RFQ GSM040/26

Request for Quotation for network penetration service (Internal & External), and ongoing active watch on hacking exploits that are applicable for South African Airways's (SAA) environment and industry.

G.1 Written Quote Form

RFQ NUMBER: GSM0040/26

ISSUE DATE: 12 June 2026

CLOSING DATE: 19 June 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: _____

RFQ NUMBER GSM040/26

SAA Business Unit: Global Supply Management

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

The scope of work includes the provision, execution, configuration, and ongoing management of enterprise-grade penetration testing (internal & external) services and active exploit monitoring capabilities for South African Airways (SAA).

The successful service provider will be responsible for delivering a fully managed network penetration testing and monitoring solution that proactively identifies vulnerabilities, simulates real-world attack scenarios, and provides actionable intelligence to strengthen SAA's overall security posture.

The service provider will be required to deploy a continuous penetration testing programme that incorporates adaptive, behaviour-driven assessments across critical systems, applications, networks, and endpoints. Testing must be automated, recurring, and tailored to SAA's evolving threat landscape, risk profile, and operational environment.

The scope further includes the implementation of an **Active Watch Exploit Monitoring capability** that enables:

- Real-time detection of exploit attempts and malicious activity.
- Continuous monitoring of threat intelligence feeds and zero-day vulnerabilities.
- Automated alerts, behavioural feedback, and incident reporting.
- Unlimited exploit simulation campaigns with scheduled testing windows and detailed reporting on system resilience.
- Expect recommendation and advisory to remediate.

Managed penetration intelligence and active watch services are required.

The solution must provide access to a continuously updated exploit and vulnerability database aligned with internationally recognised cybersecurity standards and best practices, including ISO 27001, NIST, and CIS Controls.

The service provider must ensure coverage for a minimum of 2,200 user endpoints and associated infrastructure within SAA's current environment. The licensing and service model must support scalability to accommodate additional systems and users during the contract period, without requiring a full platform reimplementation.

In addition, the service provider must enable advanced analytics, including vulnerability scoring, exploit trend analysis, maturity assessments, and risk posture measurement. The solution must provide dashboards and reports that allow SAA to track penetration test results, exploit detection metrics, remediation progress, and overall cybersecurity resilience on a monthly and quarterly basis.

A minimum of 8 years of professional experience, combined with active watch in penetration testing and within financial and aviation services. Deployment Expertise: Proven track record with active watch deployment, ensuring continuous monitoring and rapid response capabilities. Combined Expectation: Candidates must demonstrate both the depth of penetration testing expertise and the operational readiness associated with active watch deployment.

3. EVALUATION METHODOLOGY

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

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 3.2 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:

Mandatory Returnable Documents – Phase 1

Bidders must fully comply (100% compliance) with the statements of compliance below by either selecting "Yes" or "No" with supporting evidence to qualify their statements of compliance. Failure to do so will result in bid disqualification. Bidders should also note that if they select "No," South African Airways will interpret the bidder as non-compliant, leading to bid disqualification.

None Weighted, mandatory requirements must be met for the bid to qualify for further evaluation. Proof of the information below needs to be provided. A bidder who fails to meet this requirement will be disqualified.	**Comply (Make sure that you attach proof)**	
	YES	NO
The bidder must comply with internationally recognised cybersecurity and penetration testing standards, demonstrating adherence to information security, data protection, and privacy requirements relevant to SAA. Provide an Acceptable frameworks in the bidder's name which includes **ISO/IEC 27001 or NIST Cybersecurity Framework**, and any of the below certification: • **OSSTMM**, • **OWASP Testing Guide**, • **PTES**		

All bidders who do not submit all the required returnable documents (Critical Criteria) will be disqualified from further evaluation.

3.3 Technical Functional Questionnaire/Evaluation (Minimum Threshold = 80%) – Phase 02

<table>
<tr><th>Evaluation Criteria</th><th>Weight %</th></tr>
<tr><td>Implementation Lead Time – The bidder must provide a detailed implementation timeline in a table format indicating the time required to onboard SAA, configure the platform, and commence execution and active monitoring and/or simulations of attacks following contract award.

• 0-4 Weeks = 15
• 4-6 Weeks = 5
• More than 6 weeks = 0</td><td>15%</td></tr>
<tr><td>The bidder must demonstrate experience in the deployment, execution, and ongoing management of:

• Penetration testing services (both internal and external), and
• Active watch solutions (e.g., ethical hacking and simulations, continuous monitoring, SOC/watch services, active threat detection/response), within enterprise environments, with a minimum of eight (8) years relevant experience.

In addition, the bidder must demonstrate having provided skilled Information Security resources in engagements over the past eight (8) years within at least one or more of the following industries:

• Airline/Aviation
• Financial services
• Online shopping / eCommerce

Evidence requirement: Copies of Purchase Orders (POs) and/or contracts submitted with the proposal must show a combined period of service totaling at least 8 years

<table>
<tr><td>Relevant years of experience proven by POs/contracts</td><td>0 = Less than 8 years proven / no acceptable proof
3 = 8 to 10 years’ experience
6 = Above 10 years.</td></tr>
<tr><td>Scope coverage: internal + external penetration testing + active watch in enterprise</td><td>0 = Does not address scope / unclear
2 = Demonstrates either pen testing or active watch only
4 = Demonstrates pen testing (internal & external) but limited ongoing active watch capability (or vice versa)
6 = Demonstrates internal + external pen testing and active watch, including ongoing management in enterprise settings</td></tr>
<tr><td>Industry experience (airline/financial services/eCommerce)</td><td>0 = No evidence in the stated industries
1 = Evidence in one of the industries
2 = Evidence in two industries
3 = Evidence in three industries (airline + financial + eCommerce), or airline plus one other with strong enterprise proof</td></tr>
</table>
</td><td>15%</td></tr>
</table>

<table>
<tr>
<td>Experience in Network Penetration Services and Active Watch Projects – The bidder must demonstrate experience in delivering network penetration testing, active watch, or simulation of exploits programmed within the last eight (8) years from a client in the Airline, financial services, online shopping.

• 3 testimonial letters provided = 15
• 2 testimonial letters provided = 10
• 1 testimonial letter provided = 5
• 0 testimonial letter provided = 0

The information provided must be supported by 3 testimonial letters on the client's letterhead with contactable details (e.g. telephone, cell phone, email etc.) of previous/current clients testifying satisfactory service delivery on the matters cited. The letters must be supported by copies of contracts/PO's corresponding to the client, services and period; these will be bundled and scored together.</td>
<td>15%</td>
</tr>
<tr>
<td>Skills and Qualifications of Delivery Team:

The bidder must provide CVs of key personnel responsible for the delivery and management of penetration testing and active monitoring services under this proposal.

The proposed delivery team must include:

A minimum of five (5) suitably qualified security professionals, each holding OSCP certification, plus one or more of the following or equivalent:

• CREST
• PCI
• CEH
• GPEN
• CPT
• Cyber Essentials

In addition, the bidder must demonstrate:

Proven experience in penetration testing, threat monitoring, and incident response, and

Professional references validating prior engagements relevant to the scope of services.

<table>
<tr><td>Fewer than 5 OSCP-certified personnel submitted</td><td>0</td></tr>
<tr><td>All 5 CVs include OSCP certification No additional security certifications provided</td><td>5</td></tr>
<tr><td>All 5 CVs include OSCP certification and additional security certifications provided</td><td>15</td></tr>
</table>
</td>
<td>15%</td>
</tr>
<tr>
<td>The bidder must demonstrate the ability to deliver a fully managed penetration testing intelligence and active watch service, including but not limited to:

• Platform administration and management,
• Threat monitoring and ongoing surveillance,
• Vulnerability assessments and penetration testing execution,</td>
<td>30%</td>
</tr>
</table>

• Reporting (technical and management), • Continuous technical and operational support. The bidder must provide **documented evidence of prior managed service engagements**, signed off by clients, demonstrating successful delivery of managed penetration testing and active watch services. **Minimum Requirements:** The bidder must show capability to fully manage penetration testing and active watch services covering: — administration, — monitoring setup, — testing execution, — reporting, and — continuous support The bidder must submit documented evidence of three clients within the minimum of past eight years the following evidence for each project claimed: — Client-signed project completion letters or — Contract extracts / POs with formal sign-off confirmation, — Proof of service period (dates must fall within the past 8 years), — Description of managed services provided. • 3 projects signed off submitted = 30 • 2 projects signed off submitted =20 • 1 project signed off submitted =10 • 0 project signed off submitted = 0 Only airline, financial institutions and eCommerce projects and experience will be considered.	
Reporting, Analytics, and Risk Measurement Capability The bidder must demonstrate the ability to deliver measurable outcomes through dashboards, vulnerability and threat analytics, risk scoring, security posture measurement, and executive-level reporting. — Sample reports or dashboards must be provided as evidence. • Sample reports or dashboards provided =10 • No Sample reports or dashboards must be provided = 0	**10%**
Total	**100%**
Threshold	**75%**

Bidders must note that the minimum qualifying score for Functionality is 75%. All tenders that do not comply with all the Mandatory Requirements for Functionality and that fail to achieve the minimum qualifying score of 75% on services shall not be considered for further evaluation against Price and B-BBEE.

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
Bidders that are 30% 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
Bidders that are 30% Black Women Owned	B-BBEE Certificate / Sworn-Affidavit / CIPC Certificate

4. STANDARD CONDITIONS FOR REQUEST FOR QUOTATION

Conditions:

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