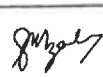
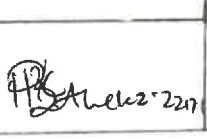
SCOPE OF WORK FOR THE PROVISION OF MANAGED CYBERSECURITY SERVICES (MSSP)

Revision: 3

Revised date: 18/06/2026

NAME	TITLE	EMPL.NO	SIGNATURE	DATE
COMPILED - RECOMMENDATION				
Dharmesh Sirpal	Specialist ICT Compliance	501103		18 June 2026

NAME	TITLE	EMPL.NO	SIGNATURE	DATE
APPROVAL TO PROCEED				
Antonio Nogueira	ICT Operations Manager (PHB)	10800		19 June 2026
Raymond Naidoo	ICT Operations Manager (RBY)	500704		19 June 2026
Sthe Mzobe	Acting GM ICT	25773		19 June 2026
Precious Buthelezi	Acting GM Acid Division	22171		23/06/2026

Contents

1. Confidentiality and Conditions 3
2. Executive Summary and Objectives 3
3. Security Monitoring 24/7/365 (24 hours/day, 7 days/week, 365 days/year) 5
4. Incident Detection and Response 6
5. Vulnerability & Risk Assessments 7
6. Cybersecurity Awareness Training 8
7. Ad-hoc Services (Consulting, advisory, and forensics) 8
8. Roles and Responsibilities 8
9. Reporting and Compliance 9
10. Governance and Service Management 9
11. Service Level Agreements (SLAs), and Key Performance Indicators (KPI) 10
12. Managed Security Services Resources (Experience and Certifications) 11
13. Submission of Proposal Requirements 12
14. Proposal Evaluation Process 13
15. Price Proposal 14

Annexures 15

1. Confidentiality and Conditions

The contractor shall not disclose any such information or specification, whether explicit or implied, to any third party without the express written permission of a duly authorized representative of FOSKOR. Any contractor electing not to respond to this Request for Proposal (RFP) shall ensure that the original correspondence and / or electronic media are returned to Foskor.

The terms set out here are for recording the basis of the principles and topics upon which the parties will be required to reach agreement in concluding on the proposed agreement. It shall not be binding until they are incorporated into a comprehensive formal and final contract agreement signed by both parties.

Contractors are required to submit full technical and support documentation of their proposed course of action where necessary. The contractor must accept Foskor's minimum standard in terms of quality and specification. The costs incurred in preparing the RFP are for the account of the contractor. Foskor (Pty) Ltd will not accept liability for the costs arising out of the delay in the Tender process.

The contractor must guarantee the validity of the response to this tender enquiry. Any arithmetical errors in pricing are the contractor's responsibility. The preferred contractor will sign a contract, after which the terms and conditions of the contract will govern them. If the contractor defaults, the Client, Foskor (Pty) Ltd, will have recourse in terms of the conditions as stipulated in the contract.

2. Executive Summary and Objectives

In today's evolving cyber threat landscape, protecting digital assets requires specialist, round-the-clock capability that is often costly and difficult to build and sustain in-house. A Managed Security Services Provider (MSSP) can act as an extension of Foskor's ICT function or as a fully outsourced Security Operations Centre (SOC) to help secure networks, endpoints, cloud services, and related digital assets. By converting security telemetry into actionable intelligence, an MSSP should reduce risk, accelerate detection and response, and improve the operational efficiency of managing a complex cybersecurity environment.

2.1. Purpose:

The purpose of this scope of work is to provide outsourced Managed Cybersecurity Services from a Managed Security Services Provider (MSSP) to strengthen Foskor's cybersecurity operations for a contract period of sixty (60) months.

2.2. Business Goals:

Foskor would like to partner with an MSSP to achieve the following foundational objectives:
Foskor intends to partner with an MSSP to achieve the following objectives:

- **Round-the-Clock Monitoring (24/7/365):** Providing continuous visibility into an organization's IT infrastructure to catch and mitigate attacks before they cause operational downtime.

- **Advanced Threat Detection & Response:** Utilizing the latest machine learning, behaviour analytics, and human intelligence to hunt for threats, triage alerts, and execute rapid incident response.

- **Bridging the Talent Gap:** Supplying immediate access to highly specialized, certified cybersecurity professionals without the heavy financial burden of recruiting and training a dedicated internal team.

- **Vulnerability and Risk Management:** Conducting regular vulnerability scanning, security assessments, and control hardening support to identify and reduce exploitable weaknesses. Patch remediation support should be clearly defined where applicable, as patch execution may remain a Foskor responsibility.

- **Compliance and Audit Readiness:** Assisting Foskor to strengthen controls, reporting, and evidence management to support applicable legal, regulatory, and governance requirements, including POPIA, the Cybercrimes Act, and relevant internal governance standards. Where relevant, alignment to recognized standards such as ISO/IEC 27001, NIST CSF, or ISA/IEC 62443 should be demonstrated.

- **Cost Efficiency & Scalability:** Offering enterprise-grade security through predictable, subscription-based pricing models that can easily scale as the client's business grows or its risk landscape changes.

- **Operational Technology (OT) and Manufacturing Resilience:** Supporting a security approach that recognizes Foskor’s manufacturing environment, prioritizes plant availability and safety, and clearly distinguishes between IT and OT/industrial control system (ICS) monitoring, escalation, and response requirements where applicable.

3. Security Monitoring 24/7/365 (24 hours/day, 7 days/week, 365 days/year)

3.1. SOC as a service

- 24/7/365 Monitoring and Detection service through a Security Operations Center (SOC) service to proactively prevent, detect, assess, and respond to cybersecurity threats.
- The SOC should comprise skilled personnel, robust technology, documented processes, and operate from secure premises.

3.2. Security Incident and Event Management (SIEM) Platform Management

- A solution must be proposed and implemented to monitor Foskor's existing security, network, cloud, and infrastructure environment.
- All applicable log sources listed in Annexure 1 must be integrated into a mature SIEM service operating on a 24/7/365 basis, with appropriate dashboards, alerting, and reporting available to Foskor ICT operations and management.
- Provision must be made for the migration or onboarding of up to twelve (12) months of historical logs and events from the current SIEM provider, subject to technical feasibility, data format compatibility, retention constraints, and agreed migration timelines.
- Health checks and optimization.
- Correlation rule tuning.

3.3. Honeypots

- Where proposed, honeypots or deception technology must be designed so that they do not introduce operational risk to production environments. Their placement, purpose, and support model must be clearly described.
- The service provider must explain how threat activity observed through such controls will be analysed, reported, and used to improve detection use cases.

3.4. Dark Web Monitoring

- Proactive monitoring of the dark web for potential threats like leaked data, compromised credentials and discussions related to Foskor.
- Provide detailed reporting with actionable recommendations to mitigate risks and prevent future breaches.

3.5. Advanced Analytics

- Recommend and provision AI-powered or advanced analytics tools, where appropriate, to support improved threat detection and investigation in near real time.
- Any such tooling should use defined baselines of normal behaviour, be explainable to Foskor, and be governed to minimise false positives and unnecessary disruption.
- Analyse network traffic, user behaviour, and other data points to identify malicious activity, including lateral movement, data exfiltration, and unusual communication patterns.

4. Incident Detection and Response

4.1. Containment & Eradication

- Provide automated quarantine of devices that exhibit anomalous network behaviour and traffic patterns.
- Security Orchestration, and Response (SOAR) to assist with breach detection as well as incident response.
- Provide visibility of suspicious and anomalous activity originating from devices or accounts not authorised to perform administrative tasks, for example finance user devices executing PowerShell or other scripts.

4.2. Coordination

- Work with Foskor's internal ICT teams to support containment, restoration of normal operations, and recovery activities, with clear escalation paths and decision rights.
- Provide adequate processes and actions to assist Foskor to contain and recover from cyberattacks or security breaches.
- Conduct at least two cyber-attack simulation exercises annually with the Foskor Team.
- Incident reporting and escalation.
- Provide an efficient and seamless process to access log source events/flows in the event of a cyber breach or incident investigation.
- The provider must maintain and test incident response playbooks for common scenarios, including ransomware, business email compromise, privileged account compromise, malware outbreaks, and unauthorised data exposure.

4.3. Threat Intelligence & Threat Hunting

- Use third-party threat intelligence sources to enhance detection of potential compromise events related to known malicious users, hosts, applications, domains, or content relevant to Foskor's environment.
- SOC analysts should be proactively working to detect indicators of compromise before they achieve full exploitation.
- Provide emerging threat advisories.

5. Vulnerability & Risk Assessments

5.1. Vulnerability Scanning

- Perform automated scans to identify weaknesses across networks, applications, and endpoints.
- Provide support and expertise to identify, prioritize, remediate, and mitigate security vulnerabilities in Foskor's ICT infrastructure.
- Collaborate with Foskor to ensure that the most important vulnerabilities are prioritized and scheduled for completion.

Note: Foskor will utilise its existing tool, Tenable One, to perform vulnerability scanning. The MSSP's responsibility should therefore focus on interpretation, prioritisation, reporting, remediation guidance, and governance support unless otherwise agreed.

5.2. Security Assessments

The service provider must provide the following assessments annually unless specified and agreed upon in the service level agreement.

- External security assessment
- External/Internal network penetration test.
- VPN access and exploitation assessment.
- Network access penetration test (wireless & wired network).
- Web site application penetration test.

- Internal security assessment
- Active directory penetration test.
- Password security assessment
- Domain policy and configuration assessment.
- Cloud tenant security assessment.

- Network and Infrastructure Hardening
- Provide recommendations/solutions on a quarterly basis to reduce vulnerabilities and strengthen the security posture of Foskor systems and networks.
- Conduct a gap assessment on controls for hardening and produce a technical report for implementation.

6. Cybersecurity Awareness Training

Provision and administration of security awareness training utilising a trusted and modern platform/solution.

- Configuration and scheduling of security awareness training modules, to include policy awareness, course completion quiz, as well as regular phishing testing to all users.
- Management and development of reports and dashboards with input from the Foskor point of contact.

7. Ad-hoc Services (Consulting, advisory, and forensics)

The provision of ad-hoc services may be required and provisioned only upon acceptance of a quote/proposal and that which is not stipulated in the formal contractual agreement.

- Provide consulting and remediation to Foskor ICT audit findings when required.
- Perform forensic audits, data recovery, analysis and investigation when a suspected breach has occurred upon receiving instruction from Foskor ICT.
- Formalise and test Incident Response Plans/Playbooks.
- The proposed hourly rate should be specified in the pricing section of the proposal.

8. Roles and Responsibilities

8.1. Foskor ICT Team

- Approving changes, implementing firewall blocks, and managing endpoint remediation.
- Granting the MSSP the necessary (and appropriately scoped) network privileges to perform their duties without over-exposing the attack surface.
- Monitoring the MSSP's Service Level Agreements (SLAs), reviewing incident reports, and holding the provider accountable for missed metrics

8.2. Vendor/MSSP

- 24/7/365 monitoring, tuning correlation rules, managing the SIEM, and escalating high-severity incidents.
- Operating a continuous SOC to review network traffic, endpoints, and system logs for anomalies.

- Rapid analysis of active breaches to contain threats and provide actionable steps for eradication.
- Conducting routine assessments to identify software vulnerabilities and misconfigurations.

9. Reporting and Compliance

- Periodic reports should include, but not be limited to, the following:
- SIEM alerts or offences must be integrated with, or communicated to, the current Foskor service desk and designated ICT stakeholders in accordance with agreed severity and escalation rules.
- Weekly reports on outstanding security awareness training, phishing campaign performance, and high-risk user trends.
- Monthly reports showing log volumes, events, offences, log source health, threat trends, dark web findings, vulnerability management support activities, awareness training status, phishing simulation results, and SLA/KPI performance.
- Log/Events Retention
- Hot/active storage for a period of 1 year.
- Archival storage for a period of 5 years (contract duration).
- Support Foskor's security posture and reporting obligations against applicable laws, regulations, and standards, including POPIA, the Cybercrimes Act, contractual requirements, and internal governance frameworks. Where international frameworks are referenced, these should be treated as good practice guidance unless specifically mandated.

10. Governance and Service Management

10.1 Service Reviews

- Bi-weekly operational service review meetings during transition and onboarding, then at a frequency agreed in the SLA.
- Monthly review of detailed SOC and SIEM reporting, incident trends, tuning actions, and risks requiring management attention.
- SLA reporting
- Executive dashboards summarizing service performance, material incidents, risk themes, and improvement actions.

10.2 Continuous Improvement

- Adjusting false positive thresholds, migrating use cases, and scaling logs.
- Risk trend analysis

11. Service Level Agreements (SLAs), and Key Performance Indicators (KPI)

11.1. Service Level Agreement

- Monitoring of the provision of services through accurate reporting.
- Incident Management – Identification, logging of calls, classification, prioritisation, and escalation of security incidents.
- Incidents to be categorised as critical, high, medium and low.
- Incident resolution knowledge transfer.
- Vulnerability Fix Rate: The number of identified vulnerabilities resolved over a given period versus the number of new vulnerabilities discovered.
- Provision of dashboards for compliance, network, threat, and security monitoring.
- Provide a detailed SLA with clearly defined KPIs, measurement methodology, service windows, exclusions, escalation thresholds, and service credit mechanisms.
- The provided SIEM solution must include a portal and dashboard that should be accessible to applicable Foskor ICT personnel.
- Applicable service credits may be applied when SLA KPIs such as MTTA (mean time to acknowledge) are not achieved.

11.2. Key Performance Indicators

Deliverable	KPI	Target
24/7/365 Security Monitoring	SOC monitoring availability	≥ 99.97%
	Critical alert acknowledgement	≤ 15 minutes
	High severity alert acknowledgement	≤ 30 minutes
	Medium severity alert acknowledgement	≤ 2 hours
	Low severity alert acknowledgement	≤ 4 hours
SIEM Platform Management	Log ingestion success rate	≥ 98%
Incident Detection & Response	Mean Time to Detect (MTTD)	< 30 minutes
	Mean Time to Respond (MTTR)	< 2–4 hours
	Incident escalation compliance	≥ 95%
	Severity classification accuracy	≥ 95%
Threat Intelligence & Threat Hunting	Threat intelligence feed updates	Daily/real-time
	Threat hunting exercises	Quarterly
Reporting & Governance	Monthly report delivery	By agreed date
	SLA reporting accuracy	≥ 99%
	Executive reporting completeness	100%
Vulnerability & Risk Assessments	Security improvement recommendations	Monthly
	Critical & High vulnerabilities on critical assets remediation	Within 48hrs
	Critical & High vulnerabilities on non- critical assets remediation	Within 14 days
Compliance	Audit support response time	≤ 2 business day
	Log retention compliance	100%
	Log accessibility	100%

12. Managed Security Services Resources (Experience and Certifications)

Respondents to this RFP must submit resumes for the resources proposed to deliver the services to FOSKOR. Resources must have the relevant experience and skills to provide the cybersecurity services required. The winning respondent must ensure that proposed resources will deliver the proposed services and complete, or where necessary, be substituted for staff with equivalent experience and skills for smooth and stable continuity without affecting the service delivery SLA.

12.1 The applicable certifications of resources, including SOC/SIEM experience as well specialist cybersecurity will be required to deliver the required security services to Foskor.

12.2 The Cybersecurity/Information security skills, and certifications that are required must comply to requirements below:

Technical Skills	
a. Threat Monitoring:	Skills in using security tools to identify and analyse threats.
b. Security Operations c. Network Security	Experience in monitoring security events, responding to incidents, and maintaining security systems. Understanding network protocols, firewalls, intrusion detection systems, and other network security technologies.
d. Risk Management	Ability to identify, assess, and mitigate cybersecurity risks.
e. Penetration Testing	Skills in identifying vulnerabilities through simulated attacks.
f. Identity and Access Management (IAM)	Expertise in managing user access and permissions.
g. Application Security	Knowledge of secure coding practices and application vulnerabilities.
h. Ethical Hacking	Understanding of hacking techniques and the ability to use them for defensive purposes.
i. Programming and Scripting	Proficiency in languages like Python, JavaScript, and PowerShell for automation and analysis.

Cybersecurity Certifications		
Role/Specialty	**Key Specialist Certifications**	
Security Analysts	CompTIA Security+ CompTIA CySA+ - Cybersecurity Analyst Microsoft Certified: Security Operations Analyst Associate (SC-200 (CSA) CDSA – Certified Defensive Security Analyst CTIA – Certified Threat Intelligence Analyst	GCIH (Incident Handler). CX-P Cybersecurity practitioner, CSA- EC-Council Certified SOC Analyst CCOA-Certified Cybersecurity Operations Analyst CC-Certified in Cybersecurity CCT – Certified Cybersecurity Technician
Architects & Engineers	CISSP (Information Systems Security), GSEC – GIAC Security Essentials CASP+ - CompTIA Advanced Security Practitioner AAISM -Advanced in AI Security Management CAISE – Certified AI Security Engineer CHFI – Computer Hacking Forensic Investigator	ISSAP-Information Systems Security Architecture Professional ISSEP-Information Systems Security Engineering Professional ISSMP-Information Systems Security Management Professional SCCP-Systems Security Certified Practitioner
Cloud Security Experts	CCSP – Certified Cloud Security Professional	Microsoft Certified: Cybersecurity Architect Expert
Penetration Testers (Offensive)	OSCP (Offensive Security) CompTIA PenTest+	CEH (Certified Ethical Hacker) CPENT – Certified Pen Testing Professional
Governance & Compliance	CISM (Security Manager) CISA (Auditing) CRISC (Risk & Info Systems Control)	CGEIT (Governance) CGRC (Certified in Governance, Risk and Compliance) AIGP – Certified AI Governance Professional

Compliance Certifications for MSSP	
SOC2 Type II	Service Organization Controls 2- assesses the effectiveness of a service organization's controls related to security, availability, processing integrity and confidentiality.
ISO 27001	Provides a framework for managing sensitive company information, aligning with regulations like POPIA in South Africa.

13. Submission of Proposal Requirements

This section provides the requirements and guidelines for submission of the Managed Security Services proposal.

13.1. Price/Costing Proposal

- Submit the cost for the managed services

13.2 Company Profile

- Submit details as per Annexure 2 requirements.

13.3. Managed Security Services Provider: Scope of Work Evaluation

- Refer to Annexure 3 and respond with either Yes/No.

13.4 Proposal/Bid Evaluation

- Refer to Annexure 4 and submit the applicable returnable documents as stipulated.

14. Proposal Evaluation Process

- Phase 1: Mandatory Requirements.

  The Tenderers will be evaluated according to the responses received. Only Bidders that meet all Mandatory Requirements will be further evaluated in Phase2.

- Phase 2: Experience, Certifications, and Technical Requirements.

  The purpose of application of qualification criteria is to determine the functionality of each proposal by assessing the quality of the technical proposal and company experience for provisioning the services thereof.

- The qualifying and/or shortlisted bidders may be requested to do an overall presentation to the Evaluation team for any further clarifications and/or demonstration of the proposed solution.

- Foskor reserve the right to conduct a due diligence on the SOC location before the successful bidder is appointed.

15. Price Proposal

15.1 Please indicate your total bid price here: R…….

15.2 Costing Model/Pricing Breakdown

Description	Qty	Rate Excl. VAT	Total Excl. VAT
Year 1: Pricing (MSSP Services)			
1. 24/7 monitoring and detection (SOC/SIEM)			
2. Incident Response			
3. Vulnerability Management			
4. Security Assessments			
5. Security Awareness Training			
6. a. Implementation and onboarding			
b. Project Management			
c. Training			
d. Software License subscription			
7. Maintenance of all provisioned software/systems (if applicable).			
Total for Year 1			
Total for Year 2			
Total for Year 3			
Total for Year 4			
Total for Year 5			
Total bid price excl. VAT			

15.3. Ad-hoc Support Costing Model (as and when required)

Where consulting and forensic investigations are required, these services will be subject to a separate quotation and purchase order approval. Provide applicable rates below.

Description	No. of Hours Per Year	Rate Per hour (Excl. VAT)
1. Forensic Investigations	**10**	
2. Consulting	**24**	
3. Cyber incident response, containment and data recovery	**20**	
4. Formalise and test Incident Response Plans/Playbooks	**5**	

Annexures

Annexure 1: ICT Infrastructure Log Sources

Data Sources	Qty- Nodes/End points/Users	Comments
Firewalls – IDS/IPS	5	Managed by service provider
Web Filter	1	Managed by service provider
Email Filter - Mimecast	1	
Network Gateway/Routers	6	Managed by service provider
Network VPN / SSL VPN	1	
Network Wireless LAN	3	
Network Switches	136	Aruba & Extreme Product
Domain Name Servers	5	
DHCP Servers	4	
Microsoft servers	100	
Linux servers	2	
HyperVisor (ESXi, Hyper-V)	16	
Windows Desktops (Laptops, Tablets,)	800	
Endpoint/Server Security – Antivirus	800	Sophos and MS Defender
Azure AD Sign-ins (Users)	1726	
ManageEngine AD Audit Plus	1	
Netwrix Change Auditor	2	

Annexure 2: Attachment (Company Profile)

Company Background	
Company Name:	
Location of Head office in South Africa:	
Parent Company, if applicable:	
SOC - Security Operations Center Location/s:	
Service Provider Experience	
# of years in Managed Security Services business:	
# of years providing SOC services:	
# of years providing SIEM services:	
Customer Base	
# of clients implemented SOC/SIEM service:	
# of clients in KwaZulu Natal:	
About Your Company	
# of Total Employees:	
# of Security/Cybersecurity Resources:	

Annexure 3: Scope of Work – Evaluation

No.	Requirement/Deliverable	Sub-Requirement	Description	Yes	No	Comments/Details	Possible Points	Actual Points
3	**Security Monitoring 24/7/365**	3.1 SOC (security operations center) as a service	• 24X7X365 Monitoring and Detection service through a Security Operations Center (SOC) service to proactively prevent, detect, assess, and respond to cybersecurity threats. • SOC should comprise skilled personnel, robust technology, documented processes, and be in secure premises.				**2**	
		3.2 SIEM (security incident & event management)	• Solution must be proposed and implemented that must monitor the existing security, network, and infrastructure as per Annexure 1 • Provision must be made for the injection of 12 months of historical logs and events from the current SIEM provider's platform to the new proposed SIEM solution. • Health checks and optimization. • Correlation rule tuning.				**4**	
		3.3 HoneyPots	• Propose and implement a minimum of three Honeypots within the Foskor ICT environment to distract potential attackers from more important information and servers on the real network. • Learn about the forms of attacks they can suffer and examine such attacks during and after the exploitation of the honeypot.				**2**	
		3.4 Dark Web Monitoring	• Proactive monitoring of the dark web for potential threats like leaked data, compromised credentials and discussions related to Foskor. • Provide detailed reporting with actionable recommendations to mitigate risks and prevent future breaches				**2**	
		3.5 Advanced Analytics	• Recommend and provision AI- powered tools to identify and tackle cyber-attacks in real-time. • The tool should use intelligence and self-learning of normal behavior to detect activities that could cause business disruption. • Analyze network traffic, user behavior, and other data points to identify malicious activity, including lateral				**3**	

			movement, data exfiltration, and unusual communication patterns.					
4	**Incident Detection & Response**	4.1 Containment & Eradication	• Provide automated quarantine of devices that exhibit anomalous network behavior and traffic patterns. • Security Orchestration, and Response (SOAR) to assist with breach detection as well as incident response. • Provide visibility on suspect and anomalous activities emanating from devices that are not authorized to perform, and execute administrative tasks, e.g., finance devices running power shell or any other scripts.				**3**	
		4.2 Coordination	• Partnering with our internal IT teams to restore normal operations, containment and recover lost data. • Provide adequate processes and actions to assist Foskor to contain and recover from cyberattacks or security breaches. • Conduct at least two cyber-attack simulation exercises annually with the Foskor Team. • Incident reporting and escalation. • Provide an efficient and seamless process to access log source events/flows in the event of a cyber breach or incident investigation.				**5**	
		4.3 Threat Intelligence & Threat Hunting	• Use of 3rd party, external threat intelligence to expand and enhance the solutions ability to detect potential breach events related to know compromised users, hotspots, applications, domains and/or content. • SOC analysts should be proactively working to detect indicators of compromise before they achieve full exploitation. • Provide emerging threat advisories				**3**	
5	**Vulnerability & Risk Assessments**	5.1 Vulnerability Scanning	• Perform automated scans to identify weaknesses across networks, applications, and endpoints. • Provide support and expertise to identify, prioritize, remediate, and mitigate security vulnerabilities in Foskor's ICT infrastructure. • Collaborate with Foskor to ensure that the most important vulnerabilities are prioritized and scheduled for completion.				**3**	

		5.2 Security Assessments	• External network penetration test. • VPN access and exploitation assessment. • Network access penetration test (wireless & wired network). • Web site application penetration test. • Active directory penetration test. • Password security assessment • Domain policy and configuration assessment. • Cloud tenant security assessment. • Provide recommendations/solutions on a quarterly basis to reduce vulnerabilities and strengthen the security posture of Foskor systems and networks. • Conduct a gap assessment on controls for hardening and produce a technical report for implementation.				**10**	
6	**Cybersecurity Awareness Training**	Cybersecurity Awareness Training Administration	• Provision and administration of security awareness training utilizing a trusted and modern platform/solution. • Configuration and scheduling of security awareness training modules, to include policy awareness, course completion quiz, as well as regular phishing testing to all users. • Management and development of reports and dashboards with input from the Foskor point of contact.				**3**	
			Total				**40**	
			Scoring				**20**	

Note: The total of max 40 points will be divided by two for a final score out of 20

Response From: _____

Signature: _____ **Date:** _____

Annexure 4: Evaluation -MSSP

No.	Mandatory Requirements		Returnable Documents	Comments
1.	The bidders SOC and SIEM services must be certified against the ISO/IEC 27001 information security standard.		Bidders must submit evidence of ISO/IEC 27001 certification.	
SCOPE OF WORK REQUIREMENTS				
	EVALUATION CRITERIA **MANAGED SECURITY SERVICES - SOC/SIEM**			
No.	**Technical Criteria Description**	**% Contribution**	**Returnable Documents**	**Comments**
1	**Technical Requirements - Understanding of Scope of Work Specifications**			
a)	Demonstrate a clear understanding of the managed services deliverables in sections 3,4,5,6 and ability to provide them. **Scoring:** The total number of points achieved out of 40 will be divided by two to give a final rating out of 20%.	**20%**	Provide proposed solutions for deliverables as per the scope of work. Refer to Annexure 3 and respond to each deliverable with either yes/no.	
b)	Project Implementation Methodology: A well-defined plan outlining activities, timelines, outputs, and reporting mechanisms. **Scoring:** 0% - No project plan submitted 5% - Project plan submitted	**5%**	Provided project implementation plan for proposed services outlined in the scope of work.	
c)	Sample Incident Response (IR) Playbooks: Documents detailing exactly how the service provider can contain and eradicate threats (e.g., Business Email Compromise or ransomware) **Scoring:** 0% - No IR Playbook submitted 5% - IR Playbook submitted	**5%**	Provide a sample IR Playbook that is utilised by the service provider.	
d)	Sample Post-Incident Report: An example of the detailed forensic reporting that the service provider can provide after an attack, showing root cause and timeline. **Scoring:** 0% - No sample incident report submitted 5% - Sample incident report submitted	**5%**	Provide a sample incident report.	

2	**Supplier experience & team competence in providing managed security services**			
a)	References: Submit client testimonial from previous or current customers for cybersecurity services provided. **Scoring:** 0% = (0) Letters 2% = (1) Letter 4% = (2) Letters 6% = (3) Letters 8% = (4) Letters 10% = (5) Letters	**10%**	Bidders must provide current and/or past customers with contactable references for similar services. The references must indicate the brief description of the services provided, customer name and valid contact details. Note: Client testimonials should be signed by the referring customer.	
b)	Submit certifications of resources in the field of cybersecurity. **Scoring:** Points will be allocated per resource submission per role/speciality (refer to section 12). • Security Analysts – (submission 0 = 0%; 1 =2.5%; 2=5%) • Architects & Engineers – (submission 0 = 0%; 1=2.5%; 2=5%) • Cloud Security Experts – (submission 0 = 0%; 1=2.5%; 2=5%) • Penetration Testers (Offensive) – (submission 0 = 0%; 1=2.5%; 2=5%) • Governance & Compliance – (submission 0 = 0%; 1=2.5%; 2=5%)	**25%**	Points will be awarded per relevant certification type according to the role/speciality. Submission of CVs with relevant certifications for each role.	
c)	Employees experience as Cybersecurity Specialists / Cybersecurity Managers. **Scoring:** 5% - Less than 5 years of combined experience 10% - 6 to 10 years 15% - 11 to 15 years 20% - 16 years and more	**20%**	Bidders must submit the CVs of their Cybersecurity Specialists and/or Managers that will be providing the services. An average of the combined years of experience related to cybersecurity will be used to determine the score rating.	

3	**SOC and SIEM Compliance/Certification**			
a)	The bidder should confirm if they are certified in accordance with the SOC 2 Type II compliance framework. **Scoring:** 0% - Audit Report Not certified 5% - Audit Report SOC 2 Type II Certified	**5%**	Provide evidence of SOC 2 Type II audit report certification or summary letter.	
b)	**SIEM Platform Specific Certification** The bidder should confirm if they are certified to implement and manage the SIEM technology/platform. **Scoring:** 0% - Not certified 5% - Certified	**5%**	Provide evidence of SIEM technology certifications for implementation and management.	

Total Evaluation Score: **100%**

NOTE: Minimum threshold is 70%

DISQUALIFICATION CRITERIA **

1 Mandatory documentation not submitted.

2 Resources and skills with certifications not submitted.