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.