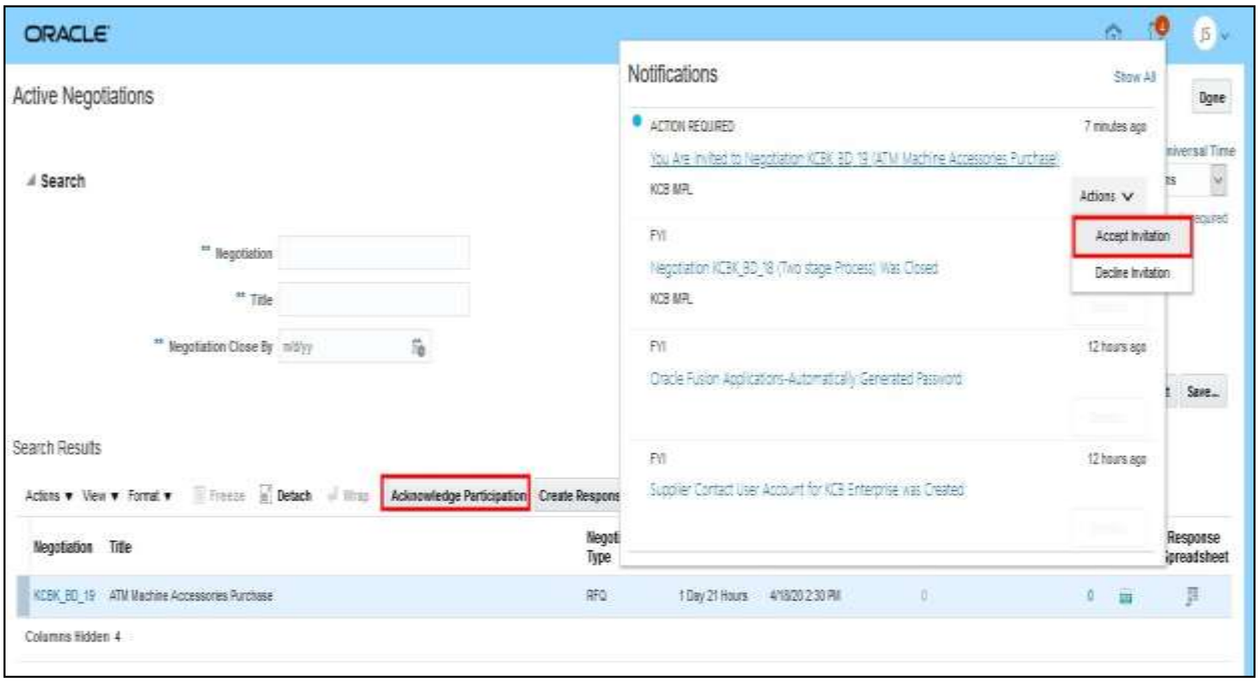
REQUEST FOR PROPOSAL FOR INTEGRATED FRAUD AND TRANSACTION MONITORING SOLUTION

Release Date:	**As per the sourcing portal**
Last Date for Receipt of bids:	**As per the Sourcing Portal**

ISSUE OF RFP DOCUMENT TO PROSPECTIVE BIDDERS

<u>TENDER FOR INTEGRATED FRAUD AND TRANSACTION MONITORING TOOL</u>

This tender is being floated electronically. You are required to accept the invite or decline as an initial step.



S

Table of Contents

DEFINITIONS

For purposes of this document, the following definitions shall apply:

The Bank	KCB Bank Ltd
Bid	The proposal or Response to this RFP submitted by prospective Suppliers for fulfilment of the Contract.
Supplier	The Company awarded the task of supplying all the items described in this document installing and commissioning them.
Contract	Supply, installation, and commissioning of all the works, equipment and/or services that are described in this document, which will contribute towards meeting the objective of the RFP
Warranty	Period from the time installation and testing is completed, during which the Contractor undertakes to replace/rectify equipment and/or installation failures at no cost to the Bank

1.0 SECTION 1 – REQUEST FOR PROPOSALS

1.1 Introduction

KCB BANK (hereinafter referred to as "the Bank") is a leading Commercial Banking Group in the East African region renowned for its diversity and growth.

The Bank's vision is to be the preferred **financial** solutions provider in Africa with global reach. The Bank has eight subsidiary companies – KCB Kenya, KCB Tanzania, KCB South Sudan, KCB Bank Uganda, BPR Bank Rwanda, KCB Burundi sand Trust Merchant Bank (TMB).

The platform is anchored on consolidation across our existing business, expanding and modernizing delivery channels, improving operational efficiencies, turning in returns commensurate with level of investment and compliance with all regulatory and internal policy guidelines.

The information in this document and its appendices and attachments is confidential and is subject to the provisions of our non-disclosure agreement and should not be disclosed to any external party without explicit prior written consent of Kenya Commercial Bank.

The bank would wish to source and implement **Integrated Fraud and Transaction monitoring tool**.

This document constitutes the formal Request for Proposal (RFP) for **Integrated Fraud and Transaction monitoring tool** and is being availed on an open tender basis and is open for bids from companies that meet the requirements stated herein.

Objective of this RFP

The primary objective of the Integrated fraud and transaction monitoring solution is to:

- **Develop higher levels of security in an efficient and cost-effective way**.
  This will involve proactively managing transaction risk exceptions before the risk materializes.
- **To improve approvals for transactions and revenues from payments, across Omni-channels, while reducing cases of false positives**

This will involve:

- Development of real-time views across all transactions, points of connectivity and payments infrastructure to speed up detection and analysis of flagged activities.
- Implementation of precise, real-time risk scoring and blocking based on configurable supervised and unsupervised machine learning models.

- **Detection and blocking of payments, across Omni-channels, in milliseconds**

This will ease operational loss cases and go a long way in improving any potential reputational hits by early detection of suspicious activities.

Man-in-the-middle attacks, Payment outliers and any other advanced persistent threats immediately – not after the damage has been done.

- **To be able to conform to regulatory and security compliance**

The system will independently log every end-to-end payment transaction and provide security status codes or response errors in real-time without compromising all necessary data and without affecting the performance or security of the payment switch.

- **Real-time optimized data collection for relaying up to Business, Transaction, Fraud Management and Governance teams**

This would ease the process of acquisition and centralization of data across different data stores, multiple schemas and various payment channels for feeding to data analytics or transaction monitoring solution of choice.

- **Inform risk rule decisions** based on multiple factors such as location identifiers, device fingerprints, IP Address, Browser details.
- **Provide Reporting capabilities -** This will be delivered on a real-time as well as at a data warehouse level while leveraging on new and existing business intelligence platforms.

Other outcome includes End to end platform, Alert triage and prioritization, Modelling and machine learning capabilities, Target an array of transaction types, Highly Available, Scalable horizontally & vertically, Intelligent middle ware, Multi tenancy, Ability for hot listing, Packaged solution ready for deployment, Dedicated support and Easily customized to meet KCB group’s unique business requirements.

1.2 Important Notes to Suppliers

a) The purpose of this document is to assist KCB Group Plc in the identification and evaluation of potential service providers who may subsequently be shortlisted.

b) **ALL Correspondences relating to this RFP MUST be through the KCB SUPPLIER PORTAL accessible on the www.kcbgroup.com website.**

c) Prospective Service Providers must have experience of offering similar solution to firms listed in the stock exchange/financial institutions comparable to The Bank and complexity and must demonstrate the willingness and commitment to meet the criteria as per the questionnaire provided.

d) To simplify this process, you need to provide copies (through the portal) of all supporting documents requested.

e) You may also be asked to clarify your answers or provide more details. Please answer every question. If the question does not apply to you, please write N/A; if you don't know the answer, please write N/A.

f) Failure to complete this questionnaire and/or provide written answers to any further questions or requests for additional information or requests for clarification will result in the supplier's elimination from further consideration.

g) Please note that by responding to this questionnaire you accept that all answers provided in this questionnaire are legally binding on the supplier and should the need arise, may be used as evidence in any court of law, which has jurisdiction. Further, KCB Bank Kenya Limited reserves the right without further recourse to verify at its own cost the accuracy of any answers provided herein.

h) All expenses and costs incurred by a respondent in connection with this RFP for preparation and lodging for submission (without limitation) shall be the sole responsibility of the respondent.

i) Without limiting its right at law or otherwise KCB Bank Kenya Limited, may at its absolute discretion, suspend or defer this RFP.

j) Where necessary and if insufficient space has been provided on the questionnaire for the answers, please provide the answers as supplements on separate sheets.

k) Canvassing the tender shall lead to automatic disqualification and subsequent elimination of the applicant.

1.2.1 KCB Bank Group Establishment

KCB Bank Group, founded in 1896, is the leading financial services provider in East and Central Africa with operations across seven countries and a customer base of over 30 million. Listed on the Nairobi Securities Exchange (NSE), the Group operates a universal banking model spanning retail, SME, corporate, and institutional banking, supported by over 400 branches, 1,000 ATMs, agency outlets, and rapidly expanding digital channels. Today, more than 95% of transactions are conducted through mobile and online platforms, underlining KCB's leadership in digital banking.

Given the scale of its customer base, transaction volumes, and digital-first agenda, KCB requires a robust

Fraud and Transaction Monitoring solution to transform data into actionable insights. This will enable the Bank to proactively detect and deter activities on a real-time basis, across multiple banking channels and to prevent operational loss exposure before transactions are committed. Thus the need for a multi-level approach to transaction exception detection and prevention that recognizes an expanded use of data both from internal and external data sources and Artificially Intelligent modelling.

The Head Office for the group is in Kencom House Nairobi, Kenya.
Further information about the bank can be obtained from the group's website (http://www.kcbgroup.com)

1.3 Format of RFP Response and Other Information for Bidders

1.3.1 The overall summary information regarding the ***Provision of an Integrated fraud and transaction monitoring solution*** is given in section 2 – Scope of Work. The bidder shall include in their offer any additional services considered necessary for the successful execution of their proposal.

1.3.2 The technical and financial response will be done through the bank's supplier portal. Please ensure your registration is active and you can respond. **Any responses outside this portal shall not be honored.**

Proposals from bidders should be submitted in two distinct parts, namely Technical Proposal and Financial Proposal.

The Technical Proposal should contain all the relevant technical details in response to the bank requirements as outlined in Section 2.

Bids that do not have this information SHALL be disqualified from further evaluation

1.3.3 The Technical Proposal should contain the following:

Bidders, willing to be considered **for Provision of & implementation of an integrated Fraud and Transaction monitoring tool** should provide company information as articulated in the Requirements section in the sourcing tool under section **1: Company Profile.**

Proposals will be evaluated based on the Supplier's distinctive plan for performing the requirements of the RFP. Therefore, the Supplier should present a written narrative, which demonstrates the method or manner in which the Supplier proposes to satisfy these requirements. The language of the narrative should be straightforward and limited to facts, solutions to problems, and plans of action.

Where the words "shall" or "must" are used, they signify a required minimum function of system capacity that will heavily impact the Bidder's final response rating.

Where the words "may" or "desired" are used, they signify that the feature or capacity is desirable but not mandatory; therefore, the specifications in question will possess minimal impact on the Bidder's final response rating.

The method by which the proposed method of performance is written will be left to the discretion of the Supplier. However, the Supplier should address each specific paragraph and subparagraph of the Specifications by paragraph and page number as an item for discussion. Immediately below these numbers, write descriptions of how, when, by whom, with what, to what degree, why, where, etc., the requirements will be satisfied.

You are required to answer all questions in the Requirements division and attach relevant information where required. Do not attach one bulk attachment as it makes it cumbersome to score your bid.

1.3.4 The Financial proposal

The Financial proposal shall clearly indicate the total cost of carrying out the solution as follows:

a. The Supplier shall provide a **firm, fixed price for the Original Contract Period**. All costs associated with the required IT System shall be included in the prices. Kindly note that the cost should include supply, installation, and commissioning of the IT System **inclusive of all freight charges and applicable duties and taxes (VAT and withholding Tax).**

Provide an itemized list of all items included and summarize your costs as shown in the table below:

No	Item Description	Qty	Unit Cost (USD)	Total cost (USD) inclusive of all applicable duties and taxes.
1	Software/Licensing Costs			
2	Implementation, installation, and configuration costs			
3	Proposed training costs (if applicable)			
4	Annual Support Costs year 2 (if applicable)			
5	Annual Support Costs year 3 (if applicable)			
6	**Partner SLA: (if applicable)**			
	Year 1			
	Year 2			
	Year 3			
	Any other costs- (if applicable) (provide details)			
	Grand total Cost (USD)			

Note: License support and maintenance can only commence after solution go-live. No support and maintenance shall be charged during project delivery. Year 1 support will kick in after the lapse of Warranty period (12 months) and Post-Go-Live free support period.

b. **Additional Cost to Complete**. Provide an itemized list of any items not included above by the Bank and related costs that the Supplier deems necessary to provide the information to meet the requirements specified in proposal. Failure to provide said list shall not relieve the Supplier from providing such items as necessary to meet all the requirements specified in proposal at the Fixed Price Purchase Costs proposed.

c. The cost should be for KCB Group. The proposed split will be shared by way of an addendum.

1.3.5 sPrice Validity

Bidders are requested to hold their proposals valid for **ninety (90) days** from the closing date for the submission. The Bank will make its best efforts to arrive at a decision within this period.

1.3.6 Commencement of Assignment

Assuming that the Contract will be satisfactorily concluded, the bidders shall be expected to commence the assignment after the final agreement is reached.

1.3.7 The Contracting Arrangements

The contracting arrangements shall clearly define the responsibilities and the services to be provided by each firm in the case of a joint venture.

1.3.8 Bid Acceptance

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

The vendor's terms and conditions will not form part of any contract with KCB in relation to this tender.

Canvassing is prohibited and will lead to automatic disqualification.

1.3.9 Cost of bidding

The Bidder shall bear all costs associated with the preparation and submission of its bid, and the Bank will in no case be responsible or liable for those costs, regardless of the conduct or outcome of the bidding process.

1.3.10 Clarification of Bidding Document

i. All correspondence related to the contract/proposal **shall be made in English.**

ii. Should there be any ambiguity, conflict, discrepancy, omission, doubt, uncertainty or other error, the Bidder shall seek clarification in writing through the sourcing portal under the messages tab.

iii. Any clarification sought by the bidder in respect of the RFP shall be addressed **at least five (5) days** before the deadline for submission of bids, in writing to the Head of Procurement through the same mail.

iv. It is the responsibility of the Bidder to obtain any further information required to complete this RFP.

v. Any clarification requests and their associated response will be circulated to all Bidders.

vi. The RFQ Clarification Template is as attached in the sourcing portal.

The queries and replies thereto shall then be circulated to all other prospective bidders (without divulging the name of the bidder raising the queries) in the form of an addendum, which shall be acknowledged in writing by the prospective bidders.

1.3.11 Amendment of Bidding Document

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

All prospective Bidders that have received the bidding documents will be notified of the amendment in writing through the Banks supplier portal, and it will be binding on them. It is therefore important that bidder registers on the KCB Supplier Portal.

To allow prospective Bidders reasonable time to take any amendments into account in preparing their bids, the Bank may at its sole discretion extend the deadline for the submission of bids based on the nature of the amendments.

1.3.12 Deadline for Submission of Bids

All Bids should be submitted through the supplier portal.

Please note:

- Soft Copies for each proposal are to be provided in PDF through the sourcing portal.
- **Any bid received by the Bank after the deadline data as specified in the supplier portal will be rejected.**

1.3.13 Responsiveness of Proposals

The responsiveness of the proposals to the requirements of this RFP will be determined. A responsive proposal is deemed to contain all documents or information specifically called for in this RFP document and in the sourcing platform. A bid determined not responsive will be rejected by the Bank and may not subsequently be made responsive by the Bidder by correction of the non-conforming item(s).

1.3.14 Cost Structure and non-escalation

The bidder shall, in their offer (Financial Proposal), detail the proposed costs. **No price escalation under this contract shall be allowed.** The Bank shall not compensate for any costs incurred in the preparation and submission of this RFP.

1.3.15 Taxes and Incidental Costs

The prices and rates in the financial offer will be deemed to be **inclusive of all applicable taxes and any other incidental costs**.

1.3.16 Currency for Pricing of Tender

All bids in response to this RFP should be expressed in **KES** or **USD**. Expressions in other currencies shall not be permitted. The portal shall calculate the currency conversion to Kenya's official currency i.e KES

1.3.17 Correction of Errors.

Bids determined to be substantially responsive will be checked by the Bank for any arithmetical errors. Errors will be corrected by the Bank as below:

- Where there is a discrepancy between the amounts in figures and in words, the amount in words will govern, and
- Where there is a discrepancy between the unit rate and the line total resulting from multiplying the unit rate by the quantity, the unit rate as quoted will govern.

The price amount stated in the Bid will be adjusted by the Bank in accordance with the above procedure for the correction of errors.

1.3.18 Evaluation and Comparison of Bids

Technical proposals will be evaluated and will form the basis for bids comparison. All tender responses will be evaluated in three phases: -

a. Preliminary evaluation that will determine administrative compliance.
b. Detailed technical evaluation to determine technical compliance and support responsiveness of the vendor (This will include presentations and reference checks)
c. financial evaluation to consider competitiveness and the financial capability of the vendors

Once the bids are opened, bid evaluation will commence. In the event that the bank may need to visit client site, vendors will be notified in writing. The bank may also make surprise unannounced visits to the vendors offices to verify any information contained in the bid document. All visits are at the discretion of the bank. Vendors may also be called upon to make brief and short presentations and/or demos on their technical solutions before a panel constituted by the bank.

Technical proposals will be evaluated based on the criteria in the online portal and summarized in **section 2 – Scope of Work below.**

Financial bids of firms whose technical proposals are found to be non-qualifying in whatever respect will not be opened.

2. SECTION 2 – SCOPE OF WORK

2.1. SPECIFIC OBJECTIVES OF THE IMPLEMENTATION

It is KCB's intent to select a vendor who will demonstrate solid experience, and capacity in the provision of & implementation of Integrated Fraud and Transaction monitoring tool that will be able to support KCB Kenya and its subsidiaries

The vendor should be able to successfully deliver the following, but not limited to the below:

- Apply machine learning and artificial intelligence enhanced capabilities that includes consolidation of historical data from both internal and external data sources for transaction analytics and reviews, reduced data inconsistencies or redundancies with automated, built in data quality tools, integrate the system seamlessly with all the business channels and related governance management applications and provide an interactive self-service environment for users.
- A solution that is scalable to handle large volume of data, adaptive to allow an array of work flows for link analysis, allow Rapid Model development and deployment, has the ability to update and refresh models and business rules as needed and has content management capabilities.
- Integrated Case Management system and forensics for investigation and reporting.
- Real-time suspicious activities monitoring
- Real time transaction risk scoring
- Independent audit of end to end transaction journey
- Provide a centralized method of acquiring payment data
- Ability to monitor any and all payment transactions, regardless of application, language, payment rail or channel.
- Ability to quickly navigate through thousands of card present and card-not-present payment transactions so that we can speed up transaction exception reviews and incident management process.
- Establish proactive action points against payment fraud and cybersecurity attacks.
- Reduction of the number of resource-intensive false positives, increase payment revenues and prevent avoidable customer friction.
- Case management and closure of payment issues within shorter SLAs.
- API Integrations and secure data movement within systems

- Optimization of the collection, storage and visualization of payment transaction data across our multi-channel banking environment.

2.2 FUNCTIONAL SPECIFICATIONS

The vendor shall implement Integrated Fraud and Transaction monitoring tool to meet the following the functional specifications:

FUNCTIONAL AREA	DESCRIPTION
Centralized Payment Data Acquisition	• Trace and record every end-to-end payment transaction, consistently and in real-time • Perform payment transaction data capture independent from payment switches and other applications • Capture payment data, using network-based data capture techniques, across every link of every end-to-end payment transaction • Capture payment data out-of-band, meaning without affecting in-path applications or payment switch speed and security • Perform data collection techniques consistently within any payment channel (e.g. ATM, POS, Mobile, Online, Cards, Real-time Payments) • Ingest other relevant sources of data, such as payment switch logs, negative country lists, BIN lists and ATM electronic journal files, to blend with transaction flow data • Perform data collection from multi-vendor ATM terminals, POS devices, and self-service checkouts, mobile and online channels applications • Automatically time stamp every payment transaction for time sequencing of incoming data • Meet PCI compliance by automatically masking or deleting sensitive and forbidden fields such as PANS and PIN blocks • Log and index every payment transaction in a centralized location for fast data retrieval and research
Transaction Decoding, Correlation and Link Analysis	• Automatically decode single- and multi-protocol transactions in real-time.

FUNCTIONAL AREA	DESCRIPTION
	• Automatically correlate in-flight transactions that traverse across multiple nodes and network links into a single, end-to-end payment journey. This means matching a user request to all the various back-end calls and services required to execute it. Using transaction profiling, graphing techniques and visualizations it is possible to show connections in your data that are strong indicators of fraudulent behavior. • Extract all application payload messages, metadata, response/request timing and network communications information for each transaction. • Extract the X-Forwarded - For HTTP header field for identifying the originating IP address of mobile and online transactions. • Ensure no contextual information (e.g. terminal ID, EMV data element, and IP address) is stripped at the terminal handler or payment switch level.
Transaction Logs, Profile Reconstruction and Fraud Attack Isolation	• Independently log all end-to-end payment transactions in real-time, without adding latency or impacting payment switch performance. • Perform complex search queries on multiple fields contained within a transaction, and quickly navigate through transaction logs. These fields include customer ID, card type, hashed PAN numbers, dollar amounts, transaction dates and times, response codes, terminal ID and ISO8583 messages etc. • Filter live transaction traffic to find transactions that meet specific criteria (e.g. customer ID, location, response time, response code, etc.) • Access full drill-down details on any individual transactions that show up in a search query. • Allow drill-down from the end-to-end transaction view into the individual links and nodes to spot attack vectors and malware. • Map the transaction to the underlying network and application components along the end-to-end journey

FUNCTIONAL AREA	DESCRIPTION
	• Present a unified view of network and application payload information inside a transaction profile for one-stop research. Highlight all TCP/IP network communications information, response/request timings, risk scores and application payload message fields contained in each transaction – in one view. • Show the technical details of how two or more components are interacting with one another (e.g. a terminal and a transaction switch, or a middleware server and a database server, etc.)

Live Dashboards, Statistics & Trends Reports	• Configure “user-friendly” web-based dashboards and trending displays for all payment channels in one place
	• Provide user-configurable dashboard options that allow for a wide range of visualization options such as pie charts etc.
	• Ability to drill-down into the underlying transactions behind the real-time dashboard graphs
	• Configure real-time dashboards that highlight:
	    o Unusual or anomalous transaction performance characteristics (e.g. missing links indicative of man-in-the-middle attacks or lack of activity during peak times)
	    o Real-time transaction statistics (e.g. completion rate, response times, etc.)
	    o Transaction rate by outcome (e.g. failures, declines, reversals)
	• Create a real-time dashboard the displays a channel topology map and in-progress payment transactions that are flowing across the network
	• Configure graphical indicators to visually highlight fraud performance indicators, thresholds and trending
	• Compile interval statistics for different fraud types
	• Create a real-time dashboard to highlight alert status and events of interest

FUNCTIONAL AREA	DESCRIPTION
	• Send periodic alerts to specific channels (configurable) to highlight alert status and events of interest
Event Monitoring and Rules-Based Alerting	• The payment monitoring and analytics system should be platform-agnostic, and have the ability to monitor any payment application environment. • Passively monitor every "in-flight" payment transaction and trace a payment transaction path through the entire enterprise infrastructure. • Monitor transaction traffic to and from external third-party applications and services (web or otherwise). • Centralize monitoring of transaction traffic across multiple data centers and multiple switch environments (e.g. active/active), including both the driving switch and the routing switch • Screen every payment transaction from a fraud perspective in near real-time • Provide user configurable performance alerts that are triggered based on data contained within individual transaction messages, such as (but not limited to): • Loss of network links, MAC or TCP errors • Lack of activity based on segments of devices, acquirer or network using BINs as a proxy • Unexpected transaction declines, EMV fallbacks, high card reversals and stand-in modes • Abnormally high or low transaction rates, failures or decline rates • Card acceptance problems due to PINs or passcodes • Transaction slowdowns • Lack of transactions or specific card rail activity during peak periods • Status and response code errors • Lack of device, issuer, host or third-party application connectivity

FUNCTIONAL AREA	DESCRIPTION
	• Slowdowns in internal switch processing times, round trip times and queue times • Provide user configurable payment alerts that are triggered based on data contained within individual transaction messages, such as: • Transaction risk score for card or customer ID exceeds threshold • Too many device fingerprint and IP geolocation changes • Cash withdrawal observed on an ISO link with no matching database transaction (man-in-the-middle attack) • Repeat card usage or customer ID by device, distance or store • Repeat account log-in attempts • Repeat terminal usage (cash-out attack) • Distance based card usage or device log-ins • High ticket purchases or rapid succession of transactions • High withdrawal velocity in a short amount of time • Unexpected EMV fallbacks, high reversals and stand-in modes • Status and response code errors • Card being used is black listed or device is being used in a country in a negative country list • Provide user configurable regulatory & compliance alerts for suspect fraud activity, hacking attempts and security incident events that are triggered based on data contained within individual transaction messages. • Send communication to a specific channel (Email, API to Mobile Apps) for users or user groups based on the problem type. • Forward alerts to other consoles via common integration mechanisms (e.g. email, syslog, APIs). • Set different alerting thresholds for different groups of objects, times of day, geographic locations. This should be configurable.

FUNCTIONAL AREA	DESCRIPTION
	• Capture and store the exact transactions that caused an alert to trigger for forensic investigations
Machine Learning, Transaction Risk Scoring & Blocking	• Use both supervised and unsupervised machine learning models to assess the validity of each transaction - pull in any message fields contained within a payment transaction (e.g. number of withdrawals, card usage velocity, number of devices used, withdrawal amounts – over 24 hours/7 days/90 days/X days(configurable)) • Build self-learning machine learning algorithms based on newer algorithms such as Isolation Forest and Gradient Boosting that are easy to configure for risk scoring and new fraud pattern detection • Automatically learn from labeled fraud cases and detect out of norm behavior patterns based on previously confirmed fraud cases. • Detect new transaction/customer behavior patterns that may have not previously been experienced. Assign different weights to extracted transaction data points to help fine tune machine learning models • Layering of real-time transaction monitoring alerts with machine learning models to immediately notice anomalous behavior as machine learning becomes more accurate over time • Continuously feed payment transaction data to machine learning and rules-based alerting risk score models and assign risk scores and advice for every transaction in milliseconds • Rebuild individual customer behavioral models for pattern recognition and transaction risk scoring in real-time (e.g. every time an event occurs) • Extract behavioral patterns from past transactions based on set rules and predisposed customer behaviors • Apply machine learning and transaction risk models to both card-present and card-not-present transactions, including ATM withdrawals,

FUNCTIONAL AREA	DESCRIPTION
	cross-channel transactions, mobile wallet and e-payments, online purchase, and in-store card payments, including contactless payments • Flag individual cards or customer ID profiles to immediately investigate and take action • Learn from the results of real-time machine learning analysis and adjust scores accordingly • Send immediate notification or trigger automated action scripts to block offending transactions at the network firewall port
Case Management and Forensics	• Configure case management workflow steps, escalation rules and checklists to automate the triage process and close out tickets faster • Configure a one-stop view into incident summary, incident details and fraud category display • Define access roles and enable multi-layer reviews and approvals • Create incident update and closure audit trails for flagged transactions with flagged payment transaction profile specifics linked directly to each task • Feed human approval/decline decisions into machine learning transaction risk scoring models as they become available
Analytics Dashboards and On-Demand Reporting	• The system will provide the option to build out payment analytics dashboards for any analytics application of choice, or any other system as prescribed by the bank • The system will make payment transaction data accessible on demand – including access to all application payload messages, metadata, network communications information and response/request times within every transaction. • The system will deliver payment transaction data in a structured, ready-to-analyze state for customized payment analytics dashboards • The system will provide offer highly scalable, cost effective data storage options

FUNCTIONAL AREA	DESCRIPTION

	• The system will apply built-in cleansing algorithms to ensure data lineage is well defined, controlled and maintained
	• The system will provide blend payment transaction data with other relevant analytics data including competitor location tables, population demographics and BIN lists
	• The system will apply industry-specific algorithms, adaptive machine learning models and predictive modelling to quickly recognize patterns, trends and predictions related to:
	    o Transaction risk scores
	    o High velocity card usage
	    o Suspicious account to account transfers and repeat login attempts
	    o Transaction status
	    o Issuer monitoring and authentication routing
	• The system will provide the option to use out-of-the-box dynamic ATM/POS/Cards dashboards designed for analyzing:
	    o Customer channel engagement
	• Card usage

System Monitoring	• Monitoring of interfaces between the transaction monitoring solution, core banking system and various banking channels. • Database performance monitoring. • Transaction throughput monitoring.
Supporting Documents	• Product Description • System Installation and integration • User Guide and Operation & Maintenance • System Integration Testing.

2.2 TECHNICAL SPECIFICATIONS

The bidder to respond to the specific technical requirements as outlined below.

NON-FUNCTIONAL REQUIREMENTS
1.The bidder should do a walkthrough to KCB team on the detailed platform architecture both physical and logical outlining the different components and functions of each. 2.Provide a Deployment architecture(Network & Infrastructure) 3.The solution should be ready for deployment either in our on-premise location, our on-premise cloud location or our private cloud location and Hybrid . This may be and not limited to either Amazon Cloud, Azure Cloud, Oracle Cloud or Google Cloud.
The bidder should do a walkthrough to KCB team on the detailed listing of required hardware and software platform, must include- all necessary modules/components, applicable licenses and the rationale for the solution to enable successful implementation of a complete solution.
The bidder must demonstrate how the solution shall supports multi-tenancy architecture, however in other bank's subsidiary the solution might be deployed as independent instances. In the event, a company want to secede from the multi-tenant deployed solution, the secession and data migration should be seamless. Similarly adding a new subsidiary should also be seamless.
The solution should be able to provide the performance in the RFP and provide a growth plan to reach the set performance levels and supported projected growth.: Data ingestion throughput: 1,000,000 records per minute Data transformation and enrichment speed: 1 minute per 1 million records Data duplication identification and resolution rate: 100% Batch processing time: < 1 hour for overnight batch jobs
The bidder must demonstrate the capability of the solution to scale the solution vertically and horizontally with an ability to scale up with no change of design.
The solution provided by the bidder should be hardware and operating system independent. It should run on any hardware either physical or virtualized. The bidder should provide quotations for both types of environments
The bidder should demonstrate how the system will handle security within the solution as well as integration touch points to interfacing systems (Security architecture). o Security of data in transit and at rest o End to end encryption capabilities - algorithms supported o Demonstrate API security. o Support for multifactor authentication o Two factor/step authentications o Network security based on request source or target. o Role based and hierarchical access controls. o User profile management
The bidder must demonstrate how the solution supports the following logging and audit trail features: o Ability to record audit trails that meet standard threshold o Ability to generate tamper proof logs and store files, database, publish to a logging service, rotating logs

NON-FUNCTIONAL REQUIREMENTS
o Ability to generate audit trail reports o Ability to manage log levels
The solution should provide adequate backup and archival of application and data.
The bidder should demonstrate the solutions data extraction capabilities, tools and technology used to extract data from our many data sources into their solutions data pool given the large volumes of data.
The bidder must showcase to KCB team how the solution supports standard interfaces which include but not limited to: o HTTPS, SOAP, REST, XML/HTTPS o Standard APIs to be hosted and exposed to partners through KCB security infrastructure o Integration to other platforms both internal and external to the bank. o Ability to support two-way SSL
The bidder should showcase how the Solution supports provision of adequate Error Handling and Logging capabilities.
The bidder shall do a walkthrough to the KCB team on the solution specifications to be provisioned by the bank and will be responsible for their setup: o Development environment o System Integration Test (SIT) environment o User Acceptance Testing (UAT) environment. o Production environment
The bidder shall highlight the supported licensing models for the solution including charges applicable for each model (inhouse/private cloud) in the financial proposal
The bidder should showcase the below capabilities of the solution 1 Monitoring tools for the solution 2 Ability to integrate with existing monitoring tools within the bank. 3 Solution service performance monitoring 4 GUI to display monitoring dashboards / reports
The solution demonstrate the capability of the solution to integrate with both internal and external systems which include but not limited to (there will be a single integrations layer through a micro-services architecture): o Card Management Systems o Multiple Core Banking Systems (T24 etc) o Multiple Mobile Banking/Money systems o Email gateway o SMS gateways o API Gateway o Master Data Management (MDM) and Data warehouse o Others

NON-FUNCTIONAL REQUIREMENTS
Configurability: The bidder demonstrate the ability of the solution to provide a mechanism by which new services and functionality can be introduced by way of configuration by bank resources and not development.
The bidder should provide the following information: 1 Support structure & models (Onsite, Offsite, Hybrid) 2 Escalation matrix 3 Service Level Agreement (SLA) template 4 Where onsite support is provided, the bidder should avail competent resources to support the system.
The bidder should provide details of the version upgrades required and frequency of the same so as to ensure that such version upgrade is in line with bidder's support model. The bidder shall provide different patches required to be implemented from time to time. Sufficient notice should be provided to the bank before such patches are deployed.
Documentation: The bidders should demonstrate how they maintain upto date business and technical documentation for all development and changes done on the solution over time.
High Availability : The bidder must demonstrate the capability of the system to support both intra-site high availability as well as high availability across multiple sites.
Failover/Business Continuity: The bidder must showcase the ability of the solution to failover the system to disaster recovery (DR) site within agreed Recovery Time Objective (RTO) of 10 minutes. The bidder should demonstrate seamless failover to internal and external partners. Partners do not have to change anything on their end to access failed over application.
Training and Knowledge Transfer: The partner is expected showcase how the will provide requisite hands on training to enable the KCB team configure, manage and monitor the CVM solution post implementation and support (business, admin, technical etc.), including location and time commitment. At a minimum, the below are expected to be clearly covered in the training plan; 1) the training program 2) the training scope 3) training approach

PROJECT MANAGEMENT

The bidder to respond to the specific requirements as outlined below.

AREA	DESCRIPTION
VENDOR EXPERIENCE & REFERENCE SITES – FRAUD & TRANSACTION MONITORING SOLUTION IMPLEMENTATION	• The bidder to provide details of experience in similar implementations in large organizations/banking/ financial institutions **(at least three references)** within the last three years, indicating the solutions/s implemented, scope, modules and the status of the implementation. • Indicate the organization, duration of the project and the number of customers supported by the solution implemented. Cite the challenges experienced, outcomes and key considerations made. Additionally, provide contact details for each reference site. • The bidder **MUST** indicate the site, duration of the project • The bidder **MUST** provide the lessons learnt from each site.
RESOURCE MATRIX	• The bidder should demonstrate the project team's capability by indicating the number and times similar projects were undertaken by individual members of the project team and the roles undertaken. • Provide a resource matrix highlighting critical roles which include but not limited to: Business Analyst, Architect, Project Manager, Developer, DBA, Data Engineer, Migration and Testing Expert, Infrastructure and Configuration Management expert, etc.
PROJECT PLAN	• The bidder should have a team that is capable of delivering the solution within stipulated time schedules (within 6 months from date of award). • The bidder shall provide a detailed project plan with a clear breakdown of phases or work streams with clear milestones. The project plan should clearly indicate expected deliverables, resources required, milestones, outcomes and time schedules. • Demonstrate ability in delivering the Integrated Fraud and Transaction Monitoring solution in both Agile and hybrid (Phased Approach) methodology, demonstrate application of each methodology in the implementation process.
RESOURCE DEPLOYMENT PLAN	• The bidder must outline your resource deployment plan including onsite/offsite working arrangements, considerations made and measures in place to ensure project is not impacted. • KCB prefers an onsite implementation team during the project the

AREA	DESCRIPTION
	analysis, low-level design, implementation, testing and Go-live
TRAINING & **POST IMPLEMENTATION SUPPORT**	• The bidder MUST provide requisite training for the Integrated Fraud and Transaction monitoring tool to enable the KCB team to support & operate the system post implementation without reliance on the vendor. • The bidder MUST provide a training plan for both technical and non-technical training, including the methodology and approach. • The bidder **MUST** include post implementation support & structure (on warranty basis) for ALL the ecosystem components capturing key service offerings.
DEPENDENCIES AND PRE-REQUISITES	The bidder **MUST** clearly indicate any dependencies and pre-requisites necessary for successful project implementation and the rationale thereof.

QUALITY ASSURANCE & TESTING	▪ The bidder **MUST** provide the Test Strategy, the Test plan & approach, indicate the tools and instrumentation for conducting and managing QA & testing, and resources required.
	▪ The following tests MUST be conducted at the QA & Testing phases of the project:
	    • **Unit testing** of the solution components and modules. Each unit (basic component) of the software is tested to verify that the detailed design for the unit has been correctly implemented. The bidder shall fully own, conduct and manage unit testing on Integrated Fraud and Transaction monitoring solution.
	    • System Integration Testing (SIT) for all Integrated Fraud and Transaction monitoring toolfunctionalities
	    • Load and Performance testing for Integrated Fraud and Transaction monitoring tooland integrated components.
	    • User Acceptance testing (UAT) is to be conducted by the end-users of the data and techno-functional analysts to validate whether to accept the project deliverables. The bidder shall manage the UAT Tests, defect triaging and defect resolution for all UAT phases.
	    • Security Testing – The bidder will be required to conduct first level security testing. The bidder shall work closely with the bank resources to carry out and sort out all security related issues. The bidder will be responsible for the resolution of all issues raised on the Integrated fraud and transaction monitoring solution. 2nd level and 3rd level security testing including Vulnerability and Penetration testing shall be conducted by the bank and other

AREA	DESCRIPTION
	third-party vendors. The bidder will be required to work with the bank and the third-party vendors to resolve all security issues that shall have been raised.
CHANGE MANAGEMENT	• The bidder MUST provide the change Management approach and methodology.
LICENSING	• The bidder shall provide the licensing models supported including charges for each model. • The bidder shall provide the hosting options supported – whether on-premise or off-premise (Private cloud preferred).

2.3 DELIVERY ACCEPTANCE (ON SUCCESSFUL BIDDING)

The product will deem to have been:

a) Delivered when

i. Respective Reports based on different aspects of the Integrated fraud and transaction monitoring solution. Implementation assessment based on tender awarded both on soft and hard copy will have been received at KCB's primary location (IT Division, 7th floor Kencom House, Nairobi); and discussed with management and inclusion of management comments and feedback.

b) Acceptance

ii. Acceptance Criteria: The Bank will accept the proposed deliverable after they deliverables by the vendor have been delivered to the clear understanding and satisfaction of the Integrated Fraud and Transaction monitoring solution project Team that will later carry out the project aimed at resolving the main issues that will have been raised.

Delivery and performance of the Services shall be made by the successful Bidder in accordance with the time schedule as per Proposal and subsequent Agreement.

Below Acceptance Criteria that will be used:

ACCEPTANCE CRITERIA

The vendor shall comply with the acceptance criteria proposed below.

Definition of Sever

Severity	Description of Business Impact
1 – Critical	▪ A total unplanned system outage which affects multiple users, performing critical functionality where there is no workaround
2 – Major	▪ Impairment of critical system functions. No workaround exists, or workaround is cumbersome and causes an impact on productivity ▪ Some requirements in scope not met
3 – Medium	▪ Impairment of less critical system functions. Useable in Production with some procedural workarounds

Severity	Description of Business Impact
	▪ The function(s) will not perform as expected and the business impact is moderate
4 – Low	▪ Inconvenience, annoyance or cosmetic

Acceptance Criteria

Severity	Acceptance Threshold (Number of outstanding Issues)
1 – Critical	0 (zero)
2 – Major	0 (zero)
3 – Medium and 4 – Low	15 ()

2.4 DOCUMENTATION AND REQUIREMENTS

All documentation and training materials (in PDF format) must be available in order to complete the process, business, technical/system, operations, and support acceptance activities.

Supplier's suggestions for documentation and training materials to support the implementation, use and maintenance of the Solution and any supporting technology components that will be provided as part of this project are to be included in the Supplier's proposal. Documentation must be in English.

2.5 TRAINING

It is expected that formal training will be given to all stakeholders of the solution. However, the solution must be intuitive and help text must be available and presented in a manner that encourages users to try to find information. Training of technical support team will be to such an extent that they will be reasonably able to handle their duties competently. Where appropriate, the supplier will be expected to discuss the technical aspects of the system to enable, for example, creation of ad-hoc reports and integration to other systems

Training will be provided in English language at the banks. If additional expenses will be incurred for offsite training, this will be borne by the supplier and must be included in the financial proposal.

2.6 TESTING AND ACCEPTANCE

The bank will test the proposed system in a test environment to ascertain that all the functionalities as put forward by the supplier are met. Incorrect information discovered at this time will constitute grounds for disqualification. It is the responsibility of the supplier to ensure the requirements defined in the proposal are achieved.

The proposal will be the sole reference document for any discussion issues arising, related to acceptance.

Acceptance Criteria: The Bank will accept the proposed deliverable after they have been fully tested by the bank and confirmed to meet the requirements as specified in the original RFP and signed RFP response.

2.7 PROOF OF COCEPT (PoC)

The bank may require proof of concept of the proposed solution as evidence that it is viable and capable of achieving requirements. All costs related to the Proof of Concept will be borne by the bidder. Prior to PoC, bidders are required to sign Non-Disclosure Agreement (NDA) and Data Protection Agreement (DPA).

2.8 DELIVERY

Delivery and performance of the Services shall be made by the successful Bidder in accordance with the time schedule as per Proposal and subsequent Agreement.

2.9 DELAYS CAUSED BY THE SUPPLIER

If at any time during the performance of the Contract, the Bidder should encounter conditions impeding timely delivery and performance of the Services, the Bidder shall promptly notify the Bank in writing of the fact of the delay, its likely duration and its cause(s). As soon as practicable after receipt of the Bidder's notice, the Bank shall evaluate the situation and may at its discretion extend the Bidder'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.

During the time of delay occasioned by Supplier KCB may require the vendor to take alternative action and meet all the costs associated with ensuring the bank remains protected to the level that would otherwise be provided by the proposed and duly accepted Product.

2.10 WARRANTY

The successful bidder shall provide at **least 12 months** Warranty for the software and ensure it is free from any sort of defects and shall perform as per expectations. The successful bidder shall provide an option for on-going warranty support beyond the warranty period. Failure to this the supplier will pay damages to the tune of the cost of the solution.

2.11 REPRESENTATION

The Supplier represents and warrants that it is entitled to respond to this RFP and that it is fully entitled to the proposed Product by way of reseller licensing or ownership and has the right to sell and/or license the Product as provided in their RFP response and shall hold KCB harmless from action for infringement of patents and/or copyrights.

2.12 SUPPORT REQUIREMENTS

The Supplier should provide and sign an Annual Maintenance Contract and provide support for the solution for the first year at no cost.

The Supplier should provide updates, upgrades toll-free technical assistance 24/7/365.

The Supplier should provide a summary of the resources (support personnel and otherwise) devoted specifically to technical issues, involving notification technology, as well as support procedures.

The technical support resource(s) should ideally be physically located / based in Kenya

The Supplier should offer various modes of communication channels for support and be available preferably 24/7/365. The methods of support include:

i. Online chat

ii. Phone and

iii. E-mail

The Supplier support website should offer the following various support specific tools:

i. Video tutorials

ii. Online user manual

iii. Archive data search

iv. FAQs

2.13 OVERALL RESPONSIBILITY

- The Bidder is obliged to work closely with the Bank's staff, act within its own authority, and abide by directives issued by the Bank that are consistent with the terms of the Contract.

- The Bidder will abide by the job safety measures and will indemnify the Bank from all demands or responsibilities arising from accidents or loss of life, the cause of which is the Bidder's negligence. The Bidder will pay all indemnities arising from such incidents and will not hold the Bank responsible or obligated.

- The Bidder is responsible for managing the activities of its personnel, or subcontracted personnel, and will hold itself responsible for any misdemeanors.

- The Bidder shall appoint an experienced counterpart / resources to handle this requirement for the duration of the Contract. The Bank may also demand a replacement of the manager/resource if it is not satisfied with their work or for any other reason.

- The Bidder shall take the lead role and be jointly responsible with the Bank for producing a finalized project plan and schedule, including identification of all major milestones and specific resources that the Bank is required to provide.

- The Bidder will not disclose the Bank's information it has access to, during the Consultancy, to any other third parties without the prior written authorization of the Bank. This clause shall survive the expiry or earlier termination of the contract

2.14 PRICING

All costs will be filled in through the sourcing portal. **The bidder is also required to attach their breakdown supporting the costs filled out in the porta**l. <u>The attachment is mandatory as the bank will use this to verify that all costs have been included.</u>

Costs (USD or KES inclusive of all applicable taxes where necessary) and Man/Day estimates, where applicable. The costs for foreign firms should be inclusive of withholding taxes. Where the awarded bidder is foreign, **the bank shall <u>deduct applicable withholding tax and provide a tax certificate</u> for onward claiming in bidder's resident country**.

All costs provided should address the following and Man/Day estimates, where appropriate, broken down by:

2.14.1 Professional fee will be broken down per subsidiary as listed in the portal. The bidder is required to provide a breakdown in their financial proposal attachment clearly indicating the various resource types, the man days rate and applicable man day per each resource. This format should follow for each subsidiary instance implementation. The implementation fees MUST include all activities that will be undertaken during the entire project up until go live, e.g migration services, testing services, development and build services etc.

as per scope given in section 2 of this document. You will be required to put indicative number of months and rate per months per each instance implementation in the portal.

2.14.2 Expenses will be broken down per subsidiary just as that of implementation fees. You will be required to put number of resources and cost per resource in the portal. The bidder will also need to provide details in their financial proposal document in terms of number of flight tickets, number of accommodation nights, rate of per diem, number of visa applications and details of local transportation. Any other expenses must be clearly tabulated in the bidder's financial proposal and built in the cost per resource.

2.14.3 Post go live support for 3 months. In your financial proposal, please detail the number and the roles of the proposed resources for post go live support and the model of delivery.

The use of Kenya shilling currency is highly recommended. If using any other currency apart from Kes i.e. USD the portal will recalculate your cost using pre-determined currency conversion rates. The quoted prices should be valid for a minimum of 90 days.

The bank <u>does NOT make ANY advance payments</u> and only pays against signed off project deliverables e.g. requirements gathering, UAT etc. as such, you will be required to provide your payment milestone taking note of the above.

2.15 BID EFFECTIVENESS

It is a condition of the bank that the vendor guarantees the sufficiency, and effectiveness of the solution proposed to meet the bank requirements as outlined in this document. The Bank will hold the vendor solely responsible for the accuracy and completeness of information supplied in response to this tender. The bank will hold the vendor responsible for the completeness of the solution proposed and that were the vendor to be awarded the tender, they would implement the solution without any additional requirements from the bank

2.16 PAYMENT TERMS

The bank will **NOT** make any payments in advance and will pay based on deliverables. The Bank will issue an LPO for all the equipment and/or services ordered. The LPO will be paid **within 45 days after delivery**, testing installation and acceptance of the equipment and/or services supplied.

The bank will not accept partial deliveries, and neither will the bank make partial payments unless agreed by both parties. Payment for equipment and/or services will only be made once the entire ordered equipment and/or services are delivered, installed, or commissioned.

2.17 STAFFING

The Supplier will provide the relevant staff and tools to carry out all the required work under this tender. The vendor needs to have certified consultants for all technical areas and all functional areas. The vendor will need to list how many certified consultants they have available in each technical and functional area.

2.18 RESPONSIBILITIES AS AN INDEPENDENT CONTRACTOR

The Supplier agrees to take overall responsibility for any services rendered; regardless of whether third parties engaged by the Supplier or the Supplier himself carry them out.

SECTION 3 - GENERAL CONDITIONS OF CONTRACT

3.1 Introduction

Specific terms of contract shall be discussed with the bidder whose proposal will be accepted by the Bank. The resulting contract shall include but not be limited to the general terms of contract as per the **draft Master Service Agreement template attached in the sourcing portal**. The resulting contract shall include but not be limited to the general terms of contract as stated below from 3.2 to 3.13.

3.2 Award of Contract

Following the opening and evaluation of proposals, the Bank will award the Contract to the successful bidder whose bid has been determined to be substantially responsive and has been determined as the best evaluated bid. The Bank will communicate to the selected bidder its intention to finalize the draft conditions of engagement submitted earlier with his proposals.

After agreement has been reached, the successful Bidder shall be invited for signing of the Contract Agreement to be prepared by the Bank in consultation with the Bidder.

3.3 Application of General Conditions of Contract

These General Conditions as per the draft Master Service Agreement template attached in the sourcing portal shall apply to the extent that they are not superseded by provisions in other parts of the Contract that shall be signed.

3.4 Bid Validity Period

Bidders are requested to hold their proposals valid for ninety (90) days from the closing date for the submission.

3.5 Performance Security

3.5.1 The Bank may at its discretion require the successful bidder to furnish it with Performance Security in the amount specified in the accepted Bid.

3.5.2 The Performance Security shall be in the form of a bank guarantee issued by a commercial bank operating in Kenya and shall be in a format prescribed by the Bank. The performance guarantee shall be submitted within 10 days of notification of award.

3.5.3 The proceeds of the Performance Security shall be payable to the KCB Bank Kenya as compensation for any loss resulting from the Bidder's failure to complete its obligations under the Contract.

3.5.4 The Performance Security will be discharged by the Company not later than two months following the date of completion of the Bidder's performance obligations, and the Bank's acceptance of the final report as specified in the contract.

3.6 Delays in the Bidder's Performance

3.6.1. Delivery and performance of the Supply, installation and Maintenance of Signage shall be made by the successful Bidder in accordance with the time schedule as per Agreement.

3.6.2. If at any time during the performance of the Contract, the Bidder should encounter conditions impeding timely delivery and performance of the Services, the Bidder shall promptly notify the Bank in writing of the fact of the delay, its likely duration and its cause(s). As soon as practicable after receipt of the Bidder's notice, the Bank shall evaluate the situation and may at its discretion extend the Bidder'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.

3.6.3. Except in the case of "force majeure" as provided in Clause 3.13, a delay by the Bidder in the performance of its delivery obligations shall render the Bidder liable to the imposition of liquidated damages pursuant to Clause 3.8.

3.7 Liquidated damages for delay

The contract resulting out of this RFP shall incorporate suitable provisions for the payment of liquidated damages by the bidders in case of delays in performance of the contract.

3.8 Governing Language

The Contract shall be written in the English Language. All correspondence and other documents pertaining to the Contract which are exchanged by the parties shall also be in English.

3.9 Applicable Law

This agreement arising out of this RFP shall be governed by and construed in accordance with the laws of Kenya and the parties submit to the exclusive jurisdiction of the Kenyan Courts.

3.10 Bidder's Obligations

3.10.1. The Bidder is obliged to work closely with the Bank's staff, act within its own authority, and abide by directives issued by the Bank that are consistent with the terms of the Contract.

3.10.2. The Bidder will abide by the job safety measures and will indemnify the Bank from all demands or responsibilities arising from accidents or loss of life, the cause of which is the Bidder's negligence. The Bidder will pay all indemnities arising from such incidents and will not hold the Bank responsible or obligated.

3.10.3. The Bidder is responsible for managing the activities of its personnel, or subcontracted personnel, and will hold itself responsible for any misdemeanors.

3.10.4. The Bidder will not disclose the Bank's information it has access to, in the course of the work, to any other third parties without the prior written authorization of the Bank. This clause shall survive the expiry or earlier termination of the contract.

3.11 The Bank's Obligations

In addition to providing Bidder with such information as may be required by the bidder the Bank shall,

(a) Provide the Bidder with specific and detailed relevant information

(b) In general, provide all relevant information and access to Bank's premises.

3.12 Confidentiality

The parties undertake on behalf of themselves and their employees, agents and permitted subcontractors that they will keep confidential and will not use for their own purposes (other than fulfilling their obligations under the contemplated contract) nor without the prior written consent of the other disclose to any third party any information of a confidential nature relating to the other (including, without limitation, any trade secrets, confidential or proprietary technical information, trading and financial details and any other information of commercial value) which may become known to them under or in connection with the contemplated contract. The terms of this Clause 2.15 shall survive the expiry or earlier termination of the contract.

3.13 Force Majeure

(a) Neither Bidder nor Bank shall be liable for failure to meet contractual obligations due to Force Majeure.

(b) Force Majeure impediment is taken to mean unforeseen events, which occur after signing the contract with the successful bidder, including but not limited to strikes, blockade, war, mobilization, revolution or riots, natural disaster, acts of God, refusal of license by Authorities or other stipulations or restrictions by authorities, in so far as such an event prevents or delays the contractual party from fulfilling its obligations, without its being able to prevent or remove the impediment at reasonable cost.

(c) The party involved in a case of Force Majeure shall immediately take reasonable steps to limit consequence of such an event.

(d) The party who wishes to plead Force Majeure is under obligation to inform in writing the other party without delay of the event, of the time it began and its probable duration. The moment of cessation of the event shall also be reported in writing.

(e) The party who has pleaded a Force Majeure event is under obligation, when requested, to prove its effect on the fulfilling of the contemplated contract.

3.14 Way Forward

Once the bids are opened, bid analysis will commence and vendors may be informed when their bid has been short-listed. Shortlisted vendors will be invited to demonstrate their proposal if need be and to make arrangements for site visits. In the event that the bank may need to visit client site, vendors will be notified in writing. The bank may also make surprise unannounced visits to the vendors offices to verify any information contained in the bid document. All visits are at the discretion of the bank.

3.15 Contract Provision

The bank will not make any payments in advance. The Bank will issue a Purchase Order for all the services ordered. The Purchase Order will be paid within 45 days after as agreed upon aforesaid herein. Any payments for the maintenance services will be subject to a contract to be agreed with the vendor. The bank will not accept partial deliveries, and neither will the bank make payments.

3.16 Buyer's Rights

The Bank reserves the right to reject any or all the tender bids without giving any reasons and the Bank has no obligation to accept any offer made. The Bank also reserves the right to keep its selection and selection criteria confidential. Bids not strictly adhering to tender document conditions may not be considered by the Bank whose decision on the matter shall be final. The vendor's terms and conditions will not form part of any contract with the Bank in relation to this tender. Bids not strictly adhering to RFP conditions may not be considered by KCB whose decision on the matter shall be final.

Canvassing is prohibited and will lead to automatic disqualification.

3.17 Responsibility as an independent contractor

The vendor agrees to take overall responsibility for any services rendered; regardless of whether third parties engaged by the vendor or the vendor himself carry them out.

3.18 Delivery

The delivery timelines shall be as specified in the scope of work, the bank will not accept any partial deliveries.

3.19 Risk of Loss

The supplier covers all risks of loss and damage to any equipment for the implementation of the solution, until the equipment has been delivered to the premises of KCB. Once the equipment /solution has been installed and tested the responsibility is transferred to KCB.

SECTION 4 – ANNEXURE

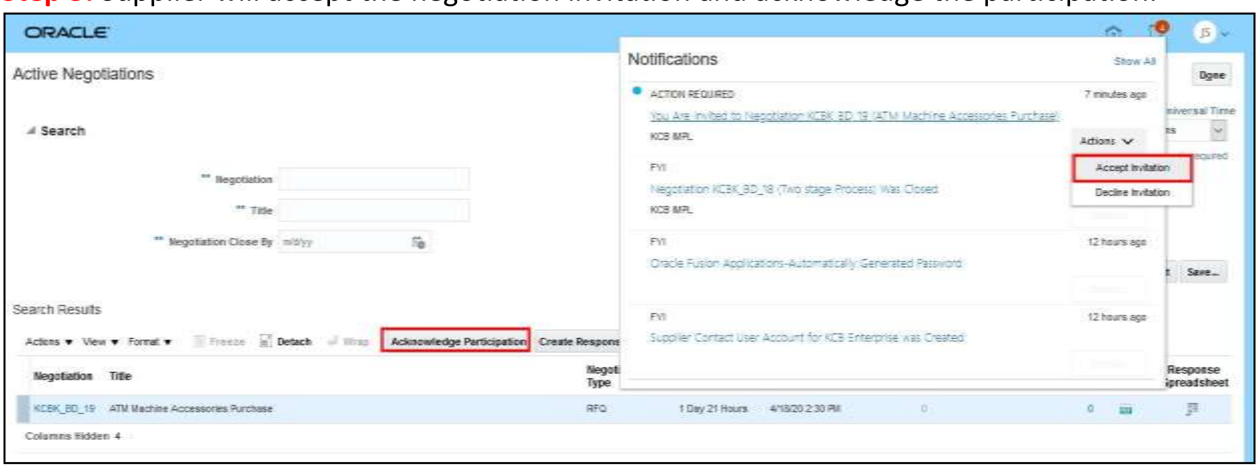
Annexure 1: Step by Step on How To Submit A Bid

Supplier Response to an invitation to submit a bid:

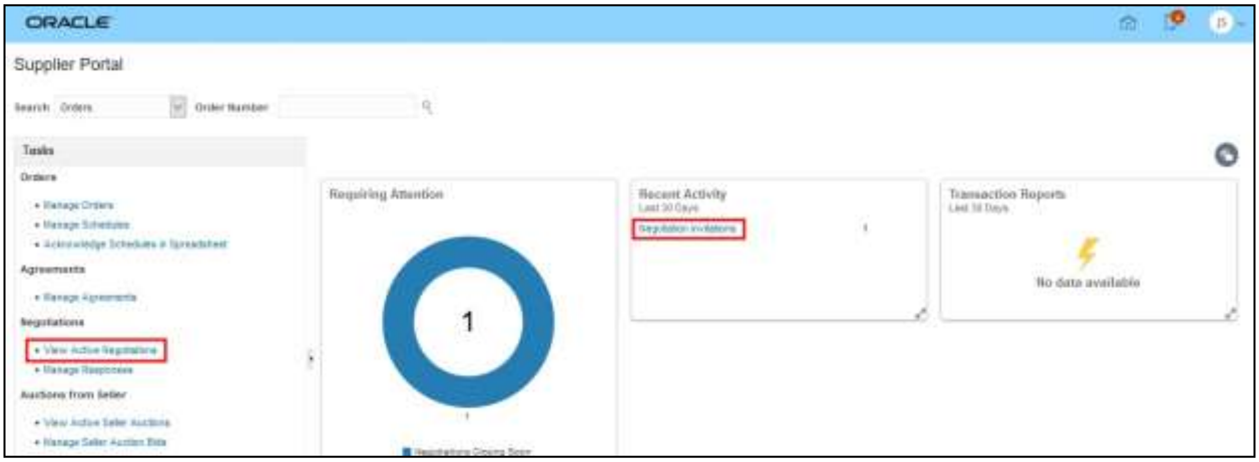
Step 1: Login into the Supplier portal using supplier user account details.

Step 2: Navigation -> Supplier Portal -> Supplier Portal.

Step 3: Supplier will accept the negotiation invitation and acknowledge the participation.



Step 4: Go to Task Pane -> Response -> View Active Response

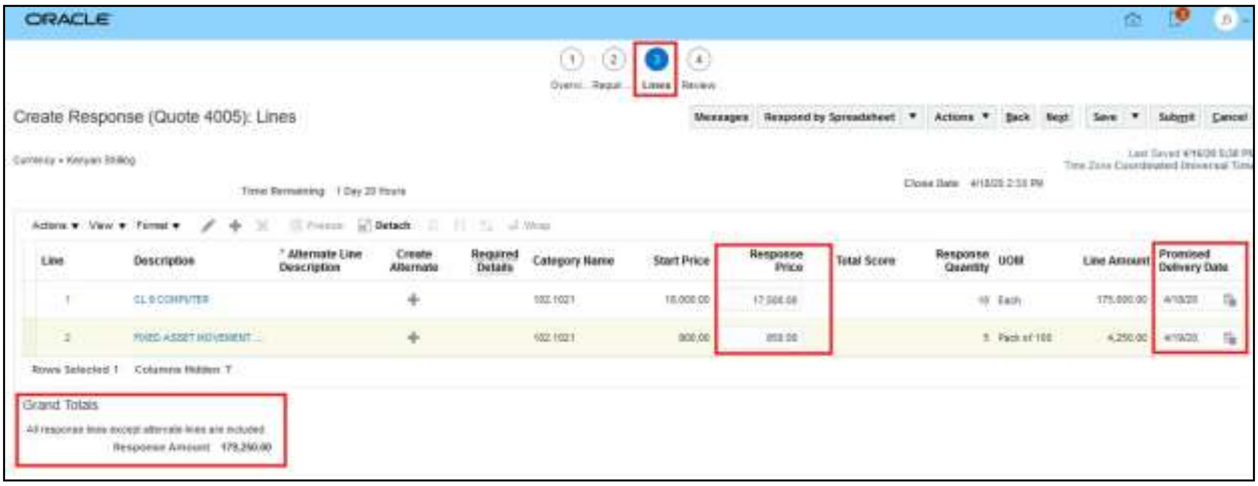


Step 5: Click on Create response button to start responding the questionnaire.

Step 6: In Overview page, select the response valid date, note to buyer information and attach supporting documents if required.

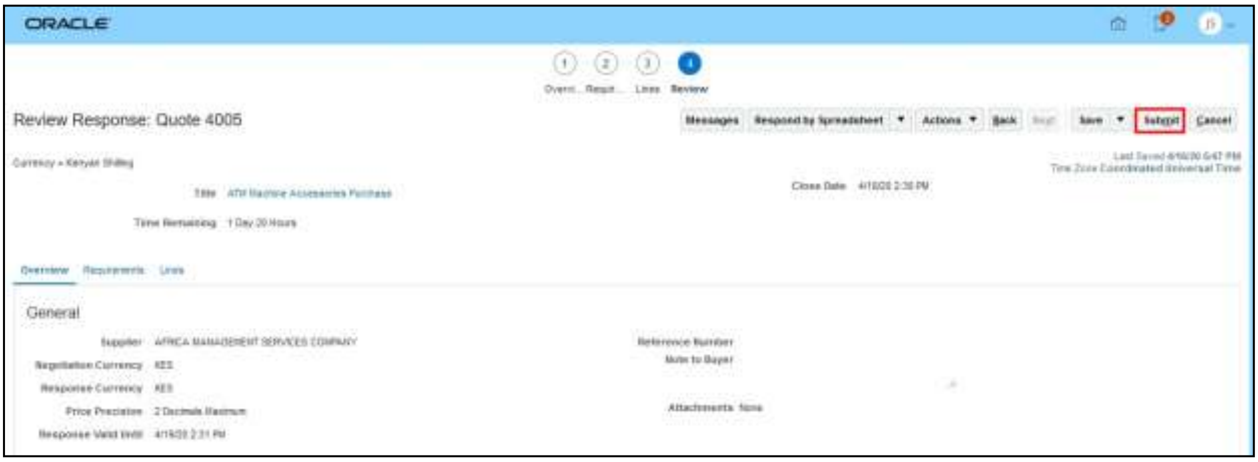
Step 7: Start responding(answering) all questions and attach the supporting documents if required in requirement page.

Step 8: Click next to move lines page to response the item price against the requirement

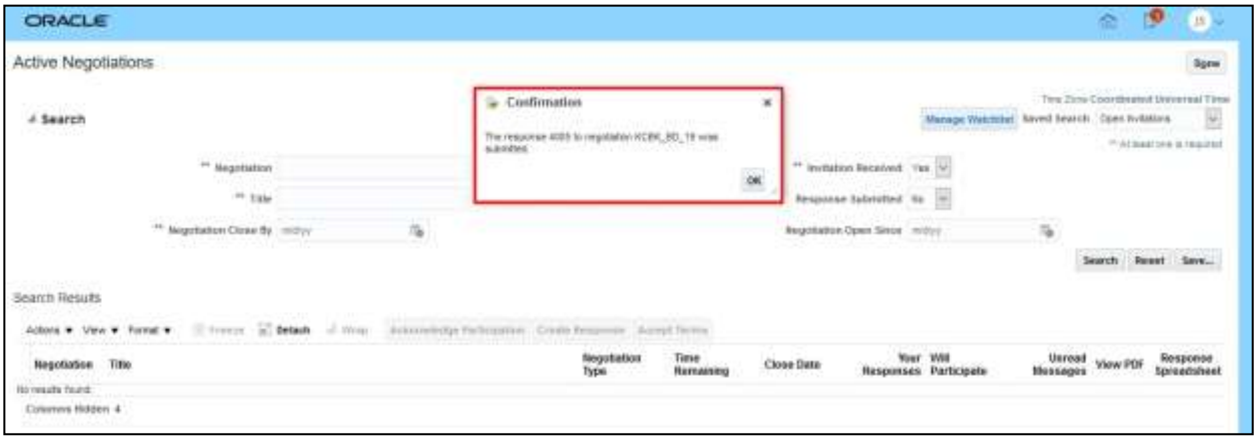


Step9: Click next to move review page to validate and review all the information before submitted the response.

Step 10: Click Submit button to submit the response.



Step 11: Same way you can capture all the supplier response.



Annexure 2: References

References of similar services

Note:

The Firms should submit the references in this format as part of the proposal.

No	Name of Firm/Company	Contract reference and brief description:	Date contract awarded/Period.	Date contract Completed / in progress	Customer contact name and phone number	Value of Contract: (KES/USD)
1						
2						
3						
4						
5						

Please note that this information should be included in the technical proposal of the bid. Incomplete / insufficient information will lead to disqualification of the bid.

Annexure 3: Company Brief Summary

Company Name	
Core Business	
Years of experience	
Physical Location of offices	
Key Contact - Include contact details	
Geographical spread	
No. of Staff	
Area of Specialization	
Names of Directors and shareholding structure	
Solution Partner Status if not owner of the solution	
List of at least four reference sites including Sites	
Company Turnover for the Last three Years	