KCB GROUP LIMITED

REQUEST FOR PROPOSAL (RFP)

SUPPLY, IMPLEMENTATION AND MAINTENANCE OF AN INTEGRATED RISK MANAGEMENT (IRMS) SOLUTION

Release Date: **13th June 2025**

Last Date for Receipt of bids: **27th June 2025**

Table of Contents

DEFINITIONS

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

The Bank KCB Ltd

Bid The Quotation 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, implementation, 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.

SECTION 1 – REQUEST FOR PROPOSALS

1.1 Background

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

The Group's vision is to be the preferred financial solutions provider in Africa with global reach. The Group has 10 subsidiary companies across the East African Region in KCB Kenya, Uganda, Rwanda, Tanzania, Burundi, and South Sudan, Democratic Republic of Congo.

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 the Group.

The delivery of Enterprise Risk Management within KCB Group is currently managed via a disparate set of systems, with each system providing capabilities around the management of one or several principal risks. The Bank is seeking to implement a robust, integrated risk & compliance management system that shall unify the management of risks across the Group (i.e. consistent, comprehensive, and holistic risk and compliance reporting and decision- making). The solution should provide a cohesive approach enabling stakeholders to effectively coordinate and unify governance, risk, compliance and controls management activities across all business functions, while aligning assurance programs, and gaining comprehensive visibility into both risk exposures and relationships.

This document constitutes the formal Request for Proposals (RFP) for ***Supply, implementation and Maintenance of an Integrated Risk Management (IRMS) Solution*** and is being availed on open tender basis and is open for bids from companies that meet the requirements stated herein.

1.2 Important Notes to Suppliers

a) The purpose of this document is to assist KCB Bank Kenya Limited 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 services to firms listed in the stock exchange/financial institutions comparable to KCB and complexity and must demonstrate willingness and commitment to meet the criteria as per the questionnaire below.

d) In order to simplify this process, you need to provide **certified copies** of all supporting documents requested under the questionnaire, for example, audited accounts, registration and compliance certificates, statements and policies among others listed.

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 to 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 for the tender shall lead to automatic disqualification and subsequent elimination of the applicant

1.3 Overview, Aims and Objectives

The objective of this RFP is to enable the Bank to acquire a fully integrated risk management solution to gain more holistic view of risk across the enterprise and support a risk-aware culture that improves decision making and performance.

The expected outcomes are enumerated here below:

1. Holistically manage risk across the organization, integrate risk management capabilities like assessments, support best practice analytics, and enhance risk communication with dashboards and reports.

2. Provide complete visibility over critical processes, anticipate and prioritize resilience, centralize resilience data across business units, and be designed to support relevant regulations and standards with the vendor expertise in required processes.
3. Automation capability for the Compliance function in the Bank, including but not limited to documentation and monitoring of the Bank’s compliance universe, managing compliance workflows, monitoring and tracking regulatory issues and gaps, enable compliance assessments and provide relevant analytics and provide customizable MIS on compliance, and ensure sensitive information security through role-based access.
4. Functionality to include management of non-traditional risk management areas including Ethics, Policy Management and Strategic Risk Management.

5. Automate integrated risk management process – from risk identification, assessment and evaluation, mitigation, monitoring, and reporting.
6. Unify the risk management tools, activities and connect all business functions and consolidate all risk-related information in one, and easily accessible place.
7. Integrate with other AML & screening solutions to provide MIS reporting capability without compromising confidentiality
8. Risk quantification - score the identified risks by severity, likelihood, Control Ratings, velocity, and duration. This will facilitate prioritization of risks, focus mitigation efforts and tracking of the Bank’s risk profile.
9. Provide automated input, consolidation and management of risk data.

Build and embed robust risk frameworks/standards such as the Committee of Sponsoring Organizations (COSO) and Basel III/IV and disseminate best practices to meet risk management requirements. Demonstrate alignment to Basel Committee guidance on Compliance and the Compliance function in Banks.

10. Creation and maintenance of a standardized risk and control taxonomy and library.
11. Consolidate manual (word, spreadsheet) from financial risk and in future ingest into a financial system
12. Schedule Work Programs triggered by risk status, time, or schedule.
13. Track and inform stakeholders of the enterprise’s risk & compliance response
14. Generate notification [emails / SMS] to different user groups based on defined rules within the system.
15. Deliver engaging and meaningful risk analytics, reports, and dashboards.
16. The software should be cloud-based for universal access, provide device-agnostic iOS and Android apps with online and offline data capture, and integrate offline data when reconnected to the internet.

1.2.1 KCB Bank Establishment

This section provides a brief overview of KCB establishment that is relevant to the proposed solution.

The Group has the following establishments:

Kenya

1. KCB Bank Kenya

East Africa

2. KCB Burundi
3. BPR Bank Rwanda Plc
4. KCB Tanzania
5. KCB Uganda
6. KCB South Sudan
7. KCB Bancassurance Intermediary Ltd.
8. KCB Capital
9. KCB Foundation

The Head Office for the Group is located at Kencom house Nairobi, Kenya.

Further information about the Bank can be obtained from the Group's website - https://www.kcbgroup.com

The Group hereby solicits proposals from eligible and competent companies for the implementation of an Integrated Risk Management Solution.

1.4 Format of RFP Response and Other Information for Bidders

1.3.1. The overall technical summary information regarding this tender is given in section 2 - Scope of Work and supplier portal. The bidder shall include in their offer, any additional services considered necessary for the successful implementation of their proposal.

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 2.2

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

1.3.2. The Technical Proposal should contain the following:

Bidders, willing to be considered for ***this RFP*** are expected to furnish the Bank with among others the following vital information, which will be treated in strict confidence by the Bank. All these will be filled in the KCB SUPPLIER portal:

- Preliminary Work plan or project plan with a clear breakdown of phases or work streams.
- Demonstrate capability and capacity to provide the functional requirements as per requirements.
- Supplier shall provide a minimum of Five (5) reference sites for the System(s) where they have been implemented successfully
- KCB IT Risk & Security requirements
- System Implementation & Technical Support Enquiry
- Provide a company profile.
- Approval licenses, by the various bodies for compliance, MUST be included where applicable.
- Audited financial statements of the company submitting the RFP bid, for the last two years.
- Any other requirement as specified in the portal

1.3.3. **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).

i. Bidder **MUST** provide an itemized list of all items included and summarize your costs as shown in the table below:

SUMMARY TOTAL COSTS			Year 1 Annual Cost		Year 2 Annual Cost		Year 3 Annual Cost	
	DESCRIPTION	**Qty**	**Unit Cost (USD)**	**Total (USD)**	**Unit Cost (USD)**	**Total (USD)**	**Unit Cost (USD)**	**Total (USD)**
	Software costs							
1	**License costs** Please provide your license costs based on the scope required. Give a detailed breakdown of your workings, including the sizing used. **Note:** 1. License support and maintenance can only commence after solution go-live. No support and maintenance shall be charged during project delivery. 2. Please indicate any third-party license requirements if any	200						
2	Implementation/Integration costs (Please provide breakdown in the next tab and attach your detailed project plan). **Note:** 1. If you are working with a partner, you should manage your relationship with the partner since you are accountable for the delivery							
3	Training costs. **The training can be remote or onsite and instructor based**. NB. Indicate if its onsite or Remote *Remote Training has no cost implication -*							
4	Annual Support Costs - **Note; License support and maintenance can only commence after solution**							

SUMMARY TOTAL COSTS			Year 1 Annual Cost		Year 2 Annual Cost		Year 3 Annual Cost	
	DESCRIPTION	**Qty**	**Unit Cost (USD)**	**Total (USD)**	**Unit Cost (USD)**	**Total (USD)**	**Unit Cost (USD)**	**Total (USD)**
	go-live. No support and maintenance shall be charged during project delivery. The support cost will be applicable from year 2, after a 1-year Warranty (Post-Go-Live free support period) Separate License support cost will only be applicable for perpetual license model. For subscription license model, the support should be part of the license subscription package							
5	Any other costs (please provide details) **Project Implementation** Estimate and breakdown on Accommodation, Flights and Incidental Costs							
	GRAND TOTAL (USD)							

Notes:

Bidder to include the license fee/costs and support that will be applicable for any additional licenses to be added within the contract period.

ii. Provide an itemized pricing for all software related aspects and include any applicable 3rd party software costs as per the format below:

			3RD PARTY SOFTWARE LICENCE AND SUPPORT	
				3 years Fees (USD)
	DESCRIPTION	**Uo M**	**Qty**	**Unit rate (USD)**	**Total cost (USD)**
1	Describe the software licensing model used: perpetual/ subscription				
2	Software Support. Support Costs (i.e. 24/7/365 maintenance/support)				
	Total Costs (USD) - Incl of all taxes				

iii. Provide a breakdown of implementation and integration costs envisioned to deliver a complete solution as per the format below:

BREAKDOWN OF PROFFESIONAL SERVICES FEES					
Activity	**Resource type**	**No. of Resources**	**Rate per man day (USD)**	**Total number of days**	**Total cost (USD)**

iv. Provide a breakdown of training as per the format below:

Training Fees - (accredited certified instructor led training for administrators)					
TRAINING	**Scope**	**Class Size**	**Rate per day (USD)**	**Duration of Training in days**	**Total Cost (USD)**
Total cost (USD) Inc of all taxes					

Note: Include the scope of training and qualification of the trainer

v. Provide a breakdown of training as per the format below:

			1 years Fees (USD)		3 years Fees (USD)	
No	DESCRIPTION	Qty	Unit rate (USD)	Total Fees (USD)	Unit rate (USD)	Total Fees (USD)
1	Hardware Costs. For On-premises deployment option, Bidder to provide hardware sizing and software specifications (including specific sizing including the no. of CPUs, amount of memory, and storage type and capacity for the size of environment that will support the deployment of the proposed solution, and include cost estimates for the same					
2	Hosting costs. For cloud option, bidder to confirm the cloud consumption model and the annual hosting estimated costs					

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 the proposal. Failure to provide said list shall not relieve the Supplier from providing such items as necessary to meeting all of the requirements specified in the proposal at the Fixed Price Purchase Costs proposed.

1.3.4. 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.

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

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

1.3.7. 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.

1.3.8. **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.

1.3.9. **Clarification of Bidding Document**

All correspondence related to the contract shall be made in English. Bidders should submit the request for clarification via the message section of the KCB Supplier's portal on or before **19th June 2025 at 3pm EAT**. Any clarification sought by the bidder in respect of the project shall be addressed at least four (4) days calendar days before the deadline for submission of bids. 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.

1.3.10. **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, and it will be binding on them. It is therefore important that bidders give the correct details in the format given on page 1 at the time of collecting/receiving the RFP document.

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.

1.3.11. Deadline for Submission of Bids

Bids should be addressed to the Head of Procurement via the KCB supplier portal which is accessible through the KCB Group Website located on the below link:
KCB Bank Tenders Bid Form - KCB Bank Kenya Ltd (kcbgroup.com)

Please note

1. Soft Copies for each proposal are to be provided in PDF or Adobe Reader.
2. Any bid received by the Bank after the deadline data as specified in the supplier portal will be rejected.

1.3.12. 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. 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).

1.3.13. Bid 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 pricing 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, The 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. The 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.

SECTION 2 – SCOPE OF WORK

2.1 Current Situation

The delivery of Enterprise Risk Management within KCB Group is currently managed via a disparate set of systems, with each system providing capabilities around the management of one or several principal risks. This contains significant gaps and exposes the Bank to several risks. Key systems in the Bank include:

Risk Area / Capability		**Solution**
1	Operational Risk Management	Currently using Risoft (an In-house developed solution) which is to be replaced by the IRMS.
2	Financial Risks (Credit, Capital, Market)	Kondor+ and other manual processes
3	Strategic Risk Management	No system
4	ICT Risk Management	Partly managed using Operational Risk System
5	Data Protection & Privacy	Automation data protection compliance on-going
6	Compliance Risk Management	Actimize, FCCM & HotScan & Risoft (an In-house developed solution) which is to be replaced by the IRMS
7	Fraud Management	Fraud Management System

2.1.1 Specific Objectives of the Implementation Include:

The objective of the RFP is to procure a tool which will help to fully integrate risk management and to enhance Bank's systems to enable management of risks in an integrated, efficient, and effective manner hence accelerate the achievement of the Group's risk management strategy and risk management maturity.

The successful bidder will be required to:

3. Supply an Integrated Risk Management System Solution (software) that meets the functional and technical requirements that are outlined in detailed technical specifications.
4. Implement the Integrated Risk Management Solution (which includes customization, development/ configuration, and testing).

5. Conduct training(s) and provide related material(s) to users.
6. Data migration & integration from the current disparate systems into the proposed application system (data will be cleaned up before it can be migrated).

A. TECHNICAL SPECIFICATION:

The bidder should provide platform architecture both physical and logical outlining the different components and functions of each. A comprehensive schematic diagram MUST be provided including details for high availability and failover.

a) System throughput

The system should be able to provide below performance levels:

7. Minimum 50 applications/ assessments per second (TPS) with growth up to 500 TPS without design change.
8. Ability to handle 8,000 staff/users with consideration of growth in future.
9. Ability to meet at most100ms response times per transaction type.
10. Ability to respond to user requests based on configurable rules such as but not limited to:
    - Number of pending requests
    - Approved request
    - Rejected request
    - Returned for review request
    - Transaction type
    - Transaction value
    - System performance
    - Unit/company workflow

The bidder should provide a growth plan to reach the set performance levels and supported projected growth.

b) Scalability

The bidder should demonstrate the ability to scale the solution vertically and horizontally with an ability to scale up from 50 TPS to 1000 TPS with no change of design. Detailed sizing for 50, 100, 150 and 200 TPS and demonstrate ability to deriving sizing from traffic projections.

The proposed solution should cover all the existing locations and should have the capability to scale up for meeting future requirements.

c) Security

The bidder should demonstrate how the system has handled security within the platform as well as integration touch points to interfacing systems (Security architecture).

11. The vendor must comply with industry standards such as ISO 27001, NIST 800-53, PCI DSS, GDPR
12. The vendor must provide details of their security governance structure, including roles, policies, and internal compliance mechanisms
13. The vendor must disclose all subcontractors handling customer data and provide assurance of their compliance with security requirements
14. The vendor must undergo independent security assessments and provide audit reports upon request
15. The vendor must encrypt sensitive data at rest and in transit using AES-256 and TLS 1.3+
16. The vendor must implement policies for secure data retention and disposal, aligned with regulatory requirements
17. The vendor must enforce RBAC and restrict system access based on least privilege principles
18. The vendor must require MFA for all privileged accounts and high-risk actions
19. The vendor must support integration with enterprise authentication systems (e.g., SAML, OAuth, OpenID Connect).
20. The vendor must integrate security into their Software Development Life Cycle (SDLC) and follow secure coding practices
21. The vendor must provide an SBOM for third-party dependencies and disclose any known vulnerabilities
22. All KCB Group source code and artifacts must reside on the approved repositories/source code and work tracking systems
23. The vendor must have a documented security incident response plan with defined roles and escalation paths
24. The vendor must maintain/facilitate 24/7 security monitoring and threat detection capabilities.
25. The vendor must provide evidence of their disaster recovery strategy, including RTO and RPO commitments
26. The vendor must retain detailed logs for forensic analysis and provide support during security incidents
27. The vendor must provide/facilitate mandatory security awareness training for employees at least annually
28. The vendor must conduct/facilitate phishing simulations and measure employee response rates

29. The vendor must perform background checks on employees handling sensitive KCB Group data
30. The vendor must have a formal program to detect and mitigate insider threats
31. The vendor must maintain/facilitate centralized log collection & automatic forwarding of defined audit logs and security events to a SIEM using common logging formats such as CLFSor CEF over syslog or other supported mechanisms for real-time threat detection
32. The vendor must remediate critical vulnerabilities within the period recommended by the KCB Group and must provide documented evidence of patching cycle and frequency
33. The vendor must share evidence of the existence of a vulnerability management program/process demonstrating SLA for remediation of the various vulnerabilities based on severity
34. The vendor must segment environments to prevent lateral movement in case of a breach
35. The vendor must support deployment of EDR (Endpoint Detection & Response), IDS/IPS, and network monitoring solutions where applicable

d) Configurability

The system should be flexible enough to support setup of new and change of existing units, branches and operational risk management tools as a configuration as opposed to development related changes. The bidder should provide a GUI based configuration tool (Configuration panel).

e) High Availability

The system should support both intra-site high availability as well as high availability across multiple sites.

f) Failover / Business Continuity

The system should support the following but not limited to:

36. Ability to failover the system to disaster recovery (DR) site within agreed Recovery Time Objective (RTO) of 10 minutes. This should conform to KCB Business Continuity Management (BCM) policy.
37. Detailed failover run book MUST be provided.
38. Ability to invoke partial fail over
39. 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

g) Archival and Backups

The system should support the following:

40. Ability to manage data lifecycle for the platform. This should be configuration based

41. Ability to support internal and external archival
42. Ability to integrate platform backups with existing Bank's backup platforms.
43. Ability to take online backups on the platform without performance degradation.
44. It should accommodate data, configuration, and files backup for recovery/restoration purposes.
45. It should be possible to fully recover/ restore the system from the backup within one hour.

h) Integration

The system should support standard interfaces which include but not limited to:

46. HTTPS, SOAP, REST, XML/HTTPS
47. Standard APIs to be hosted and exposed to partners through KCB security infrastructure
48. Integration to other platforms both internal and external to the Bank. i.e., core Banking system, customer management system, internally developed systems
49. Ability to support two-way secure socket layer (SSL).
50. Integrate data from various sources, support out-of-the-box external intelligence integration, send data to BI applications, offer a fully documented API, provide SCIM and direct file import options, and integrate with tools like Active Directory and single sign-on (SSO).

i) Transactionality

51. The system should be able to commit or rollback a transaction.
52. It should also be possible to flag transactions i.e. ability to single out a transaction across multiple nodes/ components.
53. Ability to correlate transactions based on past incomplete transactions from the staff.

j) Error Handling Framework

54. Error handling capabilities:
    - Error logging
    - Audit logging
    - Monitoring
    - Ability to categorize errors based on criticality
    - Retry mechanism / auto-resolution capability
    - Alarms and alerts mechanism
    - Different notification mechanisms depending on criticality level - SMS, Email
    - Correlation. The framework should be able to generate a global request id that should be used to correlate a single request end to end

- Gphoton glue user interface (GGUI) to support configurations, resolution, and display monitoring dashboards / reports
- Should be powered by reference data

55. Error handling framework should support:
    - File system logging
    - Database logging
    - Ability to switch off file system logging - as a configuration
    - File naming convention for log files per service

k) Usability

56. IRMS Platform user interface should be usable and Conform to IT security governance policies.
57. Follow standardized templates that uphold KCB branding guidelines

l) Environments

The bidder should provide the following environments and will be responsibility for their setup:

58. Development environment
59. System Integration Test (SIT) environment
60. User Acceptance Testing (UAT) environment.
61. Production environment

m) 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). The option proposed by the vendor should be explicitly stated in the proposal and with clear costing. Hardware and third-party software requirements for on-premises hosting must be clearly provided as part of the proposal.

n) Monitoring

The bidder should provide:

62. Monitoring tools for the solution
63. Ability to integrate with existing monitoring tools within the Bank.

o) Interfaces

The system should integrate with both internal and external systems which include but not limited to:

64. Core Banking System (T24)

65. Customer Relationship Management (CRM)
66. Email
67. Data Warehouse
68. Reconciliation System such as Corona
69. Anti-money laundering (AML)
70. Forensic System (Memento),
71. SMS
72. Oracle Financials

p) Support

The bidder should provide the following information with costing where applicable:

73. Support structure
74. Support models
75. Support Cost
76. Escalation matrix
77. Service Level Agreement (SLA) template
78. Onsite and offsite support
79. Where onsite support is provided, the bidder should avail competent resources to support the system

q) Versioning And Patch Management

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.

r) Migration

The bidder will be responsible for data and interface migration from disparate systems into the new platform.

s) Documentation

The bidder shall be required to:

i. Develop and provide system installation, support, configuration manuals.
ii. Develop and provide end-user documentation, including updates and release notes.

t) Platform support

The solution should support latest stable versions of the solution stack (Database/ web/application/Operating system and user interaction applications)

B. FUNCTIONAL SPECIFICATION:

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

a) User Management

These entails all aspects of handling users within the system which is integrated to active directory and assigning user profiles and appropriate roles in the system, ability to deactivate/ terminate, activate or update users.

Users/staff will be required to provide their details which shall include but not limited to:

80. Staff Id Number
81. Username
82. First Name
83. Middle Name
84. Last Name
85. Designation
86. User Status
87. Mobile No.

The system should:

88. Generate and send to the user via SMS/mail notification of successful set up.
89. Provide security for different user levels.
90. Define security at the function level, e.g., allow a user to access data relevant to their function.
91. Restrict certain functions to authorized personnel only, e.g., certain user group has read-only access, another user group has ability to delete records.

b) Risk and Control Self-Assessments (RCSA)

The system should:

92. Holistically manage risk across the organization, integrate risk management capabilities like assessments, support best practice analytics, and enhance risk communication with dashboards and reports.
93. Support the creation of a centralized risk taxonomy mapped to the associated controls, policies, objectives, regulations, products, assets, audit programs, contracts, and third-party business continuity/ recovery plans.
94. Support configurable methodologies for risk assessments, computations, and aggregation or consolidation to meet specific functional or enterprise-wide requirements.

95. Accommodate quantitative and qualitative risk assessment criteria with quantitative scoring, including risk impact, likelihood, velocity, duration, and control effectiveness for inherent and residual risk.
96. Integrate all related data and processes including a reusable library of risks and their corresponding controls and assessments, results from individual assessments, key risk indicators, events such as losses and near-misses, and issues and remediation plans in an integrated solution.
97. Have customizable templates for rolling out RCSAs across all the business, support units or projects.
98. Have the capability to map the existing Organization Structure to the relevant Business Lines which should contain the hierarchy and workflow for the process.
99. Be able to re-run the past assessments based on the revised scale when there is a change in the rating scales.
100. Have the capability to customize the logic and design used for creating Heat Maps.
101. Be able to generate defined and desired Heat Maps per Unit/ Division/Subsidiary/Group. Risk Ranking of units/branches per unit/per region
102. Consolidation of enterprise-wide Risk Register/Dynamic Heat Map).
103. Facilitate resource allocation and assignment of specific tasks.
104. Provide the availability to attach and store documents related to the assessment.
105. The system should enable monitoring of continuous action plans.
106. Validation/Review - Enable users (reviewer) to approve/ return for review/decline/delete risk registers
107. Alerts:
    - Generate alerts to users when tasks need to be performed and include automated escalations - notification when tasks are almost due, past due, open, closed, in-progress or identified outliers.
    - Automated alerts to action owners for actions they are tagged on and include an escalation matrix when the actions are not responded to in the system by the action owner.

108. The Bidder should aid in customization of the Risk Register and provide the Risk library database along with the system.

c) Operational Risk Capital Calculation

The system should be able to:

109. Extract and load data from the Bank's financial reporting systems for financial calculations.

110. Allow specific users to make the changes to parameters feeding into the capital calculation inputs. This should include assumptions.
111. The system should enable Trend Analysis for Group/Subsidiaries
112. Generate Ops Risk Capital Charge as per Bank approved and Regulatory approaches - Automate the computation of the capital charge based on various prescribed approaches.
113. Flexibility in incorporating future metrices in capital charge calculation
114. Enable computation of Expected Loss and Unexpected Loss
115. Basel Capital Computation, VaR (Value at Risk), Loan Pricing Risks, ICAAP, ILAAP, IRRBB, IFRS 9 Validation, Portfolio Credit Analytics, Risk Scoring, and Balance Sheet Analytics.
116. Provide automated, accurate, and real-time insights, enabling precise calculations, comprehensive portfolio analysis, and informed strategic decisions, thereby strengthening the Bank's ability to navigate complex financial risks and meet stringent regulatory requirements.

d) Key Control Self-Assessment (KCSA):

117. The system should enable users to create KCSA template for each unit in the Bank. This should outline:
    - The Key process,
    - Test objectives
    - Risk & Controls
    - Criteria/methodology for testing the control
    - Documents to review to support the test
    - Frequency of testing

118. Scheduling and conducting KCSA: the system should enable:
    - Assign a testing template to a unit- should be dynamic to allow assignment of the same template to multiple branches and Units.
    - Initiate the KCSA Test and assign specific individuals to complete specific tests.
    - Resource management-system should enable users to allocate resources & timelines to document, test, validate etc.
    - Enable users to view past KCSA findings/tracker
    - Enable users to document test results /action plan and submit. Only user assigned test should be able to amend the results.
    - Flag assessment lapses into High/Medium/Low

119. Validation of KCSA: the system should:

- o Allow for validation of the KCSA results submitted by units by operational risk or a designated oversight unit with ability to provide detailed feedback per control for the process being tested.
- o Provide ability of the validator to approve or reject KCSA findings at process/Control level.
- o Allow mechanisms for monitoring reworks for resubmission.

120. Link the KCSA to the RCSA to update on controls rating in the register depending on the testing results rating, and update on the action plans from the controls testing with ability to approve these updates by the Unit.

121. Independent KCSA Key Control Self-Assessment Module (conducted by an independent unit e.g., Risk) - the system should:
    - o Enable Risk/Regional Office users to initiate the KCSA Test and assign specific individuals to complete specific tests.
    - o Resource management - system should enable users to allocate resources and timelines to document, test, validate etc.
    - o The system should enable the users to document the background of the units being reviewed i.e., unit history, functions & objectives, Business performance, Risks, last audit findings etc.
    - o Enable users to attach work papers for samples tested and reviews done
    - o Enable user to document test results /action plan and submit.
    - o Flag assessment lapses into High/Medium/Low
    - o Inbuild Risk Profiling capability to guide units to be independently reviewed. This should also capture input from Heat Map.
    - o Allow for auto population of the issue trackers.
    - o Allow for flagging of repeat KCSA issues.
    - o Allow a process to be edited for any of the following – testing criteria/methodology, risks, controls, documents - without having to re-do an entirely new process and/or template.

e) Incident Management

122. The system should:
    - o Enable configuration of an escalation matrix.
    - o Enable users to capture all internal and external events. The system should generate unique reference numbers for each incident logged.
    - o Real time incident tracking, logging, and management
    - o System to allow for indication of the number of occurrences for the same incident
    - o Enable users to describe.

- Location
- Incident Description
- Date & Time of Occurrence
- Date Discovered
- Date Reported
- What caused the incident
- Action Taken Immediately after incident was discovered
- Impact e.g., systems, people, reputation etc.
- Incident Implication (Unit impacted by the incident)
- Notification of Incident
- Incident Status (Open or Closed)
- Estimated costs arising from incident
- Customer Information
- Enable attachment of supporting documents e.g., photos
- Lessons Learnt and closure of gaps noted

123. Alert relevant Bank authorities for action and information (as per escalation matrix)
124. Enable amendment of a captured incident e.g., information to input root cause after investigation, owner, lesson learnt, status etc
125. Shows incidents that have been escalated to different units across the Bank and this information should be available at the time of the risk register review.
126. Trigger automatic alerts and notifications to appropriate personnel for task assignments for investigation and remedial action.
127. Link reported incidences to actual Operational losses, near-misses, and comparable external loss events.

f) Loss Data Management (LDM)

The system should:

128. Incorporate Bank approved LDM workflow - to ensure that all stakeholders, including the first and second lines of defense, and senior management, have visibility of operational losses, provision to approve losses as per the set approval limits, classify losses by business lines/ Event type, risk, loss types, Causes/ Consequences, amount of loss.
129. Users to capture and document losses incurred and attach supporting documents
130. Enable tracking of captured losses and the Approval process.
131. Ability to integrate into the core Banking system i.e., T24 and enable posting of approved internal losses to the core Bank system in real-time.

132. Classify loss by business lines/ Event type, perpetrator type, risk type, loss types, Causes/ Consequences, amount of loss (Basel II classifications)

133. Apportion logged losses into loss bearing units based on the root cause analysis

134. Define risk event data and data sources

135. Manage different approval and loss assessment workflows based on the approval amount, roles, Bank wide, subsidiary, departments, and units

136. Manage user matrix and escalation matrix (incorporate approval limits)

137. Capture amount of recovery, period of recovery and scale of operations

138. Segregation of intercompany/ subsidiary postings to respective subsidiary core Banking system (same CBS and multiple CBS). Ability to support multi-currency, multi-company within same country and existing in different countries with different regulators and clear segregation due to jurisdiction and/or locality

139. Enable users to capture and calibrate External loss data collected

140. Enable the users to conduct Root cause analysis on documented loss events (at individual/aggregated views)

141. Make loss database - enable auto generated user defined reports based on the key fields i.e., Group wide, subsidiary/departmental/units, Risk types etc. (drag and drop functionality)

142. Generate summary report of Loss data by business lines/ Event type, risk, loss types, Causes/ Consequences, period, TAT, status, unit

143. Allow users to capture potential losses, near misses or indirect losses and recoveries made.

144. Enable linking of losses to controls the RCSA and the KCSA. Assign action plan and follow up triggers on action plan documented for closure.

145. Generate unique references for each reported operational loss and enable drilling of a case or a loss per their unique references.

146. Incorporation of operational risk scenario analysis and loss distribution/modelling exercises such as conducting Monte Carlo simulations to support capital allocation.

147. Support predictive analytics for improved decision making.

148. Means to change the standard workflow of who receives, reviews, and approves loss events and the monetary thresholds for such receipt, review, and approval and can these changes be made by the system administrator without assistance from the vendor

149. Application should allow the authorized user to setup Email Triggers for Loss Item and Reversal Request.

g) Key Risk Indicators (KRIs)

The system should:

150. Support collection, flexible reporting, and aggregation of qualitative and quantitative Key Risk Indicators by business unit, strategic imperative or another user defined dimension.
151. Enable users to document attributes of each key indicator such as whether it is a leading or lagging indicator, set thresholds (upper and lower boundaries), frequency of reporting, etc.
152. Enable users to populate key indicators from a key indicator library periodically or via integration(s) with source systems of record.
153. Enables users to monitor each business unit metrics for variance against their expected direction (up, down, staying the same) and/or for variance against one or more standard deviations from the historical mean
154. Allow assignment of accountability to each KRI.
155. Enables users to drill/extract KRI's per process including those that touch cross functional units.
156. Aggregate the Units KRI's to Bank wide KRI's
157. The system should enable users to add/amend & delete metrices held in the library. This should be in line with the laid down review and approval process to ensure that appropriate second line of defense stakeholders agree.
158. Provide a clear methodology for trend analysis to identify concentration of risk and or potential control failures.
159. Provide ability to associate key indicators with any record in the system including Corporate Objectives, Business Processes, Business Units, Risks and Controls (RCSA & KCSA)
160. Enable users to be able to extract a consolidated list of indicators that are operating outside thresholds, and associated stakeholder escalation and remediation plans
161. Enable Key Risk Indicator owners to record their remediation plans and commitment dates to bring key indicators back within acceptable boundaries
162. The system should give visibility on areas that have not established indicators (and reasons for exemption where applicable)
163. Provide visibility for units that have not collected data associated with established indicators or have not been collected in accordance with established schedules
164. Enable inclusion of the status of key indicators in the assessment of risk
165. Have the ability to project key indicators into the future using linear regression
166. Alerts:
    - Support automated notifications to appropriate stakeholders in case of a KRI threshold breach or past due key indicator information.
    - Automated alerts to unit and Risk teams for KRIs that are above the thresholds in the system.

167. Provide the ability to integrate with other systems to extract key control indicators.
168. Ability to monitor key indicators for variance against their expected direction (up, down, staying the same)
169. Ability to project key indicators into the future using linear regression
170. Ability to populate key indicator data via integration(s) with source systems of record
171. Ability to define and monitor key indicators against graduated thresholds such as upper and lower boundaries

h) Corrective Action Plan/Issue Management

The system should:

172. Enable users to capture corrective action plan
173. Provide ability to map controls to risks and mitigation activities.
174. Alert relevant Bank authorities for action and information
175. Enable users to document and close the action performed
176. Alert initiator of the action taken and operational risk for information
177. Generate action plan report based on date, action, pending, and severity and implement escalation matrix.
178. For issues arising from the assessment and auditing processes or from any other external events such as loss-events, scenario analyses, or "near-misses, the solution should provide seamless issue management and remediation management capabilities. It should help trigger automatic alerts and notifications for the appropriate personnel to begin investigation and remedial actions.
179. The system should provide the ability to set the frequency of review and reporting for outstanding issues.
180. The solution should enable the organization to establish clear ownership of remediation plans, route remediation plans to responsible personnel for management, track and monitor proper sign-off / approvals, and escalate plans when necessary.

i) Digital and Information Risk Module

The bidder should demonstrate ability to incorporate the below requirements:

181. Ability to quantify the potential impact by assessing the residual cyber /Information risk while linking to financial impact.
182. Identification, assessment, and mitigation of technology risks across information assets and having a view of the Bank's technology risk posture and facilitate compliance with IT risk frameworks like NIST and ISO 27000 & ISO 31000.

183. Insurance - the system should provide the capability to capture all cyber-Security risks and provide a mechanism for tracking insurance exposure.
184. Risk register dashboard, emerging risks & pending activities
185. Ability to work with scripts and robot process automation tools and AI (Artificial Intelligence)
186. Ability to integrate into other systems such as SIEM, HP ITSM and other monitoring tools
187. Reporting-the system should enable the aligning of IT and business objectives.
188. The system should enable tracking of Post Implementation Review Action points.
189. The system should enable the development of use cases
190. Offer a clear view of the vendor risk, streamline the vendor assessment and monitoring, capture key The vendor details, and provide integrated reporting linked to central risk libraries and controls.

j) Business Continuity Management

The system should:

191. The system includes a baseline Business Impact Analysis methodology that can provide a common structure for the enterprise.
192. Ability to plan and execute business continuity and disaster recovery (DR) management across the Bank's functions.
193. Effectively create, maintain, and exercise continuity and recovery plan, from pre-built templates and configurable questionnaires and maintain it with policy-driven workflows.
194. The BIA (Business Impact Assessment) methodology should include multiple impact categories to evaluate criticality of the business process.
195. The BIA methodology should include standard recovery time objective (RTO) and recovery point objective (RTO) calculations for business processes and result in an overall business criticality rating for the asset.
196. The system includes workflow for multiple participants in the business impact assessment (BIA) process, including the business process owner and others that may need to provide input, as well as review by another level and the business continuity management (BCM) team.
197. Corrective and preventive actions can be recorded against the crisis to direct and guide continuous improvement of the BCM program.
198. BC and DR plans can be activated within the system to respond to the crisis situation.
199. The system can adopt a fluid workflow, allowing incidents to follow different paths depending on their priority, source, and categorization.
200. Best practice response procedures can be stored in a library for consistent response

k) Compliance Function Management

201. Manage compliance workflows, handle regulatory changes, enable compliance assessments and control management, provide relevant analytics, and ensure sensitive information security through role-based access.
202. Regulatory Compliance Management: Regulatory requirements gap analysis, mapping and implementation, Regulatory requirements register
203. Compliance Program Management: Compliance Self Assessments/checklists, Compliance Monitoring, Compliance Trends analysis, Reporting, Compliance Dashboards, Tracking closure of compliance gaps, Compliance Universe hosting, Corrective Action Management
204. Ethics Program Management: Ethics monitoring, Ethics Assessments, Ethics Reporting, Dashboards, trend analysis
205. Policy Lifecycle Management: Policy Development, Policy Review and Approval, Policy version control
206. Tasks Management: Scheduling, reminders, surveys, questionnaires
207. Incident Management & Emergency Alerts notifications/crisis communication
208. Ability to access systems from multiple devices

l) Strategic Risk Management

Demonstrate ability to maintain a robust and dynamic strategic risks management profile and methodology, to provide visibility and early warning indicators to Senior Management and the Board on external strategic outlook risk drivers and internal risk drivers for successful strategic objectives implementation. Key elements should include:

- Documentation and tracking of assessed external strategic risk drivers
- Tracking assessments of key internal strategic plan implementation risk drivers and recommendations for mitigating actions, including likelihood assessments of achieving strategic objectives
- Monitoring progress on recommended action items
- MIS reporting and including dashboards and heat maps

m) Fraud Risk Management

The system should provide a case management workflow: -

209. For users to create, update, expunge, classify, assign and close cases.
210. Provide for annual running numbers for cases created in the system.
211. Provide capability to scan, load & expunge/drop documents.
212. Provide capability to track and generate individual case Turn Around Time (TAT) based on set thresholds.
213. Provide capability to notify users upon case assignment.
214. Provide capability to escalate cases based on set thresholds.
215. Provide capability for generation of reports, dashboards based on user defined parameters.

216. Provide capability for both front and backward integration with various systems.

217. Provide a comprehensive audit trail of user and system activities.

n) Data Connectivity and Integration

218. Data Connectivity and Integration.
Data Sources: The solution should have the ability to integrate with various data sources, including databases, applications, and external systems as well as file-based data inputs.

219. Data Integration, Connectivity and Integration.
Connectors: The solution should provide out-of-the-box connectors to popular databases and enterprise systems to facilitate seamless data integration.

220. Data Integration, Connectivity and Integration:
Realtime Integration: The solution should have the ability to access the latest data from various operational/source systems such as the core Banking solution, mobile Banking solution, the card management system, treasury management system, fraud management system etc.

221. Data Integration, Connectivity and Integration
Data transformation: The solution should have the ability to transform and aggregate data prior to, or during, ingestion.

222. Data Integration, Connectivity and Integration:
Scheduled Integration: The solution should support scheduled data syncs and extract, transform, load (ETL) workflows.

223. APIs and Extensibility
The solution provides robust APIs for integration with other systems and custom applications. It should be possible to extend the solution's functionality through customizations and extensions of the application programming interfaces (APIs).

224. Data Extracts Scheduling
The solution should be able to schedule the data extracts / delivery either of the following: Daily, Monthly, Quarterly, Yearly, Intra-day.

225. Alerts & Notifications
The solution should have the capability to send / produce notifications after certain processes are completed. Automated email notifications and alerts of key events will facilitate workflow integration.

226. Integration with Analytical Tools
The solution should provide seamless integration with business intelligence (BI) and analytics tools to enable advanced reporting, analytics, and insights generation, on premise and for cloud deployed data environments.

o) Implementation And Configuration

227. Data Migration

The bidder shall be responsible for migration dry runs and actual migration by providing the migration plan/strategy, tools, execution, testing, rollback, backup, auditing and resources required to carry out this exercise. The bidder shall be responsible for data sourcing, dry runs and actual migration including reconciliation of migrated data."

228. Integrations
The bidder shall design, build and configure the integrations necessary to support the generation of the dashboards and reports listed in the below section.

229. At a minimum, this shall require integration into the following:
    1. Kondor+
    2. T24
    3. C-Soft – inhouse etc

230. Validation and Testing
The bidder shall perform data validation checks to ensure the accuracy, integrity, and completeness of migrated data and the configured integrations.

231. Preconfigured Dashboards and Reports:

Capital:

As part of the project, the bidder shall configure, among others, the following reports and dashboards.

1. Group and Bank capital adequacy over time
2. Risk Weighted Assets (RWAs) over time by product, segment etc
3. Exposure vs RWA

Credit Risk:

As part of the project, the bidder shall configure, among others, the following reports and dashboards.

1. Credit Exposure (by product, sector, customer segment, instrument type)
2. Portfolio Quality (NPL, Ageing, Watchlist, Restructures, Moratoriums, Migration) - all by product, sector, customer segment, instrument type etc)
3. Credit Concentrations (Sectors, products, geography). Top counterparties by exposure
4. Credit Risk Limits Monitoring. Exposure vs approved limits (sectors, groups, counterparties, internal ratings etc)
5. Credit Rating Migration Matrices
6. IFRS9 Staging and ECL dashboard (by stage, ecl). Movement and migration over time.

Market & Liquidity:

As part of the project, the bidder shall configure, among others, the following reports and dashboards.

1. Liquidity Ratio, InterBank Borrowing and Loan to Deposit ratio over time
2. Core / non-core deposit analysis
3. Liquidity gap reporting
4. Interest rate risk in the Banking book

5. Liquidity Coverage Ratio and Net Stable Funding ratio
6. FX Limit monitoring report
7. Interest Rate Risk exposure vs limits (PV01)
8. Country Risk Exposure vs Limits (Nostro, Money Market, Credit, Treasury)
9. Settlement risk exposure vs limits
10. Swap PV01
11. Stress testing dashboards

p) Risk Reports and Dashboards

The bidder should demonstrate ability to generate different types of reports and dashboards that are required from time to time. The system should support below categories of reports and dashboards:

- Integrated dashboards and analytics to drive insights and actions, assess performance, and present to stakeholders without needing additional software or complex data integration.
- Comprehensive built-in reporting tools, allow non-coding dashboard and report creation using self-service tools, and offer experienced analytics consultation for bespoke reporting needs.
- Built-in, flexible reporting for various levels, support automated and ad-hoc reports, ensure data security from user roles, allow dashboard and analytics construction within the system, and provide exports to Excel, PowerPoint, and PDF.
- Automated input, consolidation and management of risk data.
- Inbuilt configurable reports and dashboards available promptly

232. Dashboards on RCSAs, KRIs, Loss data, KCSAs, Incidences, Capital calculation, Corrective action implementation whether due or overdue.
233. Risk intelligence analytics using a combination of built-in reporting and analytics engine, as well as deep integration with industry standard analytical tools.
234. Have the ability to track process ownership, assessment plans, remediation status, etc. on graphical charts that provide real-time information globally. Information can be drilled down to deeper levels or into underlying data elements.
235. Loss data management reports by period, Basel category, risk, unit, division, and casual factors
236. Key control self-assessment completion, validation and action plan tracking and alerts.
237. Enable drag and drop ad hoc dashboards and reports based on users’ needs
238. Online reports that are generated within the system
239. Offline reports where the system provides transactional and activity data as well user and organization information for use in an external system
240. Escalation Action/Gap reports

241. KCSA - Generate summary report of every self & independent assessment showing the testing results, action plans and owners.

242. KCSA - Flag repeat lapses from previous reviews

243. Incidents - Generate summary report on incidents.

244. Escalated notifications and reporting of indicators based on their attribute or ranked importance.

245. Allow users to track corrective action plans for closure within agreed timelines

246. Report highlighting users' activities - Tag and Track action plans to people responsible

247. Customizable Dashboards
The solution should allow users to create and customize dashboards to meet specific business needs, including layout adjustments, widget configurations, and data visualizations.

248. Real-Time Data Updates
Dashboards should support real-time data updates to reflect the latest information from integrated systems.

249. Interactive Visualizations
The solution should provide interactive charts, graphs, and tables that allow users to drill down into data for detailed analysis.

250. Mobile Accessibility
Dashboards should be accessible on mobile devices, ensuring users can view and interact with data on the go

251. Performance Metrics
Dashboards should include key performance indicators (KPIs) and metrics to track progress against business goals.

252. Historical Data Analysis
Dashboards should support the visualization of historical data trends for comparative analysis.

253. Scheduled Reports
The solution should enable dashboards to generate scheduled reports and distribute them automatically to designated recipients.

2.1.2 Response to the Tender

AREA OF DOCUMENTATION	KCB EXPECTATION	FULLY OFFERED/PARTIALLY OFFERED/NOT OFFERED	REFERENCE
NON-TECHNICAL REQUIREMENTS	This Section is about the company's profile and capabilities. It must be fully completed, and necessary documentation attached. Descriptive statements without attachments where relevant shall be deemed nonresponsive	The bidder shall indicate whether the relevant requirement will be part of the deliverables, and the commercial aspect should be stated clearly.	Reference to any material or websites should be provided (E.g., Chapter Number, Page Number, paragraph Number) and acknowledged.
TECHNICAL & FUNCTIONAL REQUIREMENTS	Describe how requirement is met. Please include relevant documentation or narrative to support statements. Where a bidder indicates level of support without clearly describing, this will be deemed nonresponsive	One must clearly indicate whether the capability is Fully Offered, Partially Offered or Not Offered	Reference to any material or websites should be provided (E.g., Chapter Number, Page Number, paragraph Number) and acknowledged.
SYSTEM IMPLEMENTATION & SUPPORT	Describe how requirement is met. Please include relevant documentation or narrative to support statements. Where a bidder indicates level of support without clearly describing, this will be deemed nonresponsive	One must clearly indicate whether the capability is Fully Offered, Partially Offered or Not Offered	Reference to any material or websites should be provided (E.g., Chapter Number, Page Number, paragraph Number) and acknowledged.

AREA OF DOCUMENTATION	KCB EXPECTATION	FULLY OFFERED/PARTIALLY OFFERED/NOT OFFERED	REFERENCE
KCB IT, RISK & SECURITY	Describe how requirement is met. Please include relevant documentation or narrative to support statements. Where a bidder indicates level of support without clearly describing, this will be deemed nonresponsive	One must clearly indicate whether the capability is Fully Offered, Partially Offered or Not Offered	Reference to any material or websites should be provided (E.g., Chapter Number, Page Number, paragraph Number) and acknowledged.
TRADE REFFERENCES	You are expected to fill in at least three references of similar implementation as the one you are bidding for.	Ensure to provide accurate and authentic information as the Bank can conduct due diligence with the given reference sites.	Attach recommendation letters if available

2.1.3 Documentation Requirements

All documentation and training materials (both in hardcopy as well as a softcopy 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.

2.2 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 so as to enable, for example, creation of ad-hoc reports and integration to other systems

Training will be provided in English language at the Banks premises or a convenient mutually agreed location within Kenya. If additional expenses will be incurred for offsite training, this will be borne by the supplier and must be included in the financial proposal.

2.3 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 signed 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.

2.4 Proof of Concept

The Bank may require proof of concept of the proposed solution as evidence that it is viable and capable of achieving requirements.

2.5 Overall Responsibility

254. 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.
255. 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.
256. The Bidder is responsible for managing the activities of its personnel, or subcontracted personnel, and will hold itself responsible for any misdemeanors.
257. The Bidder shall appoint an experienced counterpart resource to handle this requirement for the duration of the Contract. The Bank may also demand a replacement of the manager if it is not satisfied with the manager’s work or for any other reason.

258. 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.
259. The Bidder will not disclose the Bank's information it has access to, during the course of 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

2.6 Pricing

Costs (USD or KES inclusive VAT, withholding taxes and other applicable taxes where necessary) and Man/Day rates, where appropriate. The costs for foreign firms should be inclusive of withholding taxes, failure to which the commercial proposals will be deemed non-responsive.

The proposals should be valid for a minimum of 90 days.

2.7 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.

2.8 Delayed Delivery and Installation 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.

2.9 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.

2.10 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

2.11 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 the solution proposed and information supplied in response to this tender, and were the vendor to be awarded the tender, they would implement the solution without any additional requirements from the Bank.

2.12 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 invoice 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, and commissioned.

2.13 Staffing

The Supplier will provide the relevant staff and tools to carry out all the required work under this tender. At least two certified experts (2 in general certification and specialized) and a back-up person are required in the technical areas.

A project/account manager is also required to coordinate and account for all the Supplier's activities throughout the contract period.

2.14 Responsibility 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 themselves 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 stated below from 3.2 to 3.23.

3.2. Award of Contract

Following the opening and evaluation of proposals, the Bank will award the Contract to the successful bidder or multiple bidders whose bids have been determined to be substantially responsive. The Bank will communicate to the selected bidder its intention to finalize the draft conditions of engagement submitted earlier with his proposals. After agreement will have been reached, the successful Bidder shall be invited for agreement and 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 (sections 3.2 to 3.23) 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. Non-variation of Costs

The prices quoted for the service and subsequently agreed and incorporated into the contract shall be held fixed for the contract period.

3.6. Delays in the Bidder's Performance

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

If at any time during the performance of the Contract, the Bidder should encounter conditions impeding timely delivery and performance of the Solution, the Bidder shall promptly notify the Bank in writing of the fact of the delay, it's 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.

Except in the case of "force majeure" as provided in Clause 3.14, 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 from this RFP shall incorporate suitable provisions for the payment of liquidated damages by the bidders in case of delays in the performance of contract.

All services must be delivered and implemented within agreed timelines after the Bank issues a purchase order. Any delay in commencement of the execution of the contract will attract a penalty which will be specified in the agreement signed by both parties

Notwithstanding the provisions detailed in this section above, the Bank reserves the right to terminate the award at any time and take corrective measures as necessary to protect the Bank interests, which interest are solely determined by the Bank.

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 Request for Proposal 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

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 of all demands or responsibilities arising from accidents or loss of life, the cause of which is the Bidder's negligence. The Bidder will pay for 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 will not disclose the Bank's information it has access to, during 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 to complete the project, the Bank shall,

a) Provide the Bidder with specific and detailed relevant information concerning the contract
b) In general, provide all information and access to Bank's personnel:

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 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 the 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 for a Force Majeure event is under obligation, when requested, to prove its effect on the fulfilling of the contemplated contract.

3.14. Payments

The Bank's standard payment terms is forty-five (45) days from the date of receipt of an invoice. Please note that **KCB shall make payments through a KCB Account for local entities** and thus you are encouraged to open a KCB account in case you do not have one.

3.15. Way Forward

Once the bids are opened, bid analysis will commence and the vendors may be informed when their bid has been short-listed. Short listed the 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, The 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.

3.16. Bid Effectiveness

It is a condition of the Bank that the vendor guarantees the sufficiency and effectiveness of the service model 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 service model proposed and that were the vendor to be awarded the tender, they would implement the service model without any additional requirements from the Bank.

3.17. Contract Provision

The Bank will not make any payments in advance. The Bank will issue a Purchase Order for all the services ordered. The payment will be made within 45 days after delivery and receipt of an invoice. 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 partial payments.

3.18. Buyer's Rights

The Bank reserves the right to reject any or all the tender bids without giving any reason 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 should 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.

3.19. 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

3.20. Delivery

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

3.21. 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.

ANNEXURES

ANNEX 1 – REFERENCES

References of similar services

Note:
The Firms should submit the references in this format.

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						
6						
7						
8						
9						
10						

ANNEX 2 – COMPANY BRIEF SUMMARY

Company	
Years of experience	
Core Business	
Key Contact	
Geographical Spread in operation	
No. of Staff	
Area of Specialization	

List of Directors and shareholdings	
Customer Base	

ANNEX 3: THE VENDOR CONFLICT OF INTEREST DISCLOSURE FORM

All The vendors interested in conducting business with the Bank must complete and return the vendor Conflict of Interest Disclosure Form to be eligible to be awarded a contract. Please note that all the vendors are subject to comply with the Bank's Code of Ethical Conduct and conflict-of-interest policies as are applicable as stated within the certification section below.

Any The vendor who does not provide or provides misleading or incorrect information on the disclosure form shall be disqualified from participation. The contract shall be voidable by the Bank if the misleading or incorrect information on the form is discovered by the Bank subsequent to the execution of a contract.

If a the vendor has a relationship with a Bank official or employee, an immediate family member *(spouse, children, parents & siblings)* of a Bank official or employee, the vendor shall disclose the information required below.

Certification: I hereby certify that to my knowledge, there is no conflict of interest involving the vendor named below: -

1. No Bank official or employee or Bank employee's immediate family member has an ownership interest in the vendor's company or is deriving personal financial gain from this contract.
2. No retired or separated Bank official or employee who has been retired or separated from the Bank for less than one (1) year has an ownership interest in the vendor's Company.
3. No Bank employee is currently employed or prospectively to be employed by the vendor.
4. Please note any exceptions below: -

The vendor Name	The vendor Phone Number
Conflict of Interest Disclosure*	

Name of Bank employees, ex-employees, elected officials or immediate family members with whom there may be a potential conflict of interest ____________________________________	( ) Relationship to employee ______________________________________ ( ) Interest in the vendor's company ______________________________________ ( ) Other ______________________________________

*Disclosing a potential conflict of interest does not disqualify the vendors. In the event the vendors do not disclose potential

Conflicts of interest and they are detected by the Bank; The vendor will be disqualified from doing business with the Bank.

I certify that the information provided is true and correct by my signature below:

____________________________ __________ _______________________________

Signature of The vendor Authorized Date Printed Name of the vendor Authorized

Representative Representative

DECLARATION

Please complete the declaration below and attach this document in it's entirety to your response. Also ensure that you have indicated the areas of interest and that you have answered all questions in the same order and numbering as given in this document.

I/we certify that the information provided in response to this Questionnaire is accurate and complete as at the date set out below.

I/we understand that the provision of false information in response to this Questionnaire could result in the Company being excluded from the list of those who may be invited to tender for a contract with KCB Bank Kenya Limited.

I/we undertake to inform KCB Bank Kenya Limited Ltd promptly following any matter which would alter or add to any of the information given in response to this Questionnaire.

I/we make this declaration for and on behalf of the Company.

Signed: ……………………………………

Name: ……………………………………

Position: ……………………………………

Date: ……………………….

Company stamp