SACAA

SOUTH AFRICAN CIVIL AVIATION AUTHORITY

Keeping you safe in the sky

Request for Quotation (RFQ)

For the provision of supply, implementation, configuration, and support of a Privileged Access Management (PAM) solution for 12 months

1. INTRODUCTION

The South African Civil Aviation Authority (SACAA) is an agency of the Department of Transport (DoT), established in terms of the Civil Aviation Act, 2009 (Act No.13 of 2009), which came into effect on 31 March 2010. The Civil Aviation Act provides for the establishment of a stand-alone authority, mandated with controlling, promoting, regulating, supporting, developing, enforcing, and continuously improving levels of safety and security throughout the civil aviation industry.

The SACAA's mandate is to administer civil aviation safety and security oversight in the Republic of South Africa, in line with Civil Aviation Authority Act (the Act), and in accordance with the Standards and Recommended Practices (SARPs) prescribed by the ICAO.

The above is achieved by complying with the SARPs of the ICAO, whilst considering the local context.

The SACAA, as prescribed by the Civil Aviation Act as well as the Public Finance Management Act (PFMA), 1999 (Act No.1 of 1999) is a Schedule 3A public entity.

2. INVITATION TO BID

SACAA invites suitably qualified and experienced service providers to submit quotations for the supply, implementation, configuration, and support of a Privileged Access Management (PAM) solution to replace the existing CyberArk PAM platform for a contract period of twelve (12) months. The objective is to procure a secure, cost-effective, and scalable PAM solution that enhances privileged access control, supports audit and compliance requirements, and aligns with industry best practices.

3. SCOPE OF WORK

SACAA currently utilises a CyberArk Privileged Access Management (PAM) solution to govern and control privileged access within its ICT environment. In consideration of operational effectiveness, cost optimisation, and strategic alignment, SACAA intends to transition from the existing PAM solution to an alternative PAM platform for a period of twelve (12) months.

The SACAA operates a hybrid ICT environment that includes on-premises infrastructure, cloud-based systems (e.g., Microsoft 365, Azure,) network devices, critical servers, and business applications. Privileged accounts within these systems present elevated security risks if not properly controlled. The organisation requires a comprehensive PAM solution to safeguard these accounts and ensure compliance with internal policies, cybersecurity frameworks, and regulatory requirements.

3.1 Technical specifications

ID	Feature Category	Requirement Description
1.1	Architecture	The solution must facilitate remote access using only outbound-initiated connections (TCP 443) to eliminate inbound firewall exceptions.
1.2	Architecture	Must support a "Jump Technology" model that allows access to segmented networks (DMZ, OT) without a persistent VPN.
1.3	Architecture	The solution must be available as a hardened physical appliance, virtual appliance, or a vendor-managed SaaS.
2.1	Connectivity	**Web Jump:** Must provide brokered access to web-based admin consoles (AWS, Azure, vCenter) without exposing the browser to the local machine.
2.2	Connectivity	**Protocol Tunneling:** Must allow users to use native local tools (e.g., PuTTY, SQL Management Studio) through a secure, audited tunnel.
2.3	Connectivity	Must support "Jump Clients" for persistent, agent-based access to critical servers regardless of their network location.
2.4	Connectivity	Must support "Jumpoints" for agentless, proxy-based access to entire network segments or IP ranges.
2.5	Connectivity	The solution must support HTML5 (browser-based) access for "one-click" remote sessions without requiring local software.
3.1	Identity & Auth	Must integrate with SAML 2.0 / OIDC providers for Multi-Factor Authentication (MFA) at the point of session initiation.
3.2	Identity & Auth	Must support Virtual Smart Card authentication for environments requiring hardware-backed identity.

3.3	Identity & Auth	Support for Just-in-Time (JIT) provisioning, creating local admin accounts only for the duration of the approved session.
4.1	Credential Mgmt	The solution must include an integrated vault to store and rotate credentials for RDP, SSH, and Database systems.
4.2	Credential Mgmt	Must support automated "Credential Injection," where the solution enters passwords into the session so the user never sees them.
4.3	Credential Mgmt	Credential rotation must be triggered automatically upon the completion of a remote session.
5.1	Session Control	Ability to limit user access to specific applications (RemoteApp) rather than granting full desktop access to the server.
5.2	Session Control	Must provide a "Command Filter" to prevent the execution of restricted strings (e.g., rm -rf) in SSH sessions.
5.3	Session Control	Support for "Screen Sharing" to allow multiple administrators to collaborate on the same remote desktop in real-time.
5.4	Session Control	Administrators must have the ability to terminate any active remote session instantly from a centralized dashboard.
6.1	Database Security	Must provide protocol-level proxying for SQL databases (MS SQL, MySQL, Oracle) to log specific queries.
6.2	Database Security	Must allow for the masking of sensitive data within database query results during a proxied session.
7.1	Auditing	All sessions (RDP, SSH, Web, DB) must be recorded in a tamper-proof format that is indexed and searchable.
7.2	Auditing	Must provide a complete "Keystroke Log" for every session, even for graphical protocols like RDP.
7.3	Auditing	Forensic search capability to locate specific text or commands across all historical session recordings.
7.4	Auditing	Real-time "Attendant Mode" allowing an auditor to watch a live session in "View Only" or "Take Control" mode.
8.1	File Management	Granular control over file transfers: ability to enable/disable Upload, Download, or require approval for both.
8.2	File Management	All files transferred during a session must be logged with file name, size, and hash for audit purposes.
9.1	Integration	Native integration with ITSM platforms (ServiceNow, Jira) to require a valid ticket number before a session starts.
9.2	Integration	Real-time event streaming to SIEM platforms (Splunk, QRadar, Sentinel) via Syslog or API.

9.3	Integration	Must offer a comprehensive REST API for automating session scheduling and user provisioning.
10.1	Scalability	Architecture must support at least 1,000+ concurrent sessions across globally distributed data centers.
10.2	Scalability	Ability to deploy "Jump Zones" to provide localized access points in different geographic regions to reduce latency.
11.1	Compliance	Must facilitate "Least Privilege" by allowing permissions to be assigned based on the specific "Jump Item" rather than the user.
12.1	UX/User Tools	Support for native mobile apps (iOS/Android) for administrators to approve requests or start sessions on the go.
12.2	UX/User Tools	The solution must offer a consistent user interface across Windows, macOS, and Linux administrative consoles.
13.1	Security Hardening	The management appliance must use a hardened OS with a reduced attack surface and no unnecessary services.
13.2	Security Hardening	Support for "Clean Room" access where the administrative session is isolated from the user's potentially compromised endpoint.
14.1	Third-Party Access	Ability to provide "Vendor Invitations" where a third party can be granted time-limited access without a directory account.
15	Alerting	Automatic alerting via email when a high-risk session (e.g., Domain Controller access) is initiated.
16	Offline Access	Must provide a "Break-Glass" or "Offline" credential retrieval process in case of total network failure.
17	Licensing	Privileged Remote Access Per Named User Cloud = 40

4. EVALUATION CRITERIA

Bidders will be evaluated in accordance with the Supply Chain Management Policies as well as the Preferential Procurement Policy Framework, 2000 (Act No. 5 of 2000) and the Preferential Procurement Regulations of 2022.

4.1. PHASE 1 – SUPPLY CHAIN MANAGEMENT (SCM) ADMINISTRATIVE MANDATORY COMPLIANCE REQUIREMENTS

Bids received will be verified for completeness and correctness. The SACAA reserves the right to accept or reject a bid based on the completeness and correctness of the documentation and information provided. The set of bid documents must be completed and submitted. (**SACAA reserve the right to request information/additional documents if there are any missing from the bidder(s) submission**).

Bidders are to ensure that they submit the following documentation / information with their bid.

Document	Comments	Compulsory requirement
Proof of registration on the Central Supplier Database (CSD) of National Treasury	Prospective bidders must be registered on the Central Supplier Database (CSD) prior to submitting bids. Please indicate / **supply the supplier number.**	Yes
SBD 4 (Bidders Disclosure)	Completed and signed	Yes
Partnership letter	The bidder must submit a formal OEM authorisation letter confirming reseller, distributor, or implementation partner status.	Yes

4.2 PHASE 2 - TECHNICAL AND/ OR FUNCTIONALITY EVALUATION

Assessment of Technical / Functional evaluation of the bid will be done in terms of the criteria as stated in the table below. Bidders should take note of the Criterion, Weighting & Scoring when responding to this bid.

Table 1: Functionality Evaluation

FUNCTIONALITY EVALUATION: Functionality Description			
Technical Requirements:	**Description**	**Min**	**Max**
Company References	Provide dated and signed letters of reference on client's letterhead, including the contact person and contact details from the entity from which services were rendered. Reference must be in relation to this type of service provided in the **last five (5) years.** • Two (2) contactable trade reference letters from clients where Privileged Access Management	10	30

	(PAM) solution were provided in the past 5 years from the closing date of this RFQ – **(10 Points).** • Three (3) contactable trade reference letters from clients where Privileged Access Management (PAM) solution were provided in the past 5 years from the closing date of this RFQ – **(20 Points).** • Four (4) contactable trade reference letters from clients where Privileged Access Management (PAM) solution were provided in the past 5 years from the closing date of this RFQ – **(30 Points).**		
Methodology & Project Plan	A detailed execution plan with clear timelines, risk management, and change management strategies • Project Phases & Deliverables - **(10 Points).** • Timeline Realism - **(5 Points).** • Risk Management Quality - **(10 Points).** • Change Management Strategy - **(5 Points).**	20	30
Ability to support the Proposed Infrastructure	Certified Implementation Engineer - Privileged Remote Access accreditation - **(20 Points).** Certified Implementation Engineer - Password Safe – **(20 Points).**)	40	40
Total Points		**70**	**100**

Bidders who score **70** or more points out of **100** on "functionality" will be considered for the next evaluation phase. Any bidder scoring less than minimum **70 points** will be disqualified and won't be considered further for site inspection as per the table below.

4.3 PHASE 3 – PRICE AND SPECIFIC GOALS EVALUATION

Bidders who comply with the requirements of this bid will be evaluated according to the preference point scoring system as determined in the Preferential Procurement Regulations, 2022 pertaining to the Preferential Procurement Policy Framework Act, (Act No 5 of 2000).

For this bid 80 points will be allocated for Price and 20 points for Specific Goal.

4.3.1 This tender will be evaluated using the 80/20 preferential point system. The following PPPFA formula will be used to evaluate price:

$$Ps = 80\left(1 - \frac{Pt - P\min}{P\min}\right)$$

Ps = Points scored for price of the bid under consideration.

Pt = Rand value of bid under consideration.

Pmin = Rand value of lowest acceptable bid.

Only bidders that have achieved the minimum qualifying points on functionality will be evaluated further in accordance with the 80/20 preference point system as follows:

Points for this bid shall be awarded for:

(a) Price; and

(b) Specific Goal.

The maximum points for this bid are allocated as follows:

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

4 NON-COMPULSORY BRIEFING SESSION

There will be no briefing session and any service provider that may seek further clarity can send their queries to mthombenik@caa.co.za to seek any clarity on the tender document. All requests must be submitted through email.

5 SUBMISSION OF BID DOCUMENT

The bid submission requires a three (3) envelope system as per the evaluation criteria above.

1.1.1. Envelope 1

- All mandatory documents on Phase 1.

1.1.2. Envelope 2

- Technical proposal.

1.1.3. Envelope 3

- The pricing schedule must be submitted on a separate envelope from the technical proposal for ease of evaluation, as these will be evaluated separately. Bidders are required to provide a detailed price schedule breakdown as indicated in "**Annexure A**" below.

5. Bidders are required to submit neat and bounded documents, as SACAA will not be held responsible for any loss of documents whatsoever.

6. Bid documents shall be submitted in a sealed envelope and/or package clearly marked with the bid reference number as per the bid advert, bidder company name and be deposited in the tender box situated at the foyer of the SACAA head office, and be addressed as follows:

All bids submissions should be deposited or delivered at our Tender Box on or before 11:00am on the closing date of 4 March 2026
Adress:
Byls Bridge Office Park,11 Bylsbridge Blvd,Doringkloof,Centurion 0157

Please contact the following for gate access few hours prior delivery:
Cynthia: 083 461 6534
Or
Reneilwe: 064 601 3691

No late quotes will be accepted

Annexure A

Item	Description	Quantity	Unit Price
1	Implementation of the Privileged Access Management (PAM)	1	
2	Proposed Privileged Access Management (PAM) license for 12 months	1	
3	Health Check - Remote Only - Tier 1	1	
4	On demand support hours = 10	1	
Total Excluding VAT			
15% VAT			
Total Including VAT			