PART A
INVITATION TO BID

YOU ARE HEREBY INVITED TO BID FOR REQUIREMENTS OF THE COMMUNITY SCHEMES OMBUD SERVICE					
BID NUMBER:	**RFQ040-2026-27**	CLOSING DATE: **02 December 2026**		CLOSING TIME:	**12h00**
DESCRIPTION	**THE APPOINTMENT OF A SERVICE PROVIDER FOR A MANAGED SECURITY OPERATIONS CENTRE AS A SERVICE (SOCaaS), INCLUDING THE SIEM PLATFORM AND LICENSING, FOR A PERIOD OF TWELVE (12) MONTHS**				
BID RESPONSE DOCUMENTS MAY BE EMAILED TO THE BELOW *(EMAIL ADDRESS)*					
quotations3@csos.org.za					

BIDDING PROCEDURE ENQUIRIES MAY BE DIRECTED TO		**TECHNICAL ENQUIRIES MAY BE DIRECTED TO:**	
CONTACT PERSON	**Jabulile Sithole**	CONTACT PERSON	**Nonyameko Ngxeke**
TELEPHONE NUMBER	**(010) 593 0533/ 066 302 5937**	TELEPHONE NUMBER	**(010)593 0533/ 073 764 7629**
FACSIMILE NUMBER		FACSIMILE NUMBER	
E-MAIL ADDRESS	quotations3@csos.org.za	E-MAIL ADDRESS	Nonyameko.Ngxeke@csos.org.za

SUPPLIER INFORMATION					
NAME OF BIDDER					
POSTAL ADDRESS					
STREET ADDRESS					
TELEPHONE NUMBER	CODE		NUMBER		
CELLPHONE NUMBER					
FACSIMILE NUMBER	CODE		NUMBER		
E-MAIL ADDRESS					
VAT REGISTRATION NUMBER					
SUPPLIER COMPLIANCE STATUS	TAX COMPLIANCE SYSTEM PIN:		**OR**	CENTRAL SUPPLIER DATABASE No:	MAAA
B-BBEE STATUS LEVEL VERIFICATION CERTIFICATE	TICK APPLICABLE BOX] ☐ Yes ☐ No		B-BBEE STATUS LEVEL SWORN AFFIDAVIT	[TICK APPLICABLE BOX] ☐ Yes ☐ No	

[A DETIALED CSD REPORT REFLECTING EME OR QSE 51% OR MORE BLACK OWNERSHIP FOR AT LEAST ONE OF THE DESIGNATED GROUPS MUST BE SUBMITTED IN ORDER TO QUALIFY FOR PREFERENCE POINTS FOR SPECIFIC GOALS]

ARE YOU THE ACCREDITED REPRESENTATIVE IN SOUTH AFRICA FOR THE GOODS /SERVICES /WORKS OFFERED?	☐Yes ☐No [IF YES ENCLOSE PROOF]	ARE YOU A FOREIGN BASED SUPPLIER FOR **THE GOODS /SERVICES /WORKS OFFERED?**	☐Yes ☐No [IF YES, ANSWER PART B:3]

QUESTIONNAIRE TO BIDDING FOREIGN SUPPLIERS

IS THE ENTITY A RESIDENT OF THE REPUBLIC OF SOUTH AFRICA (RSA)? ☐
YES ☐ NO

DOES THE ENTITY HAVE A BRANCH IN THE RSA? ☐
YES ☐ NO

DOES THE ENTITY HAVE A PERMANENT ESTABLISHMENT IN THE RSA?
☐ YES ☐ NO

DOES THE ENTITY HAVE ANY SOURCE OF INCOME IN THE RSA?
☐ YES ☐ NO

IS THE ENTITY LIABLE IN THE RSA FOR ANY FORM OF TAXATION? ☐
YES ☐ NO

IF THE ANSWER IS "NO" TO ALL OF THE ABOVE, THEN IT IS NOT A REQUIREMENT TO REGISTER FOR A TAX COMPLIANCE STATUS SYSTEM PIN CODE FROM THE SOUTH AFRICAN REVENUE SERVICE (SARS) AND IF NOT REGISTER AS PER 2.3 BELOW.

PART B
TERMS AND CONDITIONS FOR BIDDING

1. BID SUBMISSION:
1.1. BIDS MUST BE DELIVERED BY THE STIPULATED TIME TO THE CORRECT ADDRESS. LATE BIDS WILL NOT BE ACCEPTED FOR CONSIDERATION.
1.2. **ALL BIDS MUST BE SUBMITTED ON THE OFFICIAL FORMS PROVIDED– (NOT TO BE RE-TYPED) OR IN THE MANNER PRESCRIBED IN THE BID DOCUMENT.**
1.3. THIS BID IS SUBJECT TO THE PREFERENTIAL PROCUREMENT POLICY FRAMEWORK ACT, 2000 AND THE PREFERENTIAL PROCUREMENT REGULATIONS, 2022 THE GENERAL CONDITIONS OF CONTRACT (GCC) AND, IF APPLICABLE, ANY OTHER SPECIAL CONDITIONS OF CONTRACT.
1.4. **THE SUCCESSFUL BIDDER WILL BE REQUIRED TO FILL IN AND SIGN A WRITTEN CONTRACT FORM (SBD7).**
2. TAX COMPLIANCE REQUIREMENTS
2.1 BIDDERS MUST ENSURE COMPLIANCE WITH THEIR TAX OBLIGATIONS.
2.2 BIDDERS ARE REQUIRED TO SUBMIT THEIR UNIQUE PERSONAL IDENTIFICATION NUMBER (PIN) ISSUED BY SARS TO ENABLE THE ORGAN OF STATE TO VERIFY THE TAXPAYER'S PROFILE AND TAX STATUS.
2.3 APPLICATION FOR TAX COMPLIANCE STATUS (TCS) PIN MAY BE MADE VIA E-FILING THROUGH THE SARS WEBSITE WWW.SARS.GOV.ZA.
2.4 BIDDERS MAY ALSO SUBMIT A PRINTED TCS CERTIFICATE TOGETHER WITH THE BID.
2.5 IN BIDS WHERE CONSORTIA / JOINT VENTURES / SUB-CONTRACTORS ARE INVOLVED; EACH PARTY MUST SUBMIT A SEPARATE TCS CERTIFICATE / PIN / CSD NUMBER.
2.6 WHERE NO TCS IS AVAILABLE BUT THE BIDDER IS REGISTERED ON THE CENTRAL SUPPLIER DATABASE (CSD), A CSD NUMBER MUST BE PROVIDED.
2.7 NO BIDS WILL BE CONSIDERED FROM PERSONS IN THE SERVICE OF THE STATE, COMPANIES WITH DIRECTORS WHO ARE PERSONS IN THE SERVICE OF THE STATE, OR CLOSE CORPORATIONS WITH MEMBERS PERSONS IN THE SERVICE OF THE STATE."

NB: FAILURE TO PROVIDE / OR COMPLY WITH ANY OF THE ABOVE PARTICULARS MAY RENDER THE BID INVALID.

SIGNATURE OF BIDDER: ……

CAPACITY UNDER WHICH THIS BID IS SIGNED: ……
(Proof of authority must be submitted e.g., company resolution)

DATE: ……...

Community Schemes Ombud Service

Affordable Reliable Justice

REQUEST FOR QUOTATION (RFQ)

THE APPOINTMENT OF A SERVICE PROVIDER FOR A MANAGED SECURITY OPERATIONS CENTRE AS A SERVICE (SOCaaS), INCLUDING THE SIEM PLATFORM AND LICENSING, FOR A PERIOD OF TWELVE (12) MONTHS

NOVEMBER 2026

Table of Contents

1. TERMS AND CONDITIONS 3
2. INTRODUCTION 5
3. PURPOSE OF THIS REQUEST FOR QUOTATION (RFQ) 6
4. CSOS OVERVIEW 7
5. SCOPE OF WORK 9
6. SERVICE LEVELS 12
7. DATA PROTECTION, POPIA COMPLIANCE AND DATA RESIDENCY 12
8. SUPPLY CHAIN MANAGEMENT COMPLIANCE REQUIREMENTS 13
9. MANDATORY REQUIREMENTS 13
10. EVALUATION 14
11. FUNCTIONALITY 15
12. PRICE & SPECIFIC GOALS 20
13. TIMELINE OF THE BID PROCESS 22
14. DURATION OF THE CONTRACT 22
15. PROJECT MANAGEMENT RESPONSIBILITY 22
16. SUPPLIER DUE DILIGENCE 22
17. RESPONSE FORMAT (SUBMISSION OF PROPOSALS) 23
18. LATE BIDS 23
19. COUNTER CONDITIONS 23
20. FRONTING 23
21. COMMUNICATION AND CONTACT DETAILS 24
22. PROPOSAL SUBMISSION REQUIREMENTS 25
23. SUBMISSION OF PROPOSALS 25

1. TERMS AND CONDITIONS

THIS REQUEST FOR QUOTATION (RFQ) HAS BEEN COMPILED BY THE CSOS AND IS MADE AVAILABLE TO BIDDERS SUBJECT TO THE FOLLOWING TERMS AND CONDITIONS, WHICH BIDDERS ARE DEEMED TO ACKNOWLEDGE AND ACCEPT:

1.1. A Bid submitted in response to this RFQ will constitute a binding offer that will remain binding and irrevocable for a period of ninety (90) days from the closing date.

1.2. Unless or until a binding contract is concluded between the CSOS and the successful Bidder, the offer constituted by the Bid will be deemed not to have been accepted and no agreement will be deemed to be reached with any Bidder.

1.3. The CSOS reserves the right to amend, modify, withdraw or terminate this RFQ or any of the requirements set out herein at any time (and from time to time), without prior notice and without liability to compensate or reimburse any Bidder or person.

1.4. Should this RFQ be amended, the CSOS undertakes to publicise or send each Bidder in writing the amended RFQ. No oral amendments by the Bidder or the CSOS shall be considered.

1.5. It is compulsory for a Bidder submitting a bid to be registered on the National Treasury's Central Supplier Database ("the CSD") and ensure that it remains registered for the duration of the services and/or contract, if successful.

1.6. The Bidder needs to ensure that it is tax compliant at the time of submitting its Bid and remains tax compliant for the duration of the contract and/or services, if successful, and undertakes to provide supporting documentation or tax compliance status confirmation issued by the South African Revenue Service ("SARS") upon request by the CSOS.

1.7. The CSOS reserves the right to conduct site inspections, including of the Bidder's Security Operations Centre, or call for additional supporting documentation to confirm any information provided by a Bidder in its response to this Bid.

1.8. This RFQ is not intended to form the basis of a decision to enter into any transaction with the CSOS and does not constitute an offer or recommendation to enter into such transaction, or an intention to enter into any legal relationship with any person.

1.9. Neither the CSOS nor any of its directors, officers, employees, agents, representatives or advisors will assume any responsibility for any costs or expenses incurred by any party in or associated with preparing or submitting a Bid in response to this RFQ.

1.10. No entity or associated entities may be involved, whether directly or indirectly, in more than one Bid in response to this RFQ. Failure to comply with this requirement may, within the sole discretion of the CSOS, result in disqualification of both entities.

1.11. Any material changes in the control and/or composition of any Bidder or any core member of a Bidder after submission of a Bid must be brought to the attention of the CSOS Supply Chain Management ("SCM") Section in writing. The CSOS shall be the sole arbiter as to what constitutes a material change and may in its sole discretion disqualify the Bidder from any further participation in the bid process.

1.12. Any requirement set out in this RFQ which stipulates the form and/or content of any aspect of a Bid is stipulated for the sole benefit of the CSOS, and unless the contrary is expressed by the CSOS, may be waived by the CSOS in its sole discretion at any stage in the bid process.

1.13. The CSOS and its advisors shall rely on a Bid as being accurate and complete in relation to the information and proposals provided therein by the Bidders.

1.14. All Bids submitted to the CSOS shall become the property of the CSOS and will not be returned to the Bidders. The CSOS will make all reasonable efforts to keep the information contained in proposals confidential.

1.15. A Bid submitted by the Bidder shall be considered non-responsive if it shows any omissions or irregularities of any kind. However, the CSOS reserves the right to waive any aspect of non-responsiveness and to make an award in the best interest of the organisation, provided that any such waiver shall be applied consistently across all Bidders.

1.16. The CSOS reserves the right to accept or reject in part or in whole any submitted Bid.

1.17. The CSOS reserves the right to require a Bidder to provide a formal presentation and demonstration of its proposal at a date and time to be determined by the CSOS. The CSOS shall provide adequate instructions regarding the purpose and scope of the presentation. All expenses shall be borne by the Bidder.

1.18. In this RFQ, the words "service provider" and "supplier" will be used interchangeably to refer to the Bidder.

1.19. All costs associated with the preparation and submission of the Bid remain the responsibility of the Bidder. The costs shall not be chargeable to the CSOS by the successful or unsuccessful Bidder.

1.20. All Bids must be formulated and submitted in accordance with the requirements of this RFQ.

1.21. Bids received after the closing date and time as specified in this RFQ shall be rejected.

1.22. The CSOS is not obliged to appoint a bidder with the lowest price if, based on its sole discretion and assessment, the said bidder does not exhibit or demonstrate adequate capacity or full comprehension of the scope of work to be undertaken. In this regard, the CSOS may appoint the lower-ranked bidder provided that the reasons for such deviation are properly justified and accurately recorded.

2. INTRODUCTION

MANDATE OF THE CSOS

2.1. The Community Schemes Ombud Service (CSOS) is established in terms of the Community Schemes Ombud Service Act, 2011 (Act No. 9 of 2011), to regulate the conduct of parties within community schemes and to ensure good governance within community schemes. To deliver on its mandate, key amongst the priorities of the organisation is to:

2.1.1. Provide an alternative dispute resolution service;

2.1.2. Regulate, monitor and quality assure all community schemes governance documentation;

2.1.3. Provide training for conciliators, adjudicators and other employees of the CSOS;

2.1.4. Act as custodian of, preserve and provide public access (electronically or by other means) to scheme governance documentation;

2.1.5. Promote good governance of community schemes;

2.1.6. Provide education, information, documentation and other such services as may be required to raise awareness among owners, occupiers, executive committees and other persons or entities who have rights and obligations in community schemes;

2.1.7. Monitor community schemes governance; and

2.1.8. Deal with any matters as may be necessary to give effect to the objectives of the CSOS Act.

2.2. To deliver on its mandate, the CSOS depends on secure and available ICT systems that hold the personal information of community scheme members, owners, trustees and other stakeholders. The protection of these systems and this information is required by the Protection of Personal Information Act, 2013 (POPIA), and by the CSOS Information and Cyber Security Policy.

3. PURPOSE OF THIS REQUEST FOR QUOTATION (RFQ)

3.1. The purpose of this RFQ is to appoint a reputable, South African-based service provider to provide a managed Security Operations Centre as a Service (SOCaaS) to the CSOS for a period of twelve (12) months, using a mature, industry-recognised SIEM platform, with all CSOS data hosted and processed in South Africa in compliance with POPIA.

3.2. The CSOS requires a managed SOC service that provides 24/7 monitoring, threat detection, threat intelligence and incident response for the CSOS ICT environment, using a Security Information and Event Management (SIEM) platform provided and operated by the service provider.

3.3. This RFQ is **technology neutral**. Bidders may propose any SIEM platform and SOC service that meets the requirements of this RFQ. No preference will be given to any product, vendor or existing arrangement, and Bids will be evaluated only against the requirements and criteria in this RFQ.

3.4. This RFQ is for a twelve (12) month contract.

3.5. The service will be an extension of the ICT unit under the IT Risk and Governance section. The service provider will proactively monitor security components in the CSOS environment, both on-premises and in the cloud, and perform security functions to maintain information security.

4. CSOS OVERVIEW

4.1. OFFICES AND USERS

Office	Address	Users
Head Office and Gauteng regional office	Die Anker Building, 1279 Mike Crawford Street, Centurion, 0169	166
Western Cape regional office	8th Floor, Constitution House, 124 Adderley Street, Cape Town	31
KwaZulu-Natal regional office	7th Floor, Aquasky Towers, 275 Anton Lembede Street, Durban	31
Gqeberha satellite office	3rd Floor, Fairview Office Park, Regus Building, 66 Ring Road, Greenacres	1
Polokwane satellite office	Office C6, Standard Bank Square, Building 5, Schoeman Street	2
George satellite office	14 CJ Langenhoven Road, George Central	1

All employees are provided with tools of trade for remote working and can access internally hosted applications remotely. The CSOS intends to expand its regional presence.

4.2. ICT ENVIRONMENT

4.2.1. The CSOS operates a Microsoft-based environment, with on-premises directory services and cloud identity services, across its Head Office and regional offices.

4.2.2. Server infrastructure is largely virtualised, with a small number of physical servers.

4.2.3. The offices are connected through a wide area network, with each internet breakout protected by a next-generation firewall.

4.2.4. Email and productivity services are cloud-based and protected by a cloud email security gateway. Endpoints are protected by an enterprise endpoint protection platform.

4.2.5. The CSOS business applications include a case management platform, an ERP system and database servers.

4.2.6. Detailed technical information, including product names, versions and network diagrams, is not published in this RFQ. It will be made available only to Bidders who sign the CSOS confidentiality undertaking, as set out in paragraph 4.4.

4.3. MONITORING SCOPE AND SIZING

4.3.1. The solution must monitor, as a minimum, the following log sources:

Log source	Quantity / indication
Next-generation firewalls (all internet breakouts)	All sites
Domain controllers (directory services)	All domain controllers
Servers (virtual and physical)	Approximately 30
Workstations and laptops	Approximately 240
Cloud productivity suite and cloud identity platform (sign-in and audit logs)	Tenant
Cloud email security gateway	Tenant
Endpoint protection platform management console	1
Critical application and database servers, including file integrity monitoring	At least 5

4.3.2. The CSOS environment generates approximately 9.8 million log records a day. Bidders must size the solution for an ingestion capacity of at least **15 GB per day**, with headroom for growth of at least 20% over the contract period and must state the capacity on which their price is based.

4.4. CONFIDENTIAL TECHNICAL INFORMATION

4.4.1. To protect the security of the CSOS environment, detailed technical information (including product names and versions, network diagrams, and the number and location of security devices) will be provided only to Bidders who request it in writing from the SCM contact in section 21 by **27 November 2026** and sign the CSOS confidentiality undertaking.

4.4.2. The same information will be provided to all Bidders who comply with paragraph 4.4.1. Bidders may prepare and submit a Bid on the basis of the information in this RFQ alone.

4.4.3. The information may be used only to prepare a Bid in response to this RFQ. It may not be published, shared with any third party (other than subcontractors bound by the same undertaking), or used for any other purpose, and must be returned or destroyed after the award.

4.4.4. Any breach of the confidentiality undertaking will result in disqualification and may lead to legal action and restriction from doing business with the public sector.

5. SCOPE OF WORK

5.1. SIEM PLATFORM AND LICENSING

5.1.1. Provide, host and operate a SIEM platform, with all licences required for the twelve (12) month contract period included in the price. The position of the platform in the most recent Gartner Magic Quadrant for SIEM will be scored under functionality (section 11).

5.1.2. Retain all CSOS log data so that it is searchable online for at least ninety (90) days and retained for at least twelve (12) months, to support investigations, audits and regulatory requests.

5.1.3. Host and process all CSOS log data, backups and analytics within the Republic of South Africa (section 7).

5.1.4. Provide OEM-backed support and escalation for the platform, and keep the platform patched and on a version supported by the OEM.

5.1.5. Give up to four (4) CSOS officials secure, web-based access to the platform, dashboards and reports, protected by multi-factor authentication.

5.2. ONBOARDING AND DEPLOYMENT

5.2.1. Complete onboarding of all log sources in paragraph 4.3 within thirty (30) days of signature of the Service Level Agreement (SLA), according to a detailed project plan approved by the CSOS.

5.2.2. Deploy all collectors, agents and integrations required, and coordinate with the CSOS ICT team so that full 24/7 monitoring is in place from the service commencement date, confirmed in writing by the CSOS at go-live.

5.2.3. Configure the detection rules and reports set out in paragraph 5.5 before the go-live date.

5.3. 24/7 MONITORING AND DETECTION

5.3.1. Provide 24/7/365 real-time monitoring of all integrated log sources from the Bidder’s Security Operations Centre physically located in South Africa (this will be

a condition of the service level agreement). No part of the monitoring, analysis or incident response may be performed from outside South Africa.

5.3.2. Correlate events continuously, raise alerts using SIEM analytics, behaviour analytics and use-case-driven rules, and filter and prioritise alerts to reduce false positives.

5.3.3. Report monthly on Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) against the service levels in section 6.

5.4. INCIDENT RESPONSE AND MANAGEMENT

5.4.1. Provide full incident response as part of the service, at no additional charge, covering triage and classification (Critical, High, Medium, Low), investigation, containment, eradication, recovery, root cause analysis, forensic support and post-incident reporting.

5.4.2. Coordinate with the CSOS ICT team and third-party providers during incidents, and be directly available to the CSOS during major incidents.

5.4.3. Assist the CSOS with the information it needs to notify the Information Regulator and affected data subjects of security compromises in terms of section 22 of POPIA.

5.5. THREAT INTELLIGENCE, THREAT HUNTING AND USE-CASE MANAGEMENT

5.5.1. Integrate internal and external threat intelligence feeds, and carry out continuous, expert-led threat hunting across the cyber kill chain.

5.5.2. Maintain and tune detection rules, and develop custom use cases aligned to CSOS risks. As a minimum, alert on privileged account and group changes, use of built-in administrator accounts, repeated account lockouts, out-of-hours administrator activity, firewall configuration changes and failed firewall configuration backups.

5.5.3. Provide file integrity monitoring on the critical application servers listed in paragraph 4.3.

5.6. ENDPOINT INTEGRATION

5.6.1. Integrate the CSOS endpoint protection platform as a log source. Bidders may offer managed endpoint detection and response (EDR) as an **optional** item in the

pricing schedule. Optional items will not be included in the price evaluation, and the CSOS is under no obligation to procure them.

5.7. VULNERABILITY MANAGEMENT

5.7.1. Carry out monthly vulnerability scans of internal and internet-facing CSOS assets, prioritise findings by risk, and track remediation in the monthly report.

5.8. PLATFORM MAINTENANCE AND OPERATIONS

5.8.1. Monitor platform health and log source status, manage patches and releases, back up the platform and its configuration, and maintain high availability and resilience.

5.9. REPORTING

5.9.1. Provide daily alerts and summaries, weekly reports and a monthly SOC performance report by the seventh (7th) working day of each month, covering incidents and trends, log source status, service level performance, vulnerabilities, risk posture and recommendations.

5.9.2. Provide incident and forensic reports, threat intelligence briefings and platform health reports, and attend a monthly service review meeting with the CSOS.

5.10. SERVICE DESK, KNOWLEDGE TRANSFER AND TRAINING

5.10.1. Provide 24/7 support by telephone, email and a ticketing system, with escalation to senior analysts and the OEM.

5.10.2. Provide hands-on training and knowledge transfer to the CSOS ICT team, including periodic co-working at the SOC, and deliver operational and administrative documentation.

5.11. EXIT MANAGEMENT AND DATA PORTABILITY

5.11.1. On expiry or termination of the contract, co-operate with the CSOS and any new service provider for up to three (3) months to ensure an orderly handover.

5.11.2. Return to the CSOS, in a standard, non-proprietary format (for example CSV, JSON or syslog), all CSOS log data retained on the platform, together with the detection rules, use cases and reports configured for the CSOS, and thereafter securely destroy all CSOS data and provide a certificate of destruction.

6. SERVICE LEVELS

6.1. The following minimum service levels will be included in the SLA. Bidders may propose better service levels.

Severity	Notification to CSOS after detection	Response and containment action
Critical	Within 15 minutes, by telephone and email	Response started within 30 minutes; containment within 4 hours
High	Within 30 minutes	Response started within 2 hours
Medium	Within 4 hours	Next business day
Low	In the daily summary	Within 5 business days

6.2. The SIEM platform and SOC service must be available at least 99.5% of each month, excluding planned maintenance agreed in advance with the CSOS. Failure to meet service levels will attract penalties in terms of the SLA.

7. DATA PROTECTION, POPIA COMPLIANCE AND DATA RESIDENCY

7.1. The service provider will process personal information on behalf of the CSOS and will be an **operator** as defined in section 1 of POPIA. The successful Bidder must sign a written operator agreement with the CSOS in terms of section 21 of POPIA, as part of the SLA.

7.2. The service provider must process CSOS information only with the knowledge or authorisation of the CSOS, treat it as confidential, and apply appropriate, reasonable technical and organisational security measures in terms of section 19 of POPIA.

7.3. **Data residency:** all CSOS log data, backups and analytics must be stored and processed within the Republic of South Africa, in line with the data sovereignty requirements of the CSOS Information and Cyber Security Policy. No CSOS data may be transferred outside South Africa without the prior written consent of the CSOS and compliance with section 72 of POPIA.

7.4. The service provider must notify the CSOS without undue delay, and in any event within twenty-four (24) hours, where there are reasonable grounds to believe that CSOS personal information has been accessed or acquired by an unauthorised person, as required by section 21(2) of POPIA.

7.5. All personnel with access to CSOS systems or data must be employed or contracted in South Africa, must have undergone criminal background checks, and must sign confidentiality undertakings.

7.6. **Key conditions of the service level agreement:** the appointed Bidder will be required, as conditions of the service level agreement, to (a) deliver all monitoring, analysis and incident response from a Security Operations Centre physically located in South Africa, by personnel based in South Africa; (b) host and process all CSOS data within South Africa; (c) conclude an operator agreement with the CSOS in terms of section 21 of POPIA; and (d) comply with paragraph 7.5. Bidders must include in their proposal a signed declaration, on their letterhead, confirming that they accept these conditions without qualification. The CSOS will not conclude a service level agreement that departs from these conditions.

8. SUPPLY CHAIN MANAGEMENT COMPLIANCE REQUIREMENTS

DOCUMENTS REQUIRED	SUBMITTED Y/N
Valid B-BBEE certificate issued by an accredited SANAS verification agency / Sworn Affidavit signed by the EME/QSE representative and attested by a Commissioner of Oath / B-BBEE certificate issued by the Companies and Intellectual Property Commission (CIPC)	
Proof of registration on the National Treasury Central Supplier Database (provide full detailed CSD report)	
Valid tax pin number / Tax compliance letter	
Fully completed SBD Documents (1, 3.3, 4 and 6.1)	

9. MANDATORY REQUIREMENTS

9.1. Bidders must attach the following to be further evaluated. **Failure to comply with any of the mandatory requirements below will result in disqualification, and the Bid will not be evaluated further on functionality.**

NO	MANDATORY REQUIREMENT	SUBSTANTIATION	COMPLY / NOT COMPLY (Y/N)
1.	**OEM authorisation:** the Bidder is the OEM of the proposed SIEM platform, or is authorised by the OEM to supply, implement, operate and support it in South Africa.	Letter from the OEM on its letterhead, dated within six (6) months of the closing date, or a valid partner certificate. This will be verified by the CSOS. The authorisation must remain valid for the full duration of the contract. Where the Bidder is itself the OEM of the proposed platform, it must also attach letters from at least two (2) other organisations confirming that the platform is in current production use at those organisations, with contact details for verification.	
2.	**Data residency:** all CSOS data will be hosted and processed within South Africa (paragraph 7.3).	Signed undertaking, and a high-level solution architecture naming the data centre(s) or cloud region(s) in South Africa where CSOS data will be stored and processed.	
3.	**POPIA compliance:** the Bidder complies with POPIA and will sign an operator agreement in terms of section 21 of POPIA.	Proof of registration of the Bidder's Information Officer with the Information Regulator, and a signed undertaking to conclude an operator agreement with the CSOS.	

10. EVALUATION

10.1. EVALUATION COMMITTEE

10.1.1. Proposals will be reviewed and evaluated by the CSOS Evaluation Committee using the 80/20 preference point system. Bidders may be invited to give written or oral presentations and/or demonstrations, and to participate in interviews with the committee.

10.1.2. Bidders may be requested to submit any additional information required by the CSOS.

10.2. EVALUATION PROCESS OF BIDS RECEIVED

10.2.1. **Stage 1 – Mandatory requirements:** Bids that do not comply with all the mandatory requirements in section 9 will be disqualified.

10.2.2. **Stage 2 – Functionality:** Bids will be evaluated on the functionality criteria in section 11. Only Bidders that achieve a minimum qualifying score of **65%** for functionality will be evaluated further.

10.2.3. **Stage 3 – Price and specific goals:** Bids will be evaluated on the 80/20 preference point system in terms of the Preferential Procurement Regulations, 2022 (section 12).

10.2.4. **Stage 4 – Pre-award due diligence:** Before making an award, the CSOS may conduct due diligence on the highest-ranked Bidder, including (a) a live demonstration of the proposed platform and services against use cases specified by the CSOS, such as the detection of privileged account changes, repeated failed logons and firewall configuration changes, and the production of a monthly service report; and (b) an inspection of the Bidder's Security Operations Centre to verify its location, 24/7 staffing and security controls.

10.2.5. If the Bidder cannot demonstrate the proposed platform and services as described in its bid, or the due diligence shows that information in the bid is materially incorrect, the CSOS may decline to award the contract to that Bidder and may proceed to the next-ranked Bidder.

11. FUNCTIONALITY

11.1. Bids received will be evaluated according to the requirements in the table below. Each criterion is scored from 0 to 5, and the score is converted to the weighting shown.

11.2. Bidders who score **less than 65% out of 100%** on the functionality requirements will be disqualified and will not be considered for further evaluation.

FUNCTIONALITY	REQUIREMENTS AND SCORE QUALIFICATION	WEIGHT	SCORE
Technical solution and methodology	A detailed proposal addressing every area of the scope of work in paragraphs 5.1 to 5.11, the service levels in section 6 and the data protection requirements in section 7. 5 = all areas addressed; 0 = not all areas addressed / no proposal.	30	

THE APPOINTMENT OF A SERVICE PROVIDER FOR A MANAGED SECURITY OPERATIONS CENTRE AS A SERVICE (SOCaaS) FOR A PERIOD OF 12 MONTHS

FUNCTIONALITY	REQUIREMENTS AND SCORE QUALIFICATION	WEIGHT	SCORE
Onboarding and deployment plan	Attach a project plan for onboarding and deployment that addresses all of the following elements: (a) onboarding of all log sources in paragraph 4.3 within thirty (30) days of signature of the SLA, with a timeline showing activities, milestones and dates; (b) the approach to achieving full 24/7 monitoring from the commencement date; (c) the risks to the deployment and the mitigation for each risk; and (d) the resources: the roles of the Bidder's personnel and their responsibilities, and the inputs required from the CSOS. **5 points** = project plan attached and addresses all elements (a) to (d); **0 point** = no project plan attached, or one or more of elements (a) to (d) not addressed.	15	
Experience of the Bidder (public sector)	Reference letters from **public sector clients** confirming managed SOC services delivered by the Bidder within the last five (5) years. Public sector clients are national and provincial departments, municipalities, constitutional institutions, and public entities and state-owned companies listed in the schedules to the PFMA or MFMA. Each letter must be on the client's letterhead, signed by the client, give the name and contact details of the client's representative, and expressly confirm the managed SOC services delivered by the Bidder and the period of delivery. In the absence of a reference letter, the assessment form in paragraph 11.4, completed and signed by the public sector client, will be accepted. Letters from private sector clients, and letters that do not meet these requirements, will not be counted. Five or more reference letters = 5 points Four reference letters = 4 points Three reference letters = 3 points Two reference letters = 2 points One reference letter = 1 point No reference letter attached = 0 point	20	

THE APPOINTMENT OF A SERVICE PROVIDER FOR A MANAGED SECURITY OPERATIONS CENTRE AS A SERVICE (SOCaaS) FOR A PERIOD OF 12 MONTHS

FUNCTIONALITY	REQUIREMENTS AND SCORE QUALIFICATION	WEIGHT	SCORE
Team qualifications	The Bidder must attach a CV and at least one valid certificate (from the list below) for each of the following five (5) key roles: • one (1) SOC manager; • two (2) SOC analysts; • one (1) security engineer; and • one (1) incident responder. A role counts only if a valid certificate from the list below is attached for the person named in that role. **Score:** **5 points=** all five (5) key roles have a listed certificate, and at least two (2) people hold an advanced certificate **4 points =** all five (5) key roles have a listed certificate **3 points =** four (4) key roles have a listed certificate **2 points =** three (3) key roles have a listed certificate **1 point =** one (1) or two (2) key roles have a listed certificate **0 point =** no certificates attached **Certifications that count:** **Advanced (weigh more):** CISSP (Certified Information Systems Security Professional); CISM (Certified Information Security Manager); any GIAC certification (Global Information Assurance Certification); OSCP (Offensive Security Certified Professional); or a certificate from the maker of the proposed SIEM platform marked “Professional” level or higher. **Other relevant:** CompTIA Security+; CompTIA CySA+ (Cybersecurity Analyst); CEH (Certified Ethical Hacker); or a certificate from the maker of the proposed SIEM platform. Certificates must be valid at the closing date. The CSOS may verify certificates with the issuing bodies.	7	

THE APPOINTMENT OF A SERVICE PROVIDER FOR A MANAGED SECURITY OPERATIONS CENTRE AS A SERVICE (SOCaaS) FOR A PERIOD OF 12 MONTHS

FUNCTIONALITY	REQUIREMENTS AND SCORE QUALIFICATION	WEIGHT	SCORE
Team experience	Using the CVs of the five (5) key roles submitted for the team qualifications criterion, count the full years each person has worked in information security, SOC or incident response roles up to the closing date. The CV must show the start and end dates of each position. **Minimum experience per role:** • SOC manager: seven (7) years; • SOC analysts: three (3) years each; • security engineer: five (5) years; and • incident responder: five (5) years. **Score:** **5 points =** all five (5) key roles meet the minimum **4 points =** four (4) key roles meet the minimum **3 points =** three (3) key roles meet the minimum **2 points =** two (2) key roles meet the minimum **1 point =** one (1) key role meets the minimum **0 point =** no key role meets the minimum, or no CVs attached	8	
Gartner Magic Quadrant position	Position of the proposed SIEM platform in the most recent Gartner Magic Quadrant for SIEM published before the closing date. Bidders must attach a copy or licensed reprint of the report, with the page showing the vendor's position. 5 points = Leader 4 points = Challenger 3 points = Visionary 2 points = Niche Player Platform not included in the Gartner Magic Quadrant, or no report submitted = 0 point *Note: a score of 1 does not apply, as the Gartner Magic Quadrant has only four categories.*	10	

FUNCTIONALITY	REQUIREMENTS AND SCORE QUALIFICATION	WEIGHT	SCORE
Information security certification	A valid ISO/IEC 27001 certificate (or SOC 2 Type II report) whose scope covers the Bidder's SOC services. Valid ISO/IEC 27001 certificate, or SOC 2 Type II report, whose scope expressly covers the Bidder's SOC services = 5 point Valid ISO/IEC 27001 certificate for the Bidder whose scope does not expressly mention the SOC services = 4 point SOC 2 Type I report covering the SOC services, or Stage 1 ISO/IEC 27001 certification audit completed by an accredited certification body (proof required) = 3 point Certification audit scheduled with an accredited body (proof required) = 2 point Documented information security management system aligned to ISO/IEC 27001, with no certification activity (signed information security policy and statement of applicability attached) = 1 point None of the above, or no documents attached = 0 point	10	
TOTAL	**Minimum threshold: 65%**	**100**	

11.3. The CSOS may verify reference letters with the clients concerned and may conduct a site visit to the Bidder's Security Operations Centre before award.

11.4. **ASSESSMENT OF BIDDER'S PERFORMANCE BY INDEPENDENT REFERENCE**

(This form must be sent to the Bidder's previous **public sector** clients to give reference to services delivered, as explained in the evaluation criteria, in the absence of a signed reference letter. All assessment forms must be attached to the Bid submission.)

Name of Bidder	
Name of public sector client	
Value of contract	
Date of commencement	
Contract duration	
Contract completion date	

Services provided	Tick
24/7 managed SOC monitoring and detection	
SIEM platform and licensing	
Incident response	
Threat intelligence and threat hunting	
Reporting and service management	

Your assessment of the Contractor's performance (1 = Poor; 5 = Excellent)	1	2	3	4	5
Turn-around times					
Quality of feedback					
Accessibility and availability					
Reliability					
Customer satisfaction					
1 = Poor; 2 = Unsatisfactory; 3 = Average; 4 = Good; 5 = Excellent					

COMMENTS:

Name of person completing this assessment form	
Designation and institution	
Telephone number	
Email address	
Date of assessment	
Signature of official responsible for completing the assessment form	

12. PRICE & SPECIFIC GOALS

12.1. PRICING INSTRUCTIONS

12.1.1. In order to facilitate a transparent selection process that allows equal opportunity to all bidders, Bids will be evaluated in terms of the CSOS Supply Chain Management Policy, using the 80/20 formula (preference point system) for price and specific goals as per the Preferential Procurement Policy Framework Act, the Preferential Procurement Regulations, 2022, and the CSOS Preferential Procurement Policy.

12.1.2. All prices must be in South African Rand, inclusive of VAT, and **firm for the twelve (12) month contract period**, with no escalation.

12.1.3. Bidders must ensure that their prices cover all requirements for a fully operational service as specified in the scope of work, including licences, hosting, onboarding,

deployment, incident response and reporting. Any omissions or errors will be provided at the Bidder's expense.

12.1.4. Services will be invoiced monthly in arrears, after delivery. Payment terms are thirty (30) days from receipt of a valid invoice.

12.2. SPECIFIC GOALS

Specific goal	Substantiation	Points (80/20)
EME or QSE at least 51% owned by black persons who are women, youth, persons living with disability, or military veterans	Full detailed CSD report and B-BBEE certificate / sworn affidavit	17
EME or QSE at least 51% owned by black people living in rural or underdeveloped areas or townships	As above, and proof of address	1
EME or QSE co-operative at least 51% owned by black people	As above, and co-operative registration	1
EME or QSE at least 51% owned by black people in general, with a focus in order of priority on Africans, Indians and Coloureds	As above	1
Total points for specific goals		**20**

12.2.1. Points claimed must be substantiated as indicated in SBD 6.1. Points that are not substantiated will not be awarded, and false claims will result in disqualification and may lead to restriction.

12.3. PRICING SCHEDULE

12.3.1. Bidders must complete the pricing schedule below and attach a detailed quotation on the company letterhead. Only items 1 to 5 will be used for price evaluation.

No.	Description	Qty	Unit price (R)	Total (R)
1	Onboarding and deployment (once-off), as per paragraph 5.2	1		
2	SIEM platform and licensing, sized for a sustained rate of at least 500 EPS (or 20 GB per day where licensed by volume, as per paragraph 4.3.3), including file integrity monitoring for at least 5 servers and retention as per paragraph 5.1.2 – per month	12		
3	24/7 managed SOC service, including incident response, threat hunting and use-case management – per month	12		

No.	Description	Qty	Unit price (R)	Total (R)
4	Vulnerability management service, as per paragraph 5.7 – per month	12		
5	Reporting, service desk and knowledge transfer (if not included in items 2 to 4) – per month	12		
	Subtotal (items 1 to 5)			
	VAT @ 15%			
	Total price for evaluation, including VAT			
6	OPTIONAL (not evaluated): managed EDR – per endpoint, per year	270		
7	OPTIONAL (not evaluated): professional services for work outside the scope – rate per hour	1		

_____ _____

Signature (Bidder) **Date**

13. TIMELINE OF THE BID PROCESS

13.1. The validity period of quotations and the withdrawal of offers, after the closing date and time, is ninety (90) days.

14. DURATION OF THE CONTRACT

14.1. The appointed service provider will be contracted for a period of twelve (12) months from the commencement date in the SLA.

14.2. Onboarding must be completed within thirty (30) days of signature of the SLA, and the Bidder must have the resources to meet this timeframe.

15. PROJECT MANAGEMENT RESPONSIBILITY

15.1. The CSOS Project Manager's responsibilities will include providing the service provider with all appropriate advice and information pertinent to the success of this project, arranging access to systems and key personnel, and assigning CSOS ICT staff to work with the SOC.

15.2. After appointment, the service provider will provide a line-item budget, sign an SLA and an operator agreement, and comply with CSOS policies, procedures and Code of Conduct while working for the CSOS.

16. SUPPLIER DUE DILIGENCE

16.1. The CSOS reserves the right to conduct supplier due diligence prior to final award or at any time during the contract period, including site visits to the Bidder's SOC, confirmation of financial stability and requests for additional information.

17. RESPONSE FORMAT (SUBMISSION OF PROPOSALS)

17.1. The proposals must be submitted in the prescribed format. Standard bidding documents attached to the Terms of Reference must be completed in full. Proposals must be organised in the following sections:

17.1.1. Section 1: SCM compliance documents (section 8);

17.1.2. Section 2: Mandatory requirements 1 to 3, with substantiation (section 9);

17.1.3. Section 3: Functionality – technical solution, onboarding plan, public sector reference letters or assessment forms, team CVs and certificates, Gartner report and ISO/IEC 27001 certificate (section 11);

17.1.4. Section 4: Pricing schedule, detailed quotation and SBD 6.1 (section 12); and

17.1.5. Section 5: Signed declaration of acceptance of the key conditions of the service level agreement (paragraph 7.6).

18. LATE BIDS

18.1. Bids received after the closing date and time will not be accepted for consideration.

19. COUNTER CONDITIONS

19.1. Bidders' attention is drawn to the fact that amendments to any of the Bid Conditions or setting of counter conditions by Bidders or qualifying any Bid Conditions will result in the invalidation of such bids.

20. FRONTING

20.1. Government supports the spirit of Broad-Based Black Economic Empowerment and recognises that real empowerment can only be achieved through individuals and businesses conducting themselves in accordance with the Constitution and in an honest, fair, equitable, transparent and legally compliant manner. Against this background, the Government condemns any form of fronting.

20.2. The Government, in ensuring that bidders conduct themselves in an honest manner, will, as part of the bid evaluation processes, conduct or initiate the necessary enquiries/investigations to determine the accuracy of the representations made in bid

documents. Should any of the fronting indicators contained in the Guidelines on Complex Structures and Transactions and Fronting, issued by the Department of Trade, Industry and Competition, be established during such enquiry/investigation, the onus will be on the Bidder/contractor to prove that fronting does not exist. Failure to do so within fourteen (14) days of notification may invalidate the bid/contract and may also result in the restriction of the Bidder/contractor from conducting business with the public sector for a period not exceeding ten (10) years, in addition to any other remedies the CSOS may have against the Bidder/contractor concerned.

21. COMMUNICATION AND CONTACT DETAILS

21.1. A nominated official of the Bidder(s) can make enquiries in writing to the specified person, Ms Nonyameko Ngxeke, via email: nonyameko.ngxeke@csos.org.za or Tel: 073 764 7629. Further information regarding Supply Chain Management matters can be sent via email to Jabulile.Sithole@csos.org.za & Thokozani.Ntuli@csos.org.za or Tel: 010 593 0533.

21.2. The delegated office of the CSOS may communicate with Bidder(s) where clarity is sought in the bid proposal.

21.3. Any communication to an official or a person acting in an advisory capacity for the CSOS in respect of the bid between the closing date and the award of the bid by the Bidder(s) is discouraged.

21.4. All communication between the Bidder(s) and the CSOS must be done in writing.

21.5. Whilst all due care has been taken in connection with the preparation of this bid, the CSOS makes no representations or warranties that the content of the bid or any information communicated to or provided to Bidder(s) during the bidding process is, or will be, accurate, current or complete. The CSOS, its employees and advisors will not be liable with respect to any information communicated which may not be accurate, current or complete.

21.6. If Bidder(s) find or reasonably believe they have found any discrepancy, ambiguity, error or inconsistency in this bid or any other information provided by the CSOS (other than

minor clerical matters), the Bidder(s) must promptly notify the CSOS in writing, to give the CSOS an opportunity to consider what corrective action is necessary (if any).

21.7. Any actual discrepancy, ambiguity, error or inconsistency in the bid or any other information provided by the CSOS will, if possible, be corrected and provided to all Bidder(s) without attribution to the Bidder(s) who provided the written notice.

21.8. All persons (including Bidder(s)) obtaining or receiving the bid and any other information in connection with the bid or the bidding process must keep the contents of the bid and such information confidential and not disclose or use the information except as required for the purpose of developing a proposal in response to this bid.

22. PROPOSAL SUBMISSION REQUIREMENTS

22.1. The service provider must present CSOS management with a comprehensive proposal and model outlining how it intends to address the CSOS's specific needs, a line-item budget and a detailed project plan.

23. SUBMISSION OF PROPOSALS

23.1. Proposal documents must be submitted by email to [quotations email address] on or before the closing date and time.

23.2. Proposal documents will only be considered if received by the CSOS before **[closing date] at 12h00**.

PRICING SCHEDULE
(Professional Services)

NAME OF BIDDER: ……**BID NO: RFQ040-2026-27: THE APPOINTMENT OF A SERVICE PROVIDER FOR A MANAGED SECURITY OPERATIONS CENTRE AS A SERVICE (SOCaaS), INCLUDING THE SIEM PLATFORM AND LICENSING, FOR A PERIOD OF TWELVE (12) MONTHS**

CLOSING TIME 12h00 am ON 02 December 2026.

OFFER TO BE VALID FOR 90 DAYS FROM THE CLOSING DATE OF BID.

ITEM NO	DESCRIPTION	BID PRICE IN RSA CURRENCY INCLUSIVE OF VALUE ADDED TAX

1. Services must be quoted in accordance with the attached terms of reference.

Total cost of the assignment (R inclusive VAT)

R……

No.	Description	Qty	Unit price (R)	Total (R)
1	Onboarding and deployment (once-off), as per paragraph 5.2	1		
2	SIEM platform and licensing, sized for a sustained rate of at least 500 EPS (or 20 GB per day where licensed by volume, as per paragraph 4.3.3), including file integrity monitoring for at least 5 servers and retention as per paragraph 5.1.2 – per month	12		
3	24/7 managed SOC service, including incident response, threat hunting and use-case management – per month	12		
4	Vulnerability management service, as per paragraph 5.7 – per month	12		
5	Reporting, service desk and knowledge transfer (if not included in items 2 to 4) – per month	12		
	Subtotal (items 1 to 5)			
	VAT @ 15%			
	Total price for evaluation, including VAT			
6	OPTIONAL (not evaluated): managed EDR – per endpoint, per year	270		
7	OPTIONAL (not evaluated): professional services for work outside the scope – rate per hour	1		

Signature (Bidder) **Date**

The financial proposal for this assignment should cover for all assignment activities as per terms of reference

2. Period required for commencement with project after acceptance of bid_____

3 Are the rates quoted firm for the full period? Yes/No

4. If not firm for the full period, provide details of the basis on which Adjustments will be applied for, for example consumer price index.

Technical enquiries regarding bidding procedures may be directed to:
Nonyameko Ngxeke
Tell: 073 764 7629
E-mail address: **Nonyameko.Ngxeke@csos.org.za**

Supply Chain queries may be directed to:
Jabulile Sithole
Tell: (010) 593 0533/ 0663025937
Email: quotations3@csos.org.za
PLEASE REFER TO THE ATTACHED TERMS OF REFERENCE FOR MORE INFORMATION.

BIDDER'S DISCLOSURE

1. PURPOSE OF THE FORM

1.1 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, 1996 (Constitution), and further expressed in the various applicable legislation, it is required for the bidder to make this declaration in respect of the details required hereunder.

1.2 If a person is 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. DECLARATION ON EMPLOYMENT BY ORGAN OF STATE

2.1 Is the bidder, or any of the directors / trustees / shareholders / members / partners of the bidder employed by an organ of state, as defined in section 239 of the Constitution? **YES/NO**

2.2 If YES, furnish particulars of the names, individual identity numbers, in the table below:

Full Name	**Identity Number**	**Name of organ of state**

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.

2.3 Do you, or any person connected with the bidder, have a relationship with any person who is employed by the procuring institution? **YES/NO**

2.3.1 If so, furnish particulars:

……
……
……

2.4 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**

2.4.1 If so, indicate all companies registered in the CSD in the table below:

Supplier registration number (MAAA)	**Status (active/inactive/deleted)**

Failure to disclose all CSD-registered active companies linked to all Directors will lead to disqualification**.**

3 GENERAL DECLARATION

I, ……....., the undersigned, 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 to be false.

3.3 The bidder has arrived at the accompanying bid independently from, and without consultation, communication, agreement or arrangement with any competitor.

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.

3.5 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.

3.6 There have been no consultations, communications, agreements or arrangements made by the bidder with any official of the procuring 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.

3.7 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, 1998 (Act No. 89 of 1998) and or may be referred to law enforcement agencies for criminal investigation and or may be restricted from conducting business with the state for a period not exceeding 10 years in terms of the Prevention and Combating of Corrupt Activities Act, 2004 (Act No. 12 of 2004) or any other applicable legislation.

I CERTIFY THAT THE ABOVE IS CORRECT.

I ACCEPT THAT THE PROCURING INSTITUTION MAY REJECT THE BID OR TAKE APPROPRIATE ACTION AGAINST ME IF THIS DECLARATION IS FALSE.

……	……
Signature	Date
……	……...
Designation	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.

---

1. 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).

1.2 **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) The 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.

2. 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).

3. 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:

80/20 **or** **90/10**

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

Where

Ps = Points scored for price of tender under consideration

Pt = Price of tender under consideration

Pmin = Price of lowest acceptable tender

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:

80/20 **or** **90/10**

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

Where

Ps = Points scored for price of tender under consideration

Pt = Price of tender under consideration

Pmax = Price of highest acceptable tender

4. 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 (80/20 system) (To be completed by the organ of state)	Number of points claimed (80/20 system) (To be completed by the tenderer)
1. EME or QSE owned by 51 % or more black person woman **and/or** ,EME or QSE owned by 51 % or more black person youth **and /or**, EME or QSE owned by 51 % or more black person living with disability **and/or**, EME or QSE owned by 51 % or more black person who is military veteran.	17	
2. EME or QSE owned by 51 % black people living in rural or underdeveloped areas or township.	1	
3. EME or QSE Cooperative owned by 51% or more black people.	1	
4. EME or QSE owned by 51% or more black people in general ,with focus in order of priority on africans, Indians and coloureds.	1	

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: .....

.....

.....

.....