, the following must be provided for each item **[reference to schedule(s), section(s), page number(s)]**.

#	Evaluation Criteria	Description	Weight	Score Matrix
1	On-Prem Infrastructure Implementation (Deployment) Methodology	The bidder must provide a clear and detailed approach to implementing the new Infrastructure: • Hardware architecture design. • OEM-led deployment. • Installation approach. • Migration strategy and rollback plan. • Security hardening approach. • Integration with existing ICT landscape. • Decommissioning methodology.	25	5: The proposal exceeds/meets all requirements (<i>Comprehensive, detailed, risk-aware, fully aligned to scope</i>). 4: The proposal adequately meets all requirements (<i>Detailed and aligned with minor gaps</i>). 3: The proposal moderately meets all requirements (<i>Adequate but lacking depth or clarity</i>). 2: The proposal does not meet all requirements (<i>Limited detail or partially aligned</i>). 1: No relevant information provided (<i>No relevant methodology provided</i>)

#	Evaluation Criteria	Description	Weight	Score Matrix
2	Managed Professional Services Methodology	The bidder must provide a clear and detailed approach to delivering Managed Professional Services as outlined in scope section 5.2, including: - On-Prem Infrastructure monitoring and maintenance model. - Network Management. - Database Management. - ICT Support and Advisory Services.	25	5: The proposal exceeds/meets all requirements. 4: The proposal adequately meets all requirements. 3: The proposal moderately meets all requirements. 2: The proposal does not meet all requirements. 1: No relevant information provided
3	Project Governance & Deployment Plan	The bidder must submit: - Detailed 3-month deployment plan. - Hardware ETA confirmation. - Risk register and mitigation strategy. - Resource allocation plan. - OEM-certified Project Manager confirmation	15	5: Fully detailed plan with timelines, risks, and OEM governance. 4: Clear plan with minor omissions. 3: Basic timeline without risk depth. 2: Incomplete or unrealistic plan. 1: No compliant deployment plan.
4	Previous Experience and Track Record	The bidder must provide at least three (3) contactable reference letters where similar projects were successfully provided by the bidder in the last six years reflecting: - Enterprise server support. - Network and database management. - SLA-driven managed services. - Regulated environment	15	5: The bidder submitted three reference letters that meet all requirements. 4: The bidder submitted two reference letters that meet all requirements. 3: The bidder submitted one reference letter that meets all requirements. 2: Letters provided but do not meet all requirements. 1: No information provided
5	Technical Resources & Team Competency	The bidder must submit the organisational structure with relevant competency of support and maintenance resources specific to this assignment: - Service Delivery Manager qualifications. - OEM Project Manager certification. - Senior Infrastructure Engineer credentials. - Network Engineer certification. - Database Administrator experience. - Organisational structure and escalation	10	5: Bidder provided the organisational structure with relevant competency, including at least 4 CVs with relevant certification and minimum of 5 years relevant experience. 4: Bidder provided the organisational structure with relevant competency, at least 3 CV and relevant certification with minimum of 5 years relevant

#	Evaluation Criteria	Description	Weight	Score Matrix
		clarity		experience. 3: Bidder did not provide organisational structure and submitted 2 CVs with relevant certification and required experience. 2: Bidder submitted Organisational structure and provided CVs without relevant certification and experience. 1: No relevant information provided
6	Support & Maintenance Methodology	The bidder must provide a clear and detailed approach to support and maintenance: • 99.9% availability commitment. • SLA response & resolution framework. • Monitoring tools and reporting approach. • Onsite support model.	10	5: The proposal exceeds/meets all requirements. 4: The proposal adequately meets all requirements. 3: The proposal moderately meets all requirements. 2: The proposal does not meet all requirements. 1: No relevant information provided
TOTAL			100	

16.2. Bidders must obtain a minimum of **75** points in order to be evaluated in the next evaluation stage. Bidders who score less than **75 out of 100** points with respect to functionality evaluation compliance will be regarded as non-responsive and will not be evaluated further.

16.3. Evaluation stage four: price and preference point system

- Only Bidders that have met a minimum of 75-points threshold in functionality evaluation will be evaluated in for price and preference points.
- The 80/20 preference point system shall be applicable to this bid, where 80 points represent maximum obtainable points for the lowest acceptable price, and 20 points represents the specific goals. Points will be awarded to a bidder for attaining the specific goals outlined in accordance with the table below:

#	Specific Goals of Preference	Proof/ Evidence required	Points Allocation
1	51% or more ownership by black people	CSD report/B-BBEE Certificate or Sworn Affidavit, CIPC Report	8
2	51% or more ownership by black women	CSD report/B-BBEE Certificate or Sworn Affidavit, CIPC Report	5
3	30% or more ownership by youth	CSD report/B-BBEE Certificate or Sworn Affidavit, CIPC Report	3
4	EME/QSE	CSD report/B-BBEE Certificate or Sworn Affidavit, CIPC Report	4
TOTAL POINTS		20	

17. PROTECTION OF PERSONAL INFORMATION

- 17.1. "Personal Information" means personal information as defined in the Protection of Personal Information Act, 2013 (Act No. 4 of 2013), as amended from time to time.
- 17.2. All information collected and submitted by the bidders will be used by the OPFA for the evaluation and adjudication of this bid to determine the bidders' suitability and compliance to deliver the services required. By submitting this bid, the bidder gives consent for the OPFA to process their personal information provided by the bidder accordingly. The information submitted by the bidder shall be verified with the relevant issuing institution(s).
- 17.3. For the purposes of this bid, the parties (OPFA and respective bidders) will come into contact with or have access to PI and other information that may be classified or deemed as private or confidential and for which the other party is responsible. Such PI may also be deemed or considered as private and confidential as it relates to any third party who may be directly or indirectly associated with this bid. Further, it is acknowledged and agreed by the parties that they have the necessary consent to share or disclose the PI and that the information may have value.
- 17.4. The parties agree that they will at all times comply with POPIA's Regulations and Codes of Conduct and that it shall only collect, use and process PI it comes into contact with pursuant to this bid in a lawful manner, and only to the extent required to evaluate and adjudicate the bid, and to perform their respective obligations in terms of this bid or agreement.
- 17.5. The bidder has a right to request the OPFA to correct, delete, and destroy its PI in terms of POPIA using form 2 of the POPIA Regulations. The bidder also has the right to object to the processing of its PI using form 1 of the POPIA Regulations. The rights of the bidder as a data subject are contained in the OPFA POPIA Policy, which can be viewed on the OPFA website.
- 17.6. The parties agree that it shall put in place, and at all times maintain, appropriate physical, technological, and contractual security measures to ensure the protection and confidentiality of PI that it, or its employees, its contractors or other authorised individuals come into contact with pursuant to this agreement.

- 17.7. Notify each other immediately where it has reasonable grounds to believe that the Personal Information in respect of this agreement, which has been provided to it, including any Personal Information which it has processed, has been lost, destroyed, accessed or acquired by any unauthorised person.
- 17.8. Unless so required by law, the parties agree that they shall not disclose any PI as defined in POPIA to any third party without the prior written consent of the other party, notwithstanding anything to the contrary contained herein, shall any party transfer any PI out of the Republic of South Africa.
- 17.9. The bidder and OPFA will implement all the necessary processes and programs to ensure that all the data is secure at all times and not accessible by any unauthorised parties.

18. GENERAL UNDERTAKINGS

- 18.1. The OPFA will not accept the bid, if the OPFA is satisfied that any person (including an employee, partner, director or shareholder of the tenderer or a person acting on behalf of or with the knowledge of the tenderer), firm or company:
- 18.1.1. Is restricted from doing business with the state or employed by the state
 - 18.1.2. Has in any manner been involved in a corrupt act in relation to or other gift or remuneration to any officer or employee of the OPFA in connection with obtaining or executing a contract.
 - 18.1.3. Has acted in bad faith, in a fraudulent manner or committed an offence in obtaining or executing a contract.
 - 18.1.4. Has in any manner influenced or attempted to influence the awarding of OPFA's bid.
 - 18.1.5. Has, when advised that their tender has been accepted, given notice of his inability to execute or sign the contract.
 - 18.1.6. Has engaged in any anti-competitive behaviour, including having entered into any agreement or arrangement, whether legally binding or not, with any other person, firm or company to refrain from tendering for this contract, or relating to the tender price to be submitted by either party.
 - 18.1.7. Has disclosed to any other person, any information relating to this bid, except where disclosure, in confidence, was necessary to obtain quotations required for the preparation of the tender or required by law.

18.1.8. The OPFA may, in addition to any other legal recourse which it may have, cancel the contract between the OPFA and such a person and/or resolve that no tender from such a person will be considered for a specified period.

18.2. The award of this tender may be subjected to price negotiation with the highest point scorer in terms of the preferential procurement regulation if the price offered is considered not to be market related.

19. TENDER ENQUIRIES AND BRIEFING

19.1. There will be NO tender briefing session on this project; for any enquiries/clarity, bidders must send enquiries to the designated email by not later than **16 March 2026** to allow the OPFA opportunity to respond to enquiries. Enquiries received after this date will not be responded to.

19.2. Any questions regarding this tender shall be submitted in writing to the official mentioned in the Tender Notice. Enquiries must be sent to tenders@pfa.org.za

20. TENDER SUBMISSIONS

20.1. Bids must be hand delivered to the OPFA's address as follows

41 Matroosberg Road
Riverwalk Office Park
Block A, Fourth Floor
Ashlea Gardens
Pretoria

20.2. Late submissions and bids submitted by means of e-mail, telegram, telex, facsimile, electronic or similar means shall not be considered.

21. TENDER SUBMISSION FORMAT

21.1. The OPFA requires one original copy of the completed bid document and supporting documents (hard copy) and one soft copy in a memory stick or compact disc; bidders must ensure the soft copy is readable. All submissions must be made as per paragraph 17 above.

22. REGISTRATION WITH CENTRAL SUPPLIER DATABASE

22.1. The OPFA will not award any bid to a supplier who is not registered as a prospective supplier on the Central Supplier Database (CSD) as required in terms of National Treasury SCM Instruction Note 4A of 2016/2017.

23. BID VALIDITY PERIOD

23.1. Bid validity period will be hundred & twenty (120) days from closing of the tender.

24. ADDITIONAL INFORMATION REQUIRED

The following additional information is required:

A sworn declaration and/or proof that a bidder:

- Is not participating in and contributing to any retirement fund for its employees; or
- Is participating and contributing to a pension or provident fund on behalf of its employees, and contributions are not in arrears. As proof, confirmation of their contribution status from their retirement fund administrator must be submitted together with the declaration.

NB: This declaration is required as part of the risk assessment, which may impact the overall outcome of the bid

ANNEXURE A: BILL OF MATERIAL: OPFA/ICT/012026

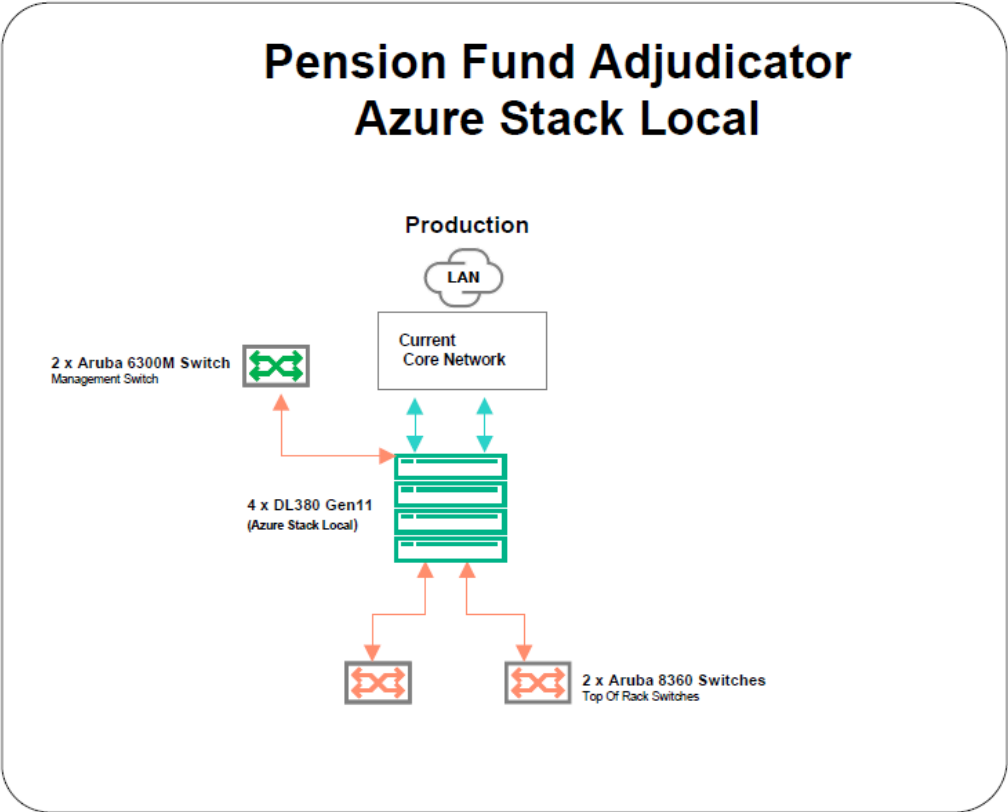
1. Technical Specifications

Qty	Product #	Product Description	Comply(Y/N)
4 x Servers with Rack & PDU			
1	P9K10A	HPE 42U 600mmx1200mm G2 Kitted Advanced Shock Rack with Side Panels and Baying	
1	P9K10A 001	HPE Factory Express Base Racking Service	
4	P52534-B21	HPE ProLiant DL380 Gen11 8SFF NC Configure-to-order Server	
4	P52534-B21 B19	HPE ProLiant DL380 Gen11 8SFF NC Configure-to-order Server Europe Multilingual	
8	P67084-B21	Intel Xeon-Gold 6544Y 3.6GHz 16-core 270W Processor for HPE	
32	P64707-B21	HPE 64GB (1x64GB) Dual Rank x4 DDR5-5600 CAS-46-45-45 EC8 Registered Smart Memory Kit	
8	P48813-B21	HPE ProLiant DL380 Gen11 2U 8SFF x1 Tri-Mode U.3 Drive Cage Kit	
40	P64848-B21	HPE 7.68TB NVMe Gen4 Mainstream Performance Read Intensive SFF BC U.3 Static V2 Multi Vendor SSD	
4	P42044-B21	Mellanox MCX631102AS-ADAT Ethernet 10/25Gb 2-port SFP28 Adapter for HPE	
4	P01366-B21	HPE 96W Smart Storage Lithium-ion Battery with 145mm Cable Kit	
4	P48918-B21	HPE ProLiant DL360 Gen11 Storage Controller Enablement Cable Kit	
4	P47781-B21	HPE MR416i-o Gen11 x16 Lanes 8GB Cache OCP SPDM Storage Controller	
4	P42041-B21	Mellanox MCX631432AS-ADAI Ethernet 10/25Gb 2-port SFP28 OCP3 Adapter for HPE	
8	P44712-B21	HPE 1800W-2200W Flex Slot Titanium Hot Plug Power Supply Kit	
4	BD505A	HPE iLO Advanced 1-server License with 3yr Support on iLO Licensed Features	
4	S1A05A	HPE Compute Cloud Management Server FIO Enablement	
4	P51911-B21	HPE ProLiant DL360 Gen11 CPU1 to OCP2 x8 Enablement Kit	
4	P48820-B21	HPE ProLiant DL380/DL560 Gen11 2U High Performance Fan Kit	
4	P50400-B21	HPE Gen11 2U Bezel Kit	
8	P49145-B21	HPE ProLiant DL380 Gen11 Standard Heat Sink Kit	
4	P52341-B21	HPE ProLiant DL3XX Gen11 Easy Install Rail 3 Kit	
4	P59520-B21	Enlogic by nVent G3 Basic 1-phase 7.3kVA/32A/200-240V Outlets (16) C13 (4) Combo C13/C19 PDU for HPE	
1	BW932A	HPE 600mm Rack Stabilizer Kit	
1	BW932A B01	HPE 600mm Rack include with Complete System Stabilizer Kit	
8	QK735A	HPE Premier Flex LC/LC Multi-mode OM4 2 Fiber 15m Cable	
1	P1F64A	HPE Inside Unpack/Clean Up w/Lift XL SVC	
1	HA114A1	HPE Installation and Startup Service	
4	HA114A1 5A6	HPE ProLiant DL/ML Startup SVC	
4	R7A11AAE	HPE Compute Ops Management Standard 5-year Upfront ProLiant SaaS	
1	HA113A1	HPE Installation Service	
2 x Top of Rack Switches			
2	JL700C	HPE Aruba Networking CX 8360-32Y4C v2 32p 25G SFP+/28 4 Sec 4p 100G QSFP+/28 FB 3 Fans 2 AC Bdl	
2	JL700C B2C	HPE Aruba Networking 8360-32Y4C v2 32p 25G SFP28 4Sec 4p 100G QSFP28 FB 3 Fans 2AC Bundle PDU	
4	J9150D	HPE Aruba Networking 10G SFP+ LC SR 300m OM3 MMF Transceiver	
2	J9281D	HPE Aruba Networking 10G SFP+ to SFP+ 1m Direct Attach Copper Cable	
2	J9281D B01	HPE Aruba Networking 10G SFP+ to SFP+ 1m Direct Attach Copper Cable	

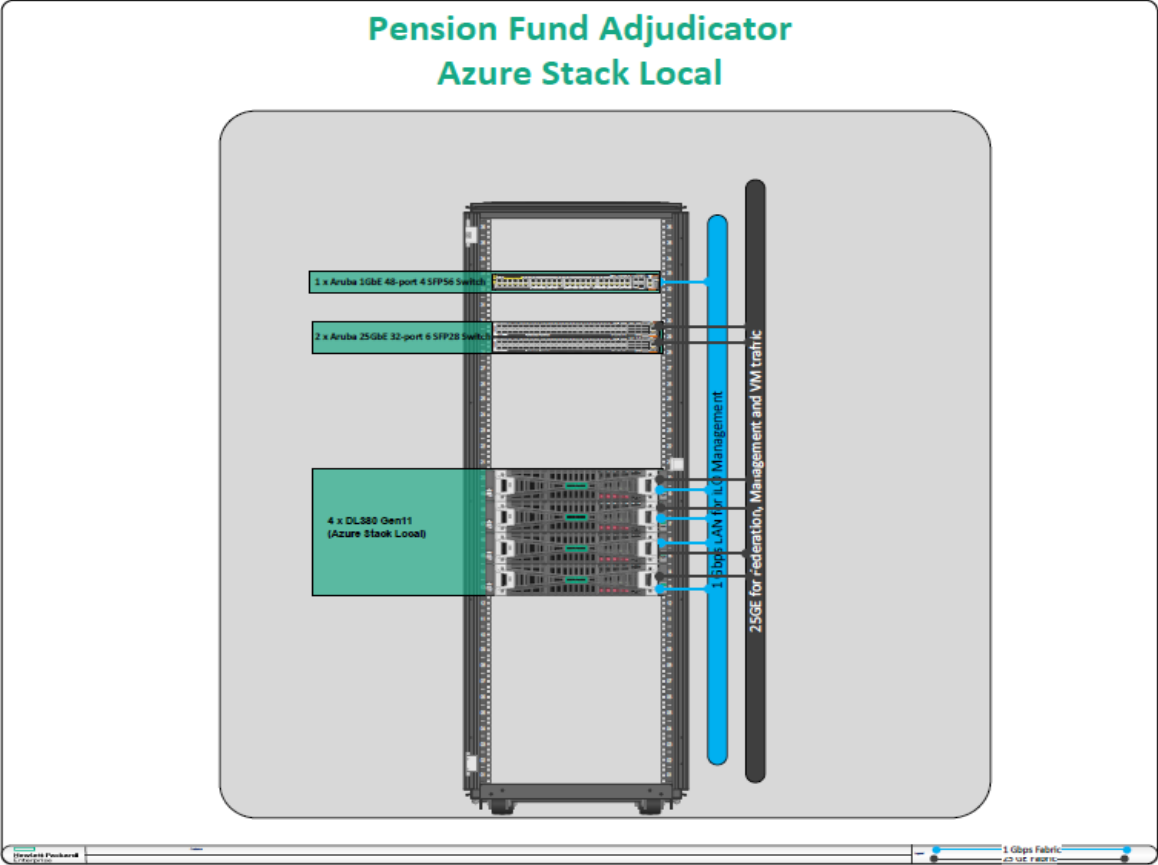
Qty	Product #	Product Description	Comply(Y/N)
32	JL488A	HPE Aruba Networking 25G SFP28 to SFP28 3m Direct Attach Copper Cable	
32	JL488A B01	HPE Aruba Networking 25G SFP28 to SFP28 3m Direct Attach Copper Cable	
2	R0Z25A	HPE Aruba Networking 100G QSFP28 to QSFP28 1m Direct Attach Copper Cable	
2	R0Z25A B01	HPE Aruba Networking 100G QSFP28 to QSFP28 1m Direct Attach Copper Cable	
2	J9583B	HPE Aruba Networking X414 1U Universal 4-post Rack Mount Kit	
8	861413-B21	HPE Synergy Frame Link Module CAT6A 3m Cable	
1	HA113A1 5BY	HPE Rack and Rack Options Install SVC	
2	HA113A1 5MW	HPE Aruba Networking 6xxxN8xxx Install Swt SVC	
1	HU4A6A5	HPE 5Y Tech Care Essential Service	
4	HU4A6A5 R2M	HPE iLO Advanced Non Blade Support	
4	HU4A6A500DK	HPE DL380 Gen11 Support	
2	HU4A6A500B9	HPE Aruba Networking 8360 32Y4C Support	
1 x Management Switch			
1	JL663A	HPE Aruba Networking CX 6300M 48-port 1GbE and 4-port SFP56 Switch	
2	J9150D	HPE Aruba Networking 10G SFP+ LC SR 300m OM3 MMF Transceiver	
1	JL085A	HPE Aruba Networking X371 12VDC 250W 100-240VAC Power Supply	
1	JL085A B2C	HPE Aruba Networking X371 12VDC 250W 100-240VAC Power Supply PDU	
2	QK735A	HPE Premier Flex LC/LC Multi-mode OM4 2 Fiber 15m Cable	
1	HA113A1	HPE Installation Service	
1	HA113A1 5MW	HPE Aruba Networking 6xxxN8xxx Install Swt SVC	
1	HU4A6A5	HPE 5Y Tech Care Essential Service	
1	HU4A6A5 Z59	HPE Aruba Networking 6300M 48 Support	

	As detailed in Scope section 5.3.3, 5.3.4 and 5.3.5 above.
Consulting and Deployment Services	• Project Management with Complete documentation of the solution (Test, sign-off and handover) • Solution design. ○ Hardware design (Server, Network and Storage). ○ Hyper-V Design. • Solution Installation and Configuration ○ Onsite Installation and start up services for Server, Network and Storage as per the design. ○ Hypervisor installation and configuration as per the design. ○ Data Migration (about ~56TB), from current environment to New Infrastructure ○ V2V migrations to new environment (About 42 VMs)
Support	• Hardware – 5 Year 24x7 Tech Care Support Care Services 6 Hours Response with Semi-annual operating-system environment patch analysis, firmware analysis, Annual System Health Check.

2. Logical Architecture-To Be



3. Rack View Architecture-To Be



STANDARD BIDDING

YOU ARE HEREBY INVITED TO BID FOR REQUIREMENTS OF THE OFFICE OF PENSION FUNDS ADJUDICATOR					
BID NUMBER:	OPFA/ICT/012026	CLOSING DATE:	24 MARCH 2026	CLOSING TIME:	11:00
DESCRIPTION	SUPPLY, DELIVERY, INSTALLATION, COMMISSIONING AND SUPPORT OF ON-PREMISE ICT INFRASTRUCTURE				
BID RESPONSE DOCUMENTS MUST BE SUBMITTED AT					
BID MUST BE SUBMITTED TO: 41 MATROOSBERG ROAD, RIVERWALK OFFICE PARK, ASHLEA GARDENS, 0081, 4 TH FLOOR BLOCK A					
BIDDING PROCEDURE ENQUIRIES MAY BE DIRECTED TO			TECHNICAL ENQUIRIES MAY BE DIRECTED TO:		
CONTACT PERSON	Magadi Tshitannye		CONTACT PERSON	Magadi Tshitannye	
TELEPHONE NUMBER	012 748 4000		TELEPHONE NUMBER	012 748 4000	
FACSIMILE NUMBER			FACSIMILE NUMBER		
E-MAIL ADDRESS	tenders@pfa.org.za		E-MAIL ADDRESS	tenders@pfa.org.za	
SUPPLIER INFORMATION					
NAME OF BIDDER					
POSTAL ADDRESS					
STREET ADDRESS					
TELEPHONE NUMBER	CODE		NUMBER		
CELLPHONE NUMBER					
FACSIMILE NUMBER	CODE		NUMBER		
E-MAIL ADDRESS					
VAT REGISTRATION NUMBER					
SUPPLIER COMPLIANCE STATUS	TAX COMPLIANCE SYSTEM PIN:		OR	CENTRAL SUPPLIER DATABASE No:	MAAA
B-BBEE STATUS LEVEL VERIFICATION CERTIFICATE	TICK APPLICABLE BOX] Yes No		B-BBEE STATUS LEVEL SWORN AFFIDAVIT		[TICK APPLICABLE BOX] Yes No
[A B-BBEE STATUS LEVEL VERIFICATION CERTIFICATE/ SWORN AFFIDAVIT (FOR EMES & QSEs) MUST BE SUBMITTED IN ORDER TO QUALIFY FOR PREFERENCE POINTS FOR B-BBEE]					
ARE YOU THE ACCREDITED REPRESENTATIVE IN SOUTH AFRICA FOR THE GOODS /SERVICES /WORKS OFFERED?	Yes No [IF YES ENCLOSE PROOF]		ARE YOU A FOREIGN BASED SUPPLIER FOR THE GOODS/SERVICES /WORKS OFFERED?		Yes No [IF YES, ANSWER THE QUESTIONNAIRE BELOW]
QUESTIONNAIRE TO BIDDING FOREIGN SUPPLIERS					
IS THE ENTITY A RESIDENT OF THE REPUBLIC OF SOUTH AFRICA (RSA)?				☐ YES ☐ NO	
DOES THE ENTITY HAVE A BRANCH IN THE RSA?				☐ YES ☐ NO	
DOES THE ENTITY HAVE A PERMANENT ESTABLISHMENT IN THE RSA?				☐ YES ☐ NO	
DOES THE ENTITY HAVE ANY SOURCE OF INCOME IN THE RSA?				☐ YES ☐ NO	
IS THE ENTITY LIABLE IN THE RSA FOR ANY FORM OF TAXATION?				☐ YES ☐ NO	
IF THE ANSWER IS "NO" TO ALL OF THE ABOVE, THEN IT IS NOT A REQUIREMENT TO REGISTER FOR A TAX COMPLIANCE STATUS SYSTEM PIN CODE FROM THE SOUTH AFRICAN REVENUE SERVICE (SARS) AND IF NOT REGISTER AS PER 2.3 BELOW.					

INITIAL HERE	
--------------	--

PART B: TERMS AND CONDITIONS FOR BIDDING

1. BID SUBMISSION:

- 1.1. BIDS MUST BE DELIVERED BY THE STIPULATED TIME TO THE CORRECT ADDRESS. LATE BIDS WILL NOT BE ACCEPTED FOR CONSIDERATION.
- 1.2. **ALL BIDS MUST BE SUBMITTED ON THE OFFICIAL FORMS PROVIDED--(NOT TO BE RE-TYPED) OR IN THE MANNER PRESCRIBED IN THE BID DOCUMENT.**
- 1.3. THIS BID IS SUBJECT TO THE PREFERENTIAL PROCUREMENT POLICY FRAMEWORK ACT, 2000 AND THE PREFERENTIAL PROCUREMENT REGULATIONS, 2022, THE GENERAL CONDITIONS OF CONTRACT (GCC) AND, IF APPLICABLE, ANY OTHER SPECIAL CONDITIONS OF CONTRACT.
- 1.4. **THE SUCCESSFUL BIDDER WILL BE REQUIRED TO FILL IN AND SIGN A WRITTEN CONTRACT FORM (SBD7).**

2. TAX COMPLIANCE REQUIREMENTS

- 2.1 BIDDERS MUST ENSURE COMPLIANCE WITH THEIR TAX OBLIGATIONS.
- 2.2 BIDDERS ARE REQUIRED TO SUBMIT THEIR UNIQUE PERSONAL IDENTIFICATION NUMBER (PIN) ISSUED BY SARS TO ENABLE THE ORGAN OF STATE TO VERIFY THE TAXPAYER'S PROFILE AND TAX STATUS.
- 2.3 APPLICATION FOR TAX COMPLIANCE STATUS (TCS) PIN MAY BE MADE VIA E-FILING THROUGH THE SARS WEBSITE WWW.SARS.GOV.ZA.
- 2.4 BIDDERS MAY ALSO SUBMIT A PRINTED TCS CERTIFICATE TOGETHER WITH THE BID.
- 2.5 IN BIDS WHERE CONSORTIA / JOINT VENTURES / SUB-CONTRACTORS ARE INVOLVED, EACH PARTY MUST SUBMIT A SEPARATE TCS CERTIFICATE / PIN / CSD NUMBER.
- 2.6 WHERE NO TCS PIN IS AVAILABLE BUT THE BIDDER IS REGISTERED ON THE CENTRAL SUPPLIER DATABASE (CSD), ACSD NUMBER MUST BE PROVIDED.
- 2.7 NO BIDS WILL BE CONSIDERED FROM PERSONS IN THE SERVICE OF THE STATE, COMPANIES WITH DIRECTORS WHO ARE PERSONS IN THE SERVICE OF THE STATE, OR CLOSE CORPORATIONS WITH MEMBERS PERSONS IN THE SERVICE OF THE STATE."

NB: FAILURE TO PROVIDE / OR COMPLY WITH ANY OF THE ABOVE PARTICULARS MAY RENDER THE BID INVALID.

SIGNATURE OF BIDDER:

.....

CAPACITY UNDER WHICH THIS BID IS SIGNED:

.....

(Proof of authority must be submitted e.g. company resolution)

DATE:.....

--

SBD 4: BIDDER'S DISCLOSURE

1. PURPOSE OF THE FORM

1. Any person (natural or juristic) may make an offer or offers in terms of this invitation to bid. In line with the principles of transparency, accountability, impartiality, and ethics as enshrined in the Constitution of the Republic of South Africa and further expressed in various pieces of legislation, it is required for the bidder to make this declaration in respect of the details required hereunder.

Where a person/s are listed in the Register for Tender Defaulters and / or the List of Restricted Suppliers, that person will automatically be disqualified from the bid process.

2. Bidder's declaration

- 2.1. Is the bidder, or any of its directors / trustees / shareholders / members / partners or any person having a controlling interest¹ in the enterprise, employed by the state? **YES/NO**

- 2.1.1. If so, furnish particulars of the names, individual identity numbers, and, if applicable, state employee numbers of sole proprietor/ directors / trustees / shareholders / members/ partners or any person having a controlling interest in the enterprise, in table below.

Full Name	Identity Number	Name of State institution

¹ the power, by one person or a group of persons holding the majority of the equity of an enterprise, alternatively, the person/s having the deciding vote or power to influence or to direct the course and decisions of the enterprise.

2.2 Do you, or any person connected with the bidder, have a relationship with any person who is employed by the procuring institution? **YES/NO**

2.2.1 If so, furnish particulars:

.....
.....

2.3 Does the bidder or any of its directors / trustees / shareholders / members / partners or any person having a controlling interest in the enterprise have any interest in any other related enterprise whether or not they are bidding for this contract? **YES/NO**

2.3.1 If so, furnish particulars:

.....
.....

3 DECLARATION

I, the undersigned, (name).....in submitting the accompanying bid, do hereby make the following statements that I certify to be true and complete in every respect:

3.1 I have read and I understand the contents of this disclosure;

3.2 I understand that the accompanying bid will be disqualified if this disclosure is found not to be true and complete in every respect;

3.3 The bidder has arrived at the accompanying bid independently from, and without consultation, communication, agreement or arrangement with any competitor. However, communication between partners in a joint venture or consortium² will not be construed as collusive bidding.

3.4 In addition, there have been no consultations, communications, agreements or arrangements with any competitor regarding the quality, quantity, specifications, prices, including methods, factors or formulas used to calculate prices, market allocation, the intention or decision to submit or not to submit the bid, bidding with the intention not to win the bid and conditions or delivery

² Joint venture or Consortium means an association of persons for the purpose of combining their expertise, property, capital, efforts, skill and knowledge in an activity for the execution of a contract.

particulars of the products or services to which this bid invitation relates.

- 3.4 The terms of the accompanying bid have not been, and will not be, disclosed by the bidder, directly or indirectly, to any competitor, prior to the date and time of the official bid opening or of the awarding of the contract.
- 3.5 There have been no consultations, communications, agreements or arrangements made by the bidder with any official of the procuring institution in relation to this procurement process prior to and during the bidding process except to provide clarification on the bid submitted where so required by the institution; and the bidder was not involved in the drafting of the specifications or terms of reference for this bid.
- 3.6 I am aware that, in addition and without prejudice to any other remedy provided to combat any restrictive practices related to bids and contracts, bids that are suspicious will be reported to the Competition Commission for investigation and possible imposition of administrative penalties in terms of section 59 of the Competition Act No 89 of 1998 and or may be reported to the National Prosecuting Authority (NPA) for criminal investigation and or may be restricted from conducting business with the public sector for a period not exceeding ten (10) years in terms of the Prevention and Combating of Corrupt Activities Act No 12 of 2004 or any other applicable legislation.

I CERTIFY THAT THE INFORMATION FURNISHED IN PARAGRAPHS 1, 2 and 3 ABOVE IS CORRECT. I ACCEPT THAT THE STATE MAY REJECT THE BID OR ACT AGAINST ME IN TERMS OF PARAGRAPH 6 OF PFMA SCM INSTRUCTION 03 OF 2021/22 ON PREVENTING AND COMBATING ABUSE IN THE SUPPLY CHAIN MANAGEMENT SYSTEM SHOULD THIS DECLARATION PROVE TO BE FALSE.

.....
Signature

.....
Date

.....
Position

.....
Name of bidder

INITIAL HERE	
--------------	--

SBD 6.1 PREFERENCE POINTS CLAIM FORM IN TERMS OF THE PREFERENTIAL PROCUREMENT REGULATIONS 2022

This preference form must form part of all tenders invited. It contains general information and serves as a claim form for preference points for specific goals.

NB: BEFORE COMPLETING THIS FORM, TENDERERS MUST STUDY THE GENERAL CONDITIONS, DEFINITIONS AND DIRECTIVES APPLICABLE IN RESPECT OF THE TENDER AND PREFERENTIAL PROCUREMENT REGULATIONS, 2022

1. GENERAL CONDITIONS

1.1 The following preference point systems are applicable to invitations to tender:

- the 80/20 system for requirements with a Rand value of up to R50 000 000 (all applicable taxes included); and
- the 90/10 system for requirements with a Rand value above R50 000 000 (all applicable taxes included).

1.2 **To be completed by the organ of state**

- a) The applicable preference point system for this tender is the 80/20 preference point system.

1.3 Points for this tender (even in the case of a tender for income-generating contracts) shall be awarded for:

- (a) Price; and
(b) Specific Goals.

1.4 **To be completed by the organ of state:**

The maximum points for this tender are allocated as follows:

	POINTS
PRICE	80
SPECIFIC GOALS	20
Total points for Price and SPECIFIC GOALS	100

1.5 Failure on the part of a tenderer to submit proof or documentation required in terms of this tender to claim points for specific goals with the tender, will be interpreted to mean that preference points for specific goals are not claimed.

1.6 The organ of state reserves the right to require of a tenderer, either before a tender is

adjudicated or at any time subsequently, to substantiate any claim in regard to preferences, in any manner required by the organ of state.

2. DEFINITIONS

- (a) “tender” means a written offer in the form determined by an organ of state in response to an invitation to provide goods or services through price quotations, competitive tendering process or any other method envisaged in legislation;
- (b) “**price**” means an amount of money tendered for goods or services, and includes all applicable taxes less all unconditional discounts;
- (c) “**rand value**” means the total estimated value of a contract in Rand, calculated at the time of bid invitation, and includes all applicable taxes;
- (d) “**tender for income-generating contracts**” means a written offer in the form determined by an organ of state in response to an invitation for the origination of income-generating contracts through any method envisaged in legislation that will result in a legal agreement between the organ of state and a third party that produces revenue for the organ of state, and includes, but is not limited to, leasing and disposal of assets and concession contracts, excluding direct sales and disposal of assets through public auctions; and
- (e) “**the Act**” means the Preferential Procurement Policy Framework Act, 2000 (Act No. 5 of 2000).

3. FORMULAE FOR PROCUREMENT OF GOODS AND SERVICES

3.1. POINTS AWARDED FOR PRICE

3.1.1 THE 80/20 OR 90/10 PREFERENCE POINT SYSTEMS

A maximum of 80 or 90 points is allocated for price on the following basis:

80/20	or	90/10
$Ps = 80 \left(1 - \frac{Pt - Pmin}{Pmin} \right)$	or	$Ps = 90 \left(1 - \frac{Pt - Pmin}{Pmin} \right)$

Where

- Ps = Points scored for price of tender under consideration
- Pt = Price of tender under consideration
- Pmin = Price of lowest acceptable tender

3.2. FORMULAE FOR DISPOSAL OR LEASING OF STATE ASSETS AND INCOME

GENERATING PROCUREMENT

3.2.1. POINTS AWARDED FOR PRICE

A maximum of 80 or 90 points is allocated for price on the following basis:

$$\begin{array}{ccc} \mathbf{80/20} & \mathbf{or} & \mathbf{90/10} \\ \mathbf{Ps = 80 \left(1 + \frac{Pt - P_{max}}{P_{max}} \right)} & \mathbf{or} & \mathbf{Ps = 90 \left(1 + \frac{Pt - P_{max}}{P_{max}} \right)} \end{array}$$

Where

Ps = Points scored for price of tender under consideration

Pt = Price of tender under consideration

Pmax = Price of highest acceptable tender

4. POINTS AWARDED FOR SPECIFIC GOALS

4.1. In terms of Regulation 4(2); 5(2); 6(2) and 7(2) of the Preferential Procurement Regulations, preference points must be awarded for specific goals stated in the tender. For the purposes of this tender the tenderer will be allocated points based on the goals stated in table 1 below as may be supported by proof/ documentation stated in the conditions of this tender:

4.2. In cases where organs of state intend to use Regulation 3(2) of the Regulations, which states that, if it is unclear whether the 80/20 or 90/10 preference point system applies, an organ of state must, in the tender documents, stipulate in the case of—

(a) an invitation for tender for income-generating contracts, that either the 80/20 or 90/10 preference point system will apply and that the highest acceptable tender will be used to determine the applicable preference point system; or

(b) any other invitation for tender, that either the 80/20 or 90/10 preference point system will apply and that the lowest acceptable tender will be used to determine the applicable preference point system,

then the organ of state must indicate the points allocated for specific goals for both the 90/10 and 80/20 preference point system.

Table 1: Specific goals for the tender and points claimed are indicated per the table below.

(Note to organs of state: Where either the 90/10 or 80/20 preference point system is applicable, corresponding points must also be indicated as such.

Note to tenderers: The tenderer must indicate how they claim points for each preference point system.)

The specific goals allocated points in terms of this tender	Number of points Allocated (80/20 system) (To be completed by the organ of state)	Number of points claimed (80/20 system) (To be completed by the tenderer)
51% or more ownership by black people	8	
51% or more ownership by black women	5	
30% or more ownership by youth	3	
EME/QSE	4	
Total points allocated	20	
Number of points claimed by the bidder		

DECLARATION WITH REGARD TO COMPANY/FIRM

4.3. Name of company/firm.....

4.4. Company registration number:

4.5. TYPE OF COMPANY/ FIRM

- ☐ Partnership/Joint Venture / Consortium
- ☐ One-person business/sole propriety
- ☐ Close corporation
- ☐ Public Company
- ☐ Personal Liability Company
- ☐ (Pty) Limited
- ☐ Non-Profit Company
- ☐ State Owned Company

[TICK APPLICABLE BOX]

4.6. I, the undersigned, who is duly authorised to do so on behalf of the company/firm, certify that the points claimed, based on the specific goals as advised in the tender, qualifies the company/ firm for the preference(s) shown and I acknowledge that:

- i) The information furnished is true and correct;
- ii) The preference points claimed are in accordance with the General Conditions as indicated in paragraph 1 of this form;
- iii) In the event of a contract being awarded as a result of points claimed as shown in paragraphs 1.4 and 4.2, the contractor may be required to furnish documentary proof to the satisfaction of the organ of state that the claims are correct;
- iv) If the specific goals have been claimed or obtained on a fraudulent basis or any of the conditions of contract have not been fulfilled, the organ of state may, in addition to any other remedy it may have –
 - (a) disqualify the person from the tendering process;
 - (b) recover costs, losses or damages it has incurred or suffered as a result of that person’s conduct;
 - (c) cancel the contract and claim any damages which it has suffered as a result of having to make less favourable arrangements due to such cancellation;
 - (d) recommend that the tenderer or contractor, its shareholders and directors, or only the shareholders and directors who acted on a fraudulent basis, be restricted from obtaining business from any organ of state for a period not exceeding 10 years, after the *audi alteram partem* (hear the other side) rule has been applied; and
 - (e) forward the matter for criminal prosecution, if deemed necessary.

.....
SIGNATURE(S) OF TENDERER(S)

SURNAME AND NAME:

.....

DATE:

.....

ADDRESS:

.....

.....

.....

.....

INITIAL HERE	
--------------	--