RFP NUMBER:	RFP/SASSETA/24251113
DESCRIPTION:	Appointment of a reputable, suitable and qualified service provider with ICT Security expertise to provide Virtual Chief Information Security Officer (VCISO) and Security Operations Centre (SOC) services from the date of appointment until 31st March 2030
PUBLISH DATE:	06 September 2024
CLOSING DATE:	30 September 2024
CLOSING TIME:	11h00 am
COMPULSORY BRIEFING SESSION DATE	N/A
VALIDITY PERIOD:	120 days from the closing date
PREFERENCE POINT SYSTEM	80/20
BID RESPONSES TO BE SUBMITTED ELECTRONICALLY ONLY	Proposals to be submitted electronically via email vciso@sasseta.org.za Quoting the reference (RFP/SASSETA/24251113)
ATTENTION:	Ms. Lebo Hlombe

The email address vciso@sasseta.org.za is for the submission of tender proposals and will only be accessed by SASSETA after the tender closing date and time.

Queries related to this tender are to be sent to scm01@sasseta.org.za.

If you receive any suspicious calls asking for payment to secure an award of a bid or that the outcome of a tender can be influenced in your favour, please immediately inform the SASSETA Anti-Corruption Hotline at 0800 204 143 for further investigation.

DOCUMENTS IN THIS BID DOCUMENT PACK

Bidders are to ensure that they have received all pages of this document, which consist of thefollowing documents:

SECTION A

1. RFP Submission Conditions and Instructions
2. Terms of Reference
3. Selection Process

SECTION B

1. Invitation to Quote (SBD 1)
2. Pricing Schedule (SBD 3.3)
3. Bidder's Disclosure (SBD 4)
4. Preference Points Claim form in terms of Preferential Procurement Regulations 2022 (SBD 6.1).
5. Submission Checklist
6. General Conditions of Contract (Annexure A)
7. Pricing schedule (Annexure B)

NB.: Bidders are required to return the SASSETA attached Standard Bidding (SBD) forms and not submit SBD forms from other entities.

1. RFP SUBMISSION CONDITIONS AND INSTRUCTIONS

1.1 FRAUD AND CORRUPTION

1.1.1 All Service Providers are to take note of the implications of contravening the Prevention and Combating of Corrupt Activities Act, Act No 12 of 2004 and any other Act applicable.

1.2 COMPULSORY BRIEFING SESSION

1.2.1 There will be no briefing session for this Request forProposal

1.3 CLARIFICATIONS/QUERIES

1.3.1 Any clarification required by a bidder regarding the meaning or interpretation of the Terms of Reference, or any other aspect concerning the bid, is to be requested in writing (e-mail) from **Ms. Lebo Hlombe** at scm01@sasseta.org.za by 12h00 on the **20 September 2024.** The bid **number** should be mentioned in all correspondence. **Telephonic requests forclarification will not be accepted**.

1.4 SUBMITTING BIDS

1.4.1 Proposals to be submitted electronically only via email to:
vciso@sasseta.org.za (**maximum size of the email 30MB)**

1.4.1.1 Bidders are advised to compress their email submission(s) to a maximum of 30MB file/folder**. Any submission(s) exceeding 30MB will be automatically rejected by the server**.
1.4.1.2 Submission(s) that exceed 30MB can be made through the method of, WeTransfer, google drive etc. **Bidders are advised NOT to set expiry date on the submission(s) made**.
1.4.1.3 Bidders are advised to double-check their submission(s) before respondingto the bid.

1.5 **Closing** date and time **30 September 2024 @11h00**

1.6 LATE BIDS

1.6.1 Bids received late shall not be considered. A bid will be considered late if it arrived only one second after 11h00 or any time thereafter. Bids arriving late will not be considered under any circumstances. Bidders are therefore strongly advised to ensure that bids be sent allowing enough time for any unforeseen events that may delay the delivery of the bid.

1.7 PRICING

1.7.1 Service Providers are requested to provide an all-inclusive cost of this project assignment on SBD 3.3

Where the contract requires the successful bidder to travel to a venue different from SASSETA, the following travel and disbursement processeswill be undertaken:

- Claim travel mileage costs applicable to this contract as per the Department of Transport rates
- Book only economy-class flights

- Book Group A hire cars, otherwise Group B are to be used following SASSETA's approval
- Utilise cost-effective mode of transport such as Uber/Taxify/Gautrain or shuttle
- services when traveling to and from the airport.
- Book only Bed and Breakfast, Hotels, or other equivalent accommodations up to a Rand value of R1 400/ per night per person (including dinner, breakfast, and parking).
- Submit all applicable invoices/receipts for the travel undertaken and also, a google map of the trip where travel by private car was undertaken for payment.
- All travel to be approved by SASSETA before being undertaken

1.8 NEGOTIATION

1.8.1 SASSETA has the right to enter into a negotiation with a prospective service provider.

1.8.2 A contract will only be deemed to be concluded when reduced to writing in a contract form signed by the designated responsible person of both parties.

1.9 REASONS FOR REJECTION

1.9.1 SASSETA shall reject a bid for the award of a contract if the recommended bidder has committed a proven corrupt or fraudulent act in competing for the particular contract.

1.9.2 SASSETA shall disregard the bid of any bidder if that bidder, or any of itsdirectors:

1.9.2.1 have abused the Supply Chain Management systems of SASSETA.

1.9.2.2 have committed proven fraud or any other improper conduct in relation to such systems.

1.9.2.3 have failed to perform on any previous contract and the proof exists.

1.9.2.4 Such actions shall be communicated to the National Treasury.

2. TERMS OF REFERENCE

2.1. BACKGROUND

2.2.1 The Safety and Security Sector Education and Training Authority (SASSETA) is an education and training authority established as a juristic person in terms Section 9 of Skills Development Act, 1998 (Act No. 97 of 1998 as amended). SASSETA's licence has been renewed until the 31 March 2030. SASSETA is classified as a schedule 3A Public entity in terms of the Public Finance Management Act No.1 of 1999 as amended (PFMA) and reports to the Department of Higher Education and Training (DHET) with the following responsibilities

- To develop and implement sector skills plans
- Establish and promote learning programmes
- Register agreements for learning programmes
- Perform functions delegated by the QCTO
- Collect and distribute skills development levies

2.2.2 In order to perform the above-mentioned responsibilities, SASSETA utilises Information and Communication Technology as a platform:

- for business operations and communications.
- to manage and provide access to its systems and communicate with its stakeholders

2.2.3 These ICT systems and infrastructure are subject to cyber-attack and must be secured internally and externally. The main reason for such protection is in line with legislation relating to the POPI Act as well as common law principles of information privacy, confidentiality and accessibility.

2.2.4 In order to ensure that business operations of SASSETA that are hosted by ICT within SASSETA are not interrupted there is a need to ensure that the entire ICT infrastructure is secured at all times.

2.2.5 The mechanisms to ensure that the SASSETA ICT infrastructure is protected and secured is to develop and implement the ICT security related policies and part of the operation related to such include the implementation of a firewall, patch management solution, end-point protection (antivirus), vulnerability assessment and penetration testing, Intrusion detection solution, ICT Infrastructure audit tool etc.

2.2.6 The SETA currently has an ongoing contract (expiring on 9 September 2026) with a service provider to implement and configure several ICT security solutions, including:

- Configuring and maintaining a next-generation 10 GB/s firewall for the Head Office and two regional sites.
- Configuring and maintaining a LanGuard solution for patch management and network auditing.
- Managing system and infrastructure vulnerabilities twice a year, including internal/external vulnerability assessments and penetration testing with reporting and remediation.
- Configuring and maintaining an endpoint protection (antivirus) solution with a centralized management console.

2.2. PURPOSE

2.2.1 SASSETA seeks to appoint a reputable, suitable and qualified service provider with ICT Security expertise to provide Virtual Chief Information Security Officer (VCISO) and Security Operations Centre **(**SOC) services from the date of appointment until 31st March 2030.

2.2.2 The service provider will provide information security governance, risk, compliance and manage cyber threats (both internal and external) against the SASSETA's resources and ensure that it addresses the cyber threat environment for all SASSETA sites (Head office in Midrand, 2 regional offices in KZN and any other future regional offices).

2.2.3 The output of this bid is to provide skilled cybersecurity experts with extensive experience delivering strategic, technical and operational information security services to SASSETA.

2.3. SCOPE OF WORK AND SERVICES AND PRODUCTS REQUIRED

2.3.2. The service provider is expected to provide the following services for the duration of the contract:

2.3.1.1. Assess and implement the organisation's security based on ISO27001:2022 in two phases:

- Conduct ISO 27001:2022 gap assessment
- Manage and maintain the Information Security Management System (ISMS) based on ISO 27001:2022 international standard for information security;

2.3.1.2. Design and implement SASSETA's information security infrastructure to monitor ICT systems for early detection and prevention of unauthorised access and use; steering to completion of SASSETA's ongoing cyber security strengthening program and conducting periodic reviews thereof to identify, assess and coordinate remediation of weaknesses in SASSETA's ICT security systems;

2.3.1.3. Conduct a cyber security risk maturity assessment (based on ISO 27001:2022) and provide a cyber security risk assessment plan to be used for implementation and monitoring for the entire duration of the contract

2.3.1.4. Provide expertise on cyber security risks, compliance, incident response, disaster recovery and business continuity;

2.3.1.5. Provide consultation to build an effective cybersecurity and resilience program;

2.3.1.6. Facilitate the integration of security into the organisation's strategy, processes and culture;

2.3.1.7. Manage the development, roll-out, and ongoing maintenance of cybersecurity programs;

2.3.1.8. Undertake the integration and interpretation of information security program controls;

2.3.1.9. Serve as security liaison to auditors, assessors, and examiners;

2.3.1.10. Cyber strategy and policy development;

2.3.1.11. Third-party security assessments;

2.3.1.12. Manage Security Operations Centre (SOC) services;

- The SOC solution should consist of security monitoring, incident response, security analytics, proactive threat hunting, threat Intelligence consisting of Indicators of Compromise (IoC) and

other threat intel (vulnerabilities, strategic, tactical etc.), Security information and event management (SIEM) engineering, User Behavioural Anomaly detection, vulnerability scanning and network threat detection;

- Detect threats across the ICT environment including data centre, users, endpoints, and network.
- Detect known as well as unknown threats by using machine learning and other security analytics.
- Consolidate data and extract actionable insight from a variety of intelligence sources and existing security technologies
- Proactive threat hunting on a daily basis, which otherwise go undetected by signature-based applications/systems.
- Complete analysis and correlation of logs from all the devices/solutions under scope.
- 24x7 uninterrupted security monitoring operations.
- Automate security processes to reduce resource drain and threat response timelines.
- Correlation of low-priority alerts with subsequent alerts to detect multi-stage attacks.
- Reduction of remediation time
  a) Automated real-time prioritization of alerts.
  b) Automated data collection for investigation followed by quick analysis on a single window.
  c) Assisted remediation steps (integration with security devices to push policy/configuration remotely) for faster mitigation of threats
- Provide a centralised dashboard to capture the risk posture and maturity levels of the organization at any given point in time.
- Detect user anomalies using a combination of rules and machine learning models.

2.3.1.13. SOC Solution Integration Required

- Fortigate Firewalls
- Windows Active Directory
- Office 365
- Kaspersky Antivirus
- Microsoft Exchange
- HP/Aruba switches
- Hyper V
- LanGuard
- MS SQL
- Financial system
- HR system
- VEEAM
- Any other related hardware and solutions hosted internally

2.3.1.14. The bidder to have expertise in at least the following domains:

- Event monitoring and analysis
- Incident detection and response
- Threat Intelligence
- Use case engineering and new integrations to increase visibility
- Threat hunting

- Security analytics

2.3.1.15. Conduct internal and external vulnerability assessment, penetration testing services, reporting and remediation services

2.4. REQUIRED DELIVERABLES

2.4.1 The successful service provider will be required to deliver on the following;

2.4.1.1. ISO 27001:2022 gap assessment report with remedial action plan
2.4.1.2. Cyber security risk maturity assessment (based on ISO 27001:2022), Cyber security risk assessment plan and risk register
2.4.1.3. Information Cyber Security Strategy, Policies, standards, processes and procedures
2.4.1.4. Information Security Governance Framework and Implementation Plan;
2.4.1.5. Information Security Roadmap;
2.4.1.6. Security assessment reports;
2.4.1.7. Risk treatments plans;
2.4.1.8. Manage Security Operations Centre (SOC) services;
2.4.1.9. Monthly SOC reports;
2.4.1.10. Vulnerability assessment and reports;
2.4.1.11. Penetration testing and reports;
2.4.1.12. Reporting to the executive management;
2.4.1.13. Support SASSETA with VCISO and SOC services for the duration of the contract.

2.5. THE CURRENT ENVIRONMENT

2.5.1 Find below details of the devices currently in the SASSETA ICT environment, these are not exact and static figures as this may change at any time due to operational requirements.

2.5.1.1. **ICT Infrastructure at current offices**

Device Type	Network Segment (e.g. Zone, Location, Data-Centre)	Quantity
Windows Active Directory Servers (Windows 2019-2022)	Waterfall	2
Windows General Purpose Servers (Windows 2019-2022)	Waterfall	15
Routers and switches	Waterfall, Durban and Newcastle	16
Firewalls	Waterfall, Durban and Newcastle	3
Wireless Access Points	Waterfall, Durban and Newcastle	20
Total Workstations on Network	Waterfall, Newcastle and Durban	160-180

2.5.1.2. **ICT Infrastructure at future locations**

Device Type	Network Segment (e.g. Zone, Location, Data-Centre)	Quantity
Routers and switches	Future locations	2
Firewalls		1
Wireless Access Points		3
Total Workstations on Network		10

2.6. SUBMISSION REQUIREMENTS

2.6.1 The Bidding company should be ISO/IEC 27001 and ISO 9001 certified. Failure to submit the required valid certificates will result in the automatic disqualification of the bidder's proposal.

2.6.2 The Bidding Company is to submit a comprehensive project plan, with timelines that align to the scope of work including but not limited to all tasks, activities and timelines, task Dependencies, resources with roles and responsibilities, milestones and contingency plan to manage milestones, risk assessment, and management plan, vCISO implementation plan, SOC implementation plan.

2.6.3 The bidding company is to provide a minimum of three (3) signed reference letters on the client's letterhead vCISO and SOC services were implemented and maintained.

2.6.4 The Bidding company is to submit a comprehensive CV of the team leader demonstrating at least ten (10) years of experience as a lead Information Security expert.

2.6.5 The Bidding company is to submit the CVs of three (3) additional team members. The three (3) members should each demonstrate at least five (5) years of experience as ICT senior security specialists.

2.6.6 The above-requested team comprising the team leader and a minimum of three (3) additional team members to possess and submit valid qualifications in the following:

a) Team Leader: BSc Computer Science/IT, CISM (Certified Information Security Manager), CISA (Certified Information Systems Auditor), CDPSE (Certified Data Privacy Solutions Engineer), and Microsoft Certified Professional (MCP).

b) The three (3) team members must collectively possess the following five certificates, with each member holding a different certification: CISM (Certified Information Security Manager), Certified Threat Intelligence Analyst (CTIA), Computer Hacking Forensic Investigator (CHFI), EC-Council Certified Incident Handler (ECIH) and Certified Information Systems Security Professional (CISSP)

Option 1:

- **Team member 1:** Must have 2 certificates
- **Team member 2:** Must have 2 different certifications from Team member 1.

- **Team member 3:** Must have 1 certification different from Team members 1 and 2.

Option 2:

- **Team member 1:** Must have 3 certifications.
- **Team member 2:** Must have 1 certification different from Team member 1.
- **Team member 3:** Must have 1 certification different from Team members 1 and 2.

2.7. DURATION

2.7.1 The assignment is expected to be from the date of appointment until 31st March 2030.

2.7.2 The implementation phase is estimated to be completed within sixty (60) days from the date of appointment. The support and maintenance services will continue from day sixty-one (61) until the end of the contract (31st March 2030).

2.8. PRICING

2.8.1 Service Providers are requested to provide an all-inclusive price on SBD 3.3 of this tender.

2.9. ACCOUNTABILITY AND REPORTING

2.9.1. The service provider will report directly to the ICT Manager for the duration of the assignment.

2.10. SUBMISSION OF THE GENERAL CONDITIONS OF CONTRACT (GCC)

1.10.1 Bidders are requested to initial each page of the General Conditions of Contract (GCC) and submit their response to this Request for Quotations. The GCC will form part of the contract with the successful Bidder.

2.11. INTELLECTUAL PROPERTY

2.11.1 The service provider will be contracting with SASSETA. All data of this project, in whatever format raw or analysed, will be confidential information for utilisation by SASSETA. All information and documents received from SASSETA is to be kept confidential and may not be used or distributed in any format without the written approval of SASSETA. To this end, the service provider will be required to sign a confidentiality agreement within the SLA.

2.12. PROTECTION OF PERSONAL INFORMATION ACT

2.12.1 All Service Providers are to take note of the implications of POPI Act and any other data privacy Act applicable that SASSETA complies to. In compliance to the act, please be advised that the following are applicable to the treatment of vendor information:

2.12.1.1 All requested bid information will be solemnly utilized for the purpose of the bid evaluation processes. The vendor hereby consents the information provided as part of this bid will be utilized for supply chain

processes of SASSETA and may be subject to multiple processing to enable the evaluation of this bid.

2.12.1.2 The vendor consents that the information collected will be retained for the duration of the evaluation and archived for records management purposes. The information will be disposed of as per the SASSETA records management policies as prescribed by the National Archives Act. Furthermore, the information owner acknowledges that the information provided will be scanned into digital records which are retained on the SASSETA backup servers and that are replicated to backup media. SASSETA does confirm that the organization adopts industry best practice with regards to the safeguarding of digital records whether locally stored or retained in backup media.

2.12.1.3 SASSETA confirms that all submitted records will be retained in their original form and will not be altered with to preserve the quality and originality of the information provided.

2.12.1.4 SASSETA confirms that the Information Officer is duly responsible for vendor information provided and exercises stringent measures to ensure that information is secured and solemnly utilized for the purpose of use. No vendor records will be distributed or utilized for any processes outside the current bid that the information has been requested for.

3. PROPOSED SELECTION CRITERIA

3.1. Compliance with minimum requirements

3.1.1 All bids duly lodged will be examined to determine compliance with bidding requirements and conditions.

3.2. Conditions for selection/shortlisting

3.2.1 **Phase 1 – Service Providers to:**

- Email their proposal by the closing date and time. **Proposals received after the closing date and time will be disqualified from further evaluation.**
- The Bidding company should be ISO/IEC 27001 and ISO 9001 certified and submit valid certificates. **Non-submission of both certificates will lead to automatic disqualification of the bidder's proposal.**
- Complete and submit all Standard Bidding Documents (SBD) forms mentioned above on page 2 of this document, namely: SBD1, SBD 3.3, SBD 4, and SBD 6.1
- Be registered on the National Treasury Central Supplier Database (CSD) by the closing date and time of this request for quotation. Bidders are to provide SASSETA with a copy of their CSD registration report downloaded from the National Treasury CSD Website.
- Initial each page of the General Condition of Contract (Annexure A) and submit with the proposal

3.2.2. **Phase 2 – Functionality evaluation**

- Bidders who meet the mandatory items requirements above will be evaluated on functionality requirements on a scale of 0 to 1:

  0: Document/item not submitted; Unacceptable, does not meet set criteria; Weak, less than acceptable. Insufficient for performance requirements

  1: Exceptional mastery of the requirement should ensure extremely effective performance.

ELEMENT	FUNCTIONALITY EVALUATION		FUNCTIONALITY WEIGHT	TOTAL SCORE
Proposed Technical approach and research methodology of the bidder:	**Rating scale of 1**			
The Bidding Company to submit a comprehensive project plan, with timelines that align to the scope of work including but not limited to: ✓ All tasks, activities and timelines ✓ Task Dependencies ✓ Resources with roles and responsibilities ✓ Milestones and contingency plan to manage milestones ✓ Risk assessment and management plan ✓ vCISO implementation plan ✓ SOC implementation plan ***(30 points)*** ***NB: Project plan which covers all elements will score maximum points.***	**0**	Bidding company did not submit a comprehensive project plan / bidder submitted an incomplete project plan which does not cover all the elements.	**30**	
	1	Bidding company submitted a 'comprehensive project plan which covers all elements.		

ELEMENT	FUNCTIONALITY EVALUATION		FUNCTIONALITY WEIGHT	TOTAL SCORE
Suitability of the bidding Company:	**Rating scale of 1**			
The bidding company to provide a minimum of three (3) signed reference letters on the client's letterhead where vCISO and SOC services were implemented and maintained. Three (3) reference letters for vCISO services and three (3) reference letters for SOC services. NB.: The signed reference letters from different clients must be on clients' letterhead, with contact details, type of services rendered, signed and dated. **(20 points)**	**0**	The Bidding has not undertaken a project where an assignment of vCISO and SOC services were rendered. service provider submitted less than three (3) signed reference letters. Company did not submit signed reference letters relevant to this assignment. Two (2) or less signed reference letters for this assignment.	**20**	
	1	The Bidding Company submitted three (3) or more signed reference letters where vCISO and SOC services were rendered. Three (3) reference letters for vCISO services and three (3) reference letters for SOC services.		
Suitability of the proposed team:	**Rating scale of 1**	**Evaluation criteria**		
The bidding company to submit the CV of the team leader demonstrating at least ten (10) or more years of experience as a lead Information Security expert. **(15 Points).** **NB: The service provider to complete SBD 3.3 on the name of the team leader.**	**0**	The Bidding Company did not submit the CV of the team leader. CV of the team leader demonstrates less than ten (10) years of experience. The submitted CV of the Team Leader does not explicitly detail the number of experience as a lead Information Security expert.	**15**	
	1	The CV of the Team Leader explicitly demonstrates ten (10) or more years' experience as a lead Information Security expert.		
The bidding company to submit the CVs of three (3) additional team members. The three (3) members should each demonstrate at least five (5) years of experience as senior security specialists. **(15 Points).** **NB: The service provider to complete SBD 3.3 on the name of the additional three (2) members.**	**0**	The Bidding Company did not submit the CVs of three (3) additional team members. Less than three (3) CVs of the additional members submitted. Each CV of the three (3) additional members demonstrates less than five (5) years of experience.	**15**	
	1	The CV for each of the three (3) additional members explicitly demonstrates a (5) or more years of experience as senior security specialists		

The bidding company to submit qualifications of the proposed Team Leader in: BSc Computer Science/IT, CISM, CISA, CDPSE and MCP **(10 points)**	**0**	The proposed Team Leader does not possess the qualification in: BSc Computer Science/IT, CISM, CISA, CDPSE and MCP	**10**	
	1	The proposed Team Leader possesses the qualification in BSc Computer Science/IT, CISM, CISA, CDPSE and MCP		
The bidding company to submit qualifications for each of the three (3) additional team members in : CISM (Certified Information Security Manager), Certified Threat Intelligence Analyst (CTIA), Computer Hacking Forensic Investigator (CHFI), EC-Council Certified Incident Handler (ECIH) and Certified Information Systems Security Professional (CISSP) **(10 points)** The three (3) team members must collectively hold the above mentioned 5 certificates different from each member:	**0**	The proposed additional team members do not possess any of the qualifications. Only 1 or 2 members have the qualifications. CISM (Certified Information Security Manager), Certified Threat Intelligence Analyst (CTIA), Computer Hacking Forensic Investigator (CHFI), EC-Council Certified Incident Handler (ECIH) and Certified Information Systems Security Professional (CISSP)	**10**	
	1	The three (3) team members proposed have different qualifications and collectively in: CISM (Certified Information Security Manager), Certified Threat Intelligence Analyst (CTIA), Computer Hacking Forensic Investigator (CHFI), EC-Council Certified Incident Handler (ECIH) and Certified Information Systems Security Professional (CISSP)		
Total points for functionality				**100**

Bidders are required to meet a minimum functionality threshold of 90% for functionality in order for them to be shortlisted for phase 3 of the evaluation. **Bidders who do not score 90% for functionality will be disqualified from further evaluation.**

3.2.3. **Phase 3 – Price and Specific Goals**

- **The value of this bid is estimated not to exceed R50 000 000 (all applicable taxes included) and therefore the 80/20 system shall be applicable where** 80 points will be allocated to price and 20 points for Specific Goals as follows:

Evaluation Criterion on Price and Specific Goals	
Relative competitiveness of proposed price	80
Specific Goals	20
TOTAL FOR PRICE AND PREFERENCE	**100**

3.2.4 **ADJUDICATION OF BID**

- The Bid Adjudication Committee will consider the recommendations of the Bid Evaluation Committee (BEC) and make a recommendation to the Award Authority to make the final award. The successful bidder will usually be the service provider scoring the highest number of points or it may be a lower scoring bid based on firm, verifiable and justifiable grounds or no award at all.

PART A - INVITATION TO BID

YOU ARE HEREBY INVITED TO BID FOR THE REQUIREMENTS OF THE (*NAME OF DEPARTMENT/ PUBLICENTITY*)					
BID NUMBER:	**RFP/SASSETA/24251113**	CLOSING DATE:	**30 September 2024**	CLOSING TIME:	**11h00**
DESCRIPTION	Appointment of a reputable, suitable and qualified service provider with ICT Security expertise to provide Virtual Chief Information Security Officer (VCISO) and Security Operations Centre (SOC) services from the date of appointment until 31st March 2030				

PROPOSALS TO BE EMAILED:			
Proposals to be submitted electronically only via email to vciso@sasseta.org.za			
BIDDING PROCEDURE ENQUIRIES MAY BE DIRECTED TO		**TECHNICAL ENQUIRIES MAY BE DIRECTED TO:**	
CONTACT PERSON	**Ms. Lebo Hlombe**	CONTACT PERSON	**Ms. Lebo Hlombe**
E-MAIL ADDRESS	**scm01@sasseta.org.za**	E-MAIL ADDRESS	**scm01@sasseta.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 B-BBEE STATUS LEVEL VERIFICATION CERTIFICATE/ SWORN AFFIDAVIT (FOR EMES & QSEs) MUST BESUBMITTED IN ORDER TO QUALIFY FOR PREFERENCE POINTS FOR B-BBEE]					
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 NOTREGISTER 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 WILLNOT BE ACCEPTED FOR CONSIDERATION.
1.2.	**ALL BIDS MUST BE SUBMITTED ON THE OFFICIAL FORMS PROVIDED–(NOT TO BE RE-TYPED) OR INTHE 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 TAXSTATUS.
2.3	APPLICATION FOR TAX COMPLIANCE STATUS (TCS) PIN MAY BE MADE VIA E-FILING THROUGH THESARS 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 PARTYMUST SUBMIT A SEPARATE TCS CERTIFICATE / PIN / CSD NUMBER.
2.6	WHERE NO TCS IS AVAILABLE BUT THE BIDDER IS REGISTERED ON THE CENTRAL SUPPLIERDATABASE (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 WITHMEMBERS PERSONS IN THE SERVICE OF THE STATE."

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

NAME OF SIGNATORY ……

SIGNATURE OF BIDDER: ……

N/B.: If a Company has one director as listed on CSD, the one Director to sign these documents on behalf of the Company. Any other member of the Company will require a Company Resolution to be attached to this submissionsigned by the duly Authorised Director.

N/B.: If the Company has more than one Director as listed on CSD, a signed Company Resolution to be attached toconfirm that the one Director can sign on behalf of the Company. Any other member of the Company will require a Company Resolution to be attached to this submission signed by the duly Authorised Directors.

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

DATE: ……...

PRICING SCHEDULE

(Professional Services)

NAME OF BIDDER: ……..……. BID NO.: **RFP/SASSETA/24251113**

CLOSING TIME: **11h00** CLOSING DATE: **30 September 2024**

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

ITEM NO | DESCRIPTION | BID PRICE IN RSA CURRENCY **(ALL APPLICABLE TAXES INCLUDED)

1. The accompanying information must be used for the formulation of proposals.
2. All delivery costs must be included in the price, for delivery at the prescribed destination. All applicable taxes" include value-added tax (VAT), etc

NB: Bidders MUST complete this amount on this document, and it MUST be the same as the total amount on the quotation incl. VAT.

A: Once-Off Costs

ITEM NO.	DESCRIPTION	QUANTITY	UNIT PRICE (Incl. VAT)
1.	ISO GAP assessment report with remedial services	**1**	**R**
2.	Information Security/Cyber Security Strategy	**1**	**R**
3.	Information Security/ Cyber Security Roadmap	**1**	**R**
4.	Information Security Governance Framework and Implementation Plan	**1**	**R**
5.	Cyber Security policy, standards, processes and procedures	**1**	**R**
6.	Cyber security risk maturity assessment (based on ISO 27001:2022), Cyber security risk assessment plan and risk register	**1**	**R**
7.	SOC solution implementation cost (setup, installation, configuration and license for YEAR 1)	**1**	**R**
	TOTAL		**R**

B: Monthly Costs

ITEM NO.	DESCRIPTION	QUANTITY	YEAR 1 (from date of appointment to 31/03/2025 (incl. of VAT)	YEAR 2 (01/04/2025 to 31/03/2026) (incl. of VAT)	YEAR 3(01/04/2026 to 31/03/2027) (incl. of VAT)	YEAR 4 (01/04/2027 to 31/03/2028) (incl. of VAT)	YEAR 5(01/04/2028 to 31/03/2029) (incl. of VAT)	YEAR 6(01/04/2029 to 31/03/2030) (incl. of VAT)	TOTAL PRICE (incl. VAT
1.	VCISO monitoring, evaluation, improvement and reporting	1	**R**	**R**	**R**	**R**	**R**	**R**	**R**
2.	24/7 SOC services support, maintenance and reporting	1	**R**	**R**	**R**	**R**	**R**	**R**	**R**
Total			**R**	**R**	**R**	**R**	**R**	**R**	**R**

C: Ad Hoc Costs

ITEM NO	DESCRIPTION	QUANTITY	YEAR 1 (from date of appointment to 31/03/2025 (incl. of VAT)	YEAR 2 (01/04/2025 to 31/03/2026) (incl. of VAT)	YEAR 3(01/04/2026 to 31/03/2027) (incl. of VAT)	YEAR 4 (01/04/2027 to 31/03/2028) (incl. of VAT)	YEAR 5(01/04/2028 to 31/03/2029) (incl. of VAT)	YEAR 6(01/04/2029 to 31/03/2030) (incl. of VAT)	TOTAL PRICE (incl. VAT
1.	Vulnerability assessment: Conducting, Reporting	1	**R**	**R**	**R**	**R**	**R**	**R**	**R**
2.	Penetration Testing: Conducting, Reporting	1	**R**	**R**	**R**	**R**	**R**	**R**	**R**
3.	**Remediation services:** Vulnerability assessment, Penetration testing	Hourly rate	**R**	**R**	**R**	**R**	**R**	**R**	**R**
4.	Cyber security risk maturity assessment (based on ISO 27001:2022)	1	**R**	**R**	**R**	**R**	**R**	**R**	**R**

5.	Review of cybersecurity policies, strategy and standards	Hourly rate	**R**	**R**	**R**	**R**	**R**	**R**	**R**
6.	SOC licenses	1	Not applicable	**R**	**R**	**R**	**R**	**R**	**R**
7.	SOC license (setup, installation, configuration) for ICT infrastructure at future locations, including integration with existing infrastructure for new office implementations.	Rate per office	R	**R**	**R**	**R**	**R**	**R**	**R**
TOTAL			**R**	**R**	**R**	**R**	**R**	**R**	**R**

Bidders are to complete the names and surnames of the **proposed team** on this assignment, and ensure that comprehensive CVs of these members are attached to the proposal as follows:

NO.	**Role in the team**	**NAME AND SURNAME** **(NB.** *Bidding company to record only one name per role. If more than one name is provided, the evaluation will be conducted on the top candidate only)*	**IS CV ATTACHED?** *(circle the response below)*	**IS THE QUALIFICATION ATTACHED** (circle the response below)
1.	Team Leader		Yes/No	Yes/No
2.	Team member 1		Yes/No	Yes/No
3.	Team member 2		Yes/No	Yes/No
4.	Team member 3		Yes/No	Yes/No

NB.: Bidders to note that SASSETA will apply CPIX on all unit prices on the anniversary of this contract for all ensuing years

…….. **....……**

Signature **Date**

…….. **…….....**

Position **Name of bidder**

(To be signed by a duly Authorised Delegate. A signed Company Resolution to be submitted).

BIDDER'S DISCLOSURE

1. PURPOSE OF THE FORM

Any person (natural or juristic) may make an offer or offers in terms of this invitation to bid. In line with the principles of transparency, accountability, impartiality, and ethics as enshrined in the Constitution of the Republic of South Africa and further expressed in various pieces of legislation, it is required for the bidder to make this declaration in respect of the details required hereunder.

Where a person/s are listed in the Register for Tender Defaulters and / or the List of Restricted Suppliers, that person will automatically be disqualified from the bid process.

2. Bidder's declaration

2.1 Is the bidder, or any of its directors / trustees / shareholders / members / partners or any person having a controlling interest in the enterprise employed by the state? **YES/NO**

2.1.1 If so, furnish particulars of the names, individual identity numbers, and, if applicable, state employee numbers of sole proprietor/ directors / trustees / shareholders / members/ partners or any person having a controlling interest in the enterprise, in table below

Full Name	Identity Number	Name of State institution

N/B. If more space required, Service providers are to copy this table onto their letterhead and provide information as per the table above

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

2.2.1 If so, furnish particulars:

……
……

2.3 Does the bidder or any of its directors / trustees / shareholders / members / partners or any person having a controlling interest in the enterprise have any interest in any other related enterprise whether or not they are bidding for this contract? **YES/NO**

2.3.1 If so, furnish particulars:

……
……

3. DECLARATION

I, the undersigned, (name) ..... in submitting the accompanying bid, do hereby make the following statements that I certify to be true andcomplete in every respect:

3.1 I have read and I understand the contents of this disclosure;
3.2 I understand that the accompanying bid will be disqualified if this disclosure is found not to betrue and complete in every respect;
3.3 The bidder has arrived at the accompanying bid independently from, and without consultation, communication, agreement or arrangement with any competitor. However, communication between partners in a joint venture or consortium1 will not be construed as collusive bidding.
3.4 In addition, there have been no consultations, communications, agreements or arrangements with any competitor regarding the quality, quantity, specifications, prices, including methods, factors or formulas used to calculate prices, market allocation, the intention or decision to submit or not to submit the bid, bidding with the intention not to win the bid and conditions or delivery particulars of the products or services to which thisbid 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 officialbid openingor 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 No 89 of 1998 and or may be reported to the National Prosecuting Authority (NPA) for criminal investigation and or may be restricted from conducting business with the public sector for a period not exceeding ten (10) years in terms of the Prevention and Combating of Corrupt Activities Act No 12 of 2004 or any other applicable legislation.

I CERTIFY THAT THE INFORMATION FURNISHED IN PARAGRAPHS 1, 2 and 3 ABOVE IS CORRECT. I ACCEPT THAT THE STATE MAY REJECT THE BID OR ACT AGAINST ME IN TERMS OF PARAGRAPH 6 OF PFMA SCM INSTRUCTION 03 OF 2021/22 ON PREVENTINGAND COMBATING ABUSE IN THE SUPPLY CHAIN MANAGEMENT SYSTEM SHOULD THIS DECLARATION PROVE TO BE FALSE.

…… **……**

1 Joint venture or Consortium means an association of persons for the purpose of combining their expertise,property, capital, efforts, skill and knowledge in an activity for the execution of a contract.

PREFERENCE POINTS CLAIM FORM IN TERMS OF THE PREFERENTIAL PROCUREMENTREGULATIONS 2022

This preference form must form part of all bids invited. It contains general information and serves as a claimform for preference points for specific goals.

NB: BEFORE COMPLETING THIS FORM, BIDDERS MUST STUDY THE GENERAL CONDITIONS, DEFINITIONS AND DIRECTIVES APPLICABLE IN RESPECT OF THE BID AND PREFERENTIAL PROCUREMENT REGULATIONS, 2022

---

1. GENERAL CONDITIONS

1.1 The following preference point systems are applicable to invitations to quote:

- the 80/20 system for requirements with a Rand value of up to R1 000 000 (all applicable taxes included).

1.2 To be completed by the organ of state

The applicable preference point system for this quotation is the **80/20** preference point system.

a) The lowest acceptable quotation will be used to determine the accurate system once quotationsare received.

1.3 Points for this quotation (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:

1.5 The maximum points for this quotation are allocated as follows:

	POINTS
PRICE	80
SPECIFIC GOALS	20
Total points for Price and SPECIFIC GOALS	**100**

1.6 Failure on the part of a bidder to submit proof or documentation required in terms of this bid to claim points for specific goals with the quotation, will be interpreted to mean that preference points for specific goals are not claimed.

1.7 The organ of state reserves the right to request a bidder, either before a quotation is adjudicated or at any time subsequently, to substantiate any claim in regard to preferences, in any manner requiredby the organ of state.

2. FORMULAE FOR PROCUREMENT OF GOODS AND SERVICES

3. POINTS AWARDED FOR PRICE

3.1 THE 80/20 PREERENCE POINT SYSTEMS

A maximum of 80 points is allocated for price on the following basis:

80/20

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

Where

Ps = Points scored for the price of the quotation under consideration

Pt = Price of the quotation under consideration

Pmin = Price of lowest acceptable quotation

3.2 POINTS AWARDED FOR SPECIFIC GOALS

a) In terms of Regulations 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 quotation.

b) For the purposes of this quotation, the bidder 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 bid:

Table 1: Specific goals for the bidder and points claimed are indicated per the table below.

The specific goals allocated pointsin terms of this bid	**Number of pointsallocated (80/20 system)**	**Bidders to record the number of points claimed in the rows below (80/20 system) (To be completed by the bidder)**
At least 100% Black people Ownership	10.00	
At least 30% Black Women Ownership	5.00	
At least 30% Black youth ownership	5.00	
Total	**20.00**	

NB: Specific goals will not be rewarded to bidders who do not record their points in the table above

DECLARATION WITH REGARD TO COMPANY/FIRM

3.3 Name of company/firm…….

3.4 Company registration number: ……...

3.5 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]

3.6 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 quotation, 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 1.4and 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 bidding 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 bidder 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 BIDDER(S)

SURNAME AND NAME: ……..

DATE: ……

ADDRESS: ……

……

……

DOCUMENTS REQUIRED FOR CLAIMING SPECIFIC GOALS

As per bullet 1.6 and 1.7 of the Preference Points Claim Form in terms of the Preferential Procurement Regulations 2022, bidders are required to submit the SASSETA verification document(s) in order to be allocated the specific goals claimed:

a) An Original/Certified copy of a valid B-BBEE Certificate or Sworn Affidavit.

b) Certified copy/ies of Identity documents of the Company Directors

c) CSD report

d) Shareholder Certificates

NB.: Non-submission of the documents required above will lead to specific goal points NOT beingawarded.

……. **....……**

Signature **Date**

……. **…….....**

Position **Name of bidder**

(To be signed by a duly authorised Delegate. A signed Company Resolution must be submitted).

If you receive any suspicious calls asking for payment to secure an award of a bid or that the outcomeof a tender can be influenced in your favour, please immediately inform the SASSETA Anti-Corruption Hotline at 0800 204 143 for further investigation.

BIDDERS ARE ENCOURAGED TO USE THE FOLLOWING CHECKLIST WHEN SUBMITITING THEIR BIDS:

NO.	DETAILS - Bidders are to set out their bid in the following format:	TICK BY BIDDER
1.	Part 1: Completed and signed the invitation to bid document (SBD 1) **To be signed by a duly Authorised Delegate.**	
2.	Part 2: Completed and signed pricing schedule (SBD 3.3) **To be signed by a duly Authorised Delegate.**	
3.	Part 3: Completed and signed the Bidder's disclosure (SBD 4). *(In case of a consortium/ joint venture, or where sub-Service providers are utilised, each party to the bid* to *complete and sign the declaration of interestdocument).* **To be signed by a duly Authorised Delegate**	
4.	Part 4: Completed and signed the Preference Points Claim form in terms of the Preferential Procurement Regulations 2022 (SBD 6.1) **To be signed by a duly Authorised Delegate. Not claiming points as perSBD 6.1 will lead to Specific Goals points not awarded**	
5.	Part 5: Submitted the General Conditions of Contract (initialed each page)	
6.	Part 6: Bidders National Treasury Central Supplier Database (CSD) forms indicating thevalidity of the bidder's registration	
7.	Part 7: Bidder's attached quotation on the Company letterhead inclusive of VAT andany other applicable costs in line with the SBD 3.3	
8.	Part 8: The Bidding company should be ISO/IEC 27001 and ISO 9001 certified. **Failure to submit the required valid certificates will result in the automatic disqualification of the bidder's proposal**	
9.	Part 9: The Bidding Company to submit a comprehensive project plan, with timelines that align to the scope of work including but not limited to all tasks, activities and timelines, task Dependencies, resources with roles and responsibilities, milestones and contingency plan to manage milestones, risk assessment and management plan, vCISO implementation plan, SOC implementation plan	
10.	Part 10: The bidding company to provide a minimum of three (3) signed reference letters on the client's letterhead vCISO and SOC services were implemented and maintained	
11.	Part 11: A comprehensive CV of the team leader demonstrating at least ten (10) years of experience as a lead Information Security expert	
12.	Part 12: CVs of three (3) additional team members. The three (3) members should each demonstrate at least five (5) years of experience as ICT senior security specialists	
13.	Part 13: The above-requested team comprising the team leader and a minimum of three (3) additional team members to possess and submit valid qualifications in the following	
	a) Team Leader: BSc Computer Science/IT, CISM (Certified Information Security Manager), CISA (Certified Information Systems Auditor), CDPSE (Certified Data Privacy Solutions Engineer), and Microsoft Certified Professional (MCP).	
	b) The three (3) team members must collectively possess the following five certificates, with each member holding a different certification: CISM (Certified Information Security Manager), Certified Threat Intelligence Analyst (CTIA), Computer Hacking Forensic Investigator (CHFI), EC-Council Certified Incident Handler (ECIH) and Certified Information Systems Security Professional (CISSP)	

14.	**Part 14: Bidders to submit the following documents. Non-submission of the below-mentioned documents (under 6) will lead to specific goal points NOT being awarded.**	
	An Original/Certified copy of a valid B-BBEE Certificate or Sworn Affidavit.	
	Certified copy/ies of Identity documents of the Company Directors	
	CSD report	