



sassa

SOUTH AFRICAN SOCIAL SECURITY AGENCY

TERMS OF REFERENCE

**REQUEST FOR PROPOSAL FROM SERVICE PROVIDERS TO PROCURE CYBER SECURITY
AWARENESS & TRAINING SOLUTION FOR A PERIOD OF THREE (3) YEARS**

Contents

1. BID OVERVIEW	3
1.1 OVERVIEW OF SASSA	3
2. BACKGROUND INFORMATION	4
3. PREPARATION OF THE RESPONSES	4
4. SPECIFICATIONS	5
4.1. Training, Awareness and Simulation	5
4.2. Reporting, Content Management and Customisation	5
4.3. Advanced Email Threat Protection	6
4.4. Cloud-based Architecture and Data Handling	6
5. PROJECT METHODOLOGY	6
5.1. Methodology Overview	6
5.2. Phase One: Planning and Preparation	6
5.3. Phase Two: Solution Design and Configuration	7
5.4. Phase Three: Testing and Piloting	7
5.5. Phase Four: Global Rollout	7
6. FINANCIAL & LICENSES PROPOSAL	7
6.1. Finance	7
6.2. Licenses	8
7. BID EVALUATION	8
7.1. Stage One: Phase One – Special Conditions	8
7.2. Stage One: Phase Two – Evaluation on Functionality Criteria	8
7.3. Stage One: Phase Three – Administrative Compliance	9
7.4. Stage Two: Price And Specific Goals (Preference Point System (80/20))	9
8. BID ENQUIRIES & NON-COMPULSORY BRIEFING SESSION	10
9. BID CONDITIONS	11

1. BID OVERVIEW

1.1 OVERVIEW OF SASSA

The South African Social Security Agency (SASSA), listed as a schedule 3A public entity in terms of the PFMA, is an extension of government's delivery arm that administers the delivery of grants to the poor in South Africa. Through SASSA, government must ensure improvement of the social security service delivery system.

The agency aims to deliver quality and comprehensive social security services in partnership with non-governmental, community-based, faith-based organisations, business, and civil society structures and labour movement.

The founding legislation of this entity, which is the South African Social Security Agency Act, 2004 was enacted at the beginning of 2004. The [SASSA Act](#) also makes provision for the effective management, administration and payment of social assistance and services through the establishment of the SA Social Security Agency.

The key functions of SASSA are the administration and payment of social grants and include:

- a) The processing of applications for social grants;
- b) Verification and approval of applications;
- c) Ongoing entitlement reviews of Beneficiaries;
- d) Disbursement and payment of grants to eligible beneficiaries; and
- e) Quality service assurance ensuring compliance with norms and standards and fraud prevention and detection.

SASSA provides the following types of social grants:

- a) Old Age;
- b) War Veterans;
- c) Disabled Persons;
- d) Grant-in-Aid;
- e) Child support;
- f) Foster Care;
- g) Social Relief;
- h) Care Dependency;
- i) As well as the correspondence related to these grants.

2. BACKGROUND INFORMATION

- 2.1. The South African Social Security Agency (SASSA) is procuring a Cyber Security Awareness & Training solution to enhance its information security posture. This solution is crucial for mitigating cyber threats, complying with regulatory requirements, and fostering a culture of security awareness among employees.
- 2.2. In today's complex cyber threat environment, employees' daily actions can significantly impact an organization's security. Simple mistakes, such as mishandling emails, can lead to severe consequences, including ransomware, exposed passwords, unauthorized data sharing, financial losses, and compliance issues.
- 2.3. Cyber Security Awareness and Training transforms employees from a security vulnerability into a valuable defence. This program equips staff with the knowledge and skills to identify, report, and prevent security incidents, resulting in reduced security expenses, enhanced compliance, and a substantial advantage in preventing cyberattacks.
- 2.4. As the digital environment evolves, organizations face increasing threats and vulnerabilities. The rapid advancement of technology and growing complexity of cyber threats present significant dangers to SASSA. Security incidents often occur due to employee carelessness, insufficient awareness, and inadequate security measures. Without a robust information security awareness strategy, organizations are susceptible to attacks, data breaches, financial losses, and reputational damage.
- 2.5. To address these risks, it is essential to implement an information security awareness solution. This solution educates and trains employees on best practices through interactive training, regular updates, and practical exercises. Key components include training programs, awareness campaigns, phishing simulations, policy and procedure updates, and metrics and reporting.
- 2.6. By investing in a Cyber Security Awareness and Training program tailored to the specific needs and roles of each employee, SASSA can significantly lower the risk of breaches, data loss, and financial harm, while ensuring compliance with regulations and industry standards.
- 2.7. The selected service provider will be accountable for the deployment and configuration of the acquired solution.

3. PREPARATION OF THE RESPONSES

- 3.1. Responses must be prepared according to the instructions provided in this bid document. Failure to comply may result in the responses being difficult or impractical to evaluate, leading to disqualification.
- 3.2. Bidders are to fully comply with the functional requirements/elements (**Annexure A– Response Template for Functional Requirements**).
- 3.3. Failure to adequately respond with any functional requirements will result in a poor evaluation of the bid response. Bidders must achieve at least 70 out of 100 points in the functionality assessment to avoid disqualification and not considered for Price and Specific Goals.

- 3.4. Service Pricing must be completed on the attached (**Annexure B** – Service Pricing Template).
- 3.5. The bidders are required to submit their proposals using the two-envelope system. Each envelope must be marked correctly and sealed separately for ease of reference during the evaluation process as follows:
 - 3.5.1. Envelope 1 – Technical Proposal;
 - 3.5.2. Envelope 2 – SBD 3.1 and Pricing Proposal (**Annexure B**).
- 3.6. The proposal must be submitted in two copies. An original response should be accompanied by a hard copy and an electronic soft copy on a memory stick. All the contents of the copies should be in the exact same order as in the hard copy to make it easier to navigate and evaluate the bid response.

4. SPECIFICATIONS

4.1. Training, Awareness and Simulation

- 4.1.1. Visual and Computer-Based Training: How does your solution deliver visual and computer-based training materials tailored to SASSA users, including assessments and simulations?
- 4.1.2. Gamified and Engaging Training: What gamified training features are included to enhance user engagement and retention?
- 4.1.3. Continuously Updated Content Library: How is the solution's content library maintained and updated, and what role does AI play in ensuring relevance and responsiveness to emerging threats?
- 4.1.4. Integration of SASSA Policies: How does your solution incorporate SASSA's internal policies and regulatory requirements (e.g., POPIA, GDPR) into training content?
- 4.1.5. Engaging Compliance Training: What mechanisms are used to deliver engaging compliance training that effectively modifies user behaviour and reduces risk?
- 4.1.6. Customized Phishing Awareness Training: How does your solution personalize phishing awareness training using AI, and what capabilities exist for simulating phishing attacks tailored to SASSA's threat landscape?
- 4.1.7. Baseline Phish-Prone Percentage: How is the baseline phish-prone percentage established, and what methods are used for continuous testing and risk assessment?
- 4.1.8. User Categorization and Classification: How does your solution support user categorization and classification to enable targeted training and reporting?
- 4.1.9. Active Feedback Loops: What analytics and feedback mechanisms are included to monitor user awareness and improve resilience against social engineering threats?

4.2. Reporting, Content Management and Customisation

- 4.2.1. Progress Reports and Recommendations: How does your solution generate progress reports and provide actionable, data-driven recommendations?

- 4.2.2. Data-Driven Dashboard: What dashboard features are available to summarize phishing assessments, detection rules, training compliance, and security events?
- 4.2.3. Training Compliance Monitoring: How does your solution monitor training completion and escalate non-compliance to supervisors?
- 4.2.4. Risk Monitoring Customisation: How does your solution enable SASSA to define and customise the monitoring of specific risky user behaviours?
- 4.2.5. Training Effectiveness Metrics: What metrics are used to assess training effectiveness and user understanding?
- 4.2.6. Compliance Overview Visualization: How does your solution visualize SASSA's overall compliance status and track improvement measures?
- 4.2.7. Customisable Templates and Landing Pages: What customisation options are available for phishing templates, landing pages, passing scores, and branding to align with SASSA's regulatory and organizational requirements?

4.3. Advanced Email Threat Protection

- 4.3.1. Automatic Blocking of Email Threats: How does your solution automatically detect and block email threats that bypass existing security measures?
- 4.3.2. Crowdsourced and AI-Driven Threat Intelligence: What role does crowdsourced intelligence and AI play in enhancing threat detection and blocklisting?
- 4.3.3. Automated Quarantine and Safe Simulations: How does your solution quarantine malicious emails and convert reported phishing attempts into safe simulations for training purposes?

4.4. Cloud-based Architecture and Data Handling

- 4.4.1. Architecture and Management: How is your solution architected for cloud-based deployment and ease of management?
- 4.4.2. Data Inventory: Can you provide a detailed inventory of the types of data processed by your cloud system (e.g., IP address, device name, user ID), and how is transparency ensured?
- 4.4.3. Data Transparency and Compliance: How does your solution ensure compliance with POPIA and GDPR when handling cross-border data transfers and processing?

5. PROJECT METHODOLOGY

5.1. Methodology Overview

- 5.1.1. This project methodology outlines the steps for deploying a Cyber Security Awareness and Training solution for SASSA. The methodology includes phases for planning, testing/piloting, and global rollout to ensure a successful implementation and adoption of the solution.

5.2. Phase One: Planning and Preparation

- 5.2.1. To establish a solid foundation for the project by defining scope, objectives, and resources.

5.2.2. Potential activities include but not limited to:

5.2.2.1. Project Kick-off meetings, project scope and objective defining, resource allocation, development of project plan and risk assessment.

5.3. Phase Two: Solution Design and Configuration

5.3.1. To design and configure the Cyber Security Awareness and Training solution to meet SASSA's specific requirements.

5.3.2. Potential activities include but not limited to:

5.3.2.1. Requirements gathering, solution design, configuration, and develop or customise.

5.4. Phase Three: Testing and Piloting

5.4.1. To test the solution in a controlled environment and conduct a pilot to validate its effectiveness and avoid service disruptions within SASSA.

5.4.2. Potential activities include but not limited to:

5.4.2.1. Unit testing, integration testing, User Acceptance Testing (UAT), pilot deployment and evaluation.

5.5. Phase Four: Global Rollout

5.5.1. To deploy the solution across the entire organization following a successful pilot.

5.5.2. Potential activities include but not limited to:

5.5.2.1. Rollout planning, training and awareness campaign, global deployment, post-deployment support, and performance monitoring.

6. FINANCIAL & LICENSES PROPOSAL

6.1. Finance

6.1.1. All prices must be inclusive of VAT.

6.1.2. Subscription Licenses: Pricing should be based on an annual subscription for 7500 licenses over a three (3) year period. Alternatively, an enterprise license that can cover 7500 SASSA users for three (3) years. On the anniversary of the subscription, the Agency may adjust (reduce/increase) the number of licenses or acquire additional licenses if needed before the subscription anniversary.

6.1.3. Professional Services for Implementation: The solution procured will have once-off professional services to ensure efficient implementation and configuration of the solution.

6.1.4. Managed Services: Post-implementation and OEM sign-off, the procured solution will necessitate professional support services from the bidder for a duration of six months.

6.1.5. Training Requirements: Training for twelve (12) SASSA super users (9 Regional ICT & 3 Head Office ICT Officials), for two sessions post implementation.

6.2. Licenses

6.2.1. Subscription based solution for a period of 3 years.

6.2.2. The licenses must be under the Agency's name.

7. BID EVALUATION

Bids will be evaluated in two stages based on the functional capability of the bidder as well as on price and specific goals where the 80/20 principle will be applied.

The bid will be evaluated as follows:

Stage One: Phase One – Special Conditions,

Stage One: Phase Two – Evaluation on Functionality Criteria

Stage One: Phase Three – Administrative Compliance,

Stage Two: Price and specific goals

7.1. Stage One: Phase One – Special Conditions

7.1.1. OEM Accreditation Letter: Bidders must submit an OEM accreditation letter, with contactable references, confirming their authorisation as OEM representatives, resellers, or registered partners. The letter must specifically name the intended bidder, not another institution.

7.1.2. Project Experience: The bidder is required to **provide a MINIMUM of two client reference letters, each containing verifiable contact information, confirming the successful implementation and configuration of a cybersecurity awareness and training solution** within the last ten years. These reference letters must be presented on official client letterhead and include valid contact details for the location where the service was rendered.

NB: Failure to comply with the above special conditions will result in your bid being disqualified.

7.2. Stage One: Phase Two – Evaluation on Functionality Criteria

7.2.1. The **Annexure A** – Response Template for Functional Requirements will be used to assess the bidders' proposals. Responses to the functional requirements should be attached as instructed, using the provided templates. The template serves as a guide on the functional criteria that will be evaluated for the bid and deemed successful.

7.2.2. The table here-below contains the weights of each Functional Requirements Components.

Values: 1 = Poor, 2 = Average, 3 = Good, 4 = Very Good, 5 = Excellent

Functionality Criteria	Weights
Training, Awareness and Simulation	40
Reporting, Content Management and Customisation	25
Advanced Email Threat Protection	20
Cloud-based Architecture and Data Handling	15
Total Weight	100

NB: Bidders who score less than 70 of the 100 points of the functionality points will be disqualified and thus will not be evaluated further.

7.3. Stage One: Phase Three – Administrative Compliance

7.3.1. Bidders are required to submit the following:

7.3.1.1. **Proof of Registration:** Proof of registration with National Treasury Central Supplier Database.

7.3.1.2. **Completed SBD Forms:** Fully completed and signed Standard Bid Document (SBD) forms.

7.3.1.3. **Tax Compliance Status Pin:** A valid tax compliance status pin.

NB: Failure to submit any of the above may render the bid invalid.

7.4. Stage Two: Price And Specific Goals (Preference Point System (80/20))

Price and Specific Goals	100
Price	80
Specific Goals	20

80 points will be for price and the 20 points will be for specific goals:

Price

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

Where

Ps = Points scored for price of tender under consideration

Pt = Price of tender under consideration

Pmin = Price of lowest acceptable tender

Specific Goals

Preference points will be awarded to a bidder for attaining the specific goals in accordance with the table below:

Specific Goals	Number of points (80/20)
B-BBEE Status Level 1 - 2 contributor with at least 51% black women ownership	20
B-BBEE Status Level 3 - 4 contributor with at least 51% women ownership	18
B-BBEE Status Level 1 - 2 contributor with at least 51% black youth or disabled ownership	16
B-BBEE Status Level 1 - 2 contributor	14
B-BBEE Status Level 3 - 8 contributor with at least 51% youth or disabled ownership	12
B-BBEE Status Level 3 - 4 contributor	8
B-BBEE Status Level 5 - 8 contributor	4
Others (Non-Compliant)	0
Note: In the event of a bidder claiming more than one specific goal category, SASSA will allocate points based on specific goal with the highest points.	

- Bidders should submit a B-BBEE verification certificate from a verification agency accredited by the South African National Accreditation System (SANAS) and/or CSD MAAA number and/or a sworn affidavit indicating the percentage of all shareholders and signed by the commissioner of oaths, all the company shareholders and/or owners
- Failure to submit the required documents shall be interpreted to mean that preference points for specific goals are not claimed.

8. BID ENQUIRIES & NON-COMPULSORY BRIEFING SESSION

- a) There will be a non-compulsory virtual briefing session to be held as per the date and time specified in the invitation to bid.
- b) All enquiries, questions and requests for clarification that may arise in relation to this bid must be directed to the CyberAwareness@sassa.gov.za email address.
- c) Bidders must register details of their representatives for the briefing session at the CyberAwareness@sassa.gov.za email address.
- d) All questions and/or enquiries must be raised within 3 working days from date of the briefing session. No questions and/or enquiries will be considered beyond that period.
- e) Responses will be provided within 5 working days from date of the briefing session.

9. BID CONDITIONS

- a) **Response Diligence:** Bidders must respond to all elements of the bid with diligence.
- b) **Contract and SLA:** SASSA will sign a contract and conclude a Service Agreement/Service Level Agreement with the successful bidder.
- c) **General Conditions of Contract:** As stipulated by the National Treasury of the Republic of South Africa will be applicable.
- d) **Data and IP Ownership:** Data and Intellectual Property will be owned by SASSA.
- e) **Compulsory Screening:** The successful bidder will be subjected to the security screening process, should the successful bidder, after being appointed service provider fail the security screening, the contract may be terminated.
- f) **Negotiation:** SASSA reserves the right to negotiate the price with the successful bidder.