Kenya Bureau of Standards
Standards for Quality life

OUR REF: KEBS/1029/0338/2025-26

5TH MAY 2026

TO ALL INTERESTED BIDDERS.

ADDENDUM NO.1 TO TENDER NO. KEBS/1029/0338/2025-26- INSTALLATION AND IMPLEMENTATION OF AN INTEGRATED APPLICATION OBSERVABILITY AND SECURITY INFORMATION AND EVENTS MANAGEMENT(SIEM) PLATFORM FOR A PERIOD OF THREE YEARS

The clarifications are made to the specified provisions of Installation and Implementation of an Integrated Application Observability and Security Information and Events Management (SIEM) Platform for a Period of Three Years.

1. RELATIONSHIP WITH THE PRINCIPAL TENDER DOCUMENT

Save where expressly amended by the terms of this Addendum, the Principal Tender Document shall continue to be in full force and effect. The provisions of this Addendum shall be deemed to have been incorporated in and shall be read as part of the Principal Tender Document.

2. CLARIFICATIONS HAVE BEEN SOUGHT AS FOLLOWS:

S/NO	TECHNICAL CLARIFICATION QUESTIONS	KEBS RESPONSE
1	*How many total devices and systems need to be monitored, including servers, endpoints, firewalls, switches, routers, applications, databases, and cloud workloads?*	*The anticipated load is approximately 5,000 Events Per Second (EPS) across all monitored systems*
2	*What is the estimated daily log volume (GB/TB per day) and expected Events Per Second (EPS) for the SIEM and observability platform?*	*We are looking for an ingest-based licensing model for log sources. The licensing requirement, as detailed in the RFP, is 150 GB per day.*
3	*What is the required log retention period for operational monitoring, compliance, and audit purposes (hot storage and archive retention)?*	*Kindly refer to the tender document on storage and retention period*
4	*Which applications are in scope for Application Observability, including business-critical applications, customer portals, APIs, ERP, CRM, middleware, and custom applications?*	*For this scope, a "monitor" refers to any individually instrumented and licensed component within the application observability platform, including application agents, infrastructure agents, database agents, and end-user monitoring components. Based on the defined scope, the monitored components are:* *Application Performance Monitoring (APM):* *• 1 Middleware Application (Spring Boot – logical application grouping)* *• 9 JVM instances (each instrumented and monitored via APM)* *Infrastructure Monitoring:* *• 1 Middleware Server (CentOS – monitored via Server Visibility)*

		Database Monitoring: *• 1 Oracle 19c Database Instance (monitored via Database Agent)* *End-User Monitoring:* *• 1 Web Application (Frontend Online Portal – BRUM)* *• 1 Mobile Application (MRUM)* *Excluded from Scope:* *• 1 Load Balancer (not instrumented in the current scope)* *• Total Monitored Components: 14 monitored components* *• All monitoring is deployed on-premises, ensuring that application, infrastructure, database, and end-user telemetry remain within the our environment while supporting full observability and security analytics.*
5	*What databases are currently in scope for monitoring (Oracle, SQL Server, PostgreSQL, MySQL, DB2, Sybase, etc.), and how many instances need to be monitored?*	*See response above on scope.*
6	*Is there an existing SIEM, observability, or monitoring platform currently deployed? If yes, what solution is being used and what are the main pain points or migration expectations?*	*Kindly refer to the tender document on scope of works*
7	*Does KEBS prefer an on-premises, cloud, or hybrid deployment model, and are there any specific data residency or data sovereignty requirements for log storage and processing?*	*On premise*
8	*Which integrations are mandatory for Phase 1 implementation, such as AD/LDAP, CMDB, firewalls, endpoint security, email security, ERP systems, cloud platforms, or ITSM platforms?*	*Kindly refer to tender document on integration.*
9	*How many datacenters need to be monitored?*	*1 (one)*
10	*Can you describe the physical locations of these DCs, are they in different locations, same location, what is the physical segmentation?*	*Same Location - KEBS HQ*
11	*Bandwidth to monitor? (i.e traffic – how many links and how much Gbps or Mbps per link and what is the current utilization per link on average) per DC, please describe in great detail for sizing for each one of the above sections and scenarios*	*The environment has two (2) network links, each with a capacity of 300 Mbps, with an average utilization of approximately 200 Mbps per li.*
12	*What network switches do you use and do they have TAP or SPAN ports available? How many ports are available and What network interfaces? (1G copper or fiber, 10G fiber, 40G fiber) please describe in great detail for sizing. Do you need a packet broker?*	*The network infrastructure supports 1G and 10G interfaces. A packet broker is not required under the current scope.*

13	*You have mentioned the following on the Tender* *(34)* a. *The solution should be in the "Leaders" Quadrant of the Gartner Magic Quadrant for SIEM for least nine consecutive times by the year 2025* b. *The solution should include intuitive product and architecture to address Gartner's 3 dimensions of Application Performance Management: ADTD, DEM and AIOps for Applications.* *Kindly confirm whether bidders are strictly required to propose solutions that meet this exact Gartner positioning criterion, or if alternative solutions may be considered provided, they fully meet or exceed all the technical and functional requirements outlined in the tender.*	*Solutions that meet or exceed all technical and functional requirements of the tender will be considered, notwithstanding the referenced Gartner positioning criteria.*
14	*Infrastructure Scope* *Server Capacity* • *Breakdown of total RAM per server (in GB)* *Any high-capacity or high-throughput systems that may require special consideration* *Kindly provide detailed Server sizing*	*Bidders are required to propose server sizing and capacity based on their solution architecture for the SIEM and Application Observability platform.* *Any high-capacity or high-throughput components requiring special consideration should be clearly identified in line with the TOR.*
15	*Application Landscape* • *Number of web applications to be monitored* *Number of mobile applications (if applicable)*	*One (1) web application* *One (1) mobile application*

16	*User Activity / Data Volume* • *Estimated number of users or sessions per month (web and mobile)* • *Approximate daily or monthly log/event volumes, if available* *Peak usage periods or seasonal variations (if applicable)*	*The solution must provide an enterprise-grade log management and analytics platform, with SIEM capabilities to handle up to 150 GB of data ingestion per day, as specified in the tender.*
17	*Integration Scope* *List of key systems/log sources to be integrated into the SIEM (e.g., firewalls, IDS/IPS, Active Directory, databases, cloud platforms, etc.)*	*Kindly refer to tender document on integration.*
18	*Request for two-week extension to the submission deadline*	*Tender requirements remain the same*

All the other terms and conditions remain as per the tender document.

JANE NDINYA, CPSP (K)
CHIEF MANAGER, SUPPLY CHAIN.