BANKI
KUU YA
KENYA

CENTRAL
BANK OF
KENYA

Haile Selassie Avenue
P.O. Box 60000 - 00200 Nairobi Kenya
Telephone: 2861000/2863000,
Email: supplies@centralbank.go.ke

ADDENDUM NO. 1

TENDER DOCUMENT FOR THE SUPPLY, IMPLEMENTATION, DEPLOYMENT AND COMMISSIONING OF AN ENTERPRISE VULNERABILITY MANAGEMENT & WEB APPLICATION SCANNING SOLUTION FOR CENTRAL BANK OF KENYA-TENDER NO. CBK/057/2022-2023

The above captioned tender was published on the Central Bank of Kenya (www.centralbank.go.ke) and the Public Procurement Information Portal (www.tenders.go.ke) websites on 10th January 2023. In response to the clarifications sought, the Bank is hereby issuing Addendum No. 1 in line with Section 75 of the Public Procurement and Asset Disposal Act 2015 and will form part of the tender document.

The clarifications are offered as indicated below: -

No	Clarification sought	Response
1	No of years the licenses are being quoted for.	The licenses are for 3 years.
2	The number of Target or (FQDN) which includes domains and subdomains to be quoted for.	As indicated in the tender document, the number of web applications for scanning are 50. The 50 are unique targets (e.g. https://abc.centralbank.go.ke, https://def.centralbank.go.ke etc)
3	Number of Servers (Windows, *UNIX, Linux, etc) to be monitored.	600
4	Number of Network devices (Switches, Routers, firewalls, etc) to be monitored.	150
5	Number of workstations (Windows XP, Windows 10, Android etc) to be monitored.	1,500
6	The bandwidth availability between each site (office).	20MBPS per site
7	Data retention period.	Minimum of 3 years to store vulnerability data

No	Clarification sought	Response
8	Current methods in use at CBK to collect security logs and user audit information.	Through standard protocols such as syslog, agents, SNMP etc. to a SIEM tool.
9	Team incharge of the security analysis and reporting Current methods used to monitor policy compliance.	Cyber Security team. Policy compliance monitoring done using compliance monitoring software. This is to be improved through the purchase of the proposed solution in the tender
10	Regulatory requirements (BASEL II, ISO27001-2, Health Insurance Portability and Accountability Act (HIPAA), GLBA (Gramm-Leach-Bliley Act), Payment Card Industry Data Security Standard (PCI DSS) Sarbanes-Oxley) that are being followed	ISO 27001, Swift CSP, Data Protection regulations
11	Mode of reporting currently in place to provide reports that demonstrate compliance to applicable regulations or organizational security policies.	Through semi-automated reporting from open-source tools
12	Number of data centres in CBK which host application service to support our business.	3 (2 Primary, 1 DR)
13	The design which includes our the branches, which would require scan engines deployed in each region's subnet as best practice.	It may not be necessary to install scanners in each branch. The information purposes.
14	Clarification on whether the system requirements covering both H/W & S/W will need to be quoted for or if the Bank is providing. e.g., InsightVM System Requirements (rapid7.com)	For any components that can run as a VM, the Bank will provide the VM environment (including the compute capacity). However, the vendor will be expected to install the server and the required components

The Tender closing date is extended to **3rd February 2023** at **10.30 a.m.**

All other terms and conditions of the tender remain the same.

DEPUTY DIRECTOR/HEAD OF PROCUREMENT
24th JANUARY 2023