RW10405769/26
3

B Ramohla
0116820815
23/02/2026

RW10405769/26 PROVISION OF DIGITAL TECHNOLOGY (IT/OT) CYBERSECURITY/SCURITY OPERATIONAL CENTRE AS A SERVICE AT RAND WATER FOR A DURATION OF 5 YEARS

The pages referenced are the pages of the **RW 10405769/26** bid document.

This clarification consists of 32 statements.

SIGNATURES

Bonolo Ramohlala
Digitally signed by Bonolo Ramohlala

Buyer Name :

Sign :

Digitally signed by Emmanuel Nzilo
Date: 2026.02.23 12:00:34 +02'00'

Supply Chain Manager Name :

Sign :

A. RW10405769/26 PROVISION OF DIGITAL TECHNOLOGY (IT/OT) CYBERSECURITY/SCURITY OPERATIONAL CENTRE AS A SERVICE AT RAND WATER FOR A DURATION OF 5 YEARS

No.	TCS Question	Response from Rand Water
1	Are all the security tool licenses already owned by Rand Water? If yes, 1. Should the supplier only operate and optimize existing investments? 2. Is there any expectation to rationalize or replace current tools? If not, 1. Is the supplier expected to procure & own the licenses and provide SOC as a service to RW?	Service provider to offer SOC solution that is optimal and suitable for the organization
2	Are there any proprietary or legacy systems that require custom log ingestion?	Yes
3	Do you anticipate transitioning fully away from existing SIEM, or should coexistence be planned during the engagement? If a phased replacement is planned?	In line with PROVISION OF DIGITAL TECHNOLOGY (IT & OT) CYBERSECURITY/SECURITY OPERATIONAL CENTRE (SOC) SERVICES proposed
4	Pls share log source inventory for SIEM coverage, volumes, eps/gb per day. Volume is critical to license sizing and service pricing.	The Service provider SOC solution to encompass all existing devices and systems in the infrastructure

5	What is Rand Water's Preference in terms of Delivery Model? Supplier can provide below 3 options- 1. Fully onsite from South Africa 2. Hybrid Onsite (Critical Staff) & Offshore Model 3. Offshore Shared Services Please indicate the model we should consider for commercials	In line with PROVISION OF DIGITAL TECHNOLOGY (IT & OT) CYBERSECURITY/SECURITY OPERATIONAL CENTRE (SOC) SERVICES proposed
6	Can you categorize log sources as high, medium, or low priority based on business value?	In line with PROVISION OF DIGITAL TECHNOLOGY (IT & OT) CYBERSECURITY/SECURITY OPERATIONAL CENTRE (SOC) SERVICES proposed
7	How many major incident are reported in last 1 year , where digital forensics services are required as part of security operation services.	Unable to disclose at this stage
8	If Possible please provide the security ticket (Incident, change, service request) data for past 6 months for each of these in scope tools/services across US region	Unable to disclose at this stage
9	Are you using any sort of log aggregation/noise reduction solution in-house already (ex. Cribl) to help reduce the ingest noise into your current SIEM platform?	Response In line with PROVISION OF DIGITAL TECHNOLOGY (IT & OT) CYBERSECURITY/SECURITY OPERATIONAL CENTRE (SOC) SERVICES proposed

10	**Do you have a bastion zone or management environment for privileged access actions? Do you have dedicated privileged access workstations for management tasks/remediations or additional needs like FIDO2 tokens on laptops for specific actions/escalations?**	**Response In line with PROVISION OF DIGITAL TECHNOLOGY (IT & OT) CYBERSECURITY/SECURITY OPERATIONAL CENTRE (SOC) SERVICES proposed**
11	**Do you have any identity detection and response solutions in your environment today (ex. Crowdstrike Identity, Semperis, Defender) that detects anomalous actions while also protecting your AD Domain(s) and Forest(s) for full automated recovery?**	**Response In line with PROVISION OF DIGITAL TECHNOLOGY (IT & OT) CYBERSECURITY/SECURITY OPERATIONAL CENTRE (SOC) SERVICES proposed**
12	**Do you have a dedicated IR retainer/team in place in the event of a cyber-attack?**	**Response In line with best PROVISION OF DIGITAL TECHNOLOGY (IT & OT) CYBERSECURITY/SECURITY OPERATIONAL CENTRE (SOC) SERVICES proposed**
13	**Given breakout and exfiltration time is shrinking, are there options to discuss reducing/revising your SLAs for automated response in the event a quarantine or shutdown is required for certain devices/identity regardless of criticality?**	**Response In line with best PROVISION OF DIGITAL TECHNOLOGY (IT & OT) CYBERSECURITY/SECURITY OPERATIONAL CENTRE (SOC) SERVICES proposed**
14	**What is your current data protection strategy and are those logs forwarded/maintained? Some backup systems have log forwarding and sometimes it's helpful to receive those signals for potential entropy changes and honeypot files being touched.**	**Response In line with best PROVISION OF DIGITAL TECHNOLOGY (IT & OT) CYBERSECURITY/SECURITY OPERATIONAL CENTRE (SOC) SERVICES proposed**

15	Are you using any network Microsegmentation services on your network today (e.g. Guardicore, Cisco ACI, Illumio)?	Response In line with best PROVISION OF DIGITAL TECHNOLOGY (IT & OT) CYBERSECURITY/SECURITY OPERATIONAL CENTRE (SOC) SERVICES proposed
16	Pls share the list and count of domains to be monitored	Unable to share at this stage
17	Is NDR amandatory requirement as part of solution stack. If yes, pls share the network segments/DMZ's to be monitored. Network diagrams etc.	Unable to share at this stage
18	Is UEBA a mandatory requirement? Pls suggest endpoints and users to be considered	Unable to share at this stage
19	What are the current security tools and platforms in use (e.g., SIEM, EDR, IAM, CASB, DLP, etc.)?	Service provider SOC solution to encompass all existing devices and systems in the infrastructure
20	Are there any preferred OEMs or existing vendor partnerships that must be considered?	Response In line with best PROVISION OF DIGITAL TECHNOLOGY (IT & OT) CYBERSECURITY/SECURITY OPERATIONAL CENTRE (SOC) SERVICES proposed
21	Are there any specific systems or platforms that the new solution must integrate with (e.g., ERP, SCADA, cloud platforms like Azure/AWS/GCP)?	In line with PROVISION OF DIGITAL TECHNOLOGY (IT & OT) CYBERSECURITY/SECURITY OPERATIONAL CENTRE (SOC) SERVICES proposed
22	Can you confirm the number of users and endpoints (IT and OT) to be covered under the scope?	+ - 3500 users
23	What are the expected SLAs for incident response, threat detection, and remediation?	SLA to be agreed upon award of service provider

24	**Is there a preference for on-premise, cloud, or hybrid deployment models?**	**Response In line with best PROVISION OF DIGITAL TECHNOLOGY (IT & OT) CYBERSECURITY/SECURITY OPERATIONAL CENTRE (SOC) SERVICES proposed**
25	**Are there any constraints or preferences regarding data residency or data sovereignty?**	**Response In line with best PROVISION OF DIGITAL TECHNOLOGY (IT & OT) CYBERSECURITY/SECURITY OPERATIONAL CENTRE (SOC) SERVICES proposed**
26	**What is the expected scope for user and technical training?**	**To be discussed upon award**
27	**Are there any existing training platforms or LMS systems to be leveraged?**	**Response In line with best PROVISION OF DIGITAL TECHNOLOGY (IT & OT) CYBERSECURITY/SECURITY OPERATIONAL CENTRE (SOC) SERVICES proposed**
28	**In order to provide cybersecurity Detection and Response capability that integrates with the Rand Water's current security investments, please advise if you have already deployed any OT threat detection platforms (eg: Nozomi Guardian, Claroty xDome, Armis Centrix etc.) in your plants.**	**Unable to disclose at this stage**
29	**What security technologies are currently deployed in OT to achieve a zero trust architecture? Eg: Network micro-segmentation, identity management, secure remote access, data classification and protection?**	**Unable to disclose at this stage**

30	**Which endpoint monitoring and response technologies are used in OT? Does this also cover legacy OS endpoints? Of the 5000 assets across IT & OT, approximately how many are OT assets & Types?**	**Unable to disclose at this stage**
31	**We presume that continuous vulnerability management is required for OT assets as well. How many vulnerabilities are currently identified across the OT assets?**	**Unable to disclose at this stage**
32	**Please elaborate on requirement for penetration testing of OT? How many OT assets would be in scope of the pen tests, and at what frequency (half-yearly, annual etc.)? Are these assets available in a test / staging environment where the tests can be conducted (to avoid operational downtime due to adverse impact of pen testing on the target)**	**The frequency of the Penetration test to be anually, Main sites but OT devices might exist across the infrastructure**