COMMON MARKET FOR EASTERN AND SOUTHERN AFRICA BUSINESS COUNCIL

CONSULTANCY

FOR THE CBC DIGITAL FINANCIAL INCLUSION PLAN FOR MICRO SMALL AND MEDIUM SIZED ENTERPRISES (MSMEs)

PROVISION OF SERVICES TOWARDS IMPLEMENTATION OF THE COMESA CROSS BORDER DIGITAL RETAIL PAYMENTS PLATFORM AND/OR FRAUD MANAGEMENT MODULE

REQUEST FOR PROPOSALS (RFP)

Ref no: CS/CBC/2024(001/75) TS/jp

Closing Date: 13th February 2024

Terms of References

Project title:	SME Digital Financial Inclusion Plan
Assignment title:	Provision of Services towards Implementation of the COMESA Cross Border Digital Retail Payments Platform And/Or Fraud Management Module
Contract Duration:	1st April 2024 – 31st July, 2025
Duty station:	Lusaka, Zambia
Travel:	Eight (8) pilot countries (Zambia, Malawi, Kenya, Uganda, Rwanda, Egypt, Ethiopia & Mauritius)
Eligibility:	Consultancy/Implementation Firms

1. INTRODUCTION

The COMESA Business Council (CBC) is currently in the process of developing a Regional Financial Inclusion Scheme for Micro Small and Medium sized Enterprises (MSMES). The program aims to facilitate the creation, advancement, and deployment of a unified regional infrastructure for digital financial services within the Common Market for Eastern and Southern Africa (COMESA) region. This infrastructure is intended to be real-time, cost-effective, interoperable, and resistant to fraudulent activities, with a focus on serving Micro, Small, and Medium-sized Enterprises (MSMEs) and their clientele.

The CBC Digital Financial Inclusion (DFI) program has undergone two distinct phases thus far. In the initial phase, a comprehensive business case report was formulated. This report guided the development of a model policy framework for a regional digital retail payments system tailored to MSMEs within the COMESA region. Concurrently, guidelines for operating this digital retail payments system have also been developed.

Subsequently, the business case and model policy framework provided the blueprint for the second phase. During this stage, CBC formulated a Business Model for the execution and management of a regional digital retail payments system, catering specifically to MSMEs operating within the COMESA region. This Business Model was crafted in accordance with the Level One Design Principles (L1DP) put forth by the Level One Project, focusing on the specific needs of low-income cross-border traders. The Business Model report underwent validation through four stakeholder Public-Private Dialogues (PPDs) and was subsequently endorsed by the COMESA Committee of Governors of Central Banks (CCGCB).

Presently, in collaboration with the COMESA Clearing House (CCH) and support from the Gates Foundation, CBC is embarking on Phase III of the DFI Program, involving the actual implementation and operation of the Regional Digital Retail Payments Scheme. Before the commencement of this Payments Scheme, CBC developed a comprehensive operational plan. The details of the plan were validated during the Fifth Stakeholder Public-Private Dialogue, which took place on July 25, 2023, in Lilongwe, Malawi. Following the dialogue, a workshop was conducted to discuss the planned Proof of Concept (PoC), focusing on cross-border transactions between Zambia and Malawi. This workshop provided a platform for stakeholders to engage in discussions regarding the intricacies of the PoC.

After effectively choosing an implementing entity for the PoC, the proof of concept was carried out between Zambia and Malawi, yielding successful results. The findings of the PoC were presented to the COMESA Committee of Central Bank Governors (CCGCB) in November 2023 and subsequently validated during a PoC workshop that was held in the same month, attended by regulators, banks, and non-bank operators. Following CCGCB's decision to present the PoC results to the COMESA Regional Payment Scheme (REPSS) User group, a meeting was convened with the REPSS user group, from which precise recommendations were formulated for the Central Bank Governors regarding the adoption of the retail payments platform.

Considering these advancements, CBC is seeking proposals from capable implementation firms to commission the COMESA Cross Border Digital Retail Payments Platform And/Or Fraud Management Module in the 8 pilot countries. This platform intends to enhance cross-border digital payment transactions among pilot Member States, fostering better financial inclusion and optimizing payments across the wider COMESA region, while ensuring efficiency and security.

2. OBJECTIVES OF THE ASSIGNMENT

The primary objectives of this assignment are to:

a) Design and develop a comprehensive COMESA Digital Retail Payments platform with Fraud Management Module that aligns with the specified key system requirements under section 9.

b) The selected firm/s shall be responsible for designing and implementing the COMESA Digital Retail Payments Platform in eight (8) COMESA Member States, with its key system features and functionalities in a production environment in line with Level One Design Principles.

c) The firm/s shall ensure strong fraud detection and enhance security for cross-border payments by identifying scams, detecting money laundering, and preventing terrorist financing activities.

d) The firm/s shall conduct rigorous testing and analysis of the payments platform to assure its performance, security measures, efficiency, and scalability across cross-border payment platforms to ensure its reliability and resilience.

e) The firm/s shall collaborate with a nominated service operator or CBC/CCH team to enable the handover of a live service to that operator, supported by knowledge transfer to develop the appropriate capacity in the operator’s staff.

f) The firm/s shall develop a ‘Post-Implementation Support and Maintenance Plan’ which maximizes independence and does not require that the implementing consultants be involved in future maintenance. Support and maintenance should be localized.

3. SCOPE OF WORK AND TASKS

Lot 1: Implementation of the COMESA Digital Retail Payments Platform

The selected firm is expected to perform the following comprehensive tasks:

a)	Design, development, and implementation of the COMESA Digital Retail Payments Platform
b)	Deploy and test the platform in a production environment, ensuring optimal performance and security by demonstrating end to end transaction lifecycle cross border among eight (8) pilot COMESA Member States.
c)	Integrate the platform with relevant financial institutions, such as commercial banks, and non-banks such as Mobile Network Operators, FinTechs and other stakeholders like Regulatory Authorities (to provide regulatory access).
d)	Engage stakeholders for appropriate feedback and incorporate necessary improvements by providing timely notifications and confirmations to participants involved in a transaction, ensuring transparency and accountability.
e)	Conduct user testing and piloting the platform in selected COMESA Member States namely Zambia, Malawi, Kenya, Uganda, Rwanda, Egypt, Ethiopia & Mauritius
f)	Conduct performance and scalability testing to assure how well the system can handle increased transaction volumes and participants load from the pilot countries.
g)	Assist Financial Service Providers in developing a front-end experience including Illustration of how the system handles exceptions, such as failed transactions or insufficient funds, by following the appropriate workflows and providing clear feedback to participants.
h)	Implement reporting and analytics capabilities to allow participants to track transaction trends, volumes, and other relevant metrics.
i)	Showcase how participant and transaction data is managed, stored, retrieved, and mined (for digital collateral purpose) securely within the system.
j)	Provide technical capacity building to relevant stakeholders, including local system integrators and FinTechs to shadow technical work.
k)	Create comprehensive documentation and training materials to guide future development and implementation efforts, as well as to assist participants in understanding the payments system.
l)	Modify and develop modules for Mojaloop or any other similar open-source modules required for the implementation, including but not limited to foreign exchange engine, clearing, settlement, dispute management, open API management, proxy look up service, custom business rules, transaction types, and participant-specific configurations.
m)	Work as part of a Mojaloop community workstream or any other similar open-source community workstream involving as many other community members as feasible and contribute all work back to the open-source community on behalf of CBC.
n)	Ensure that the implementation adheres to relevant financial regulations and compliance requirements in the chosen deployment environment.
o)	Gather input from both participants and stakeholders engaged in the implementation process to enhance its effectiveness, pinpoint areas that could be improved, and assess the feasibility of advancing towards wider integration and deployment. Ensure compatibility with other regional platforms for seamless interoperability.

p)	Go-Live support during the initial phase of deployment to address any issues and ensure a smooth transition.
q)	Post-Implementation Support on maintenance, updates, and patches.

Lot 2: Implementation of Fraud Management Module in line with the platform

The selected firm shall be expected to perform the following comprehensive tasks:

a)	Outline the architectural design of the fraud management module.
b)	Implement the functionalities and features required for the fraud management modules such as real-time monitoring, risk assessment and case management (so that the central switch operator can effectively monitor, and track cases raised)
c)	Integrate with the main payment platform and other case management systems of Digital Financial Service Providers (DFSPs).
d)	Identify and connect the data sources to be utilized for fraud detection and prevention (e.g., transaction logs, customer databases).
e)	Define the testing procedures to ensure the functionality and reliability of the fraud management modules.
f)	Establish quality assurance measures to verify compliance with defined standards and requirements in terms of compliance, security, data integrity and accuracy, integration, scalability and performance, user access permissions, reporting and analysis, regulatory reporting, continuous monitoring and improvement, training, and documentation
g)	Develop a plan to train end-users and stakeholders on using the fraud management module effectively.
h)	Create user manuals, guides, or documentation explaining the module's functionalities, procedures, and troubleshooting steps.
i)	Detail the strategy for deploying the fraud management module into the operational environment.
j)	Define the process for user acceptance testing before final deployment.
k)	Establish protocols for ongoing monitoring, maintenance, and support after deployment.
l)	Implement a mechanism to collect feedback from users and stakeholders for continuous improvement and capturing new fraud incidents
m)	Go-Live support during the initial phase of deployment to address any issues and ensure a smooth transition.
n)	Post-Implementation Support on maintenance and updates to the module to keep it effective against emerging fraud threats.

4. JOINT APPROACH AND METHODOLOGY (for lot1 and lot 2)

The proposed approach and methodology to handle both assignments shall include:

a) Detailed system design with breakdown of tasks considering the platform's complex requirements.

b) Definitions of the tangible outcomes expected at the completion of each task (e.g., system configurations, reports, user manuals).

c) Agile development methodology for iterative and flexible development.

d) Establishment of timelines with milestones and deadlines for each task.

e) Defining the responsibilities of each team or individual involved in the implementation process (e.g., project manager, developers, data analysts, end-users).

f) Establishment of a communication strategy for regular updates, meetings, and reporting structures.

g) Regular testing and validation of functionalities to ensure accuracy and adherence to requirements, industry regulations, data privacy laws, and compliance standards.

h) Continuous monitoring and refinement of security measures in alignment with Scheme Security Requirements and Controls through engaging with Mojaloop community.

i) Implementation of a robust fraud management system tailored to the platform needs that can adapt new threats and technologies

j) Integration of Scheme Cyber Resilience Requirements through robust system architecture and response mechanisms in collaboration with CBC.

k) Documentation of all issue registers, design decisions, development processes, and integration steps.

l) Eliminate technical vendor lock-in and enable CBC to control the entire payments platform, changing maintenance provider or modality at will. The implementer should explain how it will enable this independence through avoidance of proprietary and bespoke solutions, or software that is compatible with the Mojaloop license.

m) Implement the entire solution on preferred cloud hosting environment with the possibility of mirroring it on the chosen data center in one or more member countries

n) Support to scheme rule finalization

o) Build a complete generic domestic Buffer Scheme with documentation, instructions, technical manuals, and regulatory explanations which could be very quickly deployed in each country to accelerate onboarding.

5. PERFORMANCE PERIOD AND OUTPUT

The expected performance period for this assignment is 16 Months including Operation and maintenance support agreement i.e. Service Level Agreement (SLA). The primary output of this engagement is the successful implementation of a fully functional COMESA Cross Border Digital Retail Payments platform with Fraud Management Module. The platform should go live with seamless cross-border payment transactions among eight (8) pilot countries while adhering to the specified key system requirements and objectives.

6. DELIVERABLES

The selected firm shall deliver the following detailed and descriptive deliverables:

Lot 1: Implementation of the COMESA Digital Retail Payments Platform

a)	Comprehensive documentation of the implementation of the COMESA Cross Border Digital Retail Payments Platform
b)	User manuals for participants and administrators, providing step-by-step guidance on system operation and administration.
c)	Detailed system architecture documentation outlining the design principles and integration strategies.
d)	Audit trail mechanism reports capturing all user interactions and activities.
e)	Compliance reports showcasing the platform's alignment with Scheme Regulatory, Security Requirements and Controls.
f)	Mechanisms and protocols documentation for handling Scheme Cyber Resilience Requirements.
g)	Training and Knowledge transfer with user training materials (Text and Video).
h)	Collaborating with and subcontracting of local certified firms under the supervision and approval of CBC to enhance the transfer of knowledge as well as ensuring local in-country support. A minimum of 30% of the contract should be implemented by a locally-owned(COMESA Member State) company to enhance capacities and participation of local contractors in works undertaken by foreign contractors.
i)	Comprehensive technical documentation covering API integration, transaction processing, and security measures.

Lot 2: Implementation of Fraud Management Module in line with the platform

a)	A detailed document outlining the specific requirements of the fraud management system, including functionalities, data sources, user roles, etc.
b)	System design that includes system architecture, database schema, workflows, and integration points with existing systems.
c)	A comprehensive plan outlining the timeline, milestones, resources required, and dependencies for the implementation.
d)	Customization of the fraud management module to suit the organization's specific needs, including setting up rules, thresholds, and alerts.
e)	Training and Knowledge transfer with user training materials.
f)	Collaborating with and subcontracting of local implementers under the supervision and approval of CBC to enhance the transfer of knowledge.
g)	Detailed documentation of the implemented system, including technical specifications, configurations, and user guides for future reference.

7. JOINT TIMELINES FOR LOT1 and LOT2

The proposed timelines for these joint assignments are as follows:

a)	Vendor Selection and Notification: 11th March 2024
b)	Project Kick-off: 1st April 2024
c)	System Design and Architecture for the payments platform and fraud management system.: 1 Month
d)	Development and Integration of the payments platform and fraud management system: 4 Months
e)	User Acceptance Testing (UAT) of the Platform and Fraud Management Modules for Zambia, Malawi, Kenya, Uganda, Rwanda, Egypt, Ethiopia & Mauritius: 1 Month
f)	Regulatory Compliance and Security Audit: 15 Days
g)	Training and Documentation: 30 Days
h)	Launch and Go-Live: 17th November 2024

8. EXPERIENCE REQUIRED

a) Core Technical Competences

Interested firms should have substantial experience and expertise in the following areas:

Lot 1: Implementation of the COMESA Digital Retail Payments Platform

a)	Leading or contributing to Mojaloop community workstreams or any other similar open-source community workstreams.
b)	Integrating with diverse payment gateways and financial institutions using different techniques like API integration.
c)	Ability to incorporate mobile payment methods and optimize the platform for mobile transactions.
d)	Demonstrated ability to scale and manage large-scale digital payment platforms.
e)	Knowledge of regional and international payment standards and regulations.
f)	Working with Mojaloop or other open-source software for real-time cross border and cross network transactions.
g)	Proficiency in relevant programming languages and technologies.
h)	Proven experience in designing and developing digital payment solutions, preferably in a cross-border context.
i)	Implementing secure and scalable payment processing systems.
j)	Working with open-source software and as part of an open community on open payments platforms.
k)	Knowledge of compliance obligations within the payment eco systems, encompassing data privacy regulations, Anti-Money Laundering (AML), Combating the Financing of Terrorism (CFT) rules, and adhering to the mandates set by the Financial Action Task Force (FATF).
l)	Understanding encryption standards, SSL certificates, and compliance with security regulations

m) Designing platforms to handle high volumes of transactions while maintaining optimal performance.

n) Proficient in effectively managing databases to securely store transactional and creditworthiness information while upholding data integrity.

o) Incorporating intuitive payment flows and interfaces for a seamless user experience (UX)

p) Proficiency in identifying and resolving technical issues swiftly, along with regular maintenance to ensure the platform's smooth functioning.

q) Strong written and verbal communication skills to develop clear technical documentation, architectural diagrams, and presentations for stakeholders.

Lot 2: Implementation of Fraud Management Module in line with the platform

a) Leading or contributing to Mojaloop community workstreams or any other similar open-source community workstreams.

b) Knowledge of regional and international payment standards and regulations.

c) Experience working with open-source software and as part of an open community on open payments platforms.

d) Knowledge of compliance obligations within the payment eco system, encompassing data privacy regulations, Anti-Money Laundering (AML), Combating the Financing of Terrorism (CFT) rules, and adhering to the mandates set by the Financial Action Task Force (FATF).

e) Expertise in transaction monitoring systems.

f) Given the connection to transactions and customer data, it's essential for the vendor to hold ISO 27001 accreditation.

g) Understanding and implementing sophisticated algorithms to detect patterns and anomalies in transaction data that could indicate fraudulent activity.

h) Leveraging machine learning and artificial intelligence techniques to continuously improve fraud detection accuracy by learning from past data.

i) Proficiency in analyzing large volumes of transactional data and using data visualization tools to identify irregularities or suspicious patterns.

j) Implementing systems for real-time monitoring of transactions to quickly identify and flag potentially fraudulent activities as they occur.

k) Utilizing behavioral analytics to assess user behavior and detect deviations that might indicate fraudulent actions.

l) Developing and implementing rule-based systems to automatically flag transactions that meet specific predefined criteria for potential fraud.

m) Ability to integrate the fraud management module seamlessly into payment platforms or systems without disrupting the user experience.

n) Developing risk assessment models and scoring mechanisms to prioritize and handle potentially fraudulent transactions efficiently.

o) Implementing various fraud prevention techniques, such as tokenization, multi-factor authentication, and biometric verification, to enhance security.

p) Strong written and verbal communication skills to develop clear technical documentation, architectural diagrams, and presentations for stakeholders.

b) Joint Qualification Requirements of the Firms (for Lot 1 and Lot 2)

The firms experience and key experts' qualifications will be evaluated based on the following criteria (common for both lot1 and lot2)

a) Provision of details of previous projects that demonstrate their experience in implementing digital payment solutions or financial platforms.

b) Demonstration of experience in the COMESA or other African region will be an added advantage.

c) Membership or participation in Mojaloop or any other similar open-source governing bodies and community workstreams.

d) Provision of profiles of key experts who shall be involved in the assignment. The experts shall possess relevant qualifications and experience in digital payment systems, software development, and financial technology, and leadership experience in Mojaloop or similar open-source projects. Key experts should possess IIPS certification at minimum.

e) The key experts shall have a minimum of 10 years of experience in relevant fields with a minimum qualification of a master's degree in Banking, Computer Science, Finance, Information Technology, Systems Engineering, Law, and any other related fields, with a successful track record in delivering similar projects. Key experts should possess Project management skills in Agile implementation and certification.

9. KEY SYSTEM REQUIREMENTS

The selected firm or firms must demonstrate the capability to address the following key system requirements, ensuring their comprehensive and accurate implementation as specified in the Scheme's Business Requirements Document:

Lot 1: Implementation of the COMESA Digital Retail Payments Platform

Requirement	Description
1	Clearing functionality, including transfer processing, approval, and failure handling. Supports Settlement function for net value credit/debit.
2	Maintenance of ledger of transfers, with each transfer debiting one DFSP and crediting another.
3	Detection of suspicious transactions through velocity checks, identity checks, and blocking.
4	Lookup Directory Service links identifiers with BICs and MSISDNs of Participants/Parties.
5	Provision of ISO 20022 compatible API for secure interaction, standard interfaces for DFSP integration.
6	Provision of converter for integration of other legacy messaging standards such as ISO 8583
7	Processes payments in FIFO order without prioritization or reordering.
8	Clearing functionality, exchange of transfer information during various steps.
9	Support for Settlement function for net credit/debit based on Clearing.

10	Validation of payments against scheme rules (e.g., max amount, required KYC).
11	Validation of inbound transaction sender's authorization for Payer Participant.
12	Validation of intended Payee Participant/Party's reachability.
13	Validation of unique identifier for submitted payment transaction.
14	Validation of no debit attempts from blocked accounts.
15	Support for FX currency validations for debited and credited currency exchange.
16	Notification of Payer Participant of validation errors, includes reason code.
17	Immediately reserves funds on Payer Participant's Platform ledger after successful validation.
18	Rejection of payment if reserved funds on Platform Ledger are insufficient.
19	Notification of Payer Participant if funds cannot be reserved, includes reason code.
20	Forwarding of successfully validated payments to Payer Participant.
21	Forwarding successfully validated payments to Payee Participant.
22	Awaiting Payee Participant reply from the system, payment remains pending until acceptance or rejection received.
23	Rejection of payment if configurable timeout reached without Payee Participant system reply.
24	Un-reserves funds on Payer Participant account if payment triggering reservation is rejected.
26	Production and sending of reports via Application-to-Application interface.
27	Processing 24/7/365 queries: Account Balance and Payment Transaction Status.
28	Implementation of two-factor authentication for secure interactions.
29	Enabling connectivity of Participants using application-to-application mode.
30	Use of ISO 20022 compliant XML for inbound/outbound messages.
31	Informing Payer and Payee after successful settlement, including confirmation dataset.
32	Maintenance of audit trail of user activities on Platform.
33	Compliance with Scheme Security Requirements and Controls.
34	Compliance with Scheme Cyber Resilience Requirements and Controls.
35	Scalability to handle high transaction volumes across borders with very good speed.
36	The solution should offer the ability to efficiently on-board new participants / DFSPs.

Lot 2: Implementation of Fraud Management Module in line with the platform

Requirement	Description
1	Constant monitoring of transactions and user behavior in real time to detect any suspicious activities promptly.
2	Implementation of a rules engine that allows the creation of custom rules to identify and flag potentially fraudulent transactions based on predefined criteria (typology).
3	Utilization of machine learning and AI algorithms to analyze patterns, trends, and anomalies in transaction data, enabling the system to adapt and recognize new forms of fraudulent behavior.
4	Handling of increasing transaction volumes across borders without compromising performance or accuracy in fraud detection.
5	Integration with external databases, fraud blacklists, and third-party APIs to enrich data and enhance the accuracy of fraud detection.
6	Employment of multi-factor authentication (MFA), biometric verification, or other advanced authentication methods to confirm users' identities and prevent unauthorized access.
7	Provision of configurable alert mechanisms to notify stakeholders about suspicious activities or potential fraud instances for timely intervention.
8	Inclusion of a robust case management system to investigate flagged transactions, document findings, and resolve fraud incidents efficiently.
9	Ability for the case management system to seamlessly integrate and categorize alerts generated based on severity, type (fraud, AML, etc.), and other relevant criteria to prioritize cases for review.
10	Automatic creation of cases from alerts with capabilities to track the progress of each case from initiation to resolution. This should include time-stamped actions, status updates, and audit trails.
11	Features to assist in investigating cases, such as access to transaction details, customer history, related cases, and any other relevant data. The case management system should allow investigators to add notes, attach documents, and compile evidence.
12	Customizable workflows to guide the case through various stages of investigation, approval, and resolution involving different participant DFSPs working on a single case to prove the victim and the guilty party with a clear view of this investigation process.
13	Role-based access controls to ensure that sensitive case information is only accessible to authorized personnel in their respective organizations (investigators, managers, auditors, etc.)
14	The different participant DFSPs needs to be able to manage their own Users and Access Control to fulfil their roles and responsibilities.
15	Integrated communication tools to facilitate collaboration among team members, departments, and potentially external entities like law enforcement or regulatory bodies.
16	Comprehensive audit trails of all actions taken on a case, ensuring transparency and compliance with internal policies and external regulations.
17	Presence of a configurable SLA for cases before automated escalation process occurs.

18	Ensures compliance with industry standards (such as PCI DSS) and regulations related to fraud detection and prevention.
19	Compatible with ISO 20022 and other relevant financial messaging standards.
20	Generates comprehensive reports and analytics to track fraud trends, identify vulnerabilities, and improve the system's effectiveness over time.
21	Develops dynamic rules that adapt to changing fraud patterns and evolving tactics used by fraudsters.
22	Detects and prevents fraud across multiple channels (online, mobile, in-store) to provide comprehensive protection.
23	Enables sharing of fraud-related information and insights within the organization and, when appropriate, with external partners or industry networks to strengthen fraud prevention measures.
24	Provides an intuitive interface for fraud analysts and administrators to manage and investigate suspicious activities efficiently.
25	The capacity to be customizable based on specific organizational needs and processes.
26	The solution should offer the ability to efficiently on-board new participants / DFSPs.

10. EVALUATION CRITERIA AND PAYMENT MODALITIES

The firm shall be evaluated against a combination of technical and financial criteria. The firm shall be required to score a minimum of 70% of the 100% technical grade which will then qualify the firm for the next stage of financial grading. Both financial and technical scores shall be added for the final grade. The firm must list scheme development factors that are essential to the success of the project on the price and timeline that they submit.

To assist in the examination, evaluation and comparison of proposal, CBC may ask the Consultant online for clarification of its Proposal. The request for clarification and the response shall be in writing and no change in price or substance of the Proposal shall be sought, offered, or permitted.

CBC shall arrange for Question and Answer (Q & A) session on 30th January 2024 from 2:00 to 3:30 pm CAT to ensure that all vendors have a clear understanding of the Terms of Reference. To access the meeting link of the Q & A session, please contact procurement@comesabusinesscouncil.org expressing your interest to attend the meeting.

CBC shall examine the Proposals to determine whether they are complete, whether any computational errors have been made, whether the documents have been properly signed, and whether the Proposals are generally in order.

Arithmetical errors shall be rectified on the following basis: If there is a discrepancy between the unit price and the total price that is obtained by multiplying the unit price and quantity, the unit price shall prevail and the total price shall be corrected. If the firm does not accept the correction of errors, its Proposal shall be rejected. If there is a discrepancy between words and figures, the amount in words shall prevail.

Prior to the detailed evaluation, the Procurement Committee shall determine the substantial responsiveness of each Proposal to the Request for Proposals (RFP). For purposes of these Clauses, a substantially responsive Proposal is one, which conforms to all the terms and conditions of the RFP without material deviations. CBC's determination of a proposal's responsiveness is based on the contents of the Proposal itself without recourse to extrinsic evidence.

A Proposal determined as not substantially responsive shall be rejected by the CBC and may not subsequently be made responsive by the firm by correction of the non-conformity.
The bids shall be evaluated as follows:

a) The email that has technical and financial offers shall be opened.
b) The "TECHNICAL PROPOSAL" shall be opened, and the technical proposal shall be evaluated.
c) If the technical proposal is evaluated as 70 per cent (70%) or above the "FINANCIAL PROPOSAL" shall be opened.
d) The firm that has offered what is adjudged to be the best technical and financial offer shall be offered the contract.
e) If the firm that offered what was adjudged to be the best technical and financial offer declines to accept the offer, then the firm that is adjudged to have offered the second best technical and financial offer shall be offered the contract.

In evaluating the relative merits of firm's bidding for the project, the evaluation panel shall consider:

a) Understanding of the terms of reference and requirements of the assignment (10%),
b) Demonstrated experience of the firm and sample of past assignments carried out by the firm in the field of study at regional level (Africa) (25%),
c) The proposed approach and methodology to be applied by the Consultancy firm, including workplan with timelines (35%),
d) Qualification, competence and relevant experience of lead consultant and rest of the team (30%).

11. REPORTING AND MANAGEMENT

The firm shall work under the direct supervision of the CBC Chief Operating Officer- DFI Program, to implement the COMESA Digital Retail Payments Platform And/Or Fraud Management Module for the eight (8) pilot countries and under the overall management of the CBC Chief Executive Officer.

a) The Chief Executive Officer shall provide quality assurance and ensure that the Payments Platform is evaluated and meeting all the technical specifications.
b) The Chief Executive Officer shall ensure that the firm receives all relevant documentation with respect to CBC Guidelines, Rules, and Regulations necessary for the execution of the tasks.

12. CONTRACT

A formal contract specifying the scope of the assignment shall be prepared and signed between CBC and the firm prior to the beginning of the assignment. The contract shall also clearly spell out the responsibilities of the two parties.

13. PRICING

All prices MUST be indicated in USD. There will be a no price variation of the contract after signing of contract except upon a mutual written agreement between the two parties. Prices must be exclusive of all taxes within Zambia.

14. AWARD OF CONTRACTS

COMESA Business Council reserves the right to wholly or partially reject or award this contract to any bidder and has no obligation to award this contract to the lowest bidder.

15. REJECTION OF PROPOSALS

Any proposal received by CBC after the closing date and time shall be rejected.

16. TECHNICAL QUERIES

For any technical queries related to the specifications of work or TORs, kindly contact: procurement@comesabusinesscouncil.org.

17. DISCLAIMER

COMESA Business Council does not bind itself to accept any proposal and reserves the right to accept the whole or partially any of the submitted proposals.

18. SUBMISSION

Proposals from consultancy firms must be **emailed** to the address below on or before 13th February 2024 **at 17.00 hours**, CAT.

The Chairperson- Procurement Committee
COMESA Business Council
COMESA Secretariat Building
Ben Bella Road
P.O. Box 30051 Lusaka, Zambia.
Tel: (260) 211 229725.
Fax: (260) 211 225107
Email: procurement@comesabusinesscouncil.org

a) The Technical Proposal should include the following:
   i. Updated profile of the firm including CVs of key experts who will work on the project.

ii. Detailed understanding of the task and highlighting experience, especially by the Key Experts, and expertise in similar works as well as a detailed approach and methodology for carrying out the assignment including an outline of the supporting documents/ projects and their references.

iii. Copies of academic and professional qualifications of key experts.

b) The Financial Proposal shall be in line with Article 10 of this RFP.

NOTE: The firm has the option to bid for both lots or one lot. However, it's strongly advised to consider a joint venture with another firm bidding on the other lot if the firm opts to bid for only one lot (in order to have seamless coordination during implementation).