SOUTH AFRICAN

SOCIAL SECURITY AGENCY

REVIEW FOR INFORMATION AND COMMUNICATION TECHNOLOGY APPLICATIONS

Terms of Reference

Terms of reference

Audit review of the applications is required for the following systems:
SOCPEN and Special Covid-19 Social Relief of Distress R350 grant systems (ICT Security, Applications and General Controls Reviews)

Background
SASSA is responsible for the administration of social assistance in terms of the Social Assistance Act 2004. SASSA has since its establishment focused primarily on the administration of the social assistance programme which is fully funded by government.

Define the applications:
SOCPEN system is the Social Pensions System that is developed and maintained by SASSA for the registration and payment of grants in terms of the Social Assistance Act, 2004. The system stores and maintains records of active and inactive beneficiaries.

Baseline for number of grants in payments including Grant in Aid in 2022/23 financial year were 18 931 854 at a cost of R204 295 billion.

The Agency processes approximately 1, 2 million new grant applications every financial year through SOCPEN system.

SASSA is responsible for the administration of social assistance in terms of the Social Assistance Act 2004. SASSA has since its establishment focused primarily on the administration of the social assistance programme which is fully funded by government. SASSA serves a customer base including older persons, people with disabilities, and people in distress through the following grant types:

- Old Age Grant (OAG): Grant given to persons 60 years and older.
- Disability Grant (DG): Grant for persons with disability between 18 to 59 years.
- War Veterans' Grant (WVG): Grant awarded to veterans of the Second World War or the Korean War.

- Grant-in-Aid (GIA): Grant for both disabled and older people who require assistance with activities of daily living.
- Foster Child Grant (FCG): Grant for children in need of protection and placed in foster care. The grant can be extended up to the age of 21 on condition that the child is still studying.
- Child Support Grant (CSG): Grant for children 0 to 18 years.
- Care Dependency Grant (CDG): Grant awarded to care givers of children who are severely disabled and require permanent care and support services.
- Social Relief of Distress (SRD): Grant for temporary assistance for a maximum of three months, or extended to six, in stipulated situations of destitution and hardship.

The application process for Special Covid-19 Social Relief of Distress R350 grant, is entirely electronic. The measures applicable include multiple channels such as: **SASSA Special Covid-19 SRD Process**

- sending a WhatsApp message to 082 046 8553;
- sending an E-mail to SRD@sassa.gov.za;
- the USSD platform – number *134*7737#;
- the website – https://srd.sassa.gov.za;

The above channels were available during the first phase of the Special Covid-19 Social Relief of Distress R350 grant (May 2020 to April 2021). During the second phase (August 2021 to March 2022) the following channels are in place:

- GovChat platforms
- WhatsApp message to 082 046 8553;
- Facebook messenger
- GovChat.App (https://govchat.app)
- The website – https://srd.sassa.gov.za;

Technical details of systems

Name of business application	Version/ Technical details
SOCPEN	Natural ADABAS. Mainframe operating system ☐ Z/OS -version V1.12 ☐ RACF version 1.12 Complete version 6.7.1 Natural Security version 4.2.3 AOS -version 8.2.2
SRD 350 online application	Web applications developed in Angular. Consist of web server-ngix Application server-web logic Api gateway-krakend database-oracle OS-Linux

2. The service provider to perform the internal audit reviews as follows:

2.1 Applications and general controls review (SOCPEN/ SRD 350).

2.2 IT security review.

Type of review	Scope
2.1 Applications review specifics for SOCPEN/ SRDC	• Input controls • Processing controls • Output controls • Integrity controls • Audit trails • Logical access controls over infrastructure, applications, and data • System development life cycle controls • Program change management controls • Physical security controls over the data center • System and data backup and recovery controls • Computer operation controls
2.2 IT security review	• Assessment of the IT security environment/ overall security posture to identify gaps and provide for implementation of the remedial actions • Vulnerability and penetrations tests – evaluation of firewalls, encryption protocols and related security measures.

Time-frames

Two (2) months

Queries:

EVALUATION CRITERIA

Proposals will be evaluated in accordance with the 80/20 preference point system, as contemplated in the Preferential Procurement Policy Framework Act (Act 5 of 2000). The evaluation shall be conducted as follows:

Stage 1:

➢ **Phase 1: Mandatory Compliance**

➢ **Phase 2: Administrative Compliance**

➢ **Phase 3: Functionality Compliance**

Stage 2:

➢ **Phase 1: Price and Specific Goals**

STAGE 1: PHASE 1 – MANDATORY COMPLIANCE

Mandatory documents (if not attached to the proposal, bidder will be disqualified):

- **Copies of certifications to be attached (any one of the following); Certified Information Systems Auditor (CISA), or Certified Ethical Hacker (CEH), or Certified Information Systems Security Personnel (CISSP).**

STAGE 1: PHASE 2 – ADMINISTRATIVE COMPLIANCE

The bidder must submit the following:

➢ **Fully completed and signed standard bidding documents (SBD Forms)**

➢ **SARS Tax Compliance Status Pin.**

➢ **Proof of Registration with Central Supplier Database(CSD)**

STAGE1: PHASE 3: FUNCTIONALITY COMPLIANCE

Only bidders who score a minimum of 70% points on functionality will be evaluated further.

#	Functionality evaluation criteria	Weight	Scoring criteria
1	**Experience** **(Annexure B to be completed for ease reference)** **Demonstrate experience of similar work undertaken over the last five years.** **References from clients with latest contact details for verification purpose – minimum of three contactable clients:** **3 letters - Applications review** **The reference letters signed by the client should cover the following: scope of work undertaken, name of the application reviewed (for applications), date the review undertaken and duration of the project at minimum.**	**20**	**1= No response** **2 = 2 references provided** **3 = 3 references provided** **4 = 4 references provided** **5 = 5 or more references provided**
2	**(Annexure B to be completed for ease reference)** **Demonstrate experience of similar work undertaken over the last five years.**	**20**	**1= No response** **2 = 2 references provided** **3 = 3 references provided** **4 = 4 references provided**

#	Functionality evaluation criteria	Weight	Scoring criteria
	References from clients with latest contact details for verification purpose – minimum of three contactable clients: **3 letters - IT Security Assessment** **The reference letters signed by the client should cover the following: scope of work undertaken, name of the application reviewed (for applications), date the review undertaken and duration of the project at minimum.**		**5 = 5 or more references provided**
3	**Methodology/ approach** **Approach or methodology to be applied when conducting application and IT security (systems to be used for both applications and security reviews):** • **Applications controls** • **IT Security review** *NB: All methodologies must be detailed with supporting approach or standards that will be used.* *List various standards to be used and the types of toolkits for both scope.*	**10**	**1 = no response** **2 – only one methodology submitted (Addressing one area of scope .i.e Applications)** **3 – methodology for both areas of scope (Applications/ ICT security)** **4 – standards to be used referenced for various phases** **5 – systems/ software to be deployed clearly stated on the methodology**

#	Functionality evaluation criteria	Weight	Scoring criteria
4	**Project plan** **Project plan covering the scope for each review, it should entail the following:** 1. **Work breakdown structures** 2. **Timing** 3. **Resources** 4. **Deliverables**	**10**	**1 = no project plan** **2 = covers only 1 element** **3 = covers only 2 elements** **4 = covers only 3 elements** **5 = covers all elements**
5	**Resources/ qualifications** **Comprehensive CVs of the project team to carry out the work to be provided with detailed experience and qualifications.** **Project Leader:** **(Annexure A to be completed for ease reference)** **The CV should reflect the following:** 1. **Minimum 10 years' experience in IT working environment – related to applications and IT security reviews (at least 5 yrs senior management level).** 2. **NQF level 7 tertiary qualification (IT studies and relevant**	**20**	**1 = below 5 years (including below 3 years senior management experience)** **2 = above 5 years and below 10yrs (above 3 years however less than 5 years senior management)** **3 = covers 1 – 3 satisfactory** **10 years and above but below 15 (including 5 years senior management)**

#	Functionality evaluation criteria	Weight	Scoring criteria
	to applications and IT security reviews) 3. **Working experience – area of competence (previous work undertaken including organizations/ clients)** 4. **Relevant IT certifications**		**4 = 15 years and above below 20 (including above 5 years senior management)** **5 = 20 years (including 10 years and above senior management – including certifications; CISA, or CEH, or CISSP)**
6	**Comprehensive CVs of the project team to carry out the work to be provided with detailed experience and qualifications.** *Project team members (minimum of 3 resources):* **(Annexure A to be completed for ease reference)** **The CV should reflect the following:** 1. **Minimum 5 years' experience in IT working environment – related to applications and IT security reviews.** 2. **NQF level 6 tertiary qualification (IT studies and relevant**	20	**1 = below 3 years' experience** **2 = below 5 years but above 3 years** **3 = 5 years' experience** **4 = above 5 years and below 7** **5 = above 7 years (including certifications, i.e. CISA,or Ethical Hacker and others.**

#	Functionality evaluation criteria	Weight	Scoring criteria
	to applications and IT security reviews) 3. **Working experience – area of competence (previous work undertaken including organizations/ clients)** 4. **Relevant IT certifications**		

STAGE 2: PHASE 1: PRICE AND SPECIFIC GOALS

Price and Preference point system	100
Price	80
Specific Goals	20

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 must 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 must submit a B-BBEE verification certificate from a verification agency accredited by the South African National Accreditation System (SANAS) or certified copies thereof and/or a CSD MAAA number and/or a sworn affidavit indicating the percentage of ownership of all shareholders and/or owners and signed by the commissioner of oaths.

➢ Failure to submit the required documents shall be interpreted to mean that preference points for specific goals are not claimed.

Reference forms (Annexure B):

Application review:

Client/ Organization	Scope of work - *indicate the name of the applications reviewed	Date of the review	Contact person and designation (Official E-mail)

IT Security assessment:

Client/ Organization	Scope of work	Date of the review	Contact person and designation (Official E-mail)

Project Leader – Experience and qualifications (Annexure A)

Name	Title/ Designation	Qualification *indicate NQF level/ Certifications	Experience in years (indicate the total experience, highlight senior management experience. i.e. Total working experience 12 and 5 as a senior manager,	Areas of competence or work experience (separate IT security assessment and applications review.	Organisations/ Clients

Project team: Experience and qualifications (Annexure A)

Name	Title/ Designation	Qualification *indicate NQF	Experience in years	Areas of competence or work	Organisations/ Clients

		level/ Certifications		experience (separate IT security assessment and applications review.	