REFER TO ANNEXURES (PRICING SCHEDULE)

Pricing Instructions and Conditions

The bidder **MUST** take note of the following

- **Authorized Signatory:** The pricing schedule must be duly signed by the bidder or by a person duly authorized through a valid board resolution, which must be attached to the bid. Failure to provide a signed pricing schedule will result in disqualification.

- **Completeness of Pricing Schedule:** All pricing information must be fully completed. Incomplete schedules will result in disqualification. No alterations or amendments will be accepted after submission of the bid.

- **Price Adjustments:** Prices must remain firm for the first twelve (12) months of the contract. Thereafter, a once-off price adjustment may be applied in the 13th month, based on the average Consumer Price Index (CPI) as published by Stats SA.

- **Currency and VAT:** All prices must be quoted in South African Rand (ZAR) and must be VAT inclusive.

- **Travel and Accommodation:** The bidder is responsible for all travel and accommodation costs incurred during the execution of the contract, unless otherwise agreed in writing by NHBRC.

Pricing Table: Bidders must complete the pricing schedule below. **All prices must be VAT inclusive**.

REFER TO ANNEXURES

Annexure A: Detailed Technical Requirements and Bidder Response Matrix

Annexure A: Detailed Technical Requirements and Bidder Response Matrix

Instructions

Bidders must respond to each requirement in the matrix below, indicating compliance (Yes/No), providing evidence, and referencing supporting documentation.
All requirements are mandatory unless otherwise stated.

Requirement ID	Requirement Description	Mandatory	Expected Evidence	Bidder Response
A1	Provide a layered security architecture covering cloud, network, server, application, database, identity, endpoint/device, and data security.	Mandatory	Solution architecture diagrams, narrative	

A2	Integrate with NHBRC's existing Microsoft 365 E3/E5, Azure, and FortiGate/OpenVPN environment, or propose alternatives with justification.	Mandatory	Integration plan or alternative proposal	
A3	Operate a 24/7/365 SOC based in South Africa, with all analyst access performed locally.	Mandatory	SOC location, operational model	
A4	Provide SIEM/SOAR capabilities, integrating all relevant log sources and supporting automation/playbooks.	Mandatory	SIEM/SOAR platform details, integration evidence	
A5	Deliver XDR/EDR coverage for endpoints, servers, and identities.	Mandatory	EDR/XDR platform details, coverage plan	
A6	Implement vulnerability management and annual penetration testing, including retesting.	Mandatory	VA/PT methodology, sample reports	
A7	Provide incident response and forensics capability, aligned to NIST 800-61.	Mandatory	IR plan, playbooks, retainer details	
A8	Deliver threat intelligence services, including actionable TI feeds, periodic briefings, and IOC integration.	Mandatory	TI sources, sample reports	

A9	Provide continuous exposure management (ASM/CTEM), including external attack surface monitoring and credential exposure checks.	Mandatory	ASM/CTEM methodology, sample outputs	
A10	Deliver a comprehensive cyber awareness programme, including phishing simulations and reporting.	Mandatory	Awareness plan, sample materials	
A11	Implement document security (encryption/password protection/audit logging) for sensitive documents.	Mandatory	Document security policy, technical controls	
A12	Develop/update policies: CIRP, third-party access, SOC engagement, identity/PAM, vulnerability/patch, data classification/retention, acceptable use.	Mandatory	Policy documents, review schedule	
A13	Provide all deliverables as per Section 4.7 of the TOR.	Mandatory	Deliverables register	
A14	Hold valid ISO/IEC 27001:2022 certification	Mandatory	Certificates, ~~attestation letters~~	
A15	Assign qualified resources with relevant certifications and experience.	Mandatory	CVs, certification evidence	
A16	Provide three (3) contactable reference letters for similar MSSP engagements.	Mandatory	Reference letters	

Bidders may add additional rows for value-add features or alternative approaches.

Annexure B: SLA & KPI Framework (Full)

Service Level Agreements (SLAs)

Service Area	Metric	Target	Measurement	Reporting
SOC Operations	24/7 Monitoring Coverage	100%	SOC shift logs	Monthly
Incident Detection	P1 MTTD	≤ 15 minutes	SIEM timestamps	Monthly
Incident Response	P1 MTTR (Containment)	≤ 2 hours	Incident records	Monthly
Incident Handling	P2 Response Time	≤ 30 minutes (95%)	Incident records	Monthly
Vulnerability Mgmt	Critical Remediation	≤ 7 days	VA tracker	Monthly
Vulnerability Mgmt	High Remediation	≤ 14 days	VA tracker	Monthly
Endpoint Security	Device Coverage	≥ 95%	EDR reports	Monthly
Detection Quality	False Positive Rate	≤ 15%	SOC analytics	Quarterly
Use Case Delivery	Initial SOC Use Cases	≥ 30 within 60 days	Use-case register	Quarterly
Awareness	Phishing Simulations	≥ Quarterly	Awareness reports	Quarterly
Governance	Reporting Timeliness	100% on time	Submission logs	Monthly

Key Performance Indicators (KPIs)

- Reduction in MTTD and MTTR versus baseline
- Reduction in unresolved critical vulnerabilities
- Use-case effectiveness and tuning improvements
- Cyber-awareness improvement (click rate, report rate)
- Policy compliance and audit outcomes

Annexure C: Evaluation Scoring Matrix (weighted)

Annexure C: Evaluation Scoring Matrix (Weighted)

Stage 2A – Technical Evaluation (80 Points)

Criterion	Description	Weight
Bidder Experience	MSSP experience ≥ 5 years	10
References	Relevance & quality of reference letters	20
Team Capability	Skills, certifications, CVs	30
Methodology & Approach	Transition, governance & delivery	20
Subtotal		**80**

Stage 2B – Live SOC Demonstration (20 Points)

Criterion	Weight

SOC Architecture & Integration	5
Incident Detection & Response	5
Endpoint & Identity Controls	3
Vulnerability &Patch Management	2
Compliance, Data Protection & Reporting	5
Total	**20**

Minimum qualifying score: 80 / 100

Annexure D: SOC Use Case Catalogue (baseline)

Annexure D: SOC Use Case Catalogue (Baseline)

ID	Use Case
UC-01	Impossible travel / anomalous authentication
UC-02	Privilege escalation attempts
UC-03	Phishing & business email compromise
UC-04	Ransomware indicators & lateral movement
UC-05	Insider data exfiltration
UC-06	OAuth consent abuse
UC-07	Service account anomalies
UC-08	Endpoint malware & exploit detection

UC-09	Suspicious mailbox rules
UC-10	Mass data export/download
UC-11	Cloud misconfiguration events
UC-12	Password spray & brute-force attacks
UC-13	DLP policy violations
UC-14	Vulnerability exploitation activity

All use cases must be mapped to **MITRE ATT&CK** and supported by runbooks.

Annexure E: Pricing Schedule

Annexure E: Pricing Schedule

(All prices VAT inclusive, in ZAR)

Cost Category	Year 1	Year 2	Year 3	Year 4	Year 5	Total
Implementation & Transition						
SOC Operations (24/7)						
Incident Response Retainer						
Vulnerability & Penetration Testing						
Exposure Management						

Threat Intelligence						
Governance & Policy Support						
Cyber Awareness & Training						
Ad-hoc Services						
Total (Excl. VAT)						
VAT (15%)						
Total (Incl. VAT)						

NB: Bidders must include escalations for each year for the duration of the contract.

Annexure F: Glossary of Terms and Acronyms

Annexure F: Glossary of Terms and Acronyms

Purpose

This Glossary defines key technical, operational, and governance terms used throughout the Terms of Reference (TOR) and associated Annexures. The Glossary is intended to e

Instruction on Placement in the TOR

Placement Recommendation:

- This Glossary must be included as Annexure G and referenced explicitly in:
  - The *Introduction* section of the TOR (e.g. "Definitions and Acronyms used in this TOR are provided in Annexure G").
  - Annexure A (Technical Requirements) to avoid repetitive explanations.
- The Glossary must be treated as a normative reference, i.e. definitions apply wherever the terms are used in the TOR and Annexures.

A. General & Governance Terms

Acceptable Use Policy (AUP) – A policy defining acceptable and prohibited use of NHBRC systems, data, and devices.
Audit Trail – A chronological record of activities enabling reconstruction, review, and examination of events or transactions.
Compliance – Adherence to applicable laws, regulations, standards, and NHBRC internal policies including POPIA and PFMA.
Defence-in-Depth – A layered security strategy using multiple complementary security controls across people, process, and technology.
Evidence – Objective proof provided by a bidder to demonstrate compliance with a TOR requirement (e.g. certificates, reports, diagrams).
Governance – Structures, policies, and processes that ensure cybersecurity activities align with NHBRC strategy and regulatory obligations.

B. SOC, Monitoring & Response Terms

Security Operations Centre (SOC) – A centralised function responsible for continuous monitoring, detection, analysis, and response to cybersecurity threats.
SOC 2 Type II – An independent assurance report assessing the design and operating effectiveness of controls over a defined period.
SIEM (Security Information and Event Management) – Technology that collects, correlates, and analyses security log data.
SOAR (Security Orchestration, Automation and Response) – Technology enabling automated workflows, playbooks, and response actions.
Use Case – A defined detection or response scenario describing a specific threat, risk, or malicious behaviour.
Runbook / Playbook – Documented procedures describing analyst or automated actions to be performed during defined security events.
MTTD (Mean Time to Detect) – Average time taken to identify a security incident from the point of occurrence.
MTTR (Mean Time to Respond/Recover) – Average time taken to contain or remediate a security incident after detection.

C. Threat, Risk & Exposure Terms

Threat Intelligence (TI) – Evidence-based information about existing or emerging threats, threat actors, and attack techniques.
Indicator of Compromise (IOC) – Observable artefacts indicating potential malicious activity (e.g. IP addresses, hashes).
Indicator of Attack (IOA) – Behavioural indicators suggesting malicious intent or activity.
MITRE ATT&CK – A globally recognised knowledge base describing adversary tactics, techniques, and procedures.
Exposure Management – Continuous identification, prioritisation, and remediation of attack paths, vulnerabilities, and misconfigurations.
ASM (Attack Surface Management) – Discovery and monitoring of internet-facing assets and exposures.

CTEM (Continuous Threat Exposure Management) – A risk-driven approach combining ASM, vulnerability management, and attack-path analysis.

D. Vulnerability & Testing Terms

Vulnerability – A weakness that can be exploited to compromise confidentiality, integrity, or availability.
Vulnerability Assessment (VA) – Systematic identification and analysis of vulnerabilities in systems and applications.
Penetration Testing (PT) – Controlled exploitation of vulnerabilities to assess security effectiveness.
CVSS (Common Vulnerability Scoring System) – An open standard for severity rating of vulnerabilities.

E. Identity, Access & Data Protection Terms

Identity and Access Management (IAM) – Processes and technologies managing digital identities and access rights.
Privileged Access Management (PAM) – Controls governing high-risk administrative and privileged accounts.
JIT / JEA (Just-In-Time / Just-Enough-Access) – Time-bound and least-privileged access control mechanisms.
Multi-Factor Authentication (MFA) – Authentication using two or more independent credential factors.
Data Loss Prevention (DLP) – Controls designed to prevent unauthorised disclosure of sensitive information.
Document Security – Encryption, access control, and audit logging applied at document level.

F. Awareness & Human Risk Terms

Cyber Awareness Programme – Structured training and behavioural initiatives aimed at reducing human-related cyber risk.
Phishing Simulation – Controlled testing of user susceptibility to phishing techniques.
Human Risk Metrics – Measurements such as click rate, report rate, and repeat offender rate used to assess awareness effectiveness.

G. Legal & Regulatory Terms

POPIA – Protection of Personal Information Act, 2013.

PFMA – Public Finance Management Act, 1999.
ISO/IEC 27001 – International standard for information security management systems.
NIST CSF – National Institute of Standards and Technology Cybersecurity Framework.

Maintenance

The MSSP must review and update this Glossary annually or when new technologies, services, or terms are introduced.