



SOUTH AFRICAN AIRWAYS

A STAR ALLIANCE MEMBER 

RFQ GSM078/26

**Request for Quotation for supply, licensing,
implementation, and configuration of the Qualys
Vulnerability Management, Detection and Response
(VMDR) TruRisk platform, inclusive of Policy
Compliance (PC) and Web Application Scanning (WAS),
for South African Airways (SAA).**

G.1 Written Quote Form

RFQ NUMBER: 078/2026

ISSUE DATE: 13 October 2026

CLOSING DATE: 19 October 2026 at 16:00pm

VALIDITY OF RFQ: 180 days

RFQ DOCUMENTS TO BE EMAILED TO: Tenders@flysaa.com – The maximum size of documents that can be sent via the email box at once is **2MB**. If your files exceed this size, please send them in parts or provide a downloadable link. Note that South African Airways will not be responsible for links that are corrupt and cannot be opened.

Vendors must submit quotations before the specified closing date and time. If the quotation is late, it will not be considered.

South African Airways requests your quotation for the goods and/or services listed on the attached form. Please include all requested information and submit your quote by the specified deadline. Late or incomplete submissions will invalidate the quote, and the bidder will be automatically disqualified.

SUPPLIER INFORMATION:

NAME OF VENDOR:

.....

POSTAL ADDRESS:

.....

TELEPHONE NO.:

.....

CELL NO:

.....

E MAIL ADDRESS:

.....

CONTACT PERSON:

.....

This RFQ will be evaluated according to Evaluation Methodology. Bidders must meet all Administrative, Substantive, Technical, and financial requirements to be considered among the preferred bidders to be awarded the contract.

Required Documentation to be attached.

- 1. SAA Vendor Document. Refer to Annexure 1**
- 2. SBD 4 Document. Refer to Annexure 2**
- 3. General Conditions of Contract. Refer to Annexure 3**

CONDITIONS

- All goods or services purchased will be subject to the SAA General Conditions of Contract. A copy of the said conditions is available from the local Procurement office.
- The Vendor is responsible for ensuring that SAA has a valid Original Tax Clearance Certificate. The onus, therefore, rests on the vendor to ensure SAA receives a valid Tax Clearance Certificate as soon as the certificate's validity expires. Where SAA does not have a valid Tax Clearance Certificate, an Original Tax Clearance Certificate must be submitted with this RFQ. Failure to do so may invalidate the quote submitted in terms of the RFQ.
- All purchases will be made through an official purchase order. Therefore, no goods or services must be delivered before receiving an official order/contract.
- I certify that the information supplied is correct, that I have read and understood the SAA General Conditions of Contract, and that I accept the SAA General Conditions of Contract.
- I further certify that all the required information has been furnished, and the relevant forms have been completed and are herewith submitted as part of the bid.

SIGNATURE OF VENDOR: _____

CAPACITY: _____

1. **BACKGROUND**

- 1.1. Service providers are requested to provide prices with their quotation to SAA for all the services to be provided as per the specifications. Service providers are expected to submit a cost that is fair and reasonable.
- 1.2. SAA has the right to negotiate with a prospective Service Provider regarding any proposed contract terms and conditions, including price(s).

2. **Scope of work/specifications**

The scope of work includes the **supply, licensing, implementation, and configuration of the Qualys Vulnerability Management, Detection and Response (VMDR) TruRisk platform**, inclusive of **Policy Compliance (PC)** and **Web Application Scanning (WAS)**, for **South African Airways (SAA)**. The solution must provide a minimum of **3,400 VMDR vulnerability management licenses** to cover SAA's current asset population. **SAA ICT** will retain overall ownership of the environment and will lead governance, implementation oversight, and final acceptance sign-off.

The successful service provider will be responsible for operation of Qualys platform as a **managed service**, including day-to-day vulnerability tracking and resolution, compliance and web application scanning activities, in alignment with agreed service scope and reporting requirements.

The managed service must provide SAA with continuous visibility into:

- Technical vulnerabilities
- Configuration weaknesses
- Application-layer risks
- Overall cyber risk exposure across SAA's IT environment.
- Tracking and resolution of vulnerabilities.

The service provider shall enable the **Qualys VMDR TruRisk platform** to support automated discovery, assessment, prioritisation, and reporting of risks across infrastructure, endpoints, externally exposed assets, and web applications.

VMDR TruRisk Capabilities

The VMDR TruRisk licensing must support a minimum of **3,400 in-scope assets**, with the ability to scale during the contract period without requiring platform reimplementations.

License True-Up and Growth Buffer:

The proposed licensing model must include a **growth buffer of up to 10% above the baseline 3,400 assets** to accommodate asset growth, onboarding of new systems, or temporary increases in asset count during the contract period. Asset increases within this buffer must not trigger immediate commercial renegotiation. Any sustained growth beyond the agreed buffer shall be addressed through a formal license true-up process at contract renewal or as otherwise contractually agreed.

The solution must include the following VMDR TruRisk capabilities:

- Deployment and operation of **Qualys Cloud Agents** for continuous vulnerability and configuration assessment
- **Asset inventory, discovery, tagging, and classification** to ensure accurate asset visibility and risk contextualisation
- **Internal and external vulnerability scanning**, including authenticated and unauthenticated scans where applicable
- **TruRisk prioritisation**, incorporating vulnerability severity, exploitability, threat intelligence, and asset criticality
- **Patch detection and visibility** to identify missing patches and remediation gaps
- **SSL/TLS certificate discovery and monitoring**, including encryption strength and certificate expiry
- **PCI ASV external vulnerability scanning**, including generation of compliance-aligned reports where applicable.

Policy Compliance (PC)

The scope further includes **Qualys Policy Compliance** to assess system configurations against recognised security standards and hardening benchmarks. This includes:

- Configuration assessment against **CIS Benchmarks** and industry-recognised secure configuration standards
- Identification of misconfigurations, configuration drift, and deviations from approved security baselines
- Compliance dashboards and reporting aligned to standards such as **CIS Controls and ISO/IEC 27001**.

Policy Compliance activities are limited to **assessment, monitoring, and reporting**. Configuration remediation remains the responsibility of SAA unless explicitly agreed otherwise.

Web Application Scanning (WAS)

The scope includes **Qualys Web Application Scanning (WAS)** to identify application-layer vulnerabilities within SAA-hosted or externally accessible web applications.

Minimum WAS coverage requirements:

- A minimum of **ten (30) web applications** must be onboarded and scanned
- Both **authenticated and unauthenticated scans** must be supported, where technically feasible
- Automated detection of common web vulnerabilities, including **OWASP Top 10** risks such as SQL injection, cross-site scripting (XSS), insecure authentication, and misconfigurations
- Risk classification, vulnerability reporting, and remediation guidance for identified findings.

Licensing and Scope Boundaries:

The scope is strictly limited to **Qualys VMDR TruRisk, Policy Compliance, and Web Application Scanning modules that are explicitly licensed** under the approved subscription.

Modules requiring separate or additional licensing are excluded unless explicitly approved and may include, but are not limited to:

- Qualys Patch Management (remediation)
- EDR
- Container Security
- Cloud Security Posture Management (CSPM)
- File Integrity Monitoring
- Malware Protection.

Failure to meet the above scope and licensing requirements may result in disqualification from the procurement process.

To be eligible to present a proposal and deliver the scope of work outlined above, the proponent shall meet the following minimum requirements:

- The proponent must be a **Qualys accredited partner or an authorised reseller** with demonstrable experience in the supply, implementation, and configuration of **Qualys VMDR TruRisk, Policy Compliance, and Web Application Scanning (WAS)** within enterprise environments. Evidence of accreditation or authorisation must be provided as part of the proposal submission.
- The proponent must demonstrate **proven experience in delivering enterprise vulnerability management, configuration compliance, and/or web application security solutions** at an organisational scale comparable to SAA. Evidence of previous engagements must be provided.
- The proponent must demonstrate the capability to provide a **fully managed Qualys service**, including licensing, initial configuration, Cloud Agent enablement, vulnerability scanning configuration, and WAS onboarding while working in collaboration with **SAA ICT**.
- Failure to meet the above eligibility and mandatory requirements may result in **disqualification from the procurement process**.

1. Evaluation Methodology

Administrative Responsiveness	Substantive Responsiveness	Technical Functionality Evaluation	Evaluation of Price and Specific Goals	Business Award and conclusion of contract
Step 1	Step 2	Step 3	Step 4	Step 5
<i>Evaluation of returnable documents per tender requirements</i>	<i>Evaluation of Mandatory (Substantive) Returnable Documents</i>	The minimum threshold for technical functionality is 75%. Bidders must meet this minimum requirement to proceed to the next stage of evaluation.	Price [Proposed rate Structure] (80) & Specific Goals (20)	<i>Post-tender negotiations (if applicable) are held at this stage before the LOA is issued to the preferred supplier.</i>

Note: The evaluation of the various stages will generally occur sequentially. However, to speed up the process, South African Airways may choose to conduct different steps of the evaluation in parallel. In such cases, evaluating bidders at any stage should not be taken as an indication that

they have passed previous stages.

3.1 EVALUATION PROCESS

3.1.1 COMPLIANCE WITH MINIMUM REQUIREMENTS

All quotations duly lodged will be examined to determine compliance with bidding requirements and conditions. Quotations with apparent deviations from the requirements/conditions will be eliminated from further adjudication.

3.1.2 EVALUATION OF QUOTATION

The contract shall be awarded at SAA's sole and absolute discretion. SAA hereby states that it is not compelled to award this quotation to any bidder. SAA has the right to withdraw this quotation at any time from the date of issuance. SAA is not obligated to accept the lowest quotation, offer, or proposal.

SAA shall not be required to accept the lowest quotation, offer, or proposal.

All quotations will be evaluated according to the criteria, weightings, and threshold scores as indicated in 2.2 below:

3.2 ADMINISTRATIVE AND SUBSTANTIVE EVALUATION

The criteria and weights referred to in paragraph 3.1 above are as follows:

3.2.1 ADMINISTRATIVE REQUIREMENTS

This evaluation stage will confirm whether all Returnable Documents [where applicable] were completed and returned by the closing date and time. At this evaluation stage, SAA will also verify if the Bid document has been duly signed by the authorised respondent, and the validity of all returnable documents will be verified.

3.2.2 SUBSTANTIVE REQUIREMENTS

This evaluation stage will confirm if the following requirements have been met:

Phase 1 - Critical Evaluation Criteria (Mandatory)

Bidders must demonstrate compliance with the following mandatory requirements. Bidders are required to indicate compliance on a Yes / No basis and provide the supporting documentation as specified. Non-compliance with any of the criteria below will result in the bid being deemed non-responsive.

NO.	DESCRIPTION	BIDDER TO INDICATE COMPLIANCE (Attach Proof)	
		Yes	NO
1	The bidder must be a South African registered entity, or a legally recognized local partner/reseller authorized to deliver Qualys solutions within South Africa. Company registration documents must be provided.		

2	Vendor Authorization – Proof of Qualys authorized reseller / partner status for: • VMDR - Vulnerability Management, Detection, and Response • PC - Policy Compliance • WAS - Web Application Scanning Proof of accreditation or authorization in the bidders name must be submitted. Accreditation letters or partner certificates must be current		
---	--	--	--

Only bidders that meet all Phase 1 criteria will be evaluated further under Phase 2.

Phase 2 – Functional Criteria

Bidders that successfully pass Phase 1 will be evaluated on functional capability, experience, delivery approach, and value-added services. Functional evaluation will be scored out of a total of 100 points. A minimum threshold score of 75% is required to qualify for further commercial evaluation.

NO.	DESCRIPTION	SCORE/WEIGHT
1	Implementation Lead Time – The bidder must provide a detailed implementation timeline indicating the time required to onboard SAA, configure the platform, and commence scanning following contract award in a table format • 0-6 Weeks = 10 points • 6-8 Weeks = 5 points • More than 8 weeks = 0 points	10
2	The bidder must demonstrate a minimum of five (5) years' experience in delivering vulnerability management, compliance, or application security solutions at an enterprise level. Evidence in the form of PO's or Contracts or Customer reference letters showing a combined period must be provided. • List of 3 PO's or Contracts or Customer reference letters= 20 points • List of 2 PO's or Contracts or Customer reference letters= 10 points • List of 1 PO's or Contracts or Customer reference letter= 5 points • List 0 PO's or Contracts or Customer reference letter= 0 points The information provided must be supported by 3 PO's or Contracts or Customer reference letters.	20
3	Platform Coverage – Ability to deliver VMDR TruRisk (minimum 3,400 assets), Policy Compliance, and WAS (minimum 30 applications), including growth buffer and true-up mechanism.	10

	• Customer reference + platform screenshots/reports + licensing evidence depicting +2500 VMDR+ documented growth/true-up model. = 10 points • Customer reference + platform screenshots/reports + licensing evidence depicting +1500 - 2499 VMDR+ documented growth/true-up model. = 5 points • Customer reference + platform screenshots/reports + licensing evidence depicting 1-1499 VMDR+ documented growth/true-up model. = 2 points • Vendor claims without supporting documentation. = 0 points	
4	TruRisk & Reporting Capability – Operational dashboards, risk analytics, vulnerability trends, compliance posture, and WAS findings delivered through the Qualys platform. Sample reports required: Operational dashboards, TruRisk analytics, vulnerability trends, compliance posture, and WAS findings demonstrated from 5 or more enterprise customers • Demonstrated reporting from 2 - 4 enterprise customers = 10 points • Demonstrated reporting from 0 -1 customers, or partial reporting capability = 5 points • No operational dashboards, TruRisk analytics, compliance posture, or WAS reporting provided = 0 points NB: Evidence must be native Qualys dashboards/reports, Screenshots or exported reports are acceptable	10
5	Licensing Flexibility & Commercial Model – License scalability, true-up mechanism, renewal terms, and growth buffer (up to 10% of baseline assets) to accommodate asset growth during the contract period. • Clear licensing model covering 3,400 assets + 10% buffer, no penalty within buffer, formal true-up at renewal, transparent pricing, and predictable renewal terms = 10 points • Licensing includes growth buffer and true-up mechanism, but with minor commercial constraints = 5 points • Limited scalability or no growth buffer , unclear true-up terms, or restrictive renewal conditions and unclear commercial terms = 0 points	10
6	Minimum experience requirements: Technical Lead / Architect – Minimum 5 years cybersecurity experience, including 3 years managing Qualys implementations. Relevant certifications/qualification must include: Qualys VMDR/WAS Specialist and any of the below CISSP, CISM, CEH, Security+, ITIL v4 (or equivalent). The required CV's with certification/qualification must be submitted with the proposal. • 3 and more CVs provided with certification/qualification = 20 points • 2 CVs provided with certification/qualification = 10 points	20

	No CVs provided with certification/qualification = 0 points	
7	Vulnerability Management Specialist – Minimum 3–5 years' experience, including hands-on Qualys VMDR administration. Relevant certifications/qualification must include: Qualys VMDR/WAS Specialist and any of the below CISSP, CISM, CEH, Security+, ITIL v4 (or equivalent). The required CV's with certification/qualification must be submitted with the proposal. 4 and more CVs provided with certification/qualification = 10 points 3 and more CVs provided with certification/qualification = 5 points - No CVs provided with certification/qualification = 0 points	10
8	Web Application Security Specialist – Minimum 3 years web application security experience (Qualys WAS preferred). Relevant certifications/qualification must include: Qualys VMDR/WAS Specialist and any of the below CISSP, CISM, CEH, Security+, ITIL v4 (or equivalent). The required CV's with certification/qualification must be submitted with the proposal. 4 and more CVs provided with certification/qualification = 10 points 3 and more CVs provided with certification/qualification = 5 points - No CVs provided with certification/qualification = 0 points	10
THRESHOLD		75 %
TOTAL		100%

Phase 3 – Pricing and Specific Goals assessment

All bid submissions that meet the Administrative, Substantive (Mandatory), and technical requirements (minimum threshold of 75%) and have confirmed their commitment to SAA's commission structure will be further evaluated under Specific Goals (20 points) to determine if they meet the preferential procurement objectives outlined for this tender.

These specific goals have been set as follows:

Selected Specific Goal	Number of points allocated (20)
B-BBEE Level 1 and 2 (Non-Compliant and/or B-BBEE Level 3-8 contributors = 0)	10
51% or more, black women owned	10
Total Points for Specific Goals	20

Bidders should be aware that preference points will be awarded to those who provide evidence according to the table below:

Specific Goals	Acceptable Evidence
B-BBEE	B-BBEE Certificate / Sworn- Affidavit / B-BBEE CIPC Certificate (in case of JV, a consolidated scorecard will be accepted) as per DTIC (Department of Trade, Industry and Competition) guideline
EME or QSE that are 51% Black Owned	B-BBEE Certificate / Sworn-Affidavit / CIPC Certificate

4. STANDARD CONDITIONS FOR REQUEST FOR QUOTATION

- 4.1 All prices provided must be exclusive of Value Added Tax (VAT).
- 4.2 All goods/services purchased will be subject to the SAA Conditions of Contract and Order, which are available upon request.
- 4.3 All prices submitted must be firm. "Firm" prices are deemed fixed and are only subject to the following statutory changes: VAT.
- 4.4 Service, pricing, and availability will be taken into consideration.
- 4.5 Pricing should be given based on an individual component that would make up the solution, based on technical and functional requirements.

THE FOLLOWING MUST ACCOMPANY YOUR QUOTE

- ☐ SAA Vendor application and supporting documents. Refer to Annexure 1.
- ☐ SBD 4 Document. Refer to Annexure 2.
- ☐ General Conditions of Contract. Refer to Annexure 3

IF NOT QUOTING, INDICATE SO AND RETURN EMAIL TO THE RELEVANT PROCUREMENT OFFICIAL