



REQUEST FOR QUOTATION (RFQ)

**The South African Qualifications Authority (SAQA) invites Service Providers to submit
Proposals for the requirements stipulated below:**

DOCUMENT NUMBER:	SAQA RFQ – DLP 2024/25
RFQ ISSUE DATE:	20 September 2024
RFQ CLOSING DATE AND TIME:	30 September 2024 @ 11:00
PRICING VALIDITY PERIOD	90 DAYS (FROM RFQ CLOSING DATE)
PERIOD	24 months
DESCRIPTION:	Provisioning of Data Loss Prevention and Insider Threat Management solution for twenty-four (24) months
RESPONSES TO THIS RFQ SHOULD BE FORWARDED TO:	RFQ@saga.org.za
ENQUIRIES:	Mr Awonke Mamane E-mail: amamane@saga.org.za

TERMS OF REFERENCE

1. INTRODUCTION

1. The South African Qualifications Authority (SAQA) is a public entity listed in Schedule 3A of the Public Finance Management Act (PFMA). It is mandated by the National Qualifications Framework (NQF) Act, 67 of 2008, to oversee the further development and implementation of the NQF, advance the objectives of the NQF and coordinate its three Sub-Frameworks.
2. South African Qualifications Authority (SAQA) has a responsibility to ensure adequately and appropriately organised training and development for all staff to ensure the acquisition of the necessary skills, knowledge, and attitudes.

2. PURPOSE

- 2.1 SAQA seeks to appoint a competent Service Provider to provide Data Loss Prevention and Insider Threat Management solution for twenty-four (24) months

3. SCOPE OF SERVICES

- 3.1 The South African Qualifications Authority provide Data Loss Prevention and Insider Threat Management solution for 24 months. The proposed solution must support deployment in a hybrid multi-cloud environment, to have visibility of all operation environments. The service provider should offer the solution in the form of a cloud-based platform, hosted within the borders of South Africa. The solution should be based on a quantity of 150 users.

3.2 Solution functional requirements

Please answer the following questions regarding the functionality of the proposed solution.

Core Requirements	Answer
Solution must support commonly used virtualized environments like Citrix XenDesktop, Citrix XenApp, Hyper-V, Virtual box and VMWare.	
Provide a list of all supported OS versions	
Endpoint collectors/agents must not consume on average more than 1% CPU, 50MB of RAM, and transmit no more than 5MB of data per day.	
Solution must provide sufficient Chain of Custody for all activities which prove evidence is admissible, authentic, complete, reliable, and believable which can be used in legal proceedings.	
Solution must provide a health status on all installed endpoints. Status should include if the agent is installed and reporting, last check-in time, and if the policies are updated.	
Solution must be able to report on system health in terms of CPU usage, Memory usage, license status, hardware failures.	
Solution must have artificial intelligence capabilities.	
Solution must continuously audit endpoints both on-network and off-network and cache and encrypt all data locally when connection to the management server is not present and then stream all data immediately when a connection is re-established.	
Solution must encrypt the collect data in transit and at rest	
Solution must have ability to protect event logs collected and stored from modification and unauthorized access.	
Solution must collect data continuously on a 24x7 basis that can be searched quickly and easily allowing the department to assess the security posture of endpoints by group (i.e. geography, network location, business unit, domain etc.)	

Solution must provide pre-built dashboards, visualizations, reports, etc. that can provide an updated view on the security posture of an organization that can be scheduled to run automatically or on an adhoc basis.	
Solution must support agents that install and run both covertly and overtly.	
Endpoint agents must not require a reboot upon installation.	
Solution must provide the ability to customize event triggers and notifications.	
Solution must provide the ability to create and use custom workflows for event management.	
Solution must provide audit capabilities to view system functions, including but not limited to policy configurations, policy deployment, user access, and bi-directional transactions between the solution and endpoints.	
Solution must provide integration capabilities for third-party solutions such as SIEM, UBA, and TIP from vendors such as Microsoft, Splunk, Exabeam, Forcepoint, and Secureworks	
Solution must support multiple automated data export methods for a range of data sets (alerts, raw data and enriched data) using a variety of formats (including CEF, syslog, JSON, CSV, HTML, PDF and XML).	
Solution must provide the ability to integrate with software and configuration management systems. (Microsoft SCCM, GFI Languard, JAMF, etc)	
Solution must provide behavioral configuration policies based on endpoint type, operating system, user permissions, application or application sets, network accesses, etc.	
Solution must have the ability to anonymize all collected data to protect PII.	
Solution must provide the ability to store data in a consistent state and not allow data corruption and or data loss during a hardware failure, disaster recovery or	

failover.	
Solution must address the CIA security concept (Confidentiality, Integrity and Availability).	
Solution must support offline historical data sets to be immediately enabled for investigation purposes.	
Solution must support updates performed in parallel to normal operations without any system interruption on planned down-time events (i.e. minimal disruption to the business).	
Solution must provide out-of-the-box pattern matching aligned with known bad insider behavior, and also build profiles that detect anomalous behavior.	
Solution must contain a library of known high-risk activities associated with, but not limited to insider threat, general security management, data exfiltration, and identity access management.	
Solution must provide child and parent relationships of all executed programs.	
Solution must capture the command line parameters passed within and between applications.	
Solution must collect Session Activities including local terminal and remote session log on, log off, lock and unlock.	
Solution must collect Process Activities – Including process hash (MD5, SHA1 or SHA256), process parent and child relationships, applications installed, started, stopped, versions, execution paths and command line execution parameters.	
Solution must collect File System Activities – Including files or directories created, moved copied or deleted or renamed (including changes to file name extensions), file hashes (MD5, SHA1 or SHA256) as well as visibility into contents stored in the alternate data stream (ADS).	
Solution must collect Window Activities contextual task switching ‘window’ behavior generated by a given user account including application in-focus timestamps.	

Solution must collect Network Activities including endpoint net-flow data (e.g. bytes up and down, port numbers, source and destination IP address etc.) and web page data (e.g. full URL strings and web domains accessed).	
Solution must collect Network Interface Activities including WIFI SSID and public IP address information and connection change events.	
Solution must collect Device Activities including removable devices added and removed along with serial numbers for forensic review as well as Bluetooth and wireless device connection events.	
Solution must collect Window Registry Activity including the ability to capture Windows Registry modifications (e.g. create, modify, delete).	
Solution must collect Other contextual activities including print job activities and clipboard activities (e.g. copy and paste between two apps).	
Solution must have the ability to provide screen recording capabilities for persons or activities of interest.	
Solution must track file shadowing/file lineage using configurable hashing algorithms including MD5, SHA1 and SHA256 to determine the 'lineage' of a file to answer who, what, when, where, and why was this file copied, modified, obfuscated or exfiltrated.	
Solution must collect a full audit trail of file system activities from the endpoints and create a baseline of normal behavior for the user, peer groups, and/or organization.	
Solution must provide the ability to provide classification of data to inform the risk model so different classes of data assets can be treated with different levels of risk.	
Ability to configure the events received from endpoints, including but not limited to the following:	
• Authentication events (for example log-on, log-off)	
• Application Use	
• Printer Use	
• USB peripheral use	

• Internet Use	
• File access & change events	
Solution must prevent data loss of intellectual property, accidental data loss, and comply with regulatory standards for data privacy.	
Solution must provide insider threat capabilities to stop malicious insiders, educate negligent users, identify compromised employees, and secure the remote workforce.	
Solution must have non-invasive employee monitoring capabilities protect employees, maintain regulatory compliance, protect against legal liabilities and achieve operational resilience	
Solution must provide out-of-the-box risk templates that align with MITRE ATT&CK adversarial techniques.	
Solution must support advanced rule-based alerting capabilities for known threats.	
Solution must aggregate threats and provide intelligence on predicted risks.	
The proposed solution must cater for customisable online and offline data retention periods and specifically be scoped for 2 years online retention and 5 years offline retention.	
Solution must provide anomaly-based detection to alert on activity outside of normal behaviors when comparing a user against themselves, against their peer group, and against the organization.	

4. PRICING SCHEDULE

	DESCRIPTION	Year 1 Inc VAT	Year 2 Inc VAT	Line Total Inc VAT
1.	Data Loss Prevention and Insider Threat Management solution For 150 Users	R	R	R
2.	Once off Setup and Configuration costs (Year 1)	R	R	R
3.	Annual maintenance & Support fee	R	R	R
4.	Any other costs (Specify)	R	R	R
	Total including VAT	R	R	R

5. EVALUATION CRITERIA

The bid will be evaluated in two (2) stages:

Stage 1: Screening of mandatory documents.

Stage 2: Price evaluation

6. STAGE 1: MANDATORY REQUIREMENTS

Bidders **must** comply with this section as it forms the basis of the evaluation of the bidder's proposal.

MANDATORY DOCUMENTS	Comply	Not Comply
1. Submit proof of Service provider being a partner of the OEM for the proposed solution		

2.	<p>The bidder should submit a minimum of three (3) formal reference letters from clients where it has previously provided data loss prevention and insider threat management solution</p> <p>The reference letters should:</p> <ul style="list-style-type: none"> a) Be on the client's letterhead; b) Be signed and dated; c) Indicate the work done; <p>Indicate the year the work was done, (please note that the reference letters should be within 5 years of the RFQ closing date; and show the client's contact details including contact name and telephone or email address.</p>		
3.	<ul style="list-style-type: none"> a) Detailed CVs of the key personnel (Minimum of 2); and the CVs must clearly highlight security certification, areas of competence and years of experience (Minimum of 5 years) relevant to the tasks and objectives of this service request as outlined in this RFQ. b) Copies of relevant Cyber security certificates and accreditation of each resource in part (a) above. Provided certificates and accreditation must be valid and relevant to the proposed OEM security platform. 		
4.	<p>The bidder is required to provide the detailed project methodology and draft plan outlining how SAQA requirements will be implemented.</p>		

For a bidder to qualify to be evaluated for Stage 2: Price and Preference Points, **a bidder must not have been disqualified in compliance with the mandatory requirements.**

7. STAGE 2: PRICE AND PREFERENCE POINTS EVALUATIONS

Price and Preference Points Evaluation as follows:

All bidders that have passed the mandatory requirements will be evaluated in terms of the 80/20 system prescribed by SAQA in line with PPR 2022 as follows:

- i. **80** Points for pricing.
- ii. **15** preference points for the company that has at least 51% black ownership.
- iii. **5** preference Points for the company that has at least 30% black woman ownership.

SPECIAL CONDITIONS

RFQ SPECIAL CONDITIONS

1. Bidders must submit the recent National Treasury (CSD) Central Supplier Database's report.
2. Bidders are required to submit an original or certified copy of the B-BBEE certificate or Sworn Affidavit as per the B-BBEE Act. The SANAS Logo should be visible on the B-BBEE Certificate.
3. Bidders must complete, sign, and submit the attached SBD 4 and SBD 6.1 forms.
4. The proposal and required documents must be submitted using the PDF format only, through email to RFQ@saqa.org.za
5. In Instances, where brand names are mentioned, SAQA will accept equivalent items that have similar specifications.
6. The National Treasury's General Conditions of Contract (GCC) will apply and is enforceable on this RFQ.
7. The RFQ will be evaluated in terms of the 80/20 system prescribed by the Preferential Procurement Policy Framework Act (PPPFA).

PROTECTION OF PERSONAL INFORMATION

8. In this clause, the words "personal information", "processing" and "responsible party" have the meanings ascribed to them in the Protection of Personal Information Act, 2013 (Act No.4 of 2013).
9. SAQA will comply with the Protection of Personal Information Act, 2013 (Act No.4 of 2013, (POPIA) by lawfully processing personal information submitted by bidders in accordance with the conditions of lawful processing as set out in POPIA.
10. All bidders must comply with their obligations as set out in POPIA for which they are a Responsible Party before sharing any information with SAQA.
11. SAQA will not be held liable for any non-compliance with the provisions of POPIA or unlawful processing or sharing of information by a bidder.

BIDDER'S DISCLOSURE

1. PURPOSE OF THE FORM

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

- 2.2 Do you, or any person connected with the bidder, have a relationship

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.

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 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

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.

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

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

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).

To be completed by the organ of state

(delete whichever is not applicable for this tender).

- a) The applicable preference point system for this tender is the 90/10 preference point system.
- b) The applicable preference point system for this tender is the 80/20 preference point system.
- c) Either the 90/10 or 80/20 preference point system will be applicable in this tender. The lowest/ highest acceptable tender will be used to determine the accurate system once tenders are received.

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.

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).

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:

$$Ps = 80 \left(1 - \frac{Pt - P_{min}}{P_{min}} \right) \text{ or } Ps = 90 \left(1 - \frac{Pt - P_{min}}{P_{min}} \right)$$

80/20 or 90/10

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:

$$Ps = 80 \left(1 + \frac{Pt - P_{max}}{P_{max}} \right) \text{ or } Ps = 90 \left(1 + \frac{Pt - P_{max}}{P_{max}} \right)$$

80/20 or 90/10

Where

P_s = Points scored for price of tender under consideration

P_t = Price of tender under consideration P_{max} = Price of highest acceptable tender

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 (90/10 system) (To be completed by the organ of state)	Number of points allocated (80/20 system) (To be completed by the organ of state)	Number of points claimed (90/10 system) (To be completed by the tenderer)	Number of points claimed (80/20 system) (To be completed by the tenderer)
At least 51% black ownership		15		
30% black woman ownership.		5		

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: