

Request for Quotation

NATIONAL METROLOGY INSTITUTE OF SOUTH AFRICA

Requested by: Bongani Mabunda

Section: Information Technology

Telephone number: 012 947 2712

Email address: bmabunda@nmisa.org

Date: 15 October 2026

SUPPLIER'S INFORMATION

Prepared by:

Address:

Telephone no:

Email address:

Date:

APPOINTMENT OF A SERVICE PROVIDER TO CONDUCT PENETRATION TESTING AND VULNERABILITY ASSESSMENT SERVICES FOR A ONCE-OFF ENGAGEMENT OF APPROXIMATELY THREE (3) MONTHS

1. PURPOSE

NMISA seeks to appoint a suitably qualified and experienced cybersecurity service provider to conduct a once-off independent penetration testing and vulnerability assessment engagement. The anticipated period for completion of the initial assessment, reporting and remediation workshop is approximately three (3) months from the effective date. The successful bidder shall thereafter remain responsible for the two (2) included remediation retest cycles for a period of up to three (3) additional months following NMISA's written acceptance of the initial final assessment report, unless otherwise extended by NMISA in writing. The service will provide assurance over NMISA's external and internal attack surface, cloud environment, identity services, networks, wireless infrastructure, web applications and other agreed critical ICT systems.

The successful bidder shall identify, validate and risk-rate security weaknesses; demonstrate credible attack paths through controlled exploitation where authorized, provide practical remediation guidance; and retest remediated findings to confirm closure.

The objectives are to:

- Identify exploitable vulnerabilities and security weaknesses before they can be abused by threat actors.
- Assess the effectiveness of security controls across internal, external, cloud, identity, network, wireless and application environments.
- Validate the risk and business impact of identified vulnerabilities through safe and controlled testing.
- Provide prioritized, actionable remediation recommendations.
- Confirm remediation through formal retesting and closure reporting.
- Support NMISA cybersecurity governance, risk management, disaster recovery readiness and audit assurance.
- Provide knowledge transfer to NMISA ICT personnel on significant findings, attack paths and remediation priorities

2. BACKGROUND AND CURRENT ENVIRONMENT

NMISA operates a hybrid ICT environment supporting corporate, laboratory and customer-facing business processes. The environment includes Microsoft cloud services, on-premises infrastructure, internet-facing services, network and security devices, end-user computing, identity services and business applications. Some business services are hosted in Microsoft Azure and make use of Microsoft 365 and Microsoft Entra ID.

NMISA requires an independent security assessment to determine whether weaknesses in these environments could be exploited to gain unauthorized access, compromise information, escalate privileges, move laterally, disrupt services or expose critical business systems. The final list of IP addresses, URLs, applications, network segments, cloud resources and other targets will be confirmed with the successful bidder during inception and will not necessarily be published in the RFQ.

2.1 Scope Sizing and Confidential Target Information

NMISA will not publish sensitive target identifiers in the public RFQ. However, before bid closing, NMISA shall make sufficient non-sensitive sizing information available through the approved procurement process to enable comparable fixed pricing. This should include, as applicable, indicative counts or ranges for external targets, internal hosts/network segments, web applications/APIs, cloud subscriptions/resources, identity tenant(s), wireless locations and other material target categories. The detailed IP addresses, URLs, credentials and architecture information will only be provided to the successful bidder under the approved Rules of Engagement and confidentiality controls.

3. SCOPE REQUIREMENTS

The bidder must provide a complete penetration testing and vulnerability assessment service. Automated vulnerability scanning alone shall not be regarded as penetration testing. The service must combine appropriate automated discovery with manual validation, attack-path analysis and expert-led controlled exploitation, where authorized, to establish the existence and potential impact of vulnerabilities. Findings generated through automated tools must be manually validated before inclusion as confirmed findings in the final report, and false positives must be clearly identified and excluded from confirmed vulnerability counts.

3.1 Inception, Discovery and Rules of Engagement

1. Conduct an inception meeting and confirm objectives, authorized targets, exclusions, dependencies, testing windows, contacts and escalation procedures.
2. Prepare a detailed test plan and Rules of Engagement (RoE) for NMISA approval before intrusive testing begins.
3. Classify testing activities by risk and identify any tests that may affect availability or data integrity.
4. Maintain a complete target register and evidence trail for the assessment.

5. Agree emergency stop procedures and a named escalation path for any unexpected service impact.

3.2 External Penetration Testing

1. Assess authorized public-facing IP addresses, domains, DNS exposure, internet-facing hosts, portals, remote-access services and other externally accessible infrastructure.
2. Test for exposed services, weak configurations, outdated software, authentication weaknesses, exploitable vulnerabilities and attack paths.
3. Assess externally exposed firewalls, VPN services and perimeter controls where authorized.
4. Validate findings manually and conduct controlled exploitation where necessary and authorized to demonstrate risk without causing denial of service. For validated exploitable findings, provide sufficient reproducible evidence, including the affected asset/component, attack path or validation steps, impact and supporting screenshots/log evidence where appropriate, without unnecessarily exposing sensitive production data.

3.3 Internal Network Penetration Testing

1. Assess agreed internal network segments, servers, workstations and network-accessible services.
2. Test network segmentation, trust relationships, insecure protocols, credential exposure, privilege escalation and lateral movement opportunities.
3. Assess switches, routers, firewalls and other network devices for vulnerabilities and material configuration weaknesses where authorized.
4. Identify paths that could allow compromise of critical systems from lower-trust network zones.

3.4 Microsoft Azure, Microsoft 365 and Identity Security Assessment

1. Assess authorized Microsoft Azure resources and configurations for security weaknesses, excessive exposure, insecure access paths and exploitable misconfigurations.
2. Assess Microsoft Entra ID identity and access controls, privileged roles, authentication controls, application registrations, enterprise applications and material identity attack paths within authorized testing boundaries.
3. Assess relevant Microsoft 365 security exposure and configurations where technically and contractually permissible.
4. All cloud testing must comply with the applicable cloud provider penetration-testing rules and service limitations. The bidder may not conduct prohibited testing against Microsoft-managed infrastructure.

3.5 Web Application and Portal Penetration Testing

1. Assess NMISA-selected internet-facing and internal web applications, portals and APIs.
2. Test authentication, authorization, session management, input validation, access control, injection, file handling, business logic and other relevant application security risks.
3. Apply recognized web application security practices, including OWASP-aligned testing.

4. Where Dynamics 365, Power Platform, customer portals or related integrations are included, testing shall be limited to NMISA-controlled customizations, integrations, identities, configurations, exposed endpoints and authorized interfaces/components that NMISA is legally and contractually permitted to test. The bidder may not test Microsoft-managed SaaS/platform infrastructure outside NMISA's authorized control boundary.

3.6 Wireless Network Security Assessment

1. Assess authorized corporate and guest wireless networks.
2. Review wireless encryption, authentication, segmentation, rogue/unauthorized access risks and material configuration weaknesses.
3. Attempt, controlled access and segmentation validation where authorized.

3.7 Vulnerability Assessment

1. Perform authenticated and unauthenticated vulnerability assessments, where appropriate, across agreed systems and infrastructure.
2. Cover relevant Windows, Linux and other operating systems, network devices, servers, services and applications in scope.
3. Manually validate material findings to reduce false positives and distinguish theoretical exposure from credible exploitable risk. Scanner output alone will not be accepted as evidence of a confirmed penetration-testing finding.
4. Identify unsupported or end-of-life components where observable and relevant to risk.

3.8 Optional Social Engineering / Phishing Simulation

Social engineering, phishing simulation and physical-security testing are excluded from the base/core scope and Evaluated Bid Price. Where instructed by NMISA through a separately approved written work order, the bidder may conduct controlled phishing or other agreed social-engineering simulations using the separately quoted optional rate. No social-engineering or physical-security testing may occur without prior written approval of the campaign plan, scenario, target population, communication/escalation arrangements and safeguards. Physical intrusion/testing is excluded unless separately and explicitly authorized in writing.

3.9 Remediation Support and Retesting

1. For each confirmed finding, provide a remediation priority matrix showing severity (Critical, High, Medium or Low), CVSS v4.0 score/vector, affected asset/component, NMISA business impact, exploitability, recommended remediation action and suggested remediation priority/order.
2. Conduct a technical remediation workshop with NMISA ICT after each major assessment.
3. Provide practical remediation actions, prioritized according to risk and business impact.
4. The contract price must include at least two (2) remediation retest cycles. The bidder shall retest all findings that NMISA reports as remediated, including Critical, High, Medium and Low findings where applicable, and shall update their status based on validation evidence.

Retesting must remain limited to findings arising from the original agreed assessment scope unless additional testing is separately authorized.

5. Issue a retest/closure report clearly showing Closed, Partially Remediated, Open, Risk Accepted or Not Retested status.
6. Provide reasonable clarification of findings during the remediation and included retest period at no additional professional fee where the clarification relates directly to the delivered assessment.

4. TESTING RULES, CONSTRAINTS AND AUTHORISATION

1. No penetration testing may commence until NMISA has approved the scope and Rules of Engagement in writing.
2. Testing must be non-destructive and designed to avoid denial of service, corruption, deletion, unauthorized alteration of production data or material interruption of NMISA operations. Intrusive testing of production systems may only occur within approved testing windows and with explicit NMISA authorization in the Rules of Engagement.
3. Denial-of-service/distributed denial-of-service testing, destructive malware, ransomware simulation, uncontrolled persistence, data deletion/corruption, mass or bulk data extraction and other disruptive techniques are prohibited unless separately and explicitly authorized in writing by NMISA.
4. Production credentials, secrets or sensitive information obtained during testing must be protected, access restricted to named authorized personnel, and retained only for the minimum period necessary. The bidder shall access or copy only the minimum data necessary to demonstrate a finding and may not perform bulk extraction of NMISA or customer data.
5. Any evidence containing personal, confidential, security-sensitive or privileged information must be encrypted in transit and at rest.
6. The bidder must notify NMISA immediately upon validation of any Critical vulnerability presenting imminent risk, and in all cases no later than four (4) hours after validation. The bidder must not wait for the draft or final report. Critical findings must be communicated through the escalation channel defined in the approved Rules of Engagement.
7. NMISA may immediately suspend any testing activity that threatens or may reasonably threaten system availability, integrity, confidentiality, safety or business operations. The bidder must also stop the affected test immediately if unexpected service degradation or operational impact is observed and escalate in accordance with the approved Rules of Engagement.
8. Internal testing may be required onsite at NMISA. Proposed personnel must comply with NMISA access-control, safety, confidentiality and vetting requirements where applicable.
9. No target outside the written scope may be scanned, exploited or tested. If the bidder discovers or is redirected to an asset outside the authorized target inventory, the bidder may record and report the discovery but must stop further interaction with that asset and obtain written NMISA approval before any additional testing or exploitation.
10. All commercial tools used must be appropriately licensed and all tools, including open-source tools, must be lawfully authorized for commercial use. The bidder remains responsible for the safe configuration and use of all testing tools.

11. The bidder must ensure that testing infrastructure, evidence repositories and collaboration platforms used for the engagement are located and operated in a manner compliant with applicable South African data-protection requirements and NMISA-approved data-handling arrangements. NMISA information may not be transferred to or stored in an unapproved jurisdiction or third-party platform without prior written NMISA approval.
12. The bidder must maintain a detailed testing activity log sufficient to reconstruct material testing actions, including date/time, tester, source system, target and material action performed. The log must be made available to NMISA on request and handed over at close-out where required.

5. METHODOLOGY AND STANDARDS

1. The bidder must submit a detailed methodology demonstrating a balance between automated tooling and manual expert analysis. The methodology must be appropriate to the technologies in scope and aligned, where applicable, to recognized practices such as the Penetration Testing Execution Standard (PTES), OWASP Web Security Testing Guide (WSTG) / OWASP Top 10 and NIST SP 800-115. Confirmed vulnerabilities must be risk-rated using CVSS v4.0, supplemented by NMISA business impact, exploitability and operational context. MITRE ATT&CK may be used to describe relevant attack techniques and paths.
2. The methodology must explain reconnaissance, discovery, vulnerability identification, manual validation, controlled exploitation, privilege escalation, lateral movement, evidence handling, false-positive control, risk rating, reporting, remediation and retesting. The bidder must identify the principal commercial and/or open-source tools proposed. The testing approach (for example black-box and/or grey-box) will be agreed during inception. Source-code review is excluded unless specifically authorized and priced by NMISA.
3. The bidder must define how CVSS v4.0 scores are translated into Critical, High, Medium and Low reporting categories and apply that approach consistently. NMISA business impact may increase remediation priority but must not silently alter the underlying technical CVSS score/vector.

6. DELIVERABLES

No.	Deliverable	Minimum Content / Acceptance Requirement
1	Inception and Rules of Engagement Pack	Confirmed scope, targets, exclusions, testing windows, contacts, escalation process, emergency stop procedure and approved test plan.
2	Attack Surface / Vulnerability Assessment Report	Asset/target coverage against the agreed baseline, validated vulnerabilities, false-positive disposition, affected assets, reproducible evidence, CVSS v4.0 score/vector, NMISA business impact and remediation guidance.

No.	Deliverable	Minimum Content / Acceptance Requirement
3	External Penetration Test Report	Validated external findings, attack paths, controlled exploitation evidence where authorized, risk ratings and remediation recommendations; automated scanner output alone is insufficient.
4	Internal Penetration Test Report	Internal attack paths, segmentation findings, privilege escalation/lateral movement evidence and remediation recommendations.
5	Cloud and Identity Security Assessment Report	Authorized Azure, Entra ID and related cloud findings, attack paths, configuration risks and remediation guidance.
6	Web Application / Portal Report	Application-specific findings with reproducible evidence, risk, affected component, remediation and references.
7	Wireless Security Assessment Report	Wireless findings, segmentation/authentication risks and remediation recommendations.
8	Executive Summary	Management-level summary of overall security posture, top risks, business impact, trends and prioritized actions.
9	Technical Remediation Workshop	Presentation of findings and practical remediation guidance to NMISA ICT.
10	Retest and Closure Report	Evidence of up to two (2) included remediation retest cycles and status of all findings NMISA reports as remediated: Closed, Partially Remediated, Open, Risk Accepted or Not Retested.
11	Final Consolidated Report	Consolidated view of all assessments, outstanding risks, recurring themes, accepted risks, retest status and recommended security improvement roadmap.

7. SERVICE LEVEL AND TIMELINE REQUIREMENTS

Requirement	Minimum Requirement
Mobilization / inception	Within five (5) business days of appointment or as agreed with NMISA.
Rules of Engagement	Submitted and approved before any intrusive testing.
Critical finding notification	Immediately upon validation and no later than four (4) hours after validation of a Critical vulnerability presenting imminent risk.
Draft assessment report	Within five (5) business days after completion of the relevant testing activity.
Final report	Within five (5) business days after receipt of consolidated NMISA comments.
Retest	Within ten (10) business days of each NMISA retest request, measured from the date NMISA confirms the affected systems are ready for retesting and required

Requirement	Minimum Requirement
	access/change windows have been provided. Two (2) remediation cycles are included in the fixed price.
Retest report	Within three (3) business days after completion of retesting.

8. PROJECT GOVERNANCE

1. Nominate an accountable Project Lead as the primary point of contact.
2. Submit a detailed project schedule within five (5) business days of appointment.
3. Maintain scope, issue, risk, action and findings register throughout the engagement.
4. Hold inception, technical findings, remediation and close-out meetings as required.
5. Coordinate testing windows with NMISA to minimize operational impact.
6. Escalate Critical vulnerabilities and material service-impact risks immediately.
7. Ensure all deliverables are version controlled and securely transmitted to NMISA.

9. ASSUMPTIONS

1. NMISA will provide authorized access, test accounts, network connectivity and technical contacts reasonably required for approved testing.
2. NMISA will identify the final systems, URLs, IP ranges, applications, network segments and other targets in scope. To support comparable pricing without publicly disclosing sensitive technical details, NMISA shall provide bidders, before bid closing and through an approved procurement/clarification process, with an indicative target-count schedule or sizing information for the scope categories listed in this TOR. The successful bidder will receive the detailed authorized target inventory during inception. Bidders must price the stated baseline/sizing information. Any quantity above an expressly stated baseline may only be procured using approved unit rates and prior written NMISA authorization.
3. Testing will be scheduled around critical business and laboratory operations where required.
4. NMISA will remain responsible for implementing remediation unless remediation implementation is separately authorized and priced.
5. The bidder shall provide its own licensed testing tools, laptops and specialist equipment required to perform the service.
6. Cloud-platform testing will be subject to the applicable provider rules and NMISA tenant permissions.
7. Any material expansion of scope beyond the agreed target inventory or stated baseline quantities must be approved by NMISA in writing before work is undertaken. No variation or additional fee will be recognized for work performed without prior written approval.

10. CONTRACT DURATION

The appointment is a once-off penetration testing and vulnerability assessment engagement. The initial assessment, reporting and remediation workshop are anticipated to be completed within

approximately three (3) months from the commencement date. Following NMISA's written acceptance of the initial final assessment report, the successful bidder shall remain responsible for the two (2) included remediation retest cycles for a further period of up to three (3) months. Any period beyond this retesting window requires written NMISA approval. Delays attributable to the service provider shall not entitle the service provider to additional fees or an automatic extension. Any additional scope or expenditure must be approved by NMISA in writing before the relevant services are performed. Optional services will only be undertaken where specifically authorized by NMISA in writing.

11. PRICING

Bidders must submit a comprehensive, fixed and transparent pricing proposal for the complete core engagement, including inception, the initial assessments, reporting, remediation workshop, two (2) included remediation retest cycles and close-out. All prices must be quoted in South African Rand (ZAR), excluding and including VAT as applicable. Prices must include all professional fees, project management, licensed tools, reporting, workshops, local travel, subsistence and incidental costs necessary to deliver the quoted core service. The Evaluated Bid Price shall comprise Core Assessment Services only. Optional/on-demand rates shall be quoted separately and shall not be included in the Evaluated Bid Price or Total Bid Price used for bid comparison.

No.	Service / Resource Category	Pricing Basis	Unit Rate	Quantity / Period	Total Price
A	CORE ASSESSMENT SERVICES				
1	Inception, discovery and Rules of Engagement	Once-off	R	1	R
2	External vulnerability assessment and penetration test	Assessment	R	1	R
3	Internal vulnerability assessment and penetration test	Assessment	R	1	R
4	Microsoft Azure / cloud security assessment	Assessment	R	1	R
5	Microsoft Entra ID / identity security assessment	Assessment	R	1	R
6	Web application / portal penetration testing	Per application	R	Baseline: 3 applications/ APIs	R

No.	Service / Resource Category	Pricing Basis	Unit Rate	Quantity / Period	Total Price
7	Wireless network security assessment	Assessment	R	1	R
8	Technical remediation workshop and executive presentation	Once-off	R	1	R
9	Two (2) remediation retest cycles and closure verification of findings	Fixed price	R	Includes 2 retest cycles	R
10	Final consolidated close-out report	Once-off	R	1	R
B	OPTIONAL / ON-DEMAND RATE SCHEDULE - EXCLUDED FROM EVALUATED BID PRICE				
11	Additional web application / API penetration testing above baseline quantity	Per application/API	R	Rate only	N/A
12	Additional targeted penetration testing arising from an approved material infrastructure/application change during the engagement	Per day	R	Rate only	N/A
13	Social engineering / phishing simulation (only when authorized)	Per campaign	R	Rate only	N/A
14	Senior penetration tester / security specialist	Hourly rate	R	Rate only	N/A
15	Additional penetration tester / security analyst	Hourly rate	R	Rate only	N/A
	CORE SERVICES SUBTOTAL EXCLUDING VAT (EVALUATED BID PRICE)				R
	VAT ON CORE SERVICES				R
	TOTAL CORE BID PRICE INCLUDING VAT				R

Pricing Note: Only Core Assessment Services (Items 1-10) shall form part of the Evaluated Bid Price. Optional/on-demand rates (Items 11-15) are rate-only items, shall not be added to the

evaluated or total core bid price, and create no commitment or guaranteed expenditure by NMISA. Optional services may only be rendered after prior written NMISA instruction and an applicable purchase order/contract authorization.

Optional/on-demand services may only be used following a written NMISA instruction and applicable purchase order/contract authorization. Quoted optional rates do not constitute guaranteed expenditure or a commitment by NMISA to purchase those services. Optional rates shall not form part of the Evaluated Bid Price. No additional work may be undertaken or invoiced without prior written authorization.

Bidders must state the validity period of the quotation, which must be not less than ninety (90) days from the RFQ closing date unless SCM specifies otherwise. Core prices must remain firm for the engagement, subject only to applicable tax changes or formally approved contract variations.

No separate charge will be accepted for project management, standard reporting, evidence preparation, ordinary local travel, tool licensing, workshops or other activities reasonably necessary to deliver the core scope unless expressly identified as an approved optional item in this TOR.

12. MANDATORY/ LEGISLATIVE REQUIREMENT

This stage checks and validates the bidders' compliance to the legal requirements to conduct business in South Africa, as well as to the industry requirement for the supply of goods and services.

NB: No points will be allocated to this stage; however, bidders' must comply with the pre-qualification requirements below to advance to the next stage of evaluation.

Pre-Qualification Requirements		Check list ✓ Tick each box
SBD 4:	Completed, attached and signed	
SBD 6.1:	Completed, attached and signed	
CSD report	Attached	

Note: Some requirements may not be applicable to International suppliers/ bidders and only those suppliers/ bidders will be exempted from these mandatory/ legislative requirements. All SBDs must be submitted (signed) noting where it is not applicable. If any specific SBD is not submitted, documentary proof, clearly stating the reason must be attached.

Bidders must also supply the documents below (where applicable).

Other Requirements	Check list ✓ Tick each box
Valid B-BBEE Certificate attached	

13. EVALUATION PROCESS

13.1 AIM OF EVALUATION

To ensure that all bids/ proposals received are afforded the opportunity to compete equally and enable NMISA a chance to evaluate the bid received in a fair and unbiased manner as per the pre-determined evaluation criteria.

13.2 EVALUATION CRITERIA

The evaluation criteria as set out hereunder will assist NMISA to ensure conformity to tender requirements. NMISA evaluation team shall use the evaluation criteria, applicable values and/or minimum qualifying scores as indicated in the bid specification document.

The following are the stages that will be used to evaluate all bid/s received.

14. COMPULSORY TECHNICAL SPECIFICATIONS

Please complete the table below by indicating “yes” or “no” to confirm whether this requirement is met and provide explanations/ comments to support your answers. Supporting documentation or evidence should be attached to this document, if no evidence is provided, it will be assumed that the specification cannot be met. Supporting documentation should take the form of technical specifications, datasheets, technical drawings, brochures, etc. **Supporting documents should have page numbers for ease of reference.**

NB: Bids that score NO for any items in the compulsory technical specification section will be disqualified and will not advance to the next stage of evaluation.

No.	Mandatory Requirement	Minimum Evidence Required	Yes or No	Evidence/Page Reference
1.	Valid Professional Indemnity and Cyber Liability Insurance appropriate to the engagement	Bidder may submit current evidence of cover or a signed undertaking with the bid. The successful bidder must provide valid policy		

	is a condition precedent to commencement of testing.	schedules/certificates, at the minimum cover level determined by NMISA before contract commencement. Failure to provide the required cover within the stipulated contracting period may result in cancellation of the award. No testing may commence while uninsured.		
2.	The bidder must disclose any proposed subcontractors and confirm that no subcontractor will perform testing without prior written NMISA approval.	Signed declaration identifying proposed subcontractors and their scope or confirming that no subcontractors are proposed.		

15. FUNCTIONAL SPECIFICATIONS

Only bidders that meet all mandatory requirements will proceed to functional evaluation. A minimum qualifying score of **80 out of 100** is required. Only evidence relevant to penetration testing, vulnerability assessment and closely related cybersecurity assessment services will be considered for scoring.

Where project experience is claimed, evidence must sufficiently demonstrate the nature and scope of services performed. Appointment letters without evidence of the actual relevant scope may not be sufficient on their own.

Criteria	Weight	Evidence Required	Scoring Guide	Evidence/Page Reference
1. Company Experience and Track Record	20	Reference letters/completion evidence for distinct comparable penetration testing/vulnerability assessment projects completed within the last five years. Evidence must identify client, scope/services, completion date and contactable reference. Duplicate descriptions of the same engagement count once.	20 = 5 or more qualifying projects; 16 = 4; 12 = 3; 8 = 2; 4 = 1; 0 = none.	

Criteria	Weight	Evidence Required	Scoring Guide	Evidence/Page Reference
1. Proposed Technical Methodology	25	Detailed methodology covering external, internal, web/application, cloud/identity, wireless, manual validation, controlled exploitation, evidence handling, risk rating, reporting and retesting.	25 = comprehensive and fully addresses all areas with clear sequencing, controls and outputs; 20 = strong with minor gaps; 15 = adequate but material detail missing; 10 = generic/limited; 0 = absent or unsuitable.	
2. Key Personnel Experience and Capability	20	CVs showing roles, years of relevant experience and comparable projects for Project Lead and technical testers.	20 = lead 8+ years and at least two testers 5+ years each; 16 = lead 6-7 years and two testers 4+ years each; 12 = meets mandatory minimum with relevant comparable work; 0 = does not meet mandatory minimum.	
3. Professional Certifications	10	Valid certifications held by the actual proposed delivery personnel. Certificates must identify the certified individual and be current/verifiable where the certification has an expiry/maintenance requirement.	10 = strong certification coverage across the proposed team incl. 2+ hands-on offensive-security certifications; 8 = 3 relevant certifications across team incl. at least 1 hands-on; 6 = mandatory minimum met incl. at least 1 hands-on; 0 = below mandatory. Multiple certificates held by one individual do not substitute for required team capability.	

Criteria	Weight	Evidence Required	Scoring Guide	Evidence/Page Reference
4. Reporting, Remediation and Retesting Approach	15	Sample anonymized report or detailed report template plus remediation/retest approach.	15 = strong technical + executive reporting, reproducible evidence, prioritized remediation and clear closure workflow; 12 = good with minor gaps; 8 = adequate; 4 = weak/generic; 0 = absent.	
5. Project Plan, Governance and Service Protection	10	Project plan / approach covering scheduling, RoE, communications, escalation, critical finding notification, stop-test process and protection of production services.	10 = comprehensive and practical; 8 = good with minor gaps; 4 = adequate; 2 = limited; 0 = absent.	

TOTAL FUNCTIONAL SCORE: 100 POINTS. MINIMUM QUALIFYING THRESHOLD: 80 POINTS.

16. DELIVERABLE ACCEPTANCE AND PAYMENT

1. All deliverables are subject to written review and acceptance by NMISA. Submission of a deliverable or completion of a testing activity does not constitute acceptance.
2. NMISA may reject incomplete, inaccurate, unsupported, materially false-positive-heavy or non-compliant deliverables and require correction at no additional cost. A deliverable will only be considered complete once deficiencies identified by NMISA have been corrected and written acceptance has been issued.
3. Assessment deliverables will only be accepted where the agreed scope and baseline/sizing information has been tested and confirmed findings contain sufficient reproducible evidence, CVSS v4.0 risk classification, affected assets/components, NMISA business impact and remediation guidance. Before a final report is issued, the bidder shall provide NMISA a reasonable opportunity to verify factual details such as affected assets and environment context; this factual validation process may not be used to suppress, downgrade or remove a technically substantiated finding without evidence.
4. Each assessment report must include a scope-coverage statement showing targets tested, targets not tested, exclusions, failed/incomplete tests and the reason for any deviation from the approved Rules of Engagement. Unperformed scope may not be treated as completed without written NMISA acceptance.
5. Invoices must be linked to milestones/deliverables formally accepted in writing by NMISA or to optional services specifically authorized and actually performed. No payment is due merely because testing activity has commenced or a draft report has been submitted.
6. Retesting and closure deliverables must clearly distinguish between Closed, Partially Remediated, Open, Risk Accepted and Not Retested findings and provide validation evidence for status changes.

7. Final payment may be withheld until the final consolidated report, evidence handover and information-destruction obligations have been completed.

17. CONFIDENTIALITY, INFORMATION SECURITY AND DATA HANDLING

1. All information obtained during the engagement is confidential and remains the property of NMISA.
2. The bidder may not disclose, publish, demonstrate, present, reuse as a case study, or otherwise share NMISA vulnerabilities, architecture, credentials, evidence or reports with any third party, conference, training audience, research activity or marketing material without prior written NMISA approval.
3. Assessment data and evidence must be encrypted at rest and in transit and access must be restricted to authorized project personnel.
4. Credentials and secrets obtained or provided during testing must be encrypted, restricted to named authorized personnel, may not be reused outside the authorized assessment, and must be securely returned or destroyed at close-out.
5. NMISA data may not be used to train public or third-party artificial intelligence models or uploaded to unapproved external services.
 - 5.1 The bidder must notify NMISA immediately of any loss, unauthorized disclosure or compromise of assessment information.
 - 5.2 The bidder must comply with the Protection of Personal Information Act, 2013 (POPIA), where applicable, and process personal information only to the extent necessary for the authorized assessment and in accordance with NMISA instructions.
6. Any actual or suspected compromise, loss or unauthorized disclosure of NMISA assessment information must be reported to NMISA immediately, with an initial written incident summary within twenty-four (24) hours and subsequent updates as reasonably required.
7. At engagement close, the bidder must return all NMISA information and securely destroy residual copies, including reports, screenshots, credentials, scan data, exported data and other assessment evidence, subject only to lawful retention requirements. The bidder must provide a signed certificate of destruction identifying the categories of information destroyed.

18. EXIT AND CLOSE-OUT

1. Transfer all final reports, evidence, registers, presentations and agreed working documentation to NMISA.
2. Provide a final consolidated findings register and status of remediation/retesting.
3. Conduct a final knowledge-transfer and close-out session.
4. Remove NMISA credentials, test accounts under the bidder's control, data extracts, scan data and evidence from bidder-controlled systems when no longer required.
5. Provide a signed certificate confirming that NMISA information has been returned or securely destroyed in accordance with the agreed retention requirements.
6. Cooperate with NMISA or a successor service provider on reasonable clarification of outstanding findings during close-out.

19. PRICE AND B-BBEE POINTS

Bidders that met the requirements of the previous stage will be evaluated further in accordance with the 80/20 preferential points system. The 80 points will be allocated for price whilst, 20 points will be allocated for specific goals both totalling 100 points.

The formula below will be used in calculating points scored for the Preference points system.

Step 1: Calculation of points for price

Points awarded for price

The following formula would be applied:

$$P_s = 80 \left(1 - \frac{P_t - P_{min}}{P_{min}} \right)$$

Where

Ps = Points scored for comparative price of bid or offer under consideration

Pt = Comparative price of bid or offer under consideration

Pmin = Comparative price of lowest acceptable bid or offer.

Step 2: Points allocated for B-BBEE status level of contributor

A maximum of 20 points will be awarded for B-BBEE Status Level 1 of Contributor.

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

Note: Both points will be added together to obtain a final score out of 100 points in total.

NOTES TO SUPPLIER

- Suppliers are required to respond with a quotation containing their company letterhead.
- NMISA is a schedule 3A public entity according to PFMA and effects payments when all goods and services are delivered in full.
- Quotations should be firm and valid for at least a period of 30 days
- Quotations must clearly indicate delivery period.

- *All Supplier quotations are subject to the provisions of the attached SBD forms.*
- For pricing above R2 000.00 - BBBEE certificate must be attached.
- Our mailbox size is 8MB. If your proposal is above the size, please send through in part emails. It is important to note that only submissions that are submitted on time will be considered.
- Quotations should be sent to **scm3@nmisa.org**
- *The response should reach NMISA not later than **Friday, 23 October 2026 @ 14:00 pm***

For commercial queries, please contact:

Supply Chain

Tel: 012 947 2875

e-mail: scm3@nmisa.org.

For other queries, please contact:

Bongani Mabunda

Tel: 012 947 2712

e-mail: bmabunda@nmisa.org

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

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.

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 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

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.

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

PREFERENCE POINTS CLAIM FORM IN TERMS OF NMISA SCM POLICY

This preference form must form part of all bids invited. It contains general information and serves as a claim form for preference points for Broad-Based Black Economic Empowerment (B-BBEE) Status Level of Contribution

NB: BEFORE COMPLETING THIS FORM, BIDDERS MUST STUDY THE GENERAL CONDITIONS, DEFINITIONS AND DIRECTIVES APPLICABLE IN RESPECT OF B-BBEE, AS PER NMISA SCM POLICY.

1. GENERAL CONDITIONS

1.1 The following preference point systems are applicable to all bids:

- the 80/20 system for requirements with a Rand value of up to R50 000 000 (all applicable taxes included); and
- the 90/10 system for requirements with a Rand value above R50 000 000 (all applicable taxes included).

1.2

- a) The value of this bid is estimated to **exceed/not exceed** R50 000 000 (all applicable taxes included) and therefore the preference point system shall be applicable; or
- b) Either the 80/20 or 90/10 preference point system will be applicable to this tender (*delete whichever is not applicable for this tender*).

1.3 Points for this bid shall be awarded for:

- (a) Price; and
- (b) B-BBEE Status Level of Contributor.

1.4 The maximum points for this bid are allocated as follows:

	POINTS
PRICE	
B-BBEE STATUS LEVEL OF CONTRIBUTOR	
Total points for Price and B-BBEE must not exceed	100

1.5 Failure on the part of a bidder to submit proof of B-BBEE Status level of contributor together with the bid, will be interpreted to mean that preference points for B-BBEE status level of contribution are not claimed.

1.6 The purchaser reserves the right to require of a bidder, either before a bid is adjudicated or at any time subsequently, to substantiate any claim in regard to preferences, in any manner required by the purchaser.

2. DEFINITIONS

- (a) **“B-BBEE”** means broad-based black economic empowerment as defined in section 1 of the Broad-Based Black Economic Empowerment Act;
- (b) **“B-BBEE status level of contributor”** means the B-BBEE status of an entity in terms of a code of good practice on black economic empowerment, issued in terms of section 9(1) of the Broad-Based Black Economic Empowerment Act;
- (c) **“bid”** means a written offer in a prescribed or stipulated form in response to an invitation by an organ of state for the provision of goods or services, through price quotations, advertised competitive bidding processes or proposals;
- (d) **“Broad-Based Black Economic Empowerment Act”** means the Broad-Based Black Economic Empowerment Act, 2003 (Act No. 53 of 2003);
- (e) **“EME”** means an Exempted Micro Enterprise in terms of a code of good practice on black economic empowerment issued in terms of section 9 (1) of the Broad-Based Black Economic Empowerment Act;
- (f) **“functionality”** means the ability of a tenderer to provide goods or services in accordance with specifications as set out in the tender documents.
- (g) **“prices”** includes all applicable taxes less all unconditional discounts;
- (h) **“proof of B-BBEE status level of contributor”** means:
 - 1) B-BBEE Status level certificate issued by an authorized body or person;
 - 2) A sworn affidavit as prescribed by the B-BBEE Codes of Good Practice;
 - 3) Any other requirement prescribed in terms of the B-BBEE Act;
- (i) **“QSE”** means a qualifying small business enterprise in terms of a code of good practice on black economic empowerment issued in terms of section 9 (1) of the Broad-Based Black Economic Empowerment Act;
- (j) **“rand value”** means the total estimated value of a contract in Rand, calculated at the time of bid invitation, and includes all applicable taxes;

3. POINTS AWARDED FOR PRICE

3.1 THE 80/20 OR 90/10 PREFERENCE POINT SYSTEMS

A maximum of 80 or 90 points is allocated for price on the following basis:

$$\begin{array}{ccc}
 \mathbf{80/20} & \mathbf{or} & \mathbf{90/10} \\
 P_s = 80 \left(1 - \frac{P_t - P_{\min}}{P_{\min}} \right) & \text{or} & P_s = 90 \left(1 - \frac{P_t - P_{\min}}{P_{\min}} \right)
 \end{array}$$

Where

P_s = Points scored for price of bid under consideration
 P_t = Price of bid under consideration
 $P_{\min}$ = Price of lowest acceptable bid

4. POINTS AWARDED FOR B-BBEE STATUS LEVEL OF CONTRIBUTOR

- 4.1 In terms of NMISA SCM Policy, preference points must be awarded to a bidder for attaining the B-BBEE status level of contribution in accordance with the table below:

B-BBEE Status Level of Contributor	Number of points (90/10 system)	Number of points (80/20 system)
1	10	20
2	9	18
3	6	14
4	5	12
5	4	8
6	3	6
7	2	4
8	1	2
Non-compliant contributor	0	0

5. BID DECLARATION

- 5.1 Bidders who claim points in respect of B-BBEE Status Level of Contribution must complete the following:

6. B-BBEE STATUS LEVEL OF CONTRIBUTOR CLAIMED IN TERMS OF PARAGRAPHS 1.4 AND 4.1

- 6.1 B-BBEE Status Level of Contributor: . = ...(maximum of 10 or 20 points)
(Points claimed in respect of paragraph 7.1 must be in accordance with the table reflected in paragraph 4.1 and must be substantiated by relevant proof of B-BBEE status level of contributor.

7. SUB-CONTRACTING

- 7.1 Will any portion of the contract be sub-contracted?

(Tick applicable box)

YES	☐	NO	☐
-----	--------------------------	----	--------------------------

- 7.1.1 If yes, indicate:

- What percentage of the... contract will be subcontracted %
- The name of the sub-contractor.....
- The B-BBEE status level of the sub-contractor.....
- Whether the sub-contractor is an EME or QSE

(Tick applicable box)

YES	☐	NO	☐
-----	--------------------------	----	--------------------------

- v) Specify, by ticking the appropriate box, if subcontracting with an enterprise in terms of Preferential Procurement Regulations, 2017:

Designated Group: An EME or QSE which is at least 51% owned by:	EME √	QSE √
Black people	☐	☐
Black people who are youth	☐	☐
Black people who are women	☐	☐
Black people with disabilities	☐	☐
Black people living in rural or underdeveloped areas or townships	☐	☐
Cooperative owned by black people	☐	☐

Black people who are military veterans		
OR		
Any EME		
Any QSE		

8. DECLARATION WITH REGARD TO COMPANY/FIRM

8.1 Name of company/firm:.....

8.2 VAT registration number:.....

8.3 Company registration number:.....

8.4 TYPE OF COMPANY/ FIRM

- ☐ Partnership/Joint Venture / Consortium
 - ☐ One person business/sole propriety
 - ☐ Close corporation
 - ☐ Company
 - ☐ (Pty) Limited
- [TICK APPLICABLE BOX]

8.5 DESCRIBE PRINCIPAL BUSINESS ACTIVITIES

.....

.....

.....

.....

.....

8.6 COMPANY CLASSIFICATION

- ☐ Manufacturer
 - ☐ Supplier
 - ☐ Professional service provider
 - ☐ Other service providers, e.g. transporter, etc.
- [TICK APPLICABLE BOX]

8.7 Total number of years the company/firm has been in business:.....

8.8 I/we, the undersigned, who is / are duly authorised to do so on behalf of the company/firm, certify that the points claimed, based on the B-BBE status level of contributor indicated in paragraphs 1.4 and 6.1 of the foregoing certificate, qualifies the company/ firm for the preference(s) shown and I / we 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 6.1, the contractor may be required to furnish documentary proof to the satisfaction of the purchaser that the claims are correct;
- iv) If the B-BBEE status level of contributor has been claimed or obtained on a

fraudulent basis or any of the conditions of contract have not been fulfilled, the purchaser 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 by the National Treasury 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.

WITNESSES

1.
2.

.....
SIGNATURE(S) OF BIDDERS(S)

DATE:

ADDRESS

.....

.....