My Bank, My Choice, My Future

KENYA POST OFFICE SAVINGS BANK

REQUEST FOR PROPOSAL (RFP)

SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) SOLUTION

TENDER NO KPOSB/019/2018

Release Date	**30th October, 2018**
Closing Date	**13th November, 2018 at 10.00 am**

TABLE OF CONTENTS

1 INTRODUCTION AND INSTRUCTIONS

The Kenya Post Office Savings Bank (hereinafter referred to as "Postbank" or "the Bank") intends to procure a Security incident and event management solution**.**
The purpose of this Request for Proposal (RFP) is to solicit proposals from qualified vendors for the procurement of Security Information and Event Management (SIEM) system and the acquisition of professional services to install, configure, and integrate the solution with other bank systems. The RFP contains information and instructions to enable qualified bidders to prepare and submit proposals and supporting material
The document provides a standard format for vendor/bidder responses, which must be returned to the Bank, **one in soft copy and two signed hard copies.**

The document is divided into three sections:

1. Section-A

i. It provides all details and guidelines to assist the vendor in responding to the tender
ii. It consists of **Sections 2** to **7**.

2. Section-B

i. The Vendors will use this section for entering the responses to the Technical and Financial Proposals.
ii. It consists of **Sections 8** and **9**.

3. Section-C

i. It consists of the Appendices.

Where applicable, please explain with additional information since Yes/No type answers could be considered as inadequate for the purposes of evaluating this solution. **Responses must address all aspects of the RFP and should follow the chronology of the RFP.**

SECTION A:

REQUEST FOR PROPOSAL INFORMATION & COMPLETION GUIDELINES

2 TENDER OVERVIEW

2.1 Response Administration:

i. Technical and Financial Proposal Responses:

Vendor responses are to be entered in or attached to the accompanying document entitled ***"PROVISION OF SECURITY INCIDENT AND EVENT MANAGEMENT (SIEM) SOLUTION"*** The proposals should be, **IN A PLAIN SEALED ENVELOPE,** will consist of two single sided hard copies **(Marked "Original" and "Copy")** and one soft copy on CD/DVD (in PDF/Microsoft Word & Excel for Windows format). **Please also refer to clause i on the sealing and marking of bids.**

The response should be clearly marked ON THE TOP OF THE ENVELOPE as

"Private and Confidential"

PROVISION OF SECURITY INCIDENT AND EVENT MANAGEMENT (SIEM) SOLUTION (TENDER NO.)

The bids should be deposited in the Tender Box located at the Ground floor Postbank House Nairobi

Addressed to:

THE MANAGING DIRECTOR
KENYA POST OFFICE SAVINGS BANK
POSTBANK HOUSE NAIROBI
P.O. BOX 30311-00100
NAIROBI, KENYA
Tel. +254-020-2229551/2803000

☞ *Any additional information (e.g. brochures, client testimonials etc.) should be referenced in the Tender Document such that they can be easily identified.*

ii. Queries:

Any questions, issues and clarifications regarding this document or the process should be addressed to **The Managing Director, Kenya Post Office Savings Bank, P. O. Box 30311 code 00100 Nairobi or** telephone **(020) 2229551/2803000** for voice or by e-mail to **md@postbank.co.ke**

2.2 Costs:

It should be understood that the Bank is not liable for any costs incurred by vendors in the preparation of their response to this tender or negotiations during the selection process.

The preparation of your response will be made without obligation by the Bank to acquire any of the items in your tender response, or to select any Vendor's tender response. Please note that all documentation and other supporting materials provided, as part of a submission becomes the property of the Bank and is not returnable.

2.3 Timetable:

Vendors must respond by **13TH November, 2018 at 10.00 a.m**.

Following the submission of responses, the remainder will consist of:

i. **Phase 1 -** Evaluation of responses and selection of the winning tender.
ii. **Phase 2 -** Contractual negotiations and agreement.

2.4 Request for Proposal Response Content and Format:

The Request for Proposal Response should have the following summarised structure for Section-B:

This is contained in **Section 8** of this document.

i. ***Executive Overview*** - should contain a Company overview and the perceived strengths of the bidder Request for Proposal response proposal.
ii. ***Vendor Details Matrix*** – bidders should complete the matrix on their own and on any other Vendors included in their Request for Proposal response proposal.
iii. ***Technical Requirements Checklists*** - should be completed giving clear and unambiguous responses.
iv. ***Implementation Plan*** - should present the implementation methodology and project details together with estimated timing and resources split per activity and phase.
v. ***Appendices*** - should provide contents as typed, attached documents, printed material or CDs (financial reports, brochures, software demos, etc.)
vi. ***Financial Proposal:***
Should be broken down as per the Request for Proposal document (**Section 9**)

2.5 Confidentiality:

This document is issued in confidence for the purpose only for which it is supplied. No information as to the contents or subject matter of this document or any part thereof arising directly or indirectly there from shall be given orally or in writing or communicated in any manner whatsoever to any third party, being an individual firm or company or any employee thereof, without the prior consent in writing of Postbank. Likewise, all information returned by Vendors, will be treated in confidence.

3 RESPONSE GUIDELINES

It should be noted that responses to this document would form the basis of any contractual agreement concluded with the selected vendor. The vendors should be able to demonstrate their compliance to any requirement if requested when they present their proposals more so as it relates to the Bank's requirements.
Furthermore, attaching a rating, which the vendor deems to be negative, may not in fact, be viewed by Postbank in a negative light

3.1 Text and Attachments:

Where various levels of details are required.

☞ *It is left to the Vendor to decide which method is relevant.*

However, each response point will have a proposed response type, that being Textual (within the document) or Attached (to the document).

i. Text:

If the response is able to be included in the document, a prompted or free text area is provided. For example:

Company Name	
Address	
Phone Number	
FAX Number	

The package is...

ii. Attachment:

If the response is NOT able to be included in the document (e.g. a brochure or large attached document), a Reference Description and Attachment Reminder is provided. For example:

Project Organisation Chart	Attached? (Y/N)	

3.2 Quoted Currency:

All monetary values should be in Kenya Shillings and inclusive of VAT and any other taxes as applicable.

4 ABOUT THE BANK AND THE PROJECT

4.1 About the Bank:

i. Ownership and Mandate:

The was Bank started in 1910 as a savings service within the Postal Services is wholly owned by the Government of Kenya and currently operates as Kenya Post Office Savings Bank [KPOSB] as incorporated in 1978 by an Act of Parliament, KPOSB Act (CAP 493 B of the Laws of Kenya). This Act was amended in 1990 to allow the Bank to establish and operate a company or corporation for the purposes of undertaking banking business and other related financial services in Kenya.

The mandate of the Bank is to:

a. Encourage thrift and inculcate savings habits among Kenyans.
b. Provide affordable savings facilities and instruments.
c. Pool personal savings for national development.

ii. Vision:

"To be the Premier Bank"

iii. Mission:

"To provide accessible quality banking and other financial services, through innovations that build sustainable customer relationships and stakeholder value

iv. Core Values of the Bank:

- Integrity
- Customer focus
- Innovativeness
- Professionalism
- Team work
- Corporate social investment
- diligence

4.2 About the project

i. Project Overview:

Postbank depends a great deal on Information Technology solutions and services to manage its operations. The IT infrastructure currently consists of a data Centre that connects all Postbank locations and offices via a wide area network. Postbank wishes strengthen its Information Systems Security and improve the current Information Security landscape. The Company wishes to source a competent vendor to supply for the Provision of Security incident and event management (SIEM) solution. The Bank invites technical and financial proposals from qualified vendors for the execution of the required services. The proposal should include the timelines and execution schedule.

ii. Project Objectives and Expected Deliverables:

In view of the growing use of IT and the evolving threat environment, Banks threat perception is also heightened. As a measure to further strengthen the Information Security, the bank has decided to secure a Security Information and Event Management solution.

The key objective of the solution is to ensure comprehensive information security monitoring, compliance reporting, incidence response and reasonable protection for threats that may exist for Postbank's infrastructure. This shall support the overall objective of attainment of the best security practices within Post Bank in line with today's level of technology and threat environment.

Other objectives include but not limited to the following: -

- Ensure effective incident management and risk mitigation by providing effective real-time monitoring, incident detection and response capabilities.
- Streamline compliance reporting and keep up with the changing compliance regulations.
- Provide ongoing, actionable metrics to help measure the spirit of security controls.
- Availability and business continuity monitoring

Expected deliverables are:

At the end of the implementation exercise, the solution provider should provide a comprehensive report with a detail of completed implementation work. The report will consist among others the following:

- Fully installed well integrated customized and functioning Security Information and Event Management solution.
- Presentation of the working solution to the IT management and staff of the bank after completion of the implementation for review and feedback.
- An executive summary report for Management of the implemented solutions.
- Proper documentation.

iii. Project Scope

The SIEM Project includes all of the Equipment and Implementation services necessary to provide a SIEM Solution to connect to the various network elements and meet the capacity, functionality and feature requirements outlined in this RFP. The scope of this RFP includes the following:

i. Identification and recommendation of an appropriate SIEM solution, which fits the Bank's requirements and allows for future growth;

ii. Supply, configuration, installation and testing of the proposed solution, including any required interfaces and data conversions;

iii. Provision of initial and extended warranties and technical support services (including detailed initial acquisition costs and on-going support options.

iv. On-site hardware installation and setup, software configuration and user settings;

v. Training for software configuration and SIEM management software.

vi. Provision of documentation in printed and electronic format, including administrative and end user manuals, troubleshooting guides or Q&A.

vii. Functional solution that will be fully integrated into current architecture.

viii. Training of identified users: Sufficient training for employees to effectively use and maintain the proposed Solution. Vendor will provide the detailed induction training to the persons nominated by the Bank. The training will be arranged by the vendor at the cost of the vendor. All expenses related to training shall be borne by the selected vendor. The trainings should include the architecture, hardware, software, integration, customization, policy installation, trouble shooting, reporting and other aspects of the system. Vendor will ensure knowledge transfer and will involve the Bank officials during implementation.

Vendor shall provide comprehensive training manual, lecture notes, handouts and other training documentation during trainings.

iv. Key solution components

i. **Log Collection:** Logs from all the in-scope devices located at the geographically dispersed location should be collected. Vendor should develop the baseline for the level of logs to be enabled from different components of IT infrastructure assets. The log transfer shall be through secure transfer.

ii. **Log Aggregation and Normalization:** Logs collected from all the devices should be aggregated as per the user configured parameters. Logs from multiple disparate sources should be normalized in a common format for event analysis and correlation.

iii. **Log Encryption, Compression and Transmission:** Collected logs should be encrypted and compressed before the transmission to the remote Log Correlation Engine.

iv. **Log Archival:** Logs collected from all the devices should be stored in a tamper proof format on the archival device in the compressed form. Logs and storage should maintain a chain of custody to provide the same in the court of law, in case the need arises. For correlation and report generation purpose, past -3- months log data should be available online. Logs prior to -3- months period should be stored on secondary media. Retrieval of archived logs should not require any proprietary tools/protocol and should be retrievable using open standards/protocols or else the retrieval tool should be provided to the Bank at no extra cost.

v. **Log Replication:** Solution should enable replication of logs from DC to DR for redundancy. The solution should be capable of automatically moving the logs from device to archival storage based on the ageing of the logs.

vi. **Log Correlation:** Collected Logs should be correlated according to various predefined criteria for generation of alert and identification of the incident. The correlation rules should be predefined and also user configurable. Correlation rules should reduce false positives. In any case False negatives will not be permitted. In case of detection of any such incident, correlation rules must be customized immediately to capture such incidents.

vii. **Alert Generation:** Solution should be capable to generate alerts, register and send the same through message formats like SMTP, SMS Syslog, SNMP as per user configurable parameters.

viii. **Event Viewer/Dashboard/Reports/Incident Management:** SIEM Solution should provide web based facility to view security events and security posture of the Bank's Network and register incidents. Solution should have drill down capability to view deep inside the attack and analyse the attack pattern. Dash board should have filtering capability to view events based on various criteria like geographical location, Device type, attack type etc. Dashboard should have Role based as well as Discretionary access control facility to restrict access to incidents based on user security clearance level. Solution should provide various reports based on user configurable parameters and standard compliance reports like PCI-DSS, ISO27001, SOX, IT Act and regulatory reports. Selected vendor will customize incident management/dashboard/reports for the Bank and will modify the same as per the changing requirement of the Bank.

ix. **Incident management:** Solution should be able to register any security event and generate trouble ticket. Solution should provide complete life cycle management (work flow) of trouble tickets from incident generation till closure of the incident. Solution should provide the logging facility to different levels of users to monitor and manage the incidents generated for closure of the same as per the defined workflow. Incident management should include escalation as per the escalation matrix. Solution should be able to send the incident report in various forms like e-mail, SMS etc.

x. **SIEM Solution Hardware & software integration:** Vendor will integrate all the Hardware and software components supplied under this RFP.

xi. **Development of Connectors for customized applications/devices:** While it is expected that connectors for all the standard applications and devices will be readily available in the collector and Log management devices, connector for mostly in- house/custom built applications may need to be developed.

xii. **Use case support:** The solution shall support the various Use Cases in order to provide log collection, event correlation, Alert Generation and escalation. Proposed solution must demonstrate the capability to support various for the

following Use cases. For example: Use Cases for mobile and Internet Banking Transactions, ATM Transactions, RTGS / NEFT Transactions, CBS System.

xiii. **Workflow Automation:** Selected vendor will define the work flow automation so that applications are integrated and manual intervention is minimal.

xiv. **SIEM Operation:** SIEM shall be configured to generate meaningful incidents/reports and reduce the generation of false positives.

xv. **Behaviour/Activity monitoring:** Solution should provide activity monitoring capability as well as transaction related access by various applications. Solution should track user activity and monitor identities and activities of users across all devices to enable generation of ad-hoc reports on particular user/group of users.

v. Licensing:

All the tools supplied as part of this RFP should be supplied with Enterprise wide License. Bank will have the right to use the tools for the functions provided by the tools in any manner and for any number of branches, offices, subsidiary units, joint ventures, irrespective of the number of users, geographical location of the devices being monitored. Bank will also have a right to relocate any one or all the tools to different locations.

vi. Proposed methodology

Based on the study of the Banks IT Infrastructure, vendor will suggest the detailed implementation methodology acceptable to the Bank with timelines as per the RFP terms and conditions.

vii. Bank's Infrastructure Overview:

The bank's network is composed of 99 branches and a head office. The network is composed approximately 750 endpoints at Head office and regional offices. The bank's applications are located and managed centrally from the Nairobi Head Office and serve the Regions through dedicated high-speed wide area network links between the branches.

The bank's base consists of both Windows 7 (64-bit) and the office suite Microsoft Office 2010 or later release. All the banks internal users authenticate to the network through Microsoft Active Directory (AD). All clients' PC/Laptops run anti-virus/end-point security. The server infrastructure consists of Microsoft Windows Server 2008,2012 R2, with VMWare 6.0. and Oracle VM. The bank has a disaster recovery site that hosts a subset of the environment in case of disaster. In addition, the bank's server infrastructure consists of among others:

- **Web Services/Applications**: Web services, IIS, .Net Framework, Microsoft – business software & office products, Microsoft Exchange.
- **Other servers/OS**: Red Hat Linux, HP UNIX (3), Oracle Linux (2), external DNS Servers (2), VMWare ESXi (6)
- **Databases**: Oracle, MS SQLServer
- **Other components**: WiFi APs

5 EVALUATION CRITERIA

The purchaser's evaluation of the bids will take into account the bid price, the technical specification and delivery period/implementation schedule offered in the bid. The Purchaser will evaluate bids and award points as per the Evaluation Criteria and Score Board derived from the Bank's requirements.

5.1 General Requirements Evaluation:

A preliminary evaluation will be undertaken to determine:

i. Suitability of the bidder to provide the service
ii. All required documents and information have been submitted as indicated in clause **8.1**.

5.2 Technical and Financial Evaluation Criteria:

- All required documents and information has been submitted as indicated in clause **8.2.**
- The bidders must indicate how the proposed solution meets all the requirements specified in clause **8.2**
- Each of the listed categories will be assigned a weight and a score according to its importance.
- For specifications where bidder indicates compliance it will be presumed that the price of the feature is included in the commercial quote by the Bidder including customization, if any. Bidder should additionally mention in the remarks column the details of customization in brief.

Criteria Category	Weighting	Maximum Score
Mandatory Criteria	•	•
• Preliminary Evaluation	**N/A**	**Yes/No**
• Mandatory Requirements	**N/A**	**Yes/No**
Technical Criteria	•	**70%**
• Provider Stability, Experience & Capabilities	•	•
• Proposed Solution As per specifications	•	•
• Hardware & platform	•	•
• Post implementation support	•	•
• Training & documentation & Provider staff capacity	•	•
Financial Criteria	•	**30%**

Technical Evaluation Matrix

Item	Evaluation	Max Score
Mandatory	Manufacturer Authorization, Gartner Magic Quadrant listing & At least one reference site.	**N/A**
Provider Experience & Capabilities	• No. of deployments installed in the last five years At least one (1 Site) and a maximum of Three 3. • No. deployments with similar complexity i.e. No of endpoints & environment. (Maximum of two. • Deployment/System Integration/Data Connectors/Commissioning Process.	**15**
Proposed Solution	As per minimum specifications.	**70**
Appliance & Platform	Appliance to operationalize SIEM at Optimal and Peak times.	**5**
Post Implementation Support	Detailed documentation on post implementation support and capacity.	**5**
Staff Training & Staff Capacity	Installation & support Training for staff. No of Certified resources for implementation.	**5**
	Total	**100**

Note 1

The Financial evaluation shall be determined by:

i. Taking the bid prices as quoted in the proposal.
ii. Taking into account any corrections made by the Bank relating to arithmetic errors in the tender
iii. Taking into account any minor deviations that do not materially depart from the requirements set out in the tender proposal.
iv. Applying any discounts offered in the tender.
v. Converting all tenders to the same currency
vi. Applying margins of preference as prescribed by the Laws of Kenya
vii. Applying, uniformly across all the tenders, any other internal financial considerations and financial evaluation methods that the Bank will take into account in comparing and determining the option that most meets the Bank's requirements.

The Bank will evaluate bids and award points as indicated in the Evaluation Criteria set out above.

Based on the technical evaluation criteria, each Bidder will be given certain marks. Only those Bidders scoring 70% or above in the technical evaluation will be short-listed for financial evaluation.

The successful bidder shall be the responsive proposal with the highest score determined by combining, for each proposal, in accordance with the evaluation procedures and criteria, the scores assigned to the technical and the financial proposals and the results of any other additional evaluation prescribed by the purchaser.

Where the successful bidder's quote is beyond the budget of the organization, the Bank may opt for the highest ranked bidder whose quote is within the budget.

6 INSTRUCTIONS TO BIDDER (ITB)

6.1 Introduction:

i. Background:

Kenya Post Office Savings Bank is seeking for ***Provision of a Security Incident and event monitoring solution (SIEM).*** The Technical Specifications of the required items and associated services are as provided in **Section 8** of this Request For Proposal document.

ii. Eligible bidders:

This bid is open to all companies in Kenya who have the necessary qualifications as specified in **Section 8** of this document.

iii. Cost of Biding:

The bidder shall bear all costs associated with the preparation and submission of its bid, and Kenya Post Office Savings Bank, hereinafter referred to as "the Purchaser," will in no case be responsible or liable for those costs, regardless of the outcome of the bidding process.

6.2 The Bidding Documents:

i. Invitation to RFP Documents:

The goods or services required, bidding procedures and contract terms are detailed in the bidding documents. The documents are:

i. Instructions to bidders (ITB)
ii. General Conditions of Contract (GCC)
iii. Technical Specifications/Proposal
iv. Service specifications/Requirements
v. Financial Proposal
vi. Tender Form

The bidder is expected to examine, carefully, all instructions, terms and conditions, bid forms, technical and service requirement specifications in the bidding documents. Failure to furnish the information required, or submission of a bid not substantially responsive to the requirements of the bidding documents, will be at the bidders' risk and shall result in the rejection of its bid. For the purposes of these clauses, a substantially responsive bid is one

that conforms to all terms and conditions set in all of the bidding Documents without material deviations.

ii. Clarification of Bidding Documents:

A bidder requiring any clarification of the bidding documents may notify the purchaser in writing or by cable, (hereinafter the term cable is deemed to include telex, e-mail and facsimile) at the purchaser's address indicated in the invitation for bids. The Purchaser will respond in writing or by cable to any request for clarification, which it receives no later than seven (7) days prior to the deadline for submission of bids prescribed by the purchaser. Copies of the Purchaser's response (including a description of the query but without identifying its source) will be sent to all the bidders.

iii. Amendment of Bidding Documents:

At any time prior to the deadline for the submission of bids, the Purchaser may, for any reason, whether at its own initiative or in response to a clarification request by a bidder, modify the bidding documents by amendment.

The amendment will be sent in writing or by cable to all the bidders and will be binding on them. Bidders shall promptly acknowledge receipt of each amendment in writing or by cable.

In order to provide the bidders reasonable time in which to consider the amendment in preparing their bids, the Purchaser may, at its discretion, extend the deadline for the submission of bids.

6.3 Preparation of RFPs:

i. RFP Submission Documents:

The bid submitted by the bidders shall comprise the following: -

i. Price schedules completed in accordance with clause 7.3.1, 7.3.2, 7.3.3 and 7.3.4
ii. Documentary evidence established in accordance with clause 7.3.5 and 7.3.6 that the bidder is eligible to bid and is qualified to perform the contract if the bid is accepted.
iii. An Implementation Schedule detailing the activities associated with dispensing of the proposed solution, identifying the beginning and end of each activity to be undertaken, resources needed for each activity.
iv. A detailed and well-documented proposal for the provision of support services.

ii. Price List:

The bidder shall complete the Financial Proposal provided in the bidding documents or furnish an equivalent schedule, indicating the goods and

services to be supplied, a brief description of the goods and services and their country of origin. For the purposes of this clause, "origin" of goods means the place where the goods are manufactured or produced or from which the ancillary services are supplied.

iii. RFP Prices:

The bidder shall indicate on the appropriate Price Schedule (Financial Proposal) all quantities, unit prices and total bid prices of the goods and services it proposes to supply under the contract.

Unit Prices indicated on the schedule shall include all customs duties and sales and other taxes already paid or payable.

Prices quoted by the bidder and agreed at the time of signing the contract shall be fixed and shall not be subjected to variation on any account. A bid submitted with an adjustable price quotation will be treated as non-responsive and will be rejected. The Purchaser may reasonably request for the bid validity extension when necessary and the price shall be fixed for the time extended.

iv. RFP Currency:

Tender shall be priced in **Kenya shillings**.

v. Documents Establishing Bidders Qualifications:

For establishment of the bidder's qualification to perform the following shall be required:

i. Presentation of a written authority/agreement of the Manufacturer(s) to supply the required key services/items.
ii. Statements outlining the reasons that they feel they have the technical, financial and production capability to carry out the contract and the necessary details including name(s) of subcontractors and valid contract agreements that they will use if they are awarded the contract.
iii. Copies of valid agency authority/agreements from the Manufacturers or ancillary product suppliers of the goods that will be used to provide the contracted goods or services.

vi. Documents Establishing Good's Conformity to the Bidding Documents:

Pursuant to clause 7.3.5, the bidder shall furnish, as part of its bid, documents establishing the conformity to the bidding documents of all goods and services, which the bidder proposes to supply under the contract.

The documentary evidence of the conformity of goods shall establish to the purchaser's satisfaction that they will have their origin as defined under clause 7.3.5.

The documentary evidence of the goods conformity to the bidding documents may be in the form of literature, drawings and data, which shall consist of a detailed description of the good's essential and performance characteristics.

vii. Period of Validity of RFP:

RFQs shall remain valid for a period of **ninety (90)** days after the bid opening date prescribed by the purchaser. A bid, which is valid for a shorter period, shall be rejected by the purchaser as non- responsive.

viii. Format and Signing of RFP:

The bidder shall prepare one original and one copy of the documents, and they shall be clearly marked **"ORIGINAL" and "COPY"**. In the event of any discrepancy, between them the original shall govern.

The original and the copy of the bid shall be typed or written in indelible ink and shall be signed by the bidder. The bidder shall initial all pages of the bid including any amended printed literature. Failure to fulfil these requirements will result in the rejection of the bid as non-responsive.

6.4 Submission of RFP:

i. Sealing and Marking of RFP:

The bidders shall seal the original and copy of the bid in separate envelopes duly marking the envelopes as **"Original**" and **"Copy**". Please also refer to clause 2.1.1.

The envelopes shall be addressed to the purchaser at the following address:-

THE MANAGING DIRECTOR
KENYA POST OFFICE SAVINGS BANK
P.O. BOX 30311-00100
NAIROBI
KENYA
Tel. +254-020-2229551

The sealed envelopes clearly marked as indicated under clause 2.1.1 of this document shall be placed in the Tender Box situated on the ground Floor of Postbank House.

ii. Deadline for Submission of RFP:

RFP must be received by the purchaser at the address specified above not later **t*han 17*th July, 2018 at 10.00 a.m**. ***the date and time stated in this tender document.***

The purchaser may, at his discretion, extend the deadline for the submission of bids by amending the bidding documents in accordance with clause 7.2.3, in which case all rights and obligations of the purchaser and bidders previously subject to the original deadline will thereafter be subject to the deadline as extended, and the period of validity of bid date shall be adjusted accordingly.

iii. Late RFP:

Any bid received by the purchaser after the deadline for submission of bid prescribed by the purchaser, pursuant to clause 7.4.2 above, shall be disregarded and/or returned unopened to the bidder.

iv. Modification and Withdrawal of bids:

The bidder may modify or withdraw its bid after the bid's submission, provided that the purchaser receives written notice of the modification or withdrawal prior to the deadline for submission of bids.

The bidder's modification notice shall be prepared, sealed, marked and dispatched in accordance with provisions of clause 7.4.1. A withdrawal notice may also be sent in writing or by cable but must be followed by a signed confirmation copy, post-marked not later than the deadline for submission of bids.

No bid shall be modified after the deadline for submission of bids.

No bid shall be withdrawn in the interval between the deadline for submission of bids and the expiry of the period of bid validity specified by the bidder on the RFP Form.

6.5 Opening and Evaluation of RFPs:

i. Opening of RFPs by Purchaser:

The purchaser will open the bids in the presence of the bidders **on the date specified by POSTBANK in the Tender bids invitation.** The bidders present shall sign a register evidencing their attendance and the opening of the bids.

The bidder's names, modifications, discounts, if any, bid withdrawals and presence or absence of such other details as the Purchaser at its discretion, may consider appropriate will be announced at the opening.

ii. Clarification of bids:

During evaluation of the bids, the Purchaser may, at its discretion, ask the bidder for a clarification of its bid. The request for clarification and the response shall be in writing and no change in the price or substance of the bid

shall be sought, offered, or permitted. Any bidder who is not willing to respond to clarification requested within the stated time will be rejected from further evaluation and be disqualified depending on the significance of the information required.

iii. Evaluations and Comparison of RFPs:

The Purchaser will evaluate bids and award points as indicated in the Evaluation Criteria in clause 6.1.

The successful proposal shall be the responsive proposal with the highest score determined by the purchaser by combining, for each proposal, in accordance with the evaluation procedures and criteria, the scores assigned to the technical and the financial proposals and the results of any other additional evaluation prescribed by the purchaser.

iv. Contacting the Purchaser:

After the public opening of bids, information relating to the examination, clarification, evaluation and comparison of bids, and recommendations for the award of a contract shall not be disclosed to bidders or any other persons not officially concerned with such process until the award to the successful bidder has been announced.

Any attempt by a bidder to influence the purchaser's bid evaluation, bid comparison or contract award shall result in the rejection of the bidder's submission.

v. Post Qualification:

The purchaser will determine to its satisfaction whether the bidder that is selected as having submitted the best-evaluated, responsive bid is qualified to perform the contract satisfactory, and shall verify the expected winner's:

i. Professional and technical capability and experience required;
ii. Managerial ability (competence);
iii. Financial strength;
iv. Track record of bidder;
v. Continuity of the bidder in that line of business

vi. Award Criteria:

Subject to clause **6.1** above, the purchaser shall award the contract to the successful bidder whose bid has been determined to be substantially responsive, has met all the essential specifications and has been determined as the highest marked bid, provided further that the bidder is determined to be qualified to satisfactorily perform the contract.

vii. Purchaser's Right to accept any RFP, Reject any or all RFPs:

The purchaser reserves the right to accept or reject any bid and to annul the bidding process and reject all bids, at any time prior to award of contract, without thereby incurring any liability to the affected bidders or any obligation to inform the affected bidders of the grounds for the purchaser's action.

6.6 Award of Contract:

Prior to the expiration of the period of bid validity, the purchaser will notify the successful bidder in writing by a registered letter or by cable to be confirmed in writing by a registered letter, that its bid has been accepted.

6.7 Language:

All bid submissions shall be **written in the English language**, as shall all correspondence and other documents pertaining to this tender.

6.8 Further contracts Related to this Request for Proposal:

A bidder who enters into a contract resulting from procurement by a request for proposal shall not enter into any other contract for the procurement of goods or works that follows from or is related to that original contract.

7 GENERAL CONDITIONS OF CONTRACT (GCC)

7.1 Contract and Interpretation:

i. Definitions:

In this contract, the following terms shall be interpreted as indicated:

"THE CONTRACT" refers to the contract signed by the parties to which these General Conditions of Contract (GCC) form an integral part, together with all annexes, schedules or appendices as the case may be;

"THE CONTRACT PRICE" refers to the price payable to supplier under the Contract for the full and proper performance of its contractual obligations;

"THE PURCHASER" refers to Kenya Post Office Savings Bank purchasing the goods/services;

"THE SUPPLIER" refers to _____;

"THE SERVICES" refers to those services associated with the supply of the Goods, such as transportation and insurance, and any other incidental services, such as installation, commissioning, provision of technical assistance, training and other such obligations of the Supplier covered in the contract;

"THE GOODS" refers to all of the equipment, machinery, and/ or other materials, which the supplier is required to supply to the purchaser under the contract.

ii. Application:

These General Conditions are provisional. A detailed contract incorporating, all these conditions and any other will be signed upon successful bidding and award of the tender.

iii. Standards:

The goods and services supplied under this contract shall conform to the standards mentioned in the Technical specifications and, where no applicable standard is mentioned, the authoritative standard appropriate to the goods' country of origin and such standards being the latest to be issued by the manufacturer will apply.

iv. Amendments:

No variation in or modification of the terms of the contract shall be made except by written amendment signed by the parties.

v. Assignment/Sub-Contracting:

The supplier shall not assign, in whole or in part, its obligation to perform under this contract, except with the purchaser's prior written consent.

vi. Applicable Law:

The laws of Kenya shall govern the bid and this contract.

vii. Governing Language:

This contract has been executed in English language, which shall be the binding and controlling language for all matters relating to the meaning or interpretation of this contract.

viii. Notices:

Any notice given by one party to the other pursuant to this contract shall be sent to the other party in writing or by cable, telex, e-Mail or facsimile and confirmed in writing to the other party's address:

[a] The Client's Address:
The Managing Director
Kenya Post Office Savings Bank
P. O. Box 30311-00100
Nairobi
Kenya
Fax: +254-(0)20-2229186
E-Mail: md@postbank.co.ke

[b] Supplier's Address:
Contact Person
Designation
Organization's Name
P. O. Box
City
Country
Fax No:
E-Mail:

Any notice shall be effective as evidenced by either Registered Post or by Fax report.

ix. Supplier's RFP:

The following shall form part of this contract:

i. Supplier's Bidding Document
ii. Letter of award
iii. Local Purchase Order

x. Secondary Contractual Agreements:

This agreement constitutes our entire agreement and supersedes any other prior and contemporaneous communications. It prevails over general terms and conditions maintained by either party. In the event that there is

inconsistency between these general conditions and any other prior contemporaneous or subsequent communications, these terms shall prevail. However, these conditions may be changed with prior mutual written consent of both parties.

xi. Service Level Agreement:

The supplier and the purchaser shall enter into an agreement for the supply of the aforementioned goods and services where necessary.

xii. Resolution of Disputes:

The purchaser and the supplier shall make every effort to resolve amicably any disagreement or dispute arising between them under or in connection with the contract.

If, after **thirty (30) days** from the commencement of such informal negotiations, the purchaser and the supplier have been unable to resolve amicably a dispute the same shall be referred to Laws of Kenya Arbitration in accordance with the Arbitration Act.

An arbitrator who will be appointed by the Chairman of the Chartered Institute of Arbitrators will arbitrate the matter/dispute. The decision of the arbitrator will be final and binding.

7.2 Confidentiality and Property Rights:

1. Use of Contract Documents and Information:

The supplier shall not without the purchaser's written consent disclose the content of the contract, or any provision thereof, and specification of information furnished by or on behalf of the purchaser in connection therewith, to any person other than a person employed by the supplier in the performance of the contract.

Any document, other than the contract itself shall remain the property of the purchaser and shall be returned to the purchaser on completion of the supplier's performance under the contract.

2. Indemnification:

i. The supplier represents and warrants that it has the rights and authority to enter into this agreement and to grant the rights described in this agreement. The supplier shall defend and indemnify the purchaser against any claims by any third party for infringement of intellectual property rights, trademark, patent, copyright, trade secrets or industrial design rights arising from the use of the products by the purchaser. The supplier shall be responsible for all claims, including but not limited to the amount of any resulting adverse final judgment or negotiation, court and legal fees

PROVIDED that the supplier is notified promptly in writing of the claim and is given the sole control over the defence or negotiation;

The purchaser will give notice to the supplier of any such claim without delay, shall provide reasonable assistance to the supplier in disposing of the claim, and shall at no time admit to any liability for or express any intent to settle the claim. Indemnities shall not apply if any claim of infringement or misappropriation:

a) Is asserted by a parent company, subsidiary or an affiliate of the purchaser;
b) Is a direct result of a design mandated by the purchaser's Technical Specifications and the possibility of such infringement was duly noted in the supplier's bid; or
c) Results from the alteration of the products by the purchaser

ii. The supplier shall indemnify the purchaser for all losses arising out of the negligence on the part of the supplier and/or their agents while providing or supplying the said goods or services.

iii. The purchaser shall indemnify and defend the supplier against all third-party claims of infringement of Intellectual Property Rights, including patent, trademark, copyright, trade secret or industrial design rights arising from the use of any information or software provided to the supplier by the purchaser under the contract, and used for the purposes set out in this agreement.

7.3 Payments, Guarantees and Liabilities:

i. Payment:

The supplier's requests for payment shall be made to the purchaser in writing, accompanied by an invoice describing as appropriate, the goods delivered and services performed and upon fulfilment of other obligations stipulated in the contract, payment shall be made in Kenya Shillings as indicated in clause 7.3.4 of Instructions to suppliers.

ii. Prices:

Prices charged by the supplier for goods delivered and services performed under the contract shall not vary from the prices quoted by the supplier in its bid, with the exception of any price adjustments authorized at the purchaser's request for bid validity extension, as the case may be.

iii. Taxes and Duties:

Suppliers shall be entirely responsible for all taxes, duties, license fees and any levies payable to the Government of Kenya or any of its arms under this contract. Prices quoted should be inclusive of all taxes.

iv. Delays in the Supplier's Performance:

The performance of services shall be made by the supplier in accordance with the time schedule agreed between the purchaser and the supplier.

If any time during performance of the contract, the supplier or its subcontractor(s) should encounter conditions impeding timely delivery of the goods and performance of services, the supplier shall promptly notify the purchaser in writing of the fact of the delay, it's likely duration and its cause(s). As soon as practicable after receipt of the supplier's notice, the purchaser shall evaluate the situation and may at its discretion extend the supplier's time for performance, with or without liquidated damages, in which case the extension shall be ratified by the parties by amendment of the contract.

Except as provided for in the contract, a delay by the supplier in the performance of its delivery obligations shall render the supplier liable to the imposition of liquidated damages, unless an extension of time is agreed upon without the application of liquidated damages.

v. Liquidated Damages:

Subject to the **Force Majeure clause** below, if the supplier fails to deliver or install any or all of the systems and services or if any item of the system fail to gain acceptance within the timescale(s) specified in the contract, the purchaser shall, without prejudice to its other remedies under the contract, deduct from the Performance Security, as liquidated damages **1%** of the contract price for each week or part thereof of delay to deliver the services, until successful acceptance, up to a maximum deduction of **10%** of the contract price being.

Once the value of performance security is exhausted, the purchaser may consider termination of the contract pursuant to the Termination for Default clause below and the supplier shall remain liable for breach of contract.

vi. Termination for Default:

The purchaser, without prejudice to any other remedy for breach of contract, by written notice of default sent to the supplier, may terminate this contract in whole or in part:

i. If the supplier fails to deliver any or all of the goods within the agreed period
ii. If the supplier fails to perform any other obligations stipulated in this contract

In the event the purchaser terminates the contract in whole or in part, the purchaser may procure upon such terms and in such manner, as it deems appropriate, products similar to those uninstalled or services similar to those undelivered, and the supplier shall be liable to the purchaser for procurement of such extra goods and/or services. However, the supplier shall continue performance of the contract to the extent not terminated.

vii. Termination Due To Insolvency:

The purchaser may terminate this contract immediately if the supplier becomes bankrupt or otherwise insolvent. In this event, termination will be without compensation to the supplier, provided that such termination will not prejudice

or affect any right of action or remedy; this has accrued or will accrue thereafter to the purchaser.

viii. Termination without Default:

The purchaser may, by a **sixty (60) day** advance written notice sent to the supplier, terminate the contract, in whole or in part, at any time for its convenience. The notice of termination shall specify that termination for the purchaser's convenience, the extent to which performance of the supplier under the contract is terminated, and the date upon which such termination becomes effective.

The purchaser shall accept at the contract terms and prices the products that are complete and ready for shipment within **thirty (30) days** after the supplier's receipt of notice of termination. For the remaining terminated products and services, the purchaser may elect:

i. To have any portion completed and delivered under mutually agreed terms and prices; and/or

ii. To cancel the remainder and pay the supplier an agreed amount for products and services partially completed or already procured.

ix. Force Majeure:

i. For purposes of this contract, "Force Majeure" means an event which is beyond the reasonable control of a party and which makes a party's performance of its obligations under the contract impossible or so impractical as to be considered impossible under the circumstances.

ii. The failure of a party to fulfil any of its obligations under the contract shall not be considered to be a breach of or default under this contract in so far as such inability arises from an event of force majeure, provided that the party affected by such an event;

   a) has taken all reasonable precautions, due care and reasonable alternative measures in order to carry out the terms and conditions of this contract

   b) has informed the other party as soon as possible about the occurrence of such an event

iii. Extension of time: Any period within which a party shall, pursuant to this contract complete any action or task shall be extended for a period equal to the time during which such party was unable to perform such action as a result of Force Majeure.

x. Limitation of Liability:

Except in cases of criminal negligence or wilful misconduct:

i. The supplier shall not be liable to the purchaser, whether in the contract or otherwise for any indirect or consequential loss or damage, provided this exclusion shall not apply to any obligation of the supplier to pay liquidated damages to the purchaser as envisaged in clause 3.3.6.

ii. The aggregate liability of the supplier to the purchaser under the contract shall not exceed the total contract price, provided that this limitation shall not apply to any obligation of the supplier to indemnify the purchaser with respect to intellectual property rights.

7.4 Contract Execution:

i. Delivery:

The supplier shall make delivery of the required goods and services from the date as indicated in the contract.

7.5 Services:

i. Services to be provided:

The supplier is required to ***provide penetration testing and application security audit services.***

Incidental Services:

The supplier is required to provide all of the following services including services, if any, of performance or supervision of on-site assembly and/or start-up of the supplied hardware, software, communication infrastructure and other peripherals as indicated or required.

i. Furnishing of tools required for assembly and/or maintenance of the services provided;
ii. Performance and supervision of the required services
iii. Prices charged by the supplier for incidental services, if not included in the contract price shall be agreed upon in advance by the parties and shall not in any event exceed the prevailing market rates.

ii. Provision of Manuals:

The supplier shall provide the purchaser with manuals where applicable as listed:

i. Servicing, Technical and Operational manuals;
ii. Users', Administration and Diagnostic manuals;
iii. Any other manuals that may have been provided by the product manufacturer;
iv. The manuals shall be in electronic format where feasible.

iii. Goods and Services Support:

For goods and services still to be delivered, the supplier will offer to the purchaser latest versions based on the latest appropriate technology and having equal or better performance or functionality at the same or lesser unit prices.

iv. Change orders:

The purchaser may at any time, by a written order given to the supplier pursuant to ***Clause 8.1.4*** make changes within the general scope of the contract in any one or more of the following:

i. Designs or specifications for services or for systems that are to be integrated, or customized specifically for the purchaser;
ii. The method of shipment and/or schedule for and/or place of delivery;
iii. The schedule for Installation or Acceptance;
iv. The services to be provided by the supplier; and/or
v. The substitution of new products and services from the supplier

If the supplier requests such substitution, the purchaser shall notify the supplier in writing within thirty (30) days of its decision to accept or reject the proposed Change Order.

If any such change causes an increase or decrease in the cost of, or the time required for, the supplier's performance of any provisions under the contract, an equitable adjustment shall be made in the contract price or delivery schedule, or both, and the contract shall accordingly be amended.

Any claims by the supplier for adjustment under this clause (and for the delay) must be asserted within **thirty (30) days** from the date of the supplier's receipt of the purchaser's Change Order failure to which the claim will automatically lapse.

If the parties cannot agree on an equitable adjustment, the Change Order will not be implemented. However, this provision does not limit the rights of either party under Clause 3.3.

v. Purchaser's Obligations:

The purchaser will appoint a Manager responsible for managing the delivery and installation schedule, with the authority to accept or reject all deliverables and to be the Primary contact for the supplier's representative. The Manager will officially record all delays and problems, and forward them to the supplier within **two (2) weeks** of discovery of such problems.

The purchaser shall be responsible for timely provision of all resources, facilities, equipment access and information necessary for the completion of the delivery and installation schedule, as identified in the agreed implementation plan. Except where provision thereof is expressly provided in the contract as being the responsibility of the supplier. Delay by the purchaser may result in an appropriate extension of the time for Installation and Acceptance schedules by the supplier.

The purchaser will designate appropriate staff for the training courses to be given by the supplier, and shall make all appropriate logistical arrangements therefore in accordance with the agreed training plan.

The purchaser is responsible for performing and safely storing timely and regular backups of its data and Software in accordance with accepted data management principles, except where such responsibility is clearly assigned to the supplier elsewhere in the contract.

vi. Supplier Obligations:

The supplier shall abide by the job safety, insurance, customs and immigration measures and laws in force in Kenya, and shall indemnify the purchaser from all demands or responsibilities or damage arising from accidents or loss of life or damage of any nature, the cause of which is the supplier's negligence.

The Supplier shall conduct all contracted activities with due care and diligence, in accordance with the contract and using industry practices and economic principles, and exercising all reasonable means to achieve the performance specified in the contract.

The supplier shall work closely with the purchaser's appointed manager and staff, and abide by the directives issued by the purchaser that are consistent with the terms of the contract. The supplier is responsible for managing the activities of its personnel and shall be responsible for any wilful or negligent conduct of its personnel.

The supplier shall appoint subject to the purchaser's written consent, a qualified representative to manage its performance of the contract within **thirty (30) days** from the contract signature. The supplier shall furnish the purchaser with the Curriculum Vitae of the representative prior to the appointment. The representative shall be authorized to accept orders and notices on behalf of the supplier, and to generate notices and commit the supplier to specific courses of action within the scope of the contract. The representative may be replaced only with the prior written consent of the purchaser.

The supplier shall produce and submit an implementation plan to the purchaser for approval.

The supplier shall make available to the purchaser with relevant information but limited to information security and associated risks.

The supplier shall complete delivery and acceptance of the services in accordance with schedule and specification changes as the supplier may be entitled to, pursuant to Clause 3.35.

vii. Warranty

The supplier warrants that all goods and services supplied under the contract are new, are latest or current models and that they incorporate all recent improvements in design and materials unless provided otherwise in the contract. The supplier further warrants that all goods and services supplied under this contract shall have no defect arising from design, materials or workmanship or from any act or of mission of the supplied goods.

The warranty shall remain valid for at least twelve (12) months after the acceptance of the goods and services.

The purchaser shall promptly notify the supplier in writing of any claims arising under this warranty. Upon receipt of such notice of defect, the supplier shall with all reasonable speed, repair or replace the defective goods thereof, without any additional cost to the purchaser.

This is the end of Section A – Request for Proposal Completion Guidelines

SECTION B:

BIDDERS / VENDOR RESPONSE DOCUMENT

8 THE BANK'S REQUIREMENTS

8.1 General Requirements

This section relates to information to be provided by the bidder for evaluation of their suitability to supply the goods and services required by the Bank. The requirements in this section may also have been implied in other sections of the RFP document as well as by the Bank's general supplier Tender requirements-:

ITEM	SUPPLIER'S RESPONSE	
Contact	Name of Business	
	Business Address	
	Business Phone Number	
Names of Directors/Partners of Firm		
Indicate maximum value of business your firm has ever handled (Ksh.)		
Indicate Head Office Location		
Will you source for the total solution or you will partner with a third party? If yes, please provide details of the third party.		
Indicate number of employees		
A letter of introduction	A one-page cover letter introducing the company and signed by the person(s) authorized to sign on behalf of, and bind the company to the statements made in the submission	
A Qualification Statement	At least one page stating why your company qualifies for consideration taking into account the technical, financial and production capability to carry out the contract.	
Certificate of Registration	Certified copy required	
Trade License	Certified copy of your Trade License	
PIN Number	Certified copy of your PIN Document	
VAT Registration Number	Certified copy of your VAT Registration Document	
Tax Compliance Certificate	Certified copy of your Tax Compliance Certificate	

Audited Accounts Reports	The most recent audited Accounts for 3 years certified by a Certified Public Accountant.
Staff qualifications relevant to the project	Certified copies of certificates for at least **3 ICT security certified** technical support staff **MUST** be provided.
	CVs for the technical support staff **MUST** be provided by filling in the attached form (refer to **Section 10**) and must be for **Kenya based support staff only**. This is to ensure the Bank does not incur unnecessary expenses related to travel by foreign consultants.
Working with the Government of Kenya	Has your firm ever been barred by the government?
Willingness to provide a performance bond	Are you willing to provide a performance bond of 10% of contract price?
Certificate from Manufacturer	Attached authorized certificate from manufacturer.
Reference Sites	At least 3 reference sites where similar work has been successfully undertaken.
Tender Security	Bidders will be required to submit a tender security equivalent to 2% of the bid price inform of banker's cheque or Bank Guarantee and valid for a period of 120 days after the closing period. **This is a mandatory requirement.**

8.2 Technical and Business Requirements

i. SIEM Solution Specifications

Specification/Evaluation Criteria	Marks	Bidders Compliance	Remarks
Mandatory Requirement. • SIEM Solution **MUST** be listed/assessed in the latest Gartner Magic quadrant 2017. • Manufacturer Authorization: If the Provider does not manufacture the proposed solution, the Provider **MUST** provide the manufacturer's name and Provider/manufacturer relationship and manufacturers' authorization. • References**:** Provider to describe their experience in implementing SIEM solutions in similar types of environments as Postbank. Provider should have Enterprise Security or IT / Information Security as one of their primary business line and **MUST** have implemented a similar SIEM solution at an institution of similar size or greater as Postbank. At least 1(One) reference site where similar work has been successfully undertaken **MUST** be provided.			
Provider Experience/Capabilities (15 marks) • **Assessment of the Reference Sites** No. of deployments installed in the last five years At least one (1 Site) and a maximum of Three 3. Actively Supported Site: No. of deployments with similar complexity i.e. No of endpoints & environment			

• **Deployment** Provider to give brief description on how they will Implement the proposed SIEM Solution to connect to the various network elements and meet the capacity, functionality and feature requirements outlined. • **System Integration** The Proponent's proposed solution should integrate with any of the following enterprise solutions without customization (i.e. out of the box). (Firewall/UTM solutions, Intrusion detection/prevention solutions, network switches/routers, Application/Database /Web servers, Workstation security solutions (anti-virus, anti-malware, desktop IDS, etc...) • **Data Connectors** The Proponent's proposed solution should address how the Proponent will implement data connectors for devices, software and other technologies existing within network, which are not immediately compatible with the proposed solution. • **Commissioning Process** Providers should have a standard methodology and documented process for commissioning the proposed Solution. Providers should provide a high-level plan including the types of activities that will be performed to commission the proposed SIEM Solution. The plan should have defined steps with specific milestones covering all critical elements of the process. Included in the plan should be the expected outcome of the activities to be performed			

• **Version control** The Bidder should provide the latest version of the Solution (Proof of evidence).			
General Specifications (20 Marks) • **Bidder to give solution as an Appliance.** i. **Single Global View:** The solution should offer Single View of All the Data collected from in-scope devices across sites/geographies. Solution should ensure surveillance throughout the entire IT infrastructure and detect and track malicious activity to uncover advanced threats. ii. **Data/Log Enrichment & management:** Solution must support input from various log and non-log data sources (identity, database, application, configuration, net-flow, cloud, file integrity, etc. Solution should be flexible to collect from any device or software currently in use in the environment iii. **Parsing & Normalization** – Collect logs from various sources and normalize to a standard format for easy storage, analysis & reporting. iv. **Advanced Correlation:** Between Events of different type thereby helping in threat identification. Solution should support pre-built policies, user-defined policies, and behavioural policies thereby helping in threat identification. v. **Real time Notification and Alerting** – real time alert on Security threats in the			

	IT environment based on analysis of collected logs.			
vi.	**Compliance Management & Automation:** Monitoring and alerting on compliance events in real-time and provide the necessary reports and dashboards.			
vii.	**Reporting and Alerting:** Pre-built reporting and alerting libraries, customizable dashboards, compliance use-case support, various alerting options, and integration into external reporting and third-party workflow tools.			
viii.	**Asset Intelligence:** Ability to import context and keep an inventory of all data as it relates to assets automatically.			
ix.	**Threat Intelligence Feed:** Security threat intelligence feed integration with ability to update multiple uses and control updating behaviours. Integrate any public or private threat feed into SIEM, and cross-correlate.			
x.	**Scalable Architecture and Deployment Flexibility:** Solution should support multiple deployment options, platform support, and data collection methods. Support both agent and agent-less.			
xi.	**Real Time Analysis Automation:** Ability to start analysis and assist security analysts by reducing false-positives automatically. Solution should give the intelligence, without the noise.			
xii.	**Usability:** The administrative interfaces should have the ability to provide			

	intuitive user interface with features such as correlated events, unlimited drill down to packet level event details, simultaneous access to real-time, raw logs and historical events customizable at-a-glance security view for administrators. The drill down should be directly from the dashboard using a single mouse click.			
xiii.	**Full Security Threat Visibility:** Integration with existing security technologies for monitoring, incident analysis and data enrichment to support ability to track and analyse series of related events.			
xiv.	**System Integration:** The Proponent's proposed solution should integrate with existing enterprise solutions without/minimal customization.			
	Other Desired Features:			
i.	**Resource Utilization:** Consume as little resources as possible under normal operations. Solution to limit bandwidth for transmitting event data from remote sites.			
ii.	Provide an easy to use GUI interface that enables proficiency with minimal training. E.g. Web based administration (both http and https)/ user interface for device management and monitoring.			
iii.	**Data Management Security and Retention:** Granular access controls to system data, protection of SIEM data, system access monitoring, external storage integration and efficient data			

	compression **iv.** **Forensic Analysis:** Support Advanced query capabilities against all collected data with pre-built and custom drill down. **v.** **Incident Management and Remediation:** Advanced detection and incident management with pre-built and customizable remediation capabilities, integration into workflow systems, and optional automatic remediation through integration. **vi.** **File Integrity monitoring:** Monitor integrity of files **vii.** **Configuration/Change Monitoring:** Monitor and alert on system, device changes **viii.** **Application Monitoring** – Eliminate application blind spots by gaining full visibility. **ix.** **Identify APTs** – Identify and react to Advanced Persistent Threats (APTs) via suspicious pattern and automated response. **x.** **Endpoint monitoring:** Monitor networks and endpoints to ensure all of the forensic detail to detect and neutralize advanced threats. **xi.** **Security Incident Detection & Response Workflow Automation:** Operations Workflow for handling detected security incidents and threats. Automatically open and assign tickets to the appropriate team members while maintaining an audit trail for incident			

handling process. **xii.** **Insider Threat Detection:** Detect suspicious insider activity. **xiii.** **Behaviour/Activity Monitoring:** Track user activity and monitor identities and activities of users across all devices to enable generation of ad-hoc reports on particular user/group of users. **xiv.** Activity auditing, including firewalls, Servers web and intrusion Detection. **xv.** Threat Prioritization to continuously monitor, identify threats, and automatically prioritize security events. **xvi.** USB device monitoring.			
Key functionality Assessment **A. Event Collection (10 Marks)** **i.** **Multiple Source Support:** Monitoring of all types of event sources e.g. Windows, Custom (in-house) developed applications, syslog, Linux, oracle. Solution should provide support variety of common and vendor specific protocols such as syslog, SNMP, WMI, network flow, databases and more. **ii.** **Categorize Event Data:** categorize log data into an easy-to-understand format with little dependence on vendor-specific event IDs. **iii.** **Bandwidth Throttling:** Limit bandwidth for transmitting event data from remote sites. **iv.** **Event Prioritization:** Prioritization whereby high priority log events can be prioritized and sent immediately to the log management engine for analysis.			

v.	**Compression:** Compression for all transmitted data for bandwidth conservation.			
vi.	**Collection Flexibility:** Distributed event collection mechanism must have both agent-less and agent based options.			
vii.	**Centralized Collection Management**: Collection mechanism to be managed centrally allowing configuration of all collection features, backup configurations and push software updates using one, centralized interface.			
B.	**Log Management (10 Marks)**			
i.	**Log Management Scalability:** Solution must scale to larger environments and the increase of additional event sources without requiring additional hardware.			
ii.	**Log Encryption, Compression and Transmission:** Collected logs should be encrypted and compressed before the transmission to the remote Log Correlation Engine. Transport Integrity encrypt the log transport to ensure confidentiality. RAW logs that are received by the SIEM solution should be Authenticated (time-stamped), encrypted and compressed before being transmitted to the log management solution			
iii.	**Parsing & Normalization** – Collect logs and normalize to a standard format for easy storage, analysis & reporting.			
iv.	**Log Collection capabilities*:*** Agent/ Agentless approach, and support out of the box log collection support for 3rd party commercial IT products.			

v.	**Storage Integrity:** The log management system must utilize on board storage RAID levels for local data redundancy with the ability to reinitialize a failed disk from data stored in the RAID cluster.			
vi.	**Log Collection/Management Automation:** Solution should automatically scan Active Directory for the list of servers to be monitored and automatically accept events to monitor devices, introducing new event sources, managing retention policies without any administrator intervention.			
vii.	**Search Patterns:** The solution's log management system search interface must provide support for simple search patterns as well as complex.			
viii.	**Search Logic:** The vendor's log management system search interface must provide the ability to combine search operators into a single search expression.			
ix.	**Search Time Range:** Search interface must provide the option to search across time ranges using either a custom time (date / time start, end) or dynamic time.			
x.	**Scheduled Archive:** The log management system must provide a simple interface to schedule the compression and archiving of log data.			
xi.	**Enforce Retention Policies:** Provide ability to define multiple retention policies automatically.			

xii. **Automatic System Backup:** S imple method for automatically and manually backing up and restoring system data. **xiii.** **Administration Audit Trail:** The log management system must log all administrative access and activities and provide access to the audit logs through the same web interface. **xiv.** **Administration Alerting:** A bility to alert on system state activity such as low disk space, component failures, high resource utilization, etc.			
C. <u>Correlation</u> <u>(10 Marks)</u> The system must provide for correlation rules, statistical correlation, historical, session, identity, and role correlation **i.** **Real-time Prioritization:** Assessing attack vectors and the targeted systems to determine the susceptibility of a threat/ priority. **ii.** **Multiple correlation:** Support correlation of logs from all the devices and all security scenarios like spoofing, authentication failures, etc. The solution must support multi-device, multi-event and multi-site correlation across the enterprise **iii.** **Asset Intelligence:** Ability to import context and keep an inventory of all data as it relates to assets automatically. **iv.** **Business Intelligence:** Ability to logically segregate data by business role, department/domain. **v.** Solution should support the following types of correlation:			

	i. Rule-Based/Heuristic ii. Vulnerability iii. Statistical/Historical			
vi.	**Workflow:** Provide a complete audit trail and accountability during the incident handling or forensic investigations.			
vii.	**Early Threat Detection:** The solution must provide out-of-the-box detection of new/zero-day threats that are yet to be filtered/blocked by the organization's existing security defence infrastructure.			
viii.	**Zero-Day Threat Intelligence:** The solution must provide automatic detection of a 0-day worm outbreak across the enterprise when IDS or Antivirus signatures are unable to detect the incident. The system must then immediately send alerts and automatically start the incident triage and workflow.			
ix.	**Activity Baseline:** Ability to monitor network and application activity to create baselines and use these baselines to identify suspicious behaviour.			
x.	**Unaccountable User Activity:** The solution must alert or report on any activity for identities that are not automatically synchronized with the authentication directories in order to detect rogue user accounts on critical systems.			
xi.	**Activity Monitoring:** Track user activity and monitor identities and activities of users across all devices to enable			

	Analysts generate ad-hoc reports on particular user/group of users. **xii.** **Insider Threat Detection:** Detect suspicious insider activity. **xiii.** **Forensic Investigations**: Allow restoration of historical log files and analysis. **xiv.** **Threat Response:** Detect attacks and provide mechanism to respond/mitigate.			
	<u>Security Features (5 Marks)</u> **i.** **Role- based views:** The system should have a provision for the authorization for the different levels of users on the SIEM on the basis of their roles. i.e. should have the ability to create and assign role- based views **ii.** **Tamper proofing:** SIEM Database should write logs in tamper proof manner. Once the logs are written to the disk/database no one including SIEM or database/system administrator should be able to modify/tamper/delete the stored logs till correlation and archival of the same. **iii.** The system should maintain the audit trail for the management activities of individual users and administrators accessing and using the application **iv.** The system should have a mechanism for protection of unauthorized access on the Log Database by system administrator. **v.** Solution should be capable to track Access-list violations **vi.** Solution should display the health status			

of the SIEM Solution. **vii.** The vendor solution should provide user accounts with granular access permissions and roles to different accounts. **viii.** For authentication the system shall support LDAP authentication including Microsoft's Active Directory. **ix.** Log transmission between Client & central Engine should support SSL /encryption			
D. <u>Forensic and historical Data</u> <u>(5 Marks)</u> **i.** The solution should provide quick and easy access to real-time as well as historical operational data. **ii.** The solution should provide full forensic event tracking to ensure comprehensive trend and historical analysis and reporting. **iii.** Flexible dashboard interface allowing the examination of a specific event or a holistic view of the systems within the enterprise.			
<u>Alerting and viewing requirement</u> Solution should allow setting up of alerts based on event types, system event, attacks, failure count, geographical location, department wise, etc. **iv.** The solution should provide full forensic event playback to ensure comprehensive trend and historical analysis and reporting. **v.** The portal should generate e-mail and SMS notifications for all critical/high			

	risk alerts triggered from SIEM log monitoring, vulnerability assessment.			
vi.	It should allow filtered view of events classified on the basis of severity/device/traffic-on-TCP or UDP-port/location/ segment to different teams, geographical locations.			
vii.	Provide for watch list feature to enable the user to populate the list based on various parameters like IP Address, URL etc.			
viii.	E-mail notifications should contain the contents of the report as an attachment capable of being saved as Excel and or PDF.			
ix.	Solution should provide configurable automated actions in response to security problem, e.g. sending E-mail Notifications, SMTP notification, SYSLOG notifications to operators.			
x.	The system should have a provision of view filters when displaying the logs related to specific IP address, specific service or specific time duration or geographical location.			
xi.	The system should have an Event display Window for all alerts coming in real time.			
xii.	The process should allow applying filters and sorting to query results.			
xiii.	The solution should include the following categories of predefined graphs and queries out of the box: **a.** Firewall, including Top Firewall			

Interfaces, File Access through Firewall, and Login Failure **b.** Database, such as Login Activity, Authorization Level and Authorization Level by User **c.** Intrusion detection, including Top Attack Signatures, Attack Type by Severity Level, and IDS /IPS Signature Summary **d.** Operations, such as Device Activity Analysis, Activity by Event Category, and Network over Time **e.** User, including Privilege Users Monitoring, Configuration Change Details and Activity by Specific Username.			
E. <u>Tool Reports</u> <u>(5 Marks)</u> **i.** List out a full list of reports offered by the solution specifying reports included for each supported device type. **ii.** Please list reports for compliance packages offered e.g. (Sarbanes-Oxley (SOX), Payment Card Industry (PCI), ISO 27001. ***iii.*** The reports should be available in the following exported formats: *a) PDF b) XLS c) CSV* **iv.** The system should have the capability to Schedule Reports and transmit the same through e-mail on periodic basis. **v.** All raw log format fields should be available for query using the solution. **vi.** The solution should provide a process for creating and save adhoc log queries. This			

process should use standard syntax such as wildcards and regular expressions. **vii.** Compliance and security relevant reports should be available out of the box. The platform must be able to customize the out of the box reports as well. (*please specify no of reports available*) **viii.** Variety of reports with the availability of the management level reporting with full capability to customize and create new reports according to business requirements. **ix.** The system should allow email of scheduled reports to recipients. **x.** System should have inbuilt query analysis capability and should not require any third party or physically separate solution.			
F. <u>Desired Dashboard features</u> <u>(5 Marks)</u> The dashboard portal should provide the following: **i.** SIEM events/incidents related alerts, log stoppage alerts, monthly summary reports and analysis. The unified portal should provide summary of log, stoppage alerts and automatic suppression of alerts. **ii. Dashboard Standard Browser Support:** Web-based dashboards for solution should be accessible with a standard browser. **iii. Dashboard Updated in Real-**			

	Time: Dashboards should operate/update in real-time.			
iv.	**Drill down Support**: Dashboard should support drill down graphs to click and move to the level of individual assets			
v.	Dashboard should be customizable to individual user need. Dashboard should allow creation of custom displays for any group of users. The portal should allow users to view alerts raised through this portal.			
vi.	The unified portal should make use of qualified security event and incident alerts raised from SIEM into useful periodic reports (weekly, monthly basis) and analysis. These reports should be available for view or download.			
vii.	The portal should also allow users to initiate and track alert related mitigation action items. The portal should allow reports to be generated on pending mitigation activities based on ageing analysis.			
viii.	There should be a feature to create any kind of report from any of the available data from the feeds like top incidents by application, by hosts, users etc.			
ix.	Summary view for management reporting including heat maps, executive score cards for top management that covers security performance of different business units, compliance, asset status			
x.	Dashboard should display asset list and capture details including name,			

	location, owner, value, business unit, IP address, platform details			
xi.	Dashboard should capture the security status of assets and highlight risk level for each asset. The asset status & risk scores should be consolidated at a higher level to report on overall security status of bank, status of different business units within the bank, status of key locations			
xii.	Dashboard should have graphical display of asset security status based on locations, business units. Graphical display should support different methods of representing information including bar charts, pie charts, line charts as relevant to the information that is represented.			
xiii.	Dashboard should capture risks in each asset. Dashboard should have the provision to click on the asset and track mitigation status corresponding to risks			
xiv.	Dashboard should support reporting for consolidated relevant compliance across all major standards and regulatory requirements. E.g. ISO27001, ISO PCI.			
xv.	Dashboard should support different views relevant for different stake holders including top management, operations team, Information Security Department.			
xvi.	Dashboard should support export of data to multiple formats including CSV, XML, Excel, PDF, word formats			
xvii.	Ability to provide an intuitive user			

interface with features such as display correlated events, unlimited drill down to packet level event details, simultaneous access to real-time, raw logs and historical events customizable at-a-glance security view for administrators. The drill down should be directly from the dashboard using a single mouse click. **viii.** The dashboard should display the security status of IT infrastructure in the bank. (Display of asset status based on locations, business units etc.) **xix.** Dashboard should capture risks in each asset. There should be a graphical representation of risks across business units. Dashboard should support drill down the level of individual assets **xx.** The system should have a facility to view Summary of all Dashboard views for the entire enterprise.			
<u>Hardware & Platform</u> **<u>(5 Marks)</u>** • The bidder must provide an appliance that will meet requirements to operationalize the solution at Optimal and Peak times. Bidder to size the hardware needs as per solution and the scope. • The bidder to provide calculations/ logic arrived at the sizing for all hardware as part of the response. **Processor performance** The optimum performance must not exceed 60% utilization. **Memory** The optimum usage must not exceed 60%			

utilization for the capacity recommended configuration. **Storage capacity** • The storage configuration must offer a RAID configuration to allow for protection from disk failure. The Solution should have the capability to compress the logs by at least 70% for storage optimization. Documentary support should be provided. • Adequate capacity to store the all requested Application Software and the capacity should ensure past -3- months log data should be available online. Logs prior to -3- month period should be stored on secondary media.			
Post Implementation Support (5 marks) • **Service Level Agreement** Providers should provide a sample of their standard service level agreement (SLA). • **Licensing** Providers should also provide a samples of all software license agreements that would apply as part of their proposed solution. • 3 Year Software licenses and labor for all the items above to be included. • (Give details of what is included with licensing for your solution e.g. if collection, correlation, analysis and reporting functions are included within license costs). • Provider to indicate all of the licensing details for the proposed Solution, such as whether it is licensed by seat, IP address,			

named-user, events per second or per reporting device. • **Maintenance and Support** Provider to include descriptions of the support services they provide. At a minimum proposal should address the (Availability of call support; (web) service request capabilities available, On-site support when required; Technical support for upgrading the solution; Versions\updates are released at regular intervals). • **Warranty** Providers to describe the warranty program included as part of their proposed solution. All maintenance during the warranty period and under any maintenance agreements will be performed by the Successful Provider. • **Documentation** Provider to provide a copy of the system documents necessary for the proper utilization of the proposed solution. These shall include but are not limited to System drawing including critical components and troubleshooting. Operating procedures and methods including diagnostic and test procedures.			
• **Training Program & Documentation (5 Marks)** Conduct training, tailored specifically to the audience. Training of (6) Staff.			

NOTE:

The bidders must indicate how the proposed solution meets all the requirements specified above. For specifications where bidder indicates

compliance it will be presumed that the price of the feature is included in the financial quote by the Bidder.

9 FINANCIAL PROPOSAL

NO	Component Description	Unit Cost Ksh.	Total Cost in Ksh.	VAT Ksh.	Total Cost in Ksh. (VAT Inclusive)
1.	Supply, Install and Commission of Security Information and Events Management				
2.	Hardware Costs				
3.	Training for Staff				
4.	3 Year Software Support inclusive of licenses and labour for all the items above.				
5.	Other Costs (Please specify if any)				
	Total Costs				

SECTION C:

APPENDICES

10 FORMS TO BE COMPLETED AND ATTACHED

10.1. Appendix 1: Tender Form

TENDER FORM

Date……

From: ……

Address: ……

Tel. No……

Fax: ……

To: ……

RE: TENDER FOR

……

……

In accordance with Tender No…… Dated……

I/We ……

Hereby tender to ……

In accordance with the attached Tender forms/conditions of Tender/schedule of requirements at the price/fees/charges shown against item and in Conformity with the scheduled delivery arrangements stated.

I/We understand that the Kenya Post Office Savings Bank reserves the right to accept or reject this tender in part or in whole for any reason it considers justifiable.

I/We agree that terms of this Tender will remain valid for and will not be withdrawn for a period of 90 days from the final date for submission of Tender.

In the event of this Tender being accepted in part, or in full, I/We agree to provide performance guarantee against the contract issued by a reputable Bank (or other form acceptable to Postbank) and accepted in this Tender and that failure on my/our part to meet these requirements constitutes a breach of contract.

Tenderers Details:

Name……

ID No……

Address…… Occupation……

Tel. No…… Fax No……

Sign…… Date……

Stamp……

Witnessed By:

Name……

ID No……

Address…… Occupation……

Tel. No…… Fax No……

Sign…… Date……

Appendix 10.2: Firm's reference Form

Relevant similar service carried out in the last five years that best illustrate suitability. Using the format below, provide information on each reference assignment for which your firm/entity, either individually as a corporate entity or as one of the major companies within an association, was legally contracted.

<table>
<tr><td colspan="2">Assignment Name:</td><td>Country:</td></tr>
<tr><td colspan="2">Location within Country:</td><td>Professional Staff Provided By Your Firm/entity(profiles):</td></tr>
<tr><td colspan="2">Name of Client:</td><td>No of Staff:</td></tr>
<tr><td colspan="2">Address:</td><td>No of Staff-Months; duration of assignment:</td></tr>
<tr><td>Start Date (Month/Year):</td><td>Completion Date (Month/Year):</td><td>Approx. Value of Services (in Kes):</td></tr>
<tr><td colspan="2">Name of Associated Consultants, if any:</td><td>No of Months of Professional Staff Provided by Associated Consultants:</td></tr>
<tr><td colspan="3">Name of Senior Staff (Project Director/Coordinator, Team Leader) involved and functions performed:</td></tr>
<tr><td colspan="3">Narrative Description of Project:</td></tr>
<tr><td colspan="3">Description of Actual Services Provided by Your Staff:</td></tr>
</table>

Firm's Name: _____

Appendix 10.3: Methodology and Work plan for assignment

a. Proposed Approach

……

……

……

……

……

….

b. Work plan

……

……

……

……

……

c. Proposed Personnel Schedule

1. Technical/Managerial Staff			
Name	Position	Highest Qualification and Certifications(attach certified copies)	Task

Appendix 10.4: Format of Curriculum Vitae for Technical Staff

Proposed Position: .....

Name of Firm: .....

Name of Staff: .....

Profession: .....

Date of Birth: .....

Years with Firm: .....

Nationality: .....

Membership in Professional Societies: .....

.....

Detailed Tasks Assigned: .....

.....

Key Qualifications:
(Give an outline of staff member's experience and training most pertinent to tasks of this assignment. Describe degree of responsibility held by staff member on relevant previous assignments and give dates and locations).

.....

Education:
(Summarize college/university and other specialized education of staff member, giving names of schools, dates attended and degrees obtained).

.....

Employment Record:
(Starting with present position, list in reverse order every employment held. List all positions held by staff member since graduation, giving dates, names of employing organizations, titles of positions held, and locations of assignments).

.....

Certification:

I, the undersigned, certify that these data correctly describes me, my qualifications and my experience.

…… Date: ……
(Signature of staff member)

…… Date: ……
(Signature of authorized representative of the firm)

Full name of staff member: ……

Full name of authorized representative: ……

END