Kenya Bureau of Standards
Standards for Quality life

OUR REF: KEBS/1029/0037/2025-26

24TH FEBRUARY 2026

TO ALL INTERESTED BIDDERS.

ADDENDUM NO.1 TO TENDER NO. KEBS/1029/0037/2025-26- RENEWAL OF DATABASE ACTIVITY MONITORING TOOL LICENSES AND SUPPORT SERVICES FOR A PERIOD OF THREE YEARS.

The clarifications are made to the specified provisions of renewal of Database Activity Monitoring Tool Licenses and Support Services 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:

	QUESTION	ANSWER
1.	**Question:** I am seeking clarification regarding the schedule of required documents as we are currently unable to get the required document. Kindly clarify if the document is protected and how we can access the document.	We wish to clarify that for ease of reference, we have uploaded an alternative version of the schedule of requirements. Please refer to the attached document.

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

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

RENEWAL OF DATABASE ACTIVITY MONITORING TOOL LICENSES AND SUPPORT SERVICES FOR A PERIOD OF THREE YEARS

1.0 Introduction

The Kenya Bureau of Standards (KEBS) has remained the premier government agency for the provision of Standards, Metrology and Conformity Assessment (SMCA) services since its inception in 1974. Over that period its main activities have grown from the development of standards and quality control for a limited number of locally made products in the 1970s to the provision of more comprehensive Standards development, Metrology, Conformity Assessment, Training and Certification services. With the re-establishment of the East African Community (EAC) and Common Market for Eastern and Southern Africa (COMESA), KEBS activities now include participation in the development and implementation of SMCA activities at the regional level where it participates in the harmonization of standards, measurements and conformity assessment regimes for regional integration. KEBS operates the National Enquiry Point in support of the WTO Agreement on Technical Barriers to Trade (TBT).

Background

As part of overall digital strategy in implementing secure and industry standard technology, security management processes and supporting ICT management applications, KEBS is looking to renew its existing Imperva Database activity monitoring tool to monitor and secure KEBS data stored in the various application databases.

The envisioned solution will offer a comprehensive, multi-layered defense strategy for KEBS, ensuring complete management, visibility, and control over its critical data and databases. The inclusion of Warranties and Technical Support Services will further enhance the solution, ensuring its continuous optimal performance and providing ongoing support to address any challenges or evolving threats, thereby fortifying KEBS' security posture and compliance with industry standards.

1.1 Scope of Works/Service

i. Installation, configuration and implementation of the proposed solution.
ii. Provision of initial 3-year licenses extended warranties and technical support services (including detailed acquisition costs and on-going support for three (3) years however billing will be done annually as per the indicated price schedule.
iii. On-site installation and setup, software configuration and user settings
iv. Knowledge Transfer Training for software configuration for the solutions to ICT staff.
v. The Bidder will be responsible for any upgrades and patches of the proposed solution during the contract period of three (3) years.

1.2 Project Management

i. Bidders shall provide a project management methodology.
ii. A project manager shall be assigned to handle the project.
iii. Throughout the life cycle of the project, the project manager must provide regular and on-request status and progress reports on the achievement of the project.
iv. Throughout the life cycle of the project, KEBS representatives will have the right to request regular and non-regular meetings to follow up with the project manager on the achievements of the project.

1.3 Delivery, Installation, Configuration, Testing and Commissioning:

(i) The Successful Bidder must assess the existing setup before implementing the solution.
(ii) Testing and commissioning criteria shall be developed during the project plan.
(iii) All software, documentation, manuals, instructions, labels shall be in Standard English.

2.0 EVALUATION CRITERIA

STAGE 1: MANDATORY EVALUATION CRITERIA STAGE

No	Requirements	Indicate pages submitted in the tender document
MR 1	Submit a copy of company's Valid Certificate of Registration Incorporation/Business name	
MR2	Provide copy of the Company's current KRA Tax Compliance Certificate **(To be verified on the KRA TCC Checker)**	
MR3	Submit Valid CR 12 Form. Must Attach National IDs of Directors	
MR 4	Submit valid County Government Business Permit	
MR 5	Original ***tender security*** of *KES 250,000/-* in form of a Bank guarantee from a bank or micro-finance Institution licensed and operating in Kenya valid for thirty (30) days beyond the validity of the tender. (**212days).**	
MR 6	Duly filled, signed and stamped Confidential Business Questionnaire	
MR 7	Duly completed Tender form signed and stamped	
MR 8	Duly completed SD1 and SD2 form	
MR 9	Provide copies of audited accounts for the company for the years 2022 & 2023 & 2024 (Certified by a registered Certified Public Accountant) **(To be Verified)**	
MR 10	Submit with tender a valid copy of the following Accreditation/Compliance Certificate from ICT Authority: **(To be Verified)** i. ICTA 1: Information security ii. ICTA 1: Systems and Applications	
MR 11	Bidder Must Provide a Valid Manufacturer's authorization form signed by the manufacturer to sell/service the product **(To be Verified)**	
MR 12	Submit with tender a valid Office of the Data Protection Commissioner (ODPC) registration certificate license as i. Data controller ii. Data processor **(To be Verified)**	

Failure to provide any of the above-mentioned documents will lead to automatic disqualification of the firm at the mandatory evaluation stage. The bidders that will meet the mandatory requirements above will qualify to proceed to mandatory technical compliance evaluation stage.

STAGE 2: TECHNICAL COMPLIANCE EVALUATION STAGE

2.1 Mandatory Technical Compliance Evaluation Stage

(a) Compliance with Technical Specifications

Bidders are expected to demonstrate compliance with the systems specifications in the bidder response column. The response should be comprehensive to demonstrate understanding of KEBS requirements.

"Yes", "No" or "To comply" responses will not be accepted. Any bidder who gives this kind of response shall be assessed as "NO" in the Technical Compliance Evaluation column and consequently failed in this stage of evaluation.

Technical Compliance Evaluation Criteria

- Compliant - Response satisfactory and demonstrates compliance to the specification.
- Non-Complaint - Response does not demonstrate compliance to the specification

A "non-compliant" assessment in any of the specifications leads to automatic disqualification from the next stage of evaluation.

NB: The rating procedure for the technical compliance evaluation stage shall be Compliant/Non-compliant as of the specifications detailed below.

2.2 TECHNICAL COMPLIANCE SPECIFICATIONS – DATABASE ACTIVITY MONITORING TOOL

No.	Requirements	Technical Compliance (Compliant/ Non-Compliant)	Bidder's Response (Narrative answers describing how the proposed product meets the minimum specification)
1	**Architecture**		
	The solution should be a turn- key solution delivered either by virtual or appliances (Virtual Preferred).		
	The solution should only require deployment of agents on the database servers for privilege user auditing and security.		
	The solution should be able to support AWS and AZURE gateways.		
	Agents should be deployed on system platform, no changes to databases or installation in databases should be required		

	If an agent is required, then the solution should send real-time alert, when agent is stopped or deleted.		
	The solution should be agent based or agentless. If its agents based it should not consume more than 7% of the CPU.		
	The audit trail should be stored as a flat file system for scalability.		
	The solution should support SAN Adapters for extensive audit storage.		
	The solution must support the following platforms: Microsoft SQL Server, Oracle DB, PostgreSQL MySQL et al.		
	The solution should offer protection for default passwords.		
	The solution should comply with rules of audit and compliance.		
	The solution should be future proof and should be able to provide audit and protection for Files, SharePoint, Microsoft Active Directory and Web Application Form on the same Platform		
	The solution must have a centralized management that manages all gateways and agents.		
	The solution should leverage existing network availability deployment if deployed inline.		
	The solution should leverage existing network equipment for sniffing or tapping the SQL traffic from the network.		
	The solution should be deployed in the network for other protocols like CIFS, NFS, HTTP, HTTPS and LDAP		
	The solution should support a proprietary spanning tree protocol for its own High Availability deployment.		
	SSL should be used for DB communication		
2	**Database Discovery**		
	The solution should perform automated database discovery, for both new and existing database and map all on the network.		
	The solution should keep historical information about the systems and their configuration		
	The solution should provide automated discovery of database tables and schemas.		
	The solution should show change since the last scan.		

	The solution should identify rogue or test databases		
	The solution should automatically discover database instances and port listening interfaces.		
	The solution should support change management process		
	The solution should automatically assign the appropriate audit policies based on the type of data contained in the database.		
	The solution should perform data discovery and classification.		
	The solution should detect sensitive data types, such as credit card numbers, social security numbers, etc., in database objects. List supported out of the box sensitive data types.		
	The solution should locate CUSTOM data types in database objects.		
	The solution should scan views.		
	The solution should scan synonyms.		
	The solution Should Support Granular classification: i.e. the solution should identify the specific object and column that contain the sensitive data.		
	The solution should reduce the false-positives that occur when identify non-sensitive data as sensitive. Explain.		
3	**Vulnerability Assessments**		
	The solution should perform vulnerability assessment. (include vulnerability Assessment test included in your solution)		
	The solution should allow custom assessments to be added		
	The solution should utilize user created scripts as assessment tests.		
	The solution should identify missing patches in the DB.		
	The solution should verify that default database accounts do not have a "default" password.		
	The solution should be used to measure compliance with industry standards and regulations.		
	The solution should be used to measure compliance with internal policies.		
	Vulnerability Assessment Result Analysis and Reporting		

	The solution should present a view of risk in relation to the sensitive data found in the database. Both by vulnerability and the sensitivity of the data.		
	The solution should be delivered with pre-defined reports.		
	The solution should support custom report generation.		
	The solution should compare the results of a discovery, classification or assessment job with a previous run. The reports should be distributed on demand and automatically (on schedule).		
4	**User Rights Management**		
	The solution should audit all user rights across heterogeneous database platforms.		
	The solution should support the analysis of excessive rights over sensitive data, including the case where the privilege is granted indirectly via nested roles.		
	The solution should detail all privilege paths to an object.		
	The solution should automatically identify dormant user accounts.		
	The solution should help track changes to user rights.		
	The solution should include bad practices overview, e.g.Users with direct object access.		
5	**Alerting and Blocking Capabilities**		
	The solution should provide automated, real-time event alert mechanism.		
	The solution should block database attack and unauthorized activity in real-time.		
	The solution should monitor and allow for blocking privileged users.		
	The solution should monitor and prevent SQL injection attacks.		
	The activity load should not affect real-time capabilities.		
	The real-time alerts should contain all information required for understanding of the incident, including: Source and destination IP and computer name, DB and OS user name, source application, number of affected rows, database instance name and business context.		

	The solution should inspect both in-coming and out-going DB traffic to protect against data leakage.		
	The solution should provide mechanisms for Content updates e.g. Security configurations/policies, attack signatures, vulnerability tests, etc.		
	There should be an automated mechanism to ensure the solution is up to date.		
	The solution should integrate with 3rd party anti-malware products to prevent infected clients from accessing sensitive data.		
	The solution should be able to handle all the SQL traffic for protection purposes against attacks or custom policies.		
	The solution should detect and protect from non-SQL based attacks. (For example - buffer overflow attacks)		
	The solution should provide automated follow-up action in response to a security event. (E.g., Send an email, run a script, syslog, etc.)		
6	**Database Activity Monitoring**		
	The solution should make use of a centralized appliance.		
	The solution should provide centralized control of collected information.		
	The appliance should come with the latest OS.		
	The appliance package should include DBMS product; if required.		
	Database Activity Monitoring must Include 8 Database Agent licenses for Linux, UNIX, and Windows.		
	The solution should scale to meet additional capacity requirements.		
	The solution should employ the use of agents on the monitored hosts.		
	The solution should support high- availability (HA) mode.		
	The solution should allow for native database audit function		
	The solution should employ transaction log auditing.		
	The solution should be compatible with SIEM tools solution. List the SIEM tools.		
	The solution should have a means to archive and restore data.		

	The Solution should have low impact on monitored Host. Describe the solution's impact on the monitored host.		
	The auditing process should be independent from the database platform being audited (supports separation of duties)		
	The solution should capture before and after image of data that is being manipulated		
	The solution should identify differences in baseline user activity.		
	The solution should capture select, update, insert, and delete (DML) activity by user/role.		
	The solution should capture schema/object changes (DDL) activity by user/role.		
	The solution should capture manipulation of accounts, roles and privileges (DCL) by user/role.		
	The solution should be capable of identifying the real application user (in case of connection pooling) Please explain how and if it is an included feature. Also explain what the impact will be to get the application user information.		
	The solution should be capable to trace the original user account if DBA/system admin use shared accounts like root administrator etc.		
	The solution should secure audit trail.		
	The solution should provide a mechanism to easily navigate through large audit data sets.		
	The solution should add organizational context to the audited activities. (e.g. John from development accessed sensitive HR data)		
	The solution should detect and block excessive cumulative access to sensitive information within a defined time interval in real- time.		
	The solution should report on business functions on top of SQL data. Explain if adding these details require changes on the applications.		
	The solution should audit non-SQL data access such as the Oracle "export direct" operation.		
	The solution should support encryption of audit data for both on-line and archived data.		
7	**Remediation**		

	The solution should provide effective tools for managing and mitigating risk to sensitive data stored in databases.		
	The solution should actively prevent attempts to exploit known vulnerabilities.		
	The solution should offer virtual patching capabilities. (protecting the database from known vulnerabilities without deploying a patch or script on the system)		
8	**Reporting**		
	The solution should provide packaged reporting capabilities.		
	The solution should support use of pre-configured policies/reports (PCI, sOx, HIPAA) for ensuring regulatory compliance.		
	The solution should provide functionality to assist with security event forensics.		
	The solution should allow for a batch process to consolidate audit data into a central repository before creating audit reports that cross heterogeneous database systems		

STAGE 3: TECHNICAL CAPACITY EVALUATION STAGE

3.0 DATABASE ACTIVITY MONITORING TOOL

NO.	CRITERIA	POINTS	TOTAL
1	**Specific experience of the organization in similar assignments**		24
	Provide evidence of undertaking at least two (2) assignments on Imperva Database Activity Monitoring tool. Provide LPO/LSOs/Contract Documents as evidence **(8 Marks each)**	16	
	Submit Completion Certificate from the above two (2) Contracts/LPO/LSO **(4 Marks Each)**	8	
2	**Technical approach**		28
	Methodology		
	- Demonstration of clear understanding of the terms of reference.	8	
	- Provide a Technical proposal with detailed design of the DAM Solution.	8	
	- Provide a detailed work plan and project implementation Methodology Detailed activities and milestones, Timelines and Resources required	6	
	- Draft SLA on the maintenance/support services of the DAM solution with clear escalation support matrix.	6	
3	**Qualification and competence of key staff (Attach CV and relevant Certificates)**		
	Team Leader /Project Manager		18
	- Degree in ICT, computer science, or a related discipline from a recognized university.	6	
	- Management Certification — Project Management Certification for the project manager. (Prince 2 or PMP and ITIL).	6	
	- At least five (5) years' experience in project planning and management. (Attach CV)	6	
	Security Engineers (Two Engineers) (Attach CV and relevant Certificates)		30
	- Degree in information technology or related discipline from a recognized university. **(3 marks each)**	6	
	- Minimum of three (3) years' experience in the relevant field. **(Attach CV) (4 marks each)**	8	
	- Imperva Data Security Certification. **(1 Engineer)**	8	
	- Imperva Application Security Certification **(1 Engineer)**	8	
	TOTAL		**100**

NOTE: A pass score of 80 marks (**Mandatory, Technical Compliance and Technical Capacity Evaluation Stage**) and above qualifies for financial evaluation.

STAGE 4: FINANCIAL EVALUATION STAGE

4.0 PRICE SCHEDULE

NOTE: The contract duration will be 3 years, however billing will be done annually.

LOT 1 - RENEWAL OF DATABASE ACTIVITY MONITORING TOOL				
Description	**Year 1**	**Year 2**	**Year 3**	**Total Cost (KES)**
Renewal of Database Activity Monitoring Tool (DAM) Licenses for **3 Years**				
Support and maintenance cost for **3 years**				
SUB -TOTAL				
ADD LEVY ORDER (0.03%)				
SUBTOTAL + LEVY ORDER				
ADD 16% VAT				
TOTAL COST INCLUSIVE OF ALL TAXES (KES)				