REQUEST FOR PROCURING OF SERVICES

RFQ NO: 129/2026/EWSS/REDTEAM/RFQ

APPOINTMENT OF A SERVICE PROVIDER TO CONDUCT A RED TEAM ASSESSMENT

DESCRIPTION:	Appointment of a service provider to conduct a Red Team Assessment
DURATION:	6 months
PROPOSED BID PROCESS:	RFQ
BRIEFING SESSION:	Non-Compulsory
BRIEFING SESSION DATE AND TIME:	**06 November 2026** @ 11h00 a.m.
BRIEFING SESSION VENUE:	Online: Microsoft Teams Send an e-mail to tenders06@tcta.co.za to preregister and receive an invite. Registration for the briefing session will end on **05 November 2026 @14h00**
CLARIFICATION DEADLINE:	06 November 2026 **@16h00**
ISSUE DATE:	30 October 2026
CLOSING DATE:	**10 November 2026 @ 11H00 a.m.**
BID VALIDITY PERIOD:	30 days
ENQUIRIES:	tenders06@tcta.co.za
SUBMISSION OF PROPOSALS:	tenders06@tcta.co.za

1. BACKGROUND

The Trans-Caledon Tunnel Authority (TCTA) is a state-owned entity responsible for financing and implementing bulk raw water infrastructure projects in South Africa. Its operations depend on the confidentiality, integrity, and availability of its ICT systems, financial information, operational information, and supporting services.

Cybersecurity incidents could disrupt business operations, compromise sensitive information, affect the integrity of business transactions, and result in financial loss and reputational damage. Relevant threats include ransomware, unauthorized access, credential compromise, website attacks, data theft, insider threats, and social engineering.

TCTA therefore requires an independent Red Team Assessment to identify and validate exploitable weaknesses across its agreed ICT environment and evaluate the effectiveness of its technical, physical and human security controls.

The assessment must extend beyond identifying vulnerabilities through automated scanning. It must use controlled adversarial activities to demonstrate whether identified weaknesses can be exploited, how weaknesses could be combined into attack paths, and whether TCTA can prevent, detect, and respond to those activities.

The engagement will assess external and internal networks, Active Directory, wireless infrastructure, critical web applications, physical access controls, and personnel susceptibility to social engineering. Post-remediation retesting will verify the effectiveness of corrective actions and identify any residual or regressed vulnerabilities.

The assessment will support:

- Identification and validation of security weaknesses before they are exploited by an unauthorized party.
- Evaluation of security controls across technical, personnel and organisational processes.
- Assessment of potential privilege escalation, lateral movement and access to sensitive information.
- Evaluation of TCTA's ability to detect and respond to simulated adversarial behavior.
- Prioritization of remediation based on technical severity and business impact.
- Integration of findings into the enterprise risk register and cybersecurity improvement roadmap.
- Management decisions regarding security investments and control improvements.
- Alignment with the NIST Cybersecurity Framework, ISO/IEC 27001 and the compliance obligations identified in the RFQ, including POPIA and the PFMA.

2. SCOPE OF WORK

DETAILED DESCRIPTION OF GOODS/SERVICES

The appointed service provider must plan, execute, and report on controlled, ethical exploitation across selected critical systems, network zones, personnel targets, and digital assets. Each assessment module must be independently executed and auditable.

2.1 Red Team Assessment Functional Requirements

Detailed below are the requirements for the proposed Red Team Assessment. The assessment is expected to evaluate the effectiveness of TCTA's technical, physical, and human security controls through external and internal network testing, Active Directory penetration testing, wireless/Wi-Fi penetration testing, web application testing, and physical and social engineering exercises. The bidder must clearly describe the proposed methodology, tools, and approach for each assessment component, including controlled exploitation, reporting, remediation guidance, and post-remediation retesting. Any assumptions, exclusions, limitations, or deviations from the specified requirements must be clearly indicated by the bidder.

NO	FUNCTIONAL REQUIREMENTS	
2.1.1 RED TEAM ASSESSMENT FUNCTIONAL REQUIREMENTS		
FR01.1	***External Network Assessment***	

FR01.1.1	The service provider must conduct an unauthenticated, black-box assessment of TCTA's agreed internet-facing systems and services to identify exploitable vulnerabilities and weaknesses in perimeter security.
FR01.1.2	The assessment must include reconnaissance, asset and service enumeration, vulnerability analysis, and manual validation of identified weaknesses across the approved external scope.
FR01.1.3	The service provider must perform controlled exploitation of validated vulnerabilities to demonstrate potential unauthorized access, exposure of sensitive information, and associated business impact, within the approved Rules of Engagement.
FR01.1.4	Where initial access is obtained, the service provider must assess potential attack paths and opportunities for further compromise or lateral movement, subject to TCTA's authorization and agreed scope boundaries.
FR01.1.5	The service provider must document affected assets, validated findings, severity ratings, evidence, reproducible testing steps, and prioritized remediation recommendations. Testing must use approved source IP addresses and agreed testing windows.
FR01.2	***Internal Network Assessment***
FR01.2.1	The service provider must conduct an on-site assessment of TCTA's agreed internal network using both an unauthenticated or untrusted device perspective and a low-privilege authenticated domain user perspective.
FR01.2.2	The assessment must identify exploitable vulnerabilities and insecure configurations affecting in-scope servers, workstations, network devices, remote access services, and relevant monitoring or management platforms.
FR01.2.3	The service provider must assess the effectiveness of network segmentation and access controls by testing whether an unauthorized device or compromised user can access restricted systems or network segments.
FR01.2.4	The service provider must conduct controlled testing of privilege escalation, credential compromise, and lateral movement to identify attack paths from initial internal access to sensitive or business-critical systems.
FR01.2.5	The service provider must assess access to sensitive information and simulate data exfiltration where authorized, documenting the effectiveness of relevant preventive and detective controls, supporting evidence, and remediation recommendations.
FR01.3	***Active Directory Assessment***
FR01.3.1	The service provider must assess TCTA's agreed Active Directory environment for exploitable misconfigurations, weak credentials, excessive privileges, and insecure permissions.
FR01.3.2	The assessment must validate whether a low-privilege or compromised account can obtain elevated privileges through weaknesses in Active Directory configurations, permissions, or delegated access.
FR01.3.3	The service provider must assess credential compromise and lateral movement opportunities and identify attack paths that could lead to privileged account or domain compromise. All activities must comply with the approved Rules of Engagement.

FR01.3.4	The service provider must document validated Active Directory attack paths, affected accounts and systems, privileges obtained, technical evidence, business impact, and corrective actions required to prevent recurrence.
FR01.4	***Wireless or Wi-Fi Assessment***
FR01.4.1	The service provider must assess TCTA's agreed corporate and guest wireless networks for weaknesses in authentication, encryption, access controls, and security configurations.
FR01.4.2	The assessment must test whether weaknesses in wireless configurations or authentication mechanisms could permit unauthorized access to an in-scope wireless network.
FR01.4.3	The service provider must assess exposure to rogue access points and related wireless attack scenarios within the approved scope and Rules of Engagement.
FR01.4.4	The service provider must validate segregation between guest wireless networks, corporate wireless networks, and internal systems to identify unauthorized access or lateral movement opportunities.
FR01.4.5	The service provider must document affected wireless networks and infrastructure, validated findings, potential access to internal systems, severity ratings, technical evidence, and remediation recommendations.
FR01.5	***Web application security assessment***
FR01.5.1	The service provider must assess all exposed interfaces of each agreed in-scope web application using the OWASP Testing Guide, OWASP Top 10, and relevant business logic testing techniques.
FR01.5.2	The assessment must include reconnaissance and enumeration of application endpoints, user roles, and underlying technologies, followed by analysis of vulnerabilities and insecure configurations.
FR01.5.3	The service provider must assess authentication, authorization, session management, input validation, injection risks, sensitive information exposure, and business logic weaknesses through controlled testing.
FR01.5.4	Testing must include the supporting operating system, application server, and database components insofar as they directly affect the security of the in-scope application.
FR01.5.5	The service provider must safely validate application vulnerabilities and provide affected URLs or components, severity ratings, sanitized evidence, reproducible steps, business impact, and remediation guidance.
FR01.6	***Physical and social engineering assessment***
FR01.6.1	The service provider must assess the effectiveness of TCTA's agreed physical access controls through approved attempts to access restricted areas, facilities, or network connection points.
FR01.6.2	The assessment must include approved social engineering scenarios, such as pretexting and tailgating, to evaluate whether personnel or procedural weaknesses could enable unauthorized access.

FR01.6.3	The service provider must conduct approved phishing simulations through email, voice, or SMS, as agreed with TCTA, to assess personnel susceptibility and relevant reporting or response processes.
FR01.6.4	All personnel targets, scenarios, onsite activities, and any USB key-drop exercises must be approved by TCTA before execution and remain within the agreed Rules of Engagement.
FR01.6.5	The service provider must document the scenarios performed, controls tested, outcomes, potential business impact, and recommendations to improve physical security, personnel awareness, and organizational processes.
FR01.7	***Retesting and post-remediation validation***
FR01.7.1	The service provider must conduct post-remediation retesting of the original findings included in the agreed retest scope to determine whether corrective actions effectively address the identified weaknesses.
FR01.7.2	Retesting must be performed within 30 working days of the agreed remediation period, with the precise timing trigger and findings to be retested confirmed in the approved engagement plan.
FR01.7.3	The service provider must repeat relevant exploitation steps and attack chains, where authorized, to verify that previously demonstrated attack paths are closed and identify residual or regressed vulnerabilities.
FR01.7.4	The service provider must issue a Retest Validation Report identifying findings as Fixed, Partially Fixed, or Not Fixed, supported by updated risk ratings and technical validation evidence.
FR01.7.5	Retest deliverables must include the original and retested findings, revised executive and technical summaries, an updated improvement plan, and an attestation letter.

2.2 Non–Functional Requirements		
NO	**NON- FUNCTIONAL REQUIREMENTS**	**Mandatory / Non-Mandatory Requirements**
ENGAGEMENT GOVERNANCE, REPORTING AND SKILLS TRANSFER		
NFR 02.1	The service provider must conduct all assessment activities within TCTA-approved Rules of Engagement, scope boundaries and testing windows. Testing must be controlled and non-destructive, with emergency stop procedures and immediate escalation of potential business disruption.	Mandatory
NFR 02.2	The service provider must comply with POPIA, applicable data protection laws and the agreed confidentiality requirements. The parties must sign a mutual non-disclosure agreement before testing, and the assessment must limit	Mandatory

	sensitive information to what is necessary to substantiate findings.	
NFR 02.3	The service provider must plan and execute testing to minimize disruption to TCTA's operations. Any potential or actual service degradation, access to sensitive information, bypass of security controls or business disruption must be reported immediately. Findings posing an imminent threat to critical systems or business operations must be reported within 24 hours of discovery.	Mandatory
NFR 02.4	The service provider must use recognized assessment methodologies, including relevant MITRE ATT&CK techniques and OWASP testing guidance. Each assessment module must be independently auditable, with sufficient records and reproducible evidence to support findings and retest results.	Mandatory
NFR 02.5	The service provider must securely store and transfer assessment reports, logs and evidence using agreed access controls and protection measures. Evidence must be sanitized where appropriate and handled under agreed chain-of-custody arrangements.	Non - Mandatory
NFR 02.6	Changes to the agreed scope, targets, testing methods or schedule must be authorized and recorded through the agreed change-control process. Production changes require an approved Change Request and rollback plan.	Non - Mandatory
NFR 02.7	The service provider must assign suitably qualified and experienced personnel meeting the RFQ requirements. Replacement personnel must have equivalent or higher qualifications and experience and must undergo TCTA's vetting and approval process.	Mandatory
NFR 02.8	The service provider must complete the assessment, reporting, skills transfer, and agreed retesting within the six-month contract period and approved project schedule. Dependencies and any proposed timeline changes must be communicated and agreed with TCTA.	Mandatory
NFR 02.8	At engagement closure, the service provider must remove test accounts, payloads and temporary configurations introduced during testing. Assessment information must be	Mandatory

	returned, retained or securely destroyed in accordance with the non-disclosure agreement and TCTA's agreed instructions.	

2.3. ASSESSMENT COORDINATION AND SECURITY MONITORING

The appointed service provider must coordinate the Red Team Assessment with TCTA's designated cybersecurity representatives, infrastructure teams, application owners, and relevant Security Operations Center (SOC) personnel in accordance with the approved Rules of Engagement.

Before testing begins, the service provider must agree with TCTA on:

- In-scope systems, applications, networks, and personnel targets.
- Testing windows, approved source IP addresses, and required whitelisting.
- Test accounts, access requirements, and relevant technical documentation.
- Communication channels, escalation contacts, and emergency stop procedures.
- Arrangements for reviewing relevant security alerts and logs to evaluate detection and response capabilities.
- Treatment of third-party-managed systems and the authorizations required before testing.

SOC coordination must support the assessment objectives. Any restrictions on advance disclosure of individual test scenarios must be agreed during planning so that detection and response capabilities can be evaluated meaningfully.

Assessment findings must be presented in a format that supports incorporation into TCTA's enterprise risk register, remediation tracking, cybersecurity improvement roadmap, and incident response improvements.

2.4. ASSESSMENT APPROACH AND SCOPE TAILORING

The bidder must propose an assessment approach tailored to TCTA's ICT environment, business priorities, and the functional and non-functional requirements specified in this requisition.

The proposal must clearly describe:

- The methodology, tools, and techniques proposed for each assessment phase.
- The coverage of external networks, internal networks, Active Directory, wireless/Wi-Fi, web applications, and physical and social engineering assessments.
- Applicable MITRE ATT&CK techniques and OWASP testing guidance.
- Assumptions, dependencies, exclusions, limitations, and deviations from the specified requirements.
- Access, documentation, test accounts, and support required from TCTA.
- Measures to minimize operational disruption and protect sensitive information.
- The approach to controlled exploitation, evidence collection, reporting, and post-remediation retesting.

Any proposed deviation must include its justification, impact on assessment coverage, associated risks, costs, and timeline implications. Deviations do not amend the required scope unless expressly accepted by TCTA.

The agreed change-control process must authorize and document changes to the approved scope, targets, testing techniques, or schedule.

2.5. SKILLS TRANSFER AND KNOWLEDGE SHARING

The appointed service provider must deliver structured skills transfer to designated TCTA personnel as part of the Red Team Assessment. The sessions must enable relevant teams to understand validated findings, implement corrective actions, and verify remediation effectiveness.

Skills transfer must include:

- Over-the-shoulder knowledge sharing during appropriate assessment activities.
- Explanation of significant vulnerabilities, root causes, and demonstrated attack paths.
- Guidance on reproducing and validating findings safely within authorized environments.
- Practical guidance on remediation and compensating controls.
- A focused session on verifying fixes and interpreting retest results.
- Discussion of detection and response gaps identified during the assessment, where applicable.

The service provider must provide:

- Relevant presentation materials and technical reference notes.
- Sanitized examples and validation steps supporting significant findings.
- A technical feedback workshop for relevant ICT and cybersecurity personnel.
- A management presentation covering key risks, prioritized recommendations, and decisions required.
- Opportunities for TCTA personnel to raise questions regarding findings, remediation, and retesting.

Skills transfer must be coordinated with TCTA and completed within the agreed engagement schedule. Sensitive assessment information must remain subject to the confidentiality and evidence-handling requirements.

2.6. CONTRACT DURATION

The contract duration shall be six months, inclusive of:

- Project initiation, scope confirmation, and approval of the Rules of Engagement.
- External and internal network assessments.
- Active Directory and wireless/Wi-Fi assessments.
- Web application security assessment.
- Physical and social engineering assessment.
- Executive and technical reporting.
- Skills transfer and feedback presentations.
- Remediation consultation and agreed post-remediation retesting.
- Final reporting, cleanup, and engagement closure.

The service provider must submit a project schedule showing milestones, deliverables,

dependencies, and the time allocated for remediation and retesting. The schedule must accommodate the RFQ's requirement for retesting within 30 working days of the agreed remediation period, with the timing trigger confirmed during planning.

Any changes to the approved scope or schedule must be agreed with TCTA and formally documented through the applicable change-control process.

2.8. REMEDIATION SUPPORT AND POST-ASSESSMENT VALIDATION

The appointed service provider must provide technical consultation during the contract period to assist TCTA in understanding assessment findings, prioritising corrective actions, and preparing for retesting. Support must include:

- Clarification of findings, evidence, severity ratings, and business impact.
- Explanation of root causes and demonstrated attack paths.
- Guidance on immediate mitigations, longer-term remediation, and compensating controls.
- Consultation on findings that cannot be fully remediated.
- Technical feedback sessions with relevant system owners and cybersecurity personnel.
- Validation of agreed corrective actions through retesting.
- Updated reporting on resolved, partially resolved, unresolved, or re-emerged findings.

TCTA remains responsible for implementing corrective actions. The service provider must not make production changes unless specifically authorized through TCTA's change-control process.

The service provider must nominate technical contact and agree communication and escalation arrangements with TCTA. Imminent critical risks must be reported within 24 hours of discovery, while potential or actual business disruption arising during testing must be reported immediately.

Support concludes upon completion and acceptance of the agreed deliverables, retesting, and closure activities within the contract period. Ongoing platform maintenance, software upgrades, and routine system health checks are outside this assessment service unless separately scoped.

3. DELIVERABLES

Planning artifacts: kick-off minutes, agreed scope and asset list, test plan, Rules of Engagement, schedule, contact and escalation arrangements, and change-control approach.

Phase reporting: reconnaissance, exploitation and post-exploitation reports documenting activities, validated findings and attack paths.

Executive summary: management-ready results, affected business processes, key risks, prioritized recommendations, target owners and dates, risk heatmap, comparison with prior tests where available, and an attestation statement.

Detailed technical and final reports: unique finding IDs, affected assets, root causes, CVSS v3.1 scores and severity, likelihood, business impact, sanitized evidence, reproducible steps, compensating

controls, remediation guidance, and relevant OWASP or MITRE ATT&CK mapping. Include detailed vulnerability scan results per asset.

Evidence pack and findings register: sanitized payloads, screenshots, and logs; attack-path diagrams; and a CSV or XLSX register with owner, due date, status, and retest result.

Skills transfer: over-the-shoulder knowledge sharing and a focused session on reproducing findings and validating fixes.

Read-out sessions: technical workshop and management presentation, with briefing and feedback meetings before and after testing.

Retest validation or delta report: original and retested findings, Fixed / Partially Fixed / Not Fixed status, updated residual risk, revised executive and technical summaries, improvement plan and attestation letter.

Acceptance requires completion of the agreed scope and all deliverables, Critical and High findings fixed or formally risk-accepted by TCTA, and TCTA sign-off of the executive summary and technical report.

4. METHODOLOGY AND RULES OF ENGAGEMENT

Use a structured approach covering planning, OSINT and reconnaissance, automated scanning, manual validation, controlled exploitation, post-exploitation, remediation consultation, and retesting. Use MITRE ATT&CK for adversarial emulation and OWASP guidance for application testing. TCTA provides authorized access, test accounts, subject-matter experts, and approvals, and implements remediation.

Agree scope boundaries, named authorizers, target lists, maintenance windows, and source-IP whitelisting in writing before testing. Sign the mutual non-disclosure agreement; protect only the minimum necessary evidence; and maintain the chain of custody. Define emergency stop criteria and a safe word. Production changes require a Change Request and rollback plan. Remove test accounts, payloads, and temporary configurations at closure.

Testing must be non-destructive. DoS/DDoS and stress testing are excluded unless explicitly authorized in writing. Automated vulnerability spraying, password brute force, high-impact traffic floods, and exploitation targeting production-critical systems require explicit authorization. Immediately notify TCTA of service degradation, sensitive-information access, bypassed controls, or business disruption; report imminent critical risks to the designated cybersecurity representative within 24 hours.

6. RETURNABLES

SECTION	DESCRIPTION	ACTION REQUIRED	DOCUMENT STATUS
Section 1	**Organizational certifications**: Valid ISO/IEC 27001 — Information Security Management and ISO/IEC 27035 — Information Security Incident Management certificates issued by an accredited body, as required by the RFQ.	Submit	Mandatory

Section 2	**Technical Lead Certifications:**
	The nominated Technical Lead must hold at least three (3) current, recognized valid certifications comprising:
	• At least one (1) compulsory certification: OSCP, OSEP, OSWE or GIAC GPEN; and
	• Any two (2) additional certifications from the following list:
	  ○ CREST
	  ○ EC-Council ECSA
	  ○ GIAC GXPN or GWAPT
	  ○ CRTO
	  ○ PNPT
	  ○ CISSP
	  ○ CEH Master
	Evidence required: Copies of certificates showing the candidate's name, certification title, issuing organization, and issue and expiry dates, or lifetime status where applicable
	
	All submitted certifications must be valid and unexpired as at the RFQ closing date.
		Submit	Mandatory

Section 3	**Company experience**: Completed **Annexure A** with at least three (3) projects, or three (3) contactable client reference letters on official client letterhead demonstrating relevant Red Team Assessment experience. References must identify the client, scope, engagement dates, successful delivery, and contact details for verification.	Complete and submit	Non-Mandatory
Section 4	**Key personnel experience and certifications**: Complete Annexure B for the proposed Red Team Lead, showing at least three (3) Red Team or adversary-emulation engagements/projects Submit the **Annexure B** detailing each project, supporting client references or close-out evidence, and copies of at least three (3) current accepted professional certifications.	Complete and submit	Non-Mandatory

Section 5	**Financial proposal:** RFQ Pricing Schedule, covering the full six-month assessment, reporting, skills transfer, remediation consultation and retesting scope. Prices must be firm and unconditional, disclose all applicable costs, and show amounts excluding and including VAT.	Complete and submit	Mandatory
Section 6	**B-BBEE evidence**: A valid B-BBEE certificate issued by a SANAS-accredited verification agency, or a validly commissioned affidavit for an eligible EME or QSE, meeting the requirements specified in the RFQ. A joint venture or consortium must submit a consolidated B-BBEE certificate to claim preference points:	Submit	Non-Mandatory
Section 7	SBD 1: Invitation to bid and terms and conditions for bidding	Complete	Non-Mandatory
	SBD4: Declaration of interest	Complete	Non-Mandatory
	SBD6.1: Preference points claim form in terms of the Preferential Procurement Regulations 2022	Complete	Non-Mandatory
Section 8	Proof of registration on National Treasury Central Supplier Database	Submit	Non-Mandatory

Any bidder who fails to submit a mandatory document will be disqualified at this stage and not evaluated further. Any bidder who fails to submit a non-mandatory document where that document is linked to specific evaluation criteria will not be awarded points.

7. PROPOSED FUNCTIONALITY CRITERIA

TCTA will evaluate submissions for functional capacity and capability against the criteria below. TCTA reserves the right to verify references, qualifications and project evidence.

Bidders must obtain a minimum score of 30 out of 50 points to proceed to further evaluation. Bidders who do not achieve this threshold will be disqualified at this stage.

	Technical Evaluation Criteria	Max Points
1.	**Company Track Record — Red Team Assessments**	
	The bidder must demonstrate successful delivery of Red Team, adversary-emulation, or assumed-breach engagements. Acceptable engagements must have been conducted under formal Rules of Engagement and included multiple assessment vectors, such as external networks, internal networks, Active Directory, Wi-Fi/Wireless, web applications/APIs, physical security, or social engineering. Post-remediation retesting must be evidenced where it formed part of the engagement. **Evidence required** Submit completed **Annexure A** with at least three (3) RFQ scope of work projects or submission of at least three (3) client reference letters on official client letterhead containing: - Client organisation name and industry. - Engagement scope and assessment phases performed. - Relevant MITRE ATT&CK mapping, where used. - Start and end dates, or month and year of delivery. - Client contact person and contact details for verification. - Signature of an authorized client representative. Where confidentiality restricts detail, the reference must still provide sufficient high-level information to confirm the scope and satisfactory completion. **<u>Points will be allocated as follows:</u>** • **Less than 3 projects = 0** • **3 to 4 projects = 20** • **5 or more projects = 30**	**30**
2.	**Key Personnel Experience — Red Team Lead**	
2.1	The bidder must nominate a Red Team Lead who meets the mandatory experience requirements, such as having led at least three (3) eligible Red Team engagements/projects. **An eligible project must:** - Have been delivered under formal Rules of Engagement.	**20**

	- Have included at least all of these assessment vectors, such as external, internal, Active Directory, Wi-Fi/Wireless, web application/API, phishing/social engineering, or physical assessment. - Have included executive and technical reports. - Demonstrate the nominated person's role as overall or technical lead. **Evidence required:** - Completed **Annexure B** with at least three projects - Project dates in month/year format. - Scope and assessment vectors. - The nominated lead's responsibilities. - Key deliverables. **<u>Points will be allocated as follows:</u>** • **Less than 3 projects = 0** • **3 to 4 projects = 10** • **5 or more projects = 20**	
	Total Points	***50***

Minimum Functional Evaluation Threshold

Bidders must obtain a minimum score of 30 out of 50 points to be considered responsive and proceed to the next evaluation stage. Bidders who fail to achieve this score will be regarded as non-responsive, and their financial proposals will not proceed to price evaluation.

8. RFQ PRICING SCHEDULE

Bidders must submit a comprehensive financial proposal covering the full six-month Red Team Assessment.

All prices must be firm and unconditional. The proposal must disclose assessment costs, disbursements, VAT and the total contract price. Planning, project management, reporting, evidence preparation, workshops and skills transfer must be included without double counting.

No	Description	QTY	Total QTY
1.	***External Network Assessment,*** *including reconnaissance, controlled exploitation, and reporting.*	1 assessment module	**R**
2.	***Internal Network Assessment onsite,*** *including unauthenticated and low-privilege authenticated testing.)*	1 assessment module	**R**
3.	***Active Directory Assessment,*** *including credential compromise, privilege escalation, and attack-path validation.*	1 assessment module	**R**
4.	***Wireless/Wi-Fi Assessment,*** *including authentication, encryption, access controls, and segregation testing.*	1 assessment module	**R**
5.	***Web Application Security Assessment*** *covering all agreed in-scope applications and interfaces.*	1 assessment module	**R**
6.	***Physical and Social Engineering Assessment*** *covering the approved scenarios and targets.*	1 assessment module	**R**
7.	***Post-Remediation Retesting and Validation,*** *including the retest report*	1 retest phase	**R**
8.	***Skills Transfer And Knowledge Sharing***	2 TCTA resources	**R**
	Assessment subtotal excluding VAT	[redacted]	**R**
	Disbursements excluding VAT, *with an itemized breakdown*		**R**
	Total excluding VAT		**R**
	VAT at 15% on taxable costs		**R**
	Total (incl VAT)		**R**

NB: If the price offered by the highest scoring bidder is not market related, TCTA reserves the right not to award to that bidder in terms of its Procurement policies. Price must be reflected excluding and including VAT. The price must include disbursements as indicated in the RFQ Pricing Schedule. Prices must be firm and unconditional.

SPECIFIC GOALS

The table below will be used to calculate the score out of 20 for preference points:

B-BBEE Status Level of Contributor	Number of Points
1	20
2	18
3	14
4	12

5	8
6	6
7	4
8	2
Non-compliant contributor	0

Any bidder who fails to meet the specific goals will not be disqualified from the process and will score 0 for Specific Goals. NB - Bidders must submit valid certified copies of their B-BBEE Certificates/Sworn Affidavits which stipulates their B-BBEE Status Level of Contributor to claim preference points. Furthermore, no points will be awarded if the bidders' Sworn Affidavit does not comply with the requirements outlined in **ANNEXURE C.**

PREFERENTIAL POINTS CALCULATION

The weighting of the Preferential points calculation is as follows:

Price = 80

Specific Goals = 20

Total Score = 100

TERMS AND CONDITIONS

TCTA's Standard Conditions of Bid shall apply to this bid. TCTA reserves the right to cancel or not to award this bid in accordance with its standard Conditions of Bid. Bidders can obtain TCTA's standard conditions of bid upon request or on TCTA's website.

ANNEXURES

A	COMPANY EXPERIENCE
B	PROJECT LEADER EXPERIENCE
C	B-BBBEE SWORN AFFIDAVIT REQUIREMENTS FOR EME AND QSE
D	SBD 1 – INVITATION TO BID
E	SBD 4 – BIDDERS DISCLOSURE
F	SBD 6.1 – IN TERMS OF PPR 2022

ANNEXURE A: COMPANY EXPERIENCE:

CV TEMPLATE FOR COMPANY EXPERIENCE

CLIENT	PROJECTS DESCRIPTIONS	START DATE (INDICATE THE MONTH AND YEAR)	END DATE (INDICATE THE MONTH AND YEAR)	NAME & SURNAME OF CONTACT PERSON	CONTACT DETAILS : EMAIL AND TELEPHONE NUMBER

NB: No points will be allocated if this table is not completed in full. No points will be allocated for self-created templates.

SIGNATURE: .....…… NAME OF BIDDER:(of person authorized to sign on behalf of the company

ANNEXURE B: QUALIFICATIONS AND EXPERIENCE OF PROJECT LEADER:

CV TEMPLATE FOR PROJECT LEADER:

Name and Surname of Resource
Number of RFQ-relevant certificates

EMPLOYER/ CLIENT	RELEVANT EXPERIENCE	START DATE (INDICATE THE MONTH AND YEAR)	END DATE (INDICATE THE MONTH AND YEAR)	NAME & SURNAME OF CONTACT PERSON	CONTACT DETAILS: EMAIL AND TELEPHONE NUMBER

NB: No points will be allocated if this table is not completed in full. No points will be allocated for self-created templates.

SIGNATURE: .....…… NAME OF BIDDER:..... person authorised to sign on behalf of the Bidder)

NNEXURE C: B-BBEE SWORN AFFIDAVIT REQUIREMENTS FOR EME AND QSE

The following information is required for the Sworn Affidavits to be valid: -

1. Name/s of deponent as they appear in the identity document and the identity number;

2. Designation of the deponent as either the director, owner or member must be indicated in order to know that person is duly authorised to depose of an affidavit;

3. Name of enterprise as per enterprise registration documents issued by the CIPC, where applicable, and enterprise business address.;

4. Percentage of black ownership, black female ownership and designated group. In the case of specialised enterprises as per Statement 004, the percentage of black beneficiaries must be reflected;

5. Indicate total revenue for the latest financial year and whether it is based on audited financial statements or management accounts;

6. Full financial year end as per the enterprise's registration documents, which was used to determine the total revenue. Example 28 February 2022;

7. B-BBEE Status level. An enterprise can only have one status level;

8. Nature of business;

9. VAT Number;

10. Date deponent signed and date of Commissioner of Oath must be the same;

11. Commissioner of Oath cannot be an employee or ex officio of the enterprise because, a person cannot by law, commission a sworn affidavit in which they have an interest;

12. Correct Sector Codes Affidavit to be used.

ANNEXURE D **SBD 1**

PART A
INVITATION TO BID

YOU ARE HEREBY INVITED TO BID FOR REQUIREMENTS OF THE (*NAME OF DEPARTMENT/ PUBLIC ENTITY*)					
BID NUMBER:		CLOSING DATE:		CLOSING TIME:	**11H00 a.m.**
DESCRIPTION					
BID RESPONSE DOCUMENTS MAY BE DEPOSITED IN THE BID BOX SITUATED AT *(STREET ADDRESS)*					
tenders06@tcta.co.za					

BIDDING PROCEDURE ENQUIRIES MAY BE DIRECTED TO		**TECHNICAL ENQUIRIES MAY BE DIRECTED TO:**	
CONTACT PERSON		CONTACT PERSON	
TELEPHONE NUMBER	**N/A**	TELEPHONE NUMBER	**N/A**
FACSIMILE NUMBER	**N/A**	FACSIMILE NUMBER	**N/A**
E-MAIL ADDRESS	tenders06@tcta.co.za	E-MAIL ADDRESS	tenders06@tcta.co.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
1. ARE YOU THE ACCREDITED REPRESENTATIVE IN SOUTH AFRICA FOR THE GOODS /SERVICES OFFERED?	☐Yes ☐No [IF YES ENCLOSE PROOF]		**2.** ARE YOU A FOREIGN BASED SUPPLIER FOR THE GOODS /SERVICES OFFERED?	☐Yes ☐No [IF YES, ANSWER THE QUESTIONNAIRE BELOW]	

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

3. 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, 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).**

4. 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 PIN 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: ……

ANNEXURE E **SBD 4**

BIDDER'S DISCLOSURE

1. PURPOSE OF THE FORM

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

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

2. Bidder's declaration

2.1 Is the bidder, or any of its directors / trustees / shareholders / members / partners or any person having a controlling interest1 in the enterprise,
employed by the state? **YES/NO**

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

Full Name	Identity Number	Name of State institution

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

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.

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

3.1 I have read and I understand the contents of this disclosure;

3.2 I understand that the accompanying bid will be disqualified if this disclosure is found not to be true and complete in every respect;

3.3 The bidder has arrived at the accompanying bid independently from, and without consultation, communication, agreement or arrangement with any competitor. However, communication between partners in a joint venture or consortium2 will not be construed as collusive bidding.

3.4 In addition, there have been no consultations, communications, agreements or arrangements with any competitor regarding the quality, quantity, specifications, prices, including methods, factors or formulas used to calculate prices, market allocation, the intention or decision to submit or not to submit the bid, bidding with the intention not to win the bid and conditions or delivery particulars of the products or services to which this bid invitation relates.

3.4 The terms of the accompanying bid have not been, and will not be, disclosed by the bidder, directly or indirectly, to any competitor, prior to the date and time of the official bid opening or of the awarding of the contract.

3.5 There have been no consultations, communications, agreements or arrangements made by the bidder with any official of the procuring institution in relation to this procurement process prior to and during the bidding process except to provide clarification on the bid submitted where so required by the institution; and the bidder was not involved in the drafting of the specifications or terms of reference for this bid.

3.6 I am aware that, in addition and without prejudice to any other remedy provided to combat any restrictive practices related to bids and contracts, bids that are suspicious will be reported to the Competition Commission for investigation and possible imposition of administrative penalties in terms of section 59 of the Competition Act No 89 of 1998 and or may be reported to the National Prosecuting Authority (NPA) for criminal investigation and or may be restricted from conducting business with the public sector for a period not exceeding ten (10) years in terms of the Prevention and Combating of Corrupt Activities Act No 12 of 2004 or any other applicable legislation.

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

…… ……
Signature Date

…… ……
Position Name of bidder

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

ANNEXURE F **SBD 6.1**

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);

1.2 **To be completed by the organ of state**

a) The applicable preference point system for this tender is the 80/20 preference point system.

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**

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

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**

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

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)
BBBEE-LEVEL		
1	20	
2	18	
3	14	
4	12	
5	8	
6	6	
7	4	
8	2	
Non-compliant contributor	0	

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: ……