

Central Bank of Lesotho



REQUEST FOR PROPOSAL (RFP)

**RFP TITTLE:
ACQUISITION OF A CLOUD-BASED RISK AND
COMPLIANCE MANAGEMENT SYSTEM**

**RFP No:
CBL/FNC/C/TC/09/2022**

**ISSUE DATE:
05th AUGUST 2022**

Contact person:

Name: 'Matsepo Lechela
Title: Secretary, Tender Committee
Phone (266) 22232126
Fax number: (266) 22310051/22310679
Email: mlechela@centralbank.org.ls

August, 2022

1 Table of contents

2 Contents

1	TABLE OF CONTENTS	2
3	TERMINOLOGY FOR THIS RFP	4
4	LIST OF ACRONYMS	4
5	INTRODUCTION	5
6	PROJECT OBJECTIVE	5
7	SCOPE OF WORK	6
8	ORGANISATIONAL STRUCTURE	6
9	SYSTEM FUNCTIONAL REQUIREMENTS	8
9.1	RISK MANAGEMENT (3 ADMIN, 30 USER ACCESS RIGHTS)	8
9.2	INCIDENT MANAGEMENT MODULE (3 ADMIN, 30 USER ACCESS RIGHTS)	9
9.3	COMPLIANCE MANAGEMENT MODULE (3 ADMIN, 10 USER ACCESS RIGHTS)	10
10	TECHNICAL REQUIREMENTS	12
10.1	INSTALLATION	12
10.2	TECHNOLOGY SOFTWARE	12
10.3	SYSTEM PLATFORM	12
10.4	SYSTEM FEATURES.....	13
11	PROJECT IMPLEMENTATION REQUIREMENTS	14
11.1	IMPLEMENTATION STRATEGY	14
11.2	FUNCTIONAL TRAINING AND TECHNICAL SUPPORT.....	15
12	PROPOSAL PREPARATION (PROPOSAL FORMAT)	16
12.1	TECHNICAL PROPOSAL	16
12.2	FINANCIAL PROPOSAL.....	60
13	REQUEST FOR PROPOSAL PROCESS	60
13.1	CONTACT PERSONS.....	60
13.2	CLARIFICATION	60
13.3	ELIGIBILITY	60
13.4	DELIVERY OF PROPOSALS.....	60
13.4.1	<i>Technical Proposal</i>	60
13.4.2	<i>Financial Proposal</i>	61
13.5	DEADLINE FOR THE SUBMISSION OF TECHNICAL PROPOSALS	61
13.6	OPENING OF TECHNICAL PROPOSALS	61
13.7	EVALUATION OF PROPOSALS AND SELECTION	61
14	EVALUATION CRITERIA	61
14.1	MANDATORY EVALUATION CRITERIA	61
14.2	TECHNICAL EVALUATION CRITERIA.....	62
14.2.1	<i>TECHNICAL PROPOSAL EVALUATION CRITERIA</i>	62
14.2.2	PITCH EVALUATION CRITERIA.....	63
14.3	FINANCIAL EVALUATION	64
14.4	SELECTION FOR AWARD (LEAST COST BASED SELECTION)	65
15	TERMS AND CONDITIONS OF THE RFP	65
15.1	PROPOSAL VALIDITY & FIRM PRICING	65

15.2	CURRENCY.....	65
15.3	TAXES.....	65
15.3.1	<i>Value Added Tax</i>	65
15.3.2	<i>Withholding Tax</i>	65
15.4	OWNERSHIP OF PROPOSALS	65
15.5	CONFIDENTIALITY OF INFORMATION	66
15.6	AMENDMENT OF RFP DOCUMENT	66
15.7	TECHNICAL FACILITIES.....	66
15.8	COSTS OF RESPONDING	66
15.9	BACKGROUND CHECK	67
15.10	PERFORMANCE BOND	67
15.11	HEALTH AND SAFETY.....	67
15.12	LANGUAGE OF THE PROPOSAL.....	67
15.13	JOINT VENTURE	67
15.14	WITHDRAWAL, SUBSTITUTION AND MODIFICATION OF BIDS.....	68
15.15	ACCEPTANCE AND/OR REJECTION OF PROPOSALS.....	68

3 TERMINOLOGY FOR THIS RFP

Throughout this RFP, the terminology is used as follows:

- **“Bank”** means the Central Bank of Lesotho;
- **“Contract”** means the written agreement resulting from this RFP executed by the Bank and the Consultant;
- **“Service provider/ vendor”** means the successful Proponent to this RFP who enters into a written Contract with the Bank;
- **“Must”, or “Mandatory”** means a requirement that failure to meet shall result in disqualification.
- **“Business units”** refers to individual departments and divisions within the CBL
- **Recovery Point Objective:** A point to which information used by a process/ service/activity may be restored to enable the activity to operate following a disruption.
- **Recovery Time Objective:** A period of time following a disruptive event within which a service/ product or activity can be resumed.

4 LIST OF ACRONYMS

ACRONYM	DEFINITION
API	Application Programming Interface
BCI	Business Continuity Institute
BCM	Business Continuity Management
CBL	Central Bank of Lesotho
CM	Compliance Management
ERM	Enterprise Risk Management
GPG	Good Practice Guidelines
ICT	Information Communication Technology
PESTEL	Political, Economic, Social, Technological, Economic and Legal context
RFP	Request for Proposals
RM	Risk Management
SWOT	Strengths, weakness, opportunities and threats
UAT	User Acceptance Testing

5 INTRODUCTION

The Central Bank of Lesotho requires the services of a competent company to provide and implement a “Risk and Compliance Management information technology system” to automate the risk management (RM), incident management (IM) and compliance management (CM) processes that complies with relevant international standards.

Although the Central Bank of Lesotho has been using the manual tools such as excel spreadsheet and word to undertake risk assessments, compliance risk assessment and quarterly reporting, the method has proved to be challenged by increased scope of work, the hybrid working model, as well as the increasing requirements for timely and accurate information to manage uncertainties. These challenges have therefore highlighted the need for a capable information technology system that can lower the turnaround times for risk assessments and reporting to 1-2 weeks, with interactive dashboards, tasks notifications, and mobile app to enable CBL to adapt to the current and future risk landscape.

The Central Bank of Lesotho therefore invites proposals from suitably qualified service providers to implement this project and provide initial training to administrators and users of the system.

6 PROJECT OBJECTIVE

The CBL aims to procure the information technology solution that aid effective management of a wide spectrum of risk exposures across its business departments. The system must be able to interface with the email systems, be highly scalable and flexible to adapt to growing demands of the business. The complete integrated system should be able to meet the following objectives:

- Improve integrity, access and safety of information
- Improve efficiency of RM, IM and CM
- Cost savings on resources
- Improve maturity of the two functions
- Improve overall business performance

- Improve overall business resilience

7 SCOPE OF WORK

In consultation with Central Bank of Lesotho, the preferred service provider is expected to provide a cloud-based integrated system with Risk Management, Incident Management and Compliance Business modules that meet the CBL risk assessments, analysis and reporting requirements. The scope of the project includes but not limited to:

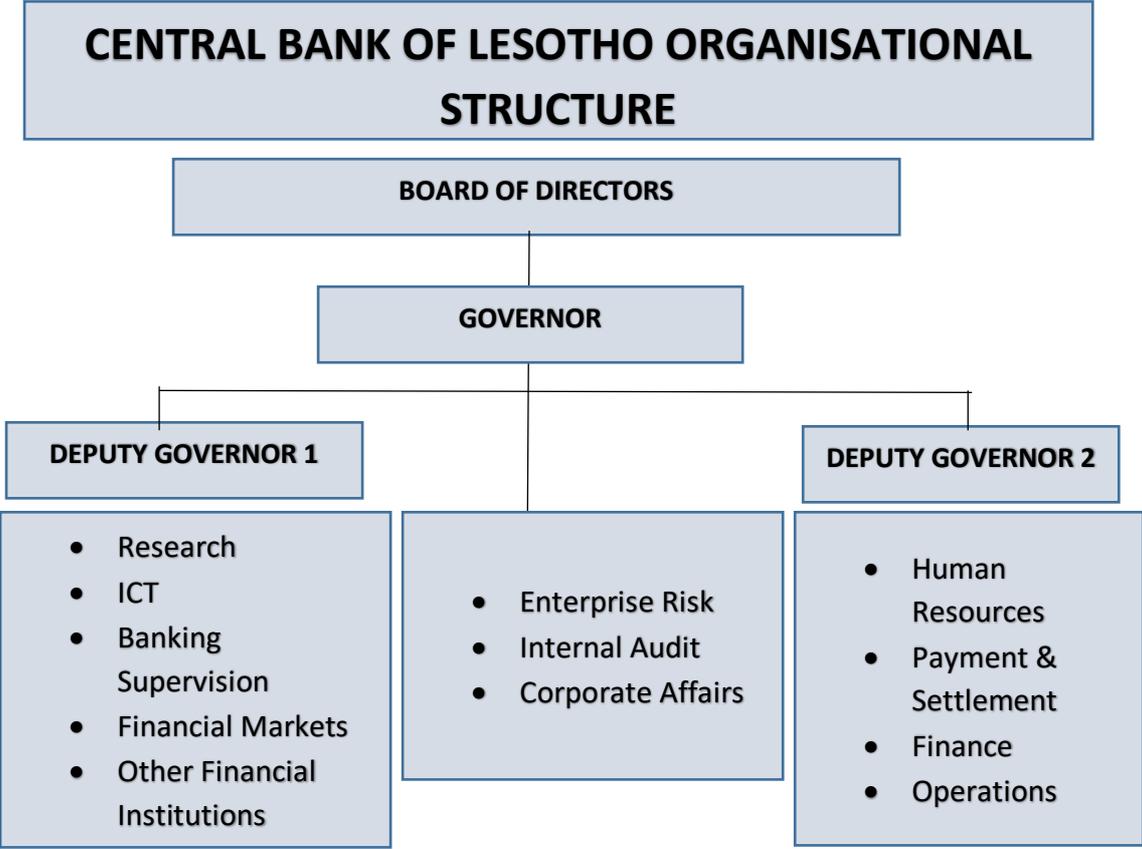
- a) Documenting and understanding the system requirements.
- b) Defining the customizable solution based on the given requirements.
- c) Configuring and testing the cloud based system
- d) Deploying and commissioning the solution
- e) Providing user and administrator trainings.

It is also of importance that the preferred vendor provides functional, technical and end-user training manuals for both business users and IT support staff.

8 ORGANISATIONAL STRUCTURE

Prescribed by the Central Bank of Lesotho Act 2000, CBL is governed by the Board of Directors, consisting of the Governor, two (2) Deputy Governors and five (5) non-executive Directors to oversee policy formulation and administrative issues of the Bank. Currently there are twelve (12) functional departments responsible for various tactical and operational business functions including management of related risks. Going further down the organisational structure comprises of forty-two (42) divisions from which most Risk Champions are drawn.

Figure 1: Central Bank of Lesotho Governance Structure



9 SYSTEM FUNCTIONAL REQUIREMENTS

9.1 RISK MANAGEMENT (3 Admin, 30 user access rights)

The CBL risk management framework seeks to provide a structure and systematic approach to implementing risk management on an enterprise-wide basis that is compatible with international risk management standards such as ISO 31000, COSO ERM, The Orange Book, ISO 31010 risk techniques, Institute of Risk Management South Africa best practice guidelines, King IV on risk governance as well as other internationally recognized RM standards. Therefore, CBL aims to acquire a system that will provide a centralized risk repository to document and define strategic objectives, business processes and projects together with the risk assessments, controls and mitigations. The system must further be able to route the results of both the bottom-up and top-down risk assessments to respective heads of departments for review and approvals. Specifically, the risk management module must be capable of automating the risk management process as prescribed by ISO 31000 (2018) below.

- i. Environmental scan:** The system must be able to capture and consider the CBL strategic and operational objectives, key drivers and trends having impact on the organisational objectives, values perceptions and relationships with stakeholders, as well as external political, economic, technological, social and legal influences.
- ii. Risk identification:** This system should enable the forward-looking and proactive anticipation, recognition and recording of all material risk events that may help or hinder the achievement of strategic, tactical and operational objectives of CBL using predictive metrics and key risk indicators. The system must align the risk events to the existing risk category matrix, while maintaining the relationships between risks, processes and strategic objectives.
- iii. Risk Analysis:** The system must enable advanced multi-factor risk scoring matrix based on both qualitative and quantitative parameters of likelihood, impact and other relevant measures. As much as possible, the risk analysis should include quantitative cost risk analysis (QCRA) techniques such as Monte Carlo simulation, scenario analysis and sensitivity analysis utilizing various risk probabilities and impacts (minimum, most likely, and maximum). These functionalities are geared towards assisting CBL with more

objective risk analysis and clear visibility of the organization's top risks. The risk analysis should also include control assessments as well as control design and effectiveness tests.

- iv. Risk Evaluation:** The results of the risk analysis shall be evaluated against the established financial and operational impact, risk appetites and tolerances. The system must be able to seamlessly incorporate the key risk indicators (KRIs), risk appetites statements and tolerances at this stage of risk management process.
- v. Risk Treatment:** The system must enable the development, monitoring, review and periodic reporting of status on all risk (hazards, uncertainties and opportunities) response measures with clear lines of accountability. The system should further enable the categorization of risk response options of risk acceptance, treatment, termination, exploitation as well as transfer.
- vi. Risk reporting:** The system must enable a multi-dimensional, interactive and real-time reporting of risk information to various organisational structures and hierarchies using advanced analytics, charts, heat maps and dashboards for timely risk-informed decisions. These include options to view organization's aggregated risks, view by business units/departments, processes, strategic objectives, impacts as well as probabilities. The system should further slice and dice data based on the user requirements, filter and track movement from inherent to residual risk in view of control effectiveness.
- vii. And any other applicable functionalities** that may be deemed necessary.

9.2 Incident Management module (3 Admin, 30 user access rights)

The CBL Incident management and reporting framework's objective is to facilitate the coordinated, standardized, integrated and comprehensive reporting of all unplanned events of any kind that disrupts or reduces the quality of service, or threatens to do so, for the purpose of:

- Timely informing the Executive and departmental management about the occurrence of an incident.
- Ensuring that prompt decisions and actions are taken to mitigate future reoccurrence
- Establishing the central repository for all incidents and related information
- Serve as inputs into the key risk indicators (KRIs)
- Therefore, the system is expected to enable business departments to:

- Log the identified incident together with relevant cause, impact, proposed response actions and time lines for implementation into the system and the responsible action owner.
- Escalate the incident to the relevant divisional and departmental heads for sign-off.
- Automatically update the incident management central database and notify the ERMD
- Register the action plans into the system which should automatically notify the implementing business unit owner.
- Provide reporting functionalities with options to view organization's aggregated incidents, view by business units/departments, processes, strategic objectives, impacts as well as proposed actions and implementation periods. The system should further slice and dice data based on the user requirements.

This will enable ERMD to escalate major incidents to Executive for decisions, monitor the action plans, including reporting the progress.

And any other applicable functionalities that may be deemed necessary.

9.3 Compliance Management module (3 Admin, 10 user access rights)

The CBL compliance management framework seeks to provide a structure and guidelines implementing Bank-wide compliance management that is compatible with generally accepted Compliance Practices, Compliance Institute of South Africa Best Practice Guidelines, King IV on risk governance as well as other internationally recognized compliance standards. Therefore, CBL aims to acquire a system that will provide a centralized compliance repository to document and define strategic objectives, business processes, Compliance universe together with the compliance risk identification, assessments, controls, and mitigations. The system must further be able to route the results of compliance risk assessments to respective compliance champions and heads of departments for review and approvals. Specifically, the compliance management module must be capable of automating the compliance management process as defined in the Generally Accepted Compliance Practices (GACP) inclusive of principles, standards and guidelines.

- i. Regulatory Compliance Universe:** The system must enable easy capturing, storage, and access to the legal and regulatory register (Compliance Universe) relevant to CBL as well

as international standards, frameworks and policies that have compliance implications for CBL. The system must further issue automated notifications and alerts on the actions and reporting requirements, breaches and content updates to departmental managers.

- ii. Compliance Risk identification:** This system should enable the forward-looking and proactive anticipation, recognition and recording of all material compliance risk events that may help or hinder the achievement of strategic, tactical and operational objectives of CBL using predictive metrics and key risk indicators. The system must have compliance assessment templates, assign responsibilities, controls self-assessments and effectiveness tests, record result and remedial actions.
- iii. Compliance Risk Analysis:** The system must enable an advanced multi-factor risk scoring matrix based on both qualitative and quantitative parameters of likelihood, impact, and other relevant measures. As much as possible, the risk analysis should include quantitative cost risk analysis (QCRA) techniques such as Monte Carlo simulation, scenario analysis, and sensitivity analysis utilizing various risk probabilities and impacts (minimum, most likely, and maximum). These functionalities are geared towards assisting CBL with more objective risk analysis and clear visibility of the organization's top risks. The risk analysis should also include control assessments as well as control design and effectiveness tests.
- iv. Compliance Risk Evaluation:** The results of the risk analysis shall be evaluated against the established financial and operational impact risk appetites and tolerances. The system must be able to seamlessly incorporate the key risk indicators (KRIs), risk appetites statements, and tolerances at this stage of the compliance risk management process.
- v. Compliance risk response monitoring:** The system must leverage on artificial intelligence to track legislative and policy updates from multiple regulators, identify control issues, create response plans, route them for reviews and approvals, track mitigation progress on real-time, and enable reporting compliance breaches with direct notifications.
- vi. Risk reporting:** The system must enable a multi-dimensional, interactive, and real-time reporting of Compliance status to meet the needs of various governance structures of the Bank using advanced analytics, charts, heat maps, and dashboards for timely risk-informed decisions. These include options to view the organization's compliance universe, annual plan, compliance profile, departmental compliance risk management plans(CRMPs), view by business units/departmental champions, processes, strategic

objectives supported, impacts as well as probabilities. The system should further slice and dice data based on the user requirements, filter, and track movement from inherent to residual risk in view of control effectiveness.

vii. And any other applicable functionalities that may be deemed necessary.

c) **Reporting:** The system must have built-in integrated, interactive and real-time reporting with configurable workflows, dashboards, and report templates to enable quick analysis and gap identifications.

d) **And any other applicable** functionalities that may be deemed necessary.

10 TECHNICAL REQUIREMENTS

10.1 INSTALLATION

Installation of the system should be an “on-cloud hosting”

10.2 TECHNOLOGY SOFTWARE

The system should support Web and mobile environments, as well as Hyper Text Transfer Protocol Secure (HTTPS).

10.3 SYSTEM PLATFORM

a) **Server**

Cloud hosting

b) **Client**

The Bank users use laptops and desktops that run on windows 10 and are connected to the main network through Wi-Fi or Ethernet. The bidder is expected to provide technical and functional specifications and quantity for the PCs, CPU, Memory, Storage and Network to ensure the system’s optimal performance.

c) **Printers**

The Bank runs a number of networked printers that are shared amongst users. There is still a small number of standalone printers, but shared printing is the preferred arrangement. The system supplier is expected to provide technical and functional specifications and quantities of printers needed for the system.

10.4 SYSTEM FEATURES

a) **Response time and throughput**

Shortest possible time between user action and response from the system, with at-least 20 users concurrently logged on.

b) **Controls and Monitoring**

Ability to, among others, operate on a business date basis, support business calendar, referential integrity, data entry integrity and validation checks, with the ability to customize password policies.

c) **User Interfaces**

- i. User-friendly system with graphical user interface features. Menu driven system, giving users easy access to functions, including customization of tool bars.
- ii. The system should also provide additional interfaces to system administrators to perform technical and administrative support functions, among others.

d) **Communication Interface**

The system should support interfacing with the Bank's internal mail system (MS Office 365) and should have the ability to attach and reference electronic data.

In addition, the system should be able to interface with other systems within the CBL if need be

e) **System Tools**

The system must support the following functionalities/tools

- i. Inputs and view by nominated business unit Risk and Compliance Champions to granular level functionality;
- ii. Notifications and reviews by supervisors (Head of Department) without prejudice of such information to ERMD
- iii. Easy archiving and retrieval of historical data;
- iv. Provision of a detailed audit trail functionality, where all actions/changes are logged with date, time, changes, users etc.
- v. Provision of context-sensitive on-line help;
- vi. Report writer for customization of reports;
- vii. Standard reports with drill-down capabilities across all levels
- viii. Reports with search, filter and sort features;
- ix. Scheduling of risk and compliance action plans, including, but not limited to report generation at specific times or event driven;

f) **Workflow and Document Management**

Storage of documents, including, but not limited to agreements with business functions and suppliers, authorization and escalation of information among different roles players.

g) **System Security**

- i. Data encryption when in rest mode, as well as during transmission and multi-factor authentication, among others;
- ii. Prevention of concurrent multiple-entry logging by any single user;
- iii. Have two-factor authentication
- iv. Enable approval and review functions by supervisors
- v. Availability of online “self-manage password” services;
- vi. Minimized mean-time-to-repair (MTTR), such that recovery entails only starting up the database and application with only a few checks.

11 PROJECT IMPLEMENTATION REQUIREMENTS

11.1 IMPLEMENTATION STRATEGY

The overall project management responsibilities of this project will be overseen by the CBL. The CBL has adopted PRINCE 2 as a project management methodology of choice; therefore, the bidder is expected to conform to the PRINCE 2 reporting standards.

The following are deemed important in the implementation of the project:

- a) The project management will consist, at a minimum, of a project plan, project governance, change management and project risk management along with key project team personnel. Detailed breakdown structure of the implementation using Gantt Chart, as a minimum, shall be provided by the bidder to CBL to be assimilated into the overall plan;
- b) While the overall responsibility of the program management will be with CBL, the bidder is expected to dedicate adequate resources for the successful implementation of the project. As far as possible, and for better coordination, the bidder shall have a dedicated project manager for the duration of the project. The proposed replacement of any key personnel will require prior consent;

- c) The implementation may be virtual with functional and technical training to be conducted on specific modules of the system and targeted to project team members who will be from different offices based on their roles and responsibilities;
- d) Installation, configuration, testing and implementation services in three (3) environments, including Development (DEV), Test (TST), and live (PRD).
- e) In UAT, testing should be conducted based on the business/user requirements as defined in this RFP. The testing will support all possible business processes, which could happen in the system. The testing will include integration with the email system.
- f) For data migration, the bidder MUST provide clear written guidelines for migrating data from the manual systems to the proposed Risk and Compliance Management system.

11.2 FUNCTIONAL TRAINING AND TECHNICAL SUPPORT

- a) The Bidder shall provide onsite/ virtual functional, technical, and end user training.
 - i. Functional Training** - Classroom / virtual sessions on all required modules for the Project Team (RM, and CM system administrators/ super users) around the time of system installation. This training should include configuration, processing, query, and reporting aspects of the system. Training materials should be designed and provided to the participants;
 - ii. Technical Training** - Classroom / virtual sessions for CBL ICT technical staff on the system aspects like data organization, customization and interfacing with email and other internal systems. The training should include installation and maintenance aspects of the system. The training should be given to the Project Technical Team around the time of product installation. Training materials should be provided to the participants;
 - iii. End User Training** – Classroom/ virtual sessions for End Users (Risk Champions and Compliance Champions together with the inquiry users) prior to going live.

- b) The winning Bidder shall provide to the CBL all current and relevant default user manuals, security, API and operations documentation for the selected modules, within one week after contract signature. All documents related to the project such as business process maps, functional and technical specifications and training resources must be in hard and soft copies and provided to CBL. The Bidder and CBL are required to participate in this process. All final relevant manuals/documentations related to the system shall be provided to CBL.

- c) Support and Maintenance Requirements
 - i. Go-live support
 - ii. Prepare a checklist for readiness to go live and verify status and work with the project team to address lack of readiness. (The Bidder's implementation team should provide the plan for going live in the initial phases of the project to avoid late surprises.)
 - iii. Work with the project team to execute the cut over plan.
 - iv. Advise and work with the project team to address issues before going live.
 - v. Post go-live, assign issues the highest priority for resolution and escalate issues quickly and to the right party within the Bidder's company.
 - vi. Maintenance/Services, Methodology
 - vii. The Bidder is required to provide, at a minimum, coverage of CBL's hours of operation with multi-level support with various communication channels such as phone, email, and instant messenger. A 24/7 system availability required and support is desirable.
 - viii. Any new version (major or minor or patch) release on the product by the bidder can be optimally opted by CBL to be implemented in their installations. During implementation, all required technical, functional documentation and support/training should be provided.

12 PROPOSAL PREPARATION (Proposal Format)

12.1 TECHNICAL PROPOSAL

Evaluation of proposals is made easier when proponents respond in a similar manner. The following format and sequence should be followed in order to provide consistency in proponent responses and to ensure that each proposal receives full consideration:

a) The proposed solution/system

In this part of the proposal the Proponent shall clearly provide details of the solution proposed, explain how it meets the functional requirements and summarize concisely its suitability to the CBL environment. Proponents are also requested to fully fill/ respond to the requirements matrix in the subsequent section.

b) Project Plan and detailed project approach

A detailed project plan should be mapped, indicating the duration of the project. The proponents are required to detail the approach or process they propose to deliver the project and where possible indicate in stages, as well as key deliverables to be achieved at each stage. The training offering, project implementation capabilities and support and maintenance offering should be clearly indicated as part of the approach.

c) Proponent Financial capability

Proponents should demonstrate their financial capability to meet their financial obligations under the assignment. A Recent financial statement of the bidder duly signed by an Audit Firm or practicing Chartered Accountant for the past two years or a credit line letter from an authorized Financial Institution should be provided. The bidder's financial statements should be unqualified and show no financial losses in the most recent financial years or the bidder's credit line letter from an authorized Financial Institution should indicate a positive credit /loan support.

d) Proponent Experience

Proponents should provide a brief summary of their suitability, outlining specifically the proponent's track record and nature of assignments relevant to this project. The proponent's relevant experience in the last five years should be supported by a minimum of two reference letters.

e) Project Implementation Team Composition

The composition of the implementation team for the project should be clearly shown and the roles they will play. A Curriculum Vitae (limited to 3 pages) for each professional staff and key sub-professional team members should be provided and should show clearly following details:

- Name, Age, Nationality and Position in Team;
- Educational Qualifications;
- Professional Qualifications (professional registration, societies, honours, publications
- Experience implementing similar projects

(The Team Leaders should possess experience of at least 3 years in assignments of similar nature.)

f) MANDATORY DOCUMENTS (REQUIRED AS PART OF THE PROPOSAL):

The proponents should have the following documents as attachments to their proposals:

Requirement	Supported by:
Trading compliance	Valid copy of the trader's license or company registration certificate issued by each proponent's inland registrar of companies.
Tax Compliance	Valid copy of the tax clearance certificate or Tax Compliance Certificate issued by each proponent's Inland tax authority. E.g SARS or LRA.
Letter of Introduction	One-page letter of introduction identifying the proponent (proponent's name and physical address together with contact details; contact person, telephone number and e-mail address) and signed by the person or persons authorized to sign on behalf of, and bind the proponent to statements made in the proposal.

Proponents should provide actual documents in the manner requested. Provision of a Link or Website referring the Bank to access the documents shall not be accepted.

g) Proponents should fully fill and/or respond to the questions on the attached forms as follows:

- Form 1: Instructions to Bidders
- Form 2: Company Background
- Form 3: Functional Requirements Matrix
- Form 4: Technical Requirements Matrix

FORM 1: INSTRUCTIONS TO BIDDERS

PROJECT: RISK AND COMPLIANCE MANAGEMENT SYSTEM

NAME OF Vendor/Service provider: _____

INSTRUCTIONS TO SERVICE PROVIDER(S):

- Service Provider shall fill-up the “Name of Service provider/Vendor” above, and the availability column.
- Each Service provider shall identify the Availability of the Central Bank of Lesotho's specifications based on the following:
 - (i) Available (A): Requirement is fully available
 - (ii) Unavailable (U): Requirement Not Available
 - (iii) Partially Available (P): Requirement ONLY partially available
- For all questions as identified in the requirement matrix, Service provider must ensure, along with their responses, to check either:
 - (i) 1 = Core Risk and Compliance Management
 - (ii) 2 = Optional/modular add-on (MUST specify which module or add-on)
- Each Service provider must respond to every stated request or requirement providing very clear description and explanation on how the system complies with the requirement. The Service provider should identify any substantive assumption made in preparing its responses.
- Failure to provide an answer to an item with complete descriptive response will be viewed as non-responsive. Where a requirement is Partially Available or Unavailable, the Service provider must indicate / describe what is partially supported and what is not supported, clearly providing its reasons and explain its proposed alternative, if applicable, and the advantages and disadvantages to CBL of such proposal.

FORM 2: COMPANY BACKGROUND

COMPANY BACKGROUND		
REFERENCE NO.	QUESTIONS/REQUIREMENTS	
CB	COMPANY BACKGROUND	DESCRIPTION
COR	CORPORATE	
CB-COR-01	How many subsidiaries does your company have, and in which regions are they located?	
CB-COR-02	From which location/subsidiary will the Central Bank of Lesotho be receiving services?	
CB-COR-03	What percentage of the company's annual revenue is sale of risk management systems	
CB-COR-04	Is your company involved in any merger or acquisition? Provide details, including expected timelines	
CB-COR-05	Please provide a copy of your audited financial statements for the past two years. Attach the financial statements and clearly label them exhibit "CB-COR-05"	

CB-COR-06	<p>Are there any other finance-related challenges that will affect implementation of Risk and Compliance management system?</p> <p>If Yes, provide details.</p>	
CLM	CLIENT MANAGEMENT	
CB-CLM-01	How many Central Bank clients do you have, and how many of them are in Africa?	
CB-CLM-02	How long ago was you last business relating to supply of risk and compliance management systems?	
CB-CLM-03	How many of your current clients still use risk and compliance management systems supplied by your company?	
CB-CLM-04	<p>Having supplied many of your clients with this or similar solutions in the past, do you believe you satisfied all their needs so much that the challenges they used to face before implementation are no longer there?</p> <p>Provide details.</p> <p>Please attach a minimum Two (2) positive reference letters from Clients that were provided with a similar service in the last five years.</p> <p>The reference letters should clearly indicate the duration of association and the contact details of the client for verification.</p>	
LEG	LEGAL	

CB-LEG-01	<p>Has there ever been any litigation against your organization initiated by any of your clients?</p> <p>If yes, please provide details and results for each, as well as the status of those that are still outstanding.</p>	
CB-LEG-02	<p>Have any of your risk and compliance management systems projects been terminated prior to completion? If yes, please provide details.</p>	
CB-LEG-03	<p>Has your organization ever filed for bankruptcy?</p>	
GEN	GENERAL	
CB-GEN-01	<p>What are the primary benefits to your organization if you get this contract awarded to you?</p>	
CB-GEN-02	<p>What is the competitive advantage does you company have over other in terms the product?</p>	
CB-GEN-03	<p>Please describe other specific challenges that you may face in the implementation of this project.</p>	

FORM 3: FUNCTIONAL REQUIREMENTS MATRIX

FUNCTIONAL REQUIREMENTS		Offerror's Response			
REFERENC E NUMBER	QUESTIONS/REQUIREMENTS	AVAILIB ILITY (A) - Available (U) - Unavailabl e (P) - Partially Available	FUNCTION ALITY (1) - Core RM & CM (2) - Optional / modular add- on	If (2) Optional /mo dular add-on, MUST specify which module or add-on	1) Please provide clear description and explanation on how the system complies with the requirement. Where applicable, provide evidence. 2) Where Partially Available or Unavailable, describe what is partially supported and what is not supported explaining proposed alternative, if applicable, and the advantages and disadvantages to the Central Bank of Lesotho of such a proposal.
RM	RISK MANAGEMENT	A / U / P	1 / 2	ADDITIONAL MODULE	DESCRIBE THE SYSTEM'S FEATURE

RMP	RISK MANAGEMENT PROCESS				
RM-RMP-01	Does your system support environmental scan? (SWOT, PESTEL)				
RM-RMP-02	Does the system support the risk identification with root cause analysis and type of consequences the CBL is likely to suffer? If Yes, provide the list of RM techniques your system offers (Bow-tie, Cause-Impact analysis etc)				
RM-RMP-03	Does the system support both qualitative and quantitative risk analysis? Please provide the evidence as Exhibit "RM-RMP-03"				
RM-RMP-04	Does the system have functional capability to perform quantitative analyses such Monte Carlo simulation, scenario analysis and sensitivity analysis				
RM-RMP-05	Does the system support internal controls assessments?				
RM-RMP-06	Does the system support the inclusion of risk appetite and tolerances in the risk evaluation? Please attach the evidence and label the attachment "Exhibit RM-RMP-05 ".				

RM-RMP-07	Does the system support the risk ratings at both inherent and residual levels?				
RM-RMP-08	Does the system support the aggregated risk calculation and ratings?				
RM-RMP-09	Does the system support various risk response strategies?				
RM-RMP-10	Does the system support development, implementation, review and monitoring of risk mitigations?				
RM-RMP-11	Does the system support allocation of risk mitigation responsibilities to risk owners and have implementation timelines?				
RR	RISK REPORTING				
RM-RR-01	Does the system support multi-dimensional, interactive and real-time reporting of risk information to various organisational structures and hierarchies with charts, heat maps and dashboards for timely risk-informed decisions? These include options to view organisation's aggregated risks, view by business units/departments, processes, strategic objectives, impacts as well as probabilities. The system should further slice and dice data based on the user requirements, filter and track movement from inherent to residual risk in view of internal controls effectiveness.				
	a) Does the system allow use of advanced analytics?				

	b) Does the system supports real-time reporting to various governance structures?				
	c) Does the system allow use of charts, heat maps and dashboards in displaying risk information?				
	d) Does the system support various drilling-down of information, slicing and dicing it to suit different stakeholders?				
	e) Does the system support exporting of reports to Microsoft office formats such as word, excel and power point?				
	Does the system support aggregated organization-wide risk profile?				
	Is the system capable of hosting various functional risk registers?				
IMR	INCIDENT MANAGEMENT AND REPORTING	A / U / P	1 / 2	Additional Module	DESCRIBE THE SYSTEM'S FEATURE
IM	INCIDENT MANAGEMENT				
IMR – IM-01	Does the system offer incident reporting template? Please provide the template marked as exhibit “ IMR – IM-01 ”				
IMR – IM-02	Does the system support the identification of a loss event, its cause and impact?				
IMR – IM-03	Does the system able to map the incident to the specific risk category, and key risk indicators?				

IMR – IM-04	Does the system support various authorization of an incident (At-least 2 levels)?				
IMR – IM-05	Does the system support development of incident prevention plans, monitoring and reporting?				
IMR – IM-06	Does the system support rating and escalation of incidents?				
CM	COMPLIANCE MANAGEMENT	A / U / P	1 / 2	Additional Module	DESCRIBE THE SYSTEM'S FEATURE
CMP	COMPLIANCE MANAGEMENT PROCESS				
CM-CMP-01	Does the system support the aggregation of organization-wide compliance universe?				
CM-CMP-02	Does the system support automation of legislation updates and alerts?				
CM-CMP-03	Does the system support capturing, storage and easy access to legal and regulatory registers? Please provide template as Exhibit “CM-CMP-03”				
CM-CMP-04	Does the system support the compliance risk identification with root cause analysis and type of consequences the CBL is likely to suffer?				
CM-CMP-05	Does the system support both qualitative and quantitative compliance risk analysis? Please provide the evidence as Exhibit “CM-CMP-05”				

CM-CMP-06	Does the system support the compliance risk ratings at both inherent and residual levels?				
CM-CMP-07	Does the system support the aggregated compliance risk calculation and ratings?				
CM-CMP-08	Does the system support various compliance risk response strategies?				
CM-CMP-09	Does the system support development, implementation, review and monitoring of compliance risk mitigations?				
CM-CMP-10	Does the system support allocation of compliance risk mitigation responsibilities to various departmental compliance champions with implementation timelines?				
CM-CMP-11	Does the system support multi-dimensional, interactive and real-time reporting of compliance risk information to various organisational structures and hierarchies with charts, heat maps and dashboards for timely decisions? These include options to view organisation's aggregated compliance universe, view by legislation/ policy, standards departments, types of breaches, impacts as well as probabilities. The system should further slice and dice data based on the user requirements, filter and track movement from inherent to residual risk in view of internal controls effectiveness.				

CM-CMP-12	Does the system enable departments to track and manage their compliance program independently with notifications to the compliance function?				
FLX	FLEXIBILITY				
RP-FLX-01	Describe the ease and user skill required to create customized and user defined reports.				
RP-FLX-02	Does the system allow the user to alter standard formats and set user-defined templates for online reporting?				
RP-FLX-03	Does the system allow user-defined sorting and grouping for each report? Please list any limitations and which reports are not customizable.				
RP-FLX-04	Does the system support the generation of graphical reports (e.g. Plots, Histogram, Pie Chart, etc.)				
RP-FLX-05	Does the system have drill-down capabilities down to the lowest level? For example, the user reaches the per individual risk or legislation level.				
RP-FLX-06	Does the system have the capability to allow users to view a list of reportable data elements and drag/drop them to create ad-hoc reports?				
RP-FLX-07	Does the system allow users to run reports from the front-end by specifying various parameters, scheduling options and output formats?				

RP-FLX-08	Does the system have the ability to allow users to explore data and perform analysis - sorting, grouping, drill-down, slice and dice functions?				
RP-FLX-09	Does the system support the extraction of data into excel spreadsheets/PDF/CSV files, print and publish report, save reports?				
RP-FLX-10	Does the system have the capability to schedule periodic reports based on users' needs to monitor performance/progress and alert them about variations?				
RP-FLX-11	Does the system have the feature to generate Cross-tabulation and variance reports?				
RP-FLX-12	Does the system have an on-screen or on-line help facility?				
HDT	HISTORIC DATA				
RP-HDT-01	CBL policy requires that records be kept for at least 10 years. How much data can be stored online in the system and how far back can historical data be accessed?				
RP-HDT-02	Does the system allow users to retrieve and generate reports from online or archived data?				
RP-HDT-03	The system must store detailed historical risk and compliance information for historical reporting. What historical data is stored and at what level is data retained?				

RP-HDT-04	Does the system have the ability to store all historical reference information(environmental scans, risk causes and sources etc)				
RP-HDT-05	Does the system have the ability to store all relevant information on risk management framework, compliance policy, BCP, key risk indicators, tolerances limits, risk appetite statements, and compliance limits?				
RP-HDT-06	Does the system have the ability to store and provide online risk mitigation progress status reports, risk appetite status, compliance risk status as well as RTOs, RPO, and MTPD status reports after BCP testing and exercising?				

FORM 4: TECHNICAL REQUIREMENTS MATRIX

TECHNICAL REQUIREMENTS		Offerror's Response			
REFERENCE NO.	QUESTIONS/REQUIREMENTS	AVAILIBILIT Y (A) - Available (U) - Unavailable (P) - Partially Available	FUNCTIONALIT Y (1) - Core RMS (2) - Optional / modular add-on	If (2) Optional/modul ar add-on, MUST specify which module or add-on	1) Please provide clear description and explanation on how the system complies with the requirement. Where applicable, provide evidence. 2) Where Partially Available or Unavailable, describe what is partially supported and what is not

					supported explaining proposed alternative, if applicable, and the advantages and disadvantages to the Central Bank of Lesotho of such a proposal.
GSR	GENERAL SYSTEM REQUIREMENTS	A / U / P	1 / 2	ADDITIONAL MODULE	DESCRIBE THE SYSTEM'S FEATURE
UIF	USER INTERFACE				
GSR-UIF-01	Will the system be accessible, subject to proper authentication, from any environment (i.e., desktop laptop, and/or internet)?				
GSR-UIF-02	Does the system have a user-friendly GUI allowing the user to view and manage data in the most flexible way?				
GSR-UIF-03	Does the system support a UI based role management, allowing configuration of individual users, groups as well as administrator roles, based on user responsibilities?				
GSR-UIF-04	Does the system allow assignment of functions to individual as well as groups, as part of role management?				

GSR-UIF-05	Does the system have a "Save-As" function to allow copying outputs reports and allow changing relevant fields?				
GSR-UIF-06	Does the system allow field validation to prevent erroneous inputs?				
GSR-UIF-07	Does the system have dashboard capabilities including built-in dashboards to allow the users in different functional areas to see the relevant data and reports				
GSR-UIF-08	Does the dashboard provide graphic reporting capability?				
GSR-UIF-09	Does the system allow easy configuration of the UI - allowing users to personalize their views using drag/drop, sorting columns, re-arranging data, viewing or hiding fields, and filtering data?				
GSR-UIF-10	Does the system allow saving the personalized dashboard views to the user profiles?				
GSR-UIF-11	Does the system allow sharing of the personalized views with other users within the user group?				
GSR-UIF-12	Does the system allow users to search for data using various applicable search parameters such as ability to add/remove search criteria, add/remove output fields, search using wild cards, and search in ranges?				

GSR-UIF-13	Does the system allow basic data analysis in the search output, for example summing data, filtering, and grouping?				
GSR-UIF-14	Does the system allow exporting all data into excel spreadsheets/PDF or other formats?				
GSR-UIF-15	Does the system have the capability to open an information (risk event, legislation, report) and drill down to all applicable data elements?				
GSR-UIF-16	Is the system accessible from multiple locations and by multiple users at the same time?				
GSR-UIF-17	Does the system have capabilities to prevent the same user from accessing from multiple locations at the same time?				
GSR-UIF-18	Does the system have real time capabilities to process in real time all updates to static data, reference data, and similar functions requiring immediate update?				
	AUDIT				
GRS-AUD-01	Does the system record a full audit trail of any event change to data? Describe the list of processes that are tracked by the Audit trail.				

GRS-AUD-02	Does the system have requirements that the audit trail must capture the date, time, data attribute changed, computer or host name and state of system from where data changes were made?				
GRS-AUD-03	Does the system have audit capabilities wherein an audit trail for all user-initiated actions, login/logout/failed login, add/modify/approve/reject of input, reference/static data and availability of online inquiry of audit trail for at least 18-24 months, audit trail prior to that archived and retrievable?				
GRS-AUD-04	Does the system allow users to add comments when changing data and will the comments be viewable in the audit history?				
GRS-AUD-05	Does the system have the capability to generate report of any changes?				
GRS-AUD-06	Does the system have the ability to provide the following information at any time: active users, active files or directories, active workstations/ PC's/ Terminals and location, AND active services. Provide details and attach an exhibit labeled IT-AUD-07				

GRS-AUD-08	Does the system have a built-in health check processes and mechanisms and provide warnings or alerts to business or administrators, depending on status? Provide details and attach an exhibit labeled IT-AUD-08.				
GRS-AUD-09	Does system have capabilities to disable automatically if functionality that provides the audit trails is not working?				
ACL	ACCESS CONTROL				
GSR-ACL-01	To what extent does the system have the ability to extensively leverage web technology?				
GSR-ACL-02	Does the system have ability to support web-based access to system functions? Give details.				
GSR-ACL-03	If available, does the system's web solution offer current, top-level security and authentication mechanisms such as SSL, S-HTTP, digital signatures, and public/private key encryption, or any other? Please specify.				
GSR-ACL-04	IF available, does the web solution offer remote system user and admin access via VPN?				
GSR-ACL-05	Does the system support customized menus and screens? Explain how this functionality works in the system.				

GSR-ACL-06	Does the system allow suppression of menu items where certain functionality is not required or not allowed for certain user? Give details.				
GSR-ACL-07	Does the system provide ability to control access to system menus, forms, reports and system administration sections? Provide details.				
GSR-ACL-08	For all data entry screens, does the system facilitate retrieval of data records based on key fields?				
GSR-ACL-09	Does the system allow for creation and customization of user defined fields and parameters? Provide details.				
GSR-ACL-10	Does the system allow granular access control mechanism that allows separation of duties?				
GSR-ACL-11	Does the system support the mobile App?				
GSR-ACL-12	Does the system enable lock-out policy, history, and mixture of alpha numeric characters and numbers in a password?				
OPT	OPERATIONS/PROCESSING/TIMING				
GRS-OPS-01	CBL continuously monitors systems at various layers of the environment, such as, but not limited to network, host, application and database. Provide details of any monitoring tools and capabilities built into the system.				

GRS-OPS-02	Does the system support monitoring by network management systems such as, but not limited to Tivoli, HP Open View etc.? Provide details of the system's network requirements.				
GRS-OPS-03	Does the system support constant monitoring by antivirus software systems such as, but not limited to Symantec without adversely affecting system performance? Provide details.				
GRS-OPS-04	Does the system support sending application or database alerts and notification when performance/ risk/compliance/recovery thresholds are breached? Please provide details.				
GRS-OPT-05	Does the system support automatic time-outs for inactive sessions over a user specified period of time? Provide details.				
GRS-OPT-06	Does the system allow user acting for role(s) delegation for a certain period? Describe how it works.				
IT	INFORMATION TECHNOLOGY	A / U / P	1 / 2	Additional Module	DESCRIBE THE SYSTEM'S FEATURE
	GENERAL				

IT-GEN-01	The system must be scalable, secure and resilient, scalable in terms of number of users, volume of transactions and computational tasks, suppliers must provide details of scalability matrix and testing. Please describe how the system meets this requirement.				
IT-GEN-02	The Production environment must be implemented in a manner that allows for High Availability (99.5% uptime). Please describe how the system's architecture designs to achieve high availability.				
SEC	SECURITY				
IT-SEC-01	Does the system have the capability to provide multi-factor authentication for user logon to the system?				
IT-SEC-02	Does the system supports the encryption of passwords and sensitive data during transmission and encrypts and store passwords and sensitive data in the database?				
IT-SEC-03	It is a requirement by CBL that vulnerability scan and analysis of the IT systems be undertaken periodically. Does the vendor/supplier plan to undertake such either by themselves or with the assistance of a reputable third party provider?				
IT-SEC-04	Does the system support data encryption in rest mode and during transmission? Explain how the functionality is supported.				

IT-SEC-05	Describe background check and clearance procedure for personnel who will have access to the IT assets supporting CBL so that no individuals other than those authorized will be provided with access to CBL systems and information.				
IT-SEC-06	Does your company undertake, on a yearly basis, audit of the IT systems? If "Yes", please confirm that you will provide CBL with an audit report of their information security management system conducted by a certified auditor. Provide the latest auditor's report and mark it IT-SEC-06				
IT-SEC-07	Does the vendor/supplier undertake to record all transactions with date, time, description of access, and authenticated identities of vendor's/supplier's employees accessing CBL information or the systems that support the CBL application?				
IT-SEC-08	Does the vendor/supplier undertake to have privacy and data protection incident response and breach notification plan and procedures in place, and will immediately notify CBL in the event of any incident that could potentially compromise the confidentiality, integrity, or availability of CBL information or information systems. If "Yes", provide a sample document and mark it IT-SEC-08.				

IT-SEC-09	Does the system provide a means to protect against OWASP top vulnerabilities? If Yes. Does the system allow use of commercial certified rule set that protect against known attacks? Does the system allow for ad-hoc update of Security Rule Set				
ARC	ARCHITECTURE				
IT-ARC-01	Does the system provide a tool for validation of results in a test environment? Please explain.				
IT-ARC-02	CBL intends to have the application run on a secure, robust, scalable platform. Does your solution support this? Provide details.				
IT-ARC-03	CBL may wish to operate on standardized database for all its Database Management requirements in the future. Does your solution support Oracle, MS SQL, Informix, etc.? Provide details.				
IT-ARC-05	CBL wishes to have its system hosted on cloud. Does the system support cloud computing technology?				
IT-ARC-06	Is the system support provided on a variety of Operating Systems (Windows, Linux, AIX, and other)? Provide details.				

IT-ARC-07	<p>Does the system support configuration of business processes on external solutions? If Yes, provide the list of supported business processes management engines and integration mechanism.</p>				
IT-ARC-08	<p>Will the software have the capacity to support and provide access to at least 30 concurrent users?</p>				
IT-ARC-09	<p>Does the system provide the user the capability to extract data from the system and deliver it using standard data transmission formats to other systems and/or databases? Explain in detail how these extractions would be performed in the system. Identify standard mechanisms and data formats that are available.</p>				
IT-ARC-10	<p>Please describe the Report Writer abilities of the solution and the ability to connect other reporting tools to the system and report seamlessly from system.</p>				
BCM	BUSINESS CONTINUITY MANAGEMENT				
IT-BCM-01	<p>It is important that the system has a cloud back-up and contingency plan mechanisms in case of disruptions. Provide details of the arrangements that the vendor/supplier has on this part.</p>				

IT-BCM-02	CBL systems operate with a goal of high availability and reliability. It is important that the system is not vulnerable to single point of failure (SPOF). Explain how the system has been built to handle SPOFs.				
IT-BCM-03	Does the system allow for complete data backup at end of the day?				
IT-BCM-04	Does the system have the ability to restore to a point from backups? Provide details.				
IT-BCM-05	How does the system enable disaster recovery and management? Provide details of the disaster recovery solution.				
IT-BCM-06	Describe the Backup and Restoration procedures implemented in the solution.				
IT-BCM-07	How does the Application/System/RDBMS replicates? Provide details				
IT-BCM-08	Does the system have an archiving facility? Describe how it performs this function.				
IT-BCM-09	How does the system support referential integrity? Provide more details.				
IFR	INFRASTRUCTURE				
IT-IFR-01	Will the vendor/supplier identify and illustrate the components or tiers of the software solution/package for it to successfully operate (e.g. Web Tier, Application Tier, Database Tier)				

IT-IFR-02	Will the vendor/supplier provide system architecture (physical and logical) showing the connectivity of server, network and workstations, plus hardware detail specification?				
IT-IFR-03	Will the vendor/supplier identify or disclose all system services that are needed by the software/package to be fully operational e.g. directory services?				
ITF	INTERFACES				
IT-ITF-01	For each of the interfaces required, please describe the process that will be used to connect systems, as well as interface that will provide support to third party software and the potential number of clients the interface is capable of connecting, along with list all techniques, tools and standards adopted.				
IT-ITF-02	Will the vendor/supplier provide the necessary interfaces and tools needed for the system to seamlessly and securely integrate with existing systems of the CBL and third-party systems, such as but not limited to those listed below. This includes necessary development and/or configuration of the integration tools/system. CBL mainly uses IBM MQ for integration between systems. Provide details.				
IT-ITF-02.1	a) MS OFFICE 365 – The email system that shall be used for communicating actions reminders, deadlines and reporting				

IT-ITF-02.2	b) Team-Mate: An audit system that is used for auditing purposes.				
IT-ITF-03	In the case that the system is unable to communicate with other systems, does it offer the capabilities to re-trigger the events to send data to those systems once they are available? Please describe.				
IT-ITF-04	Confirm that the vendor/supplier will identify all APIs available for interacting with the system. Describe the capabilities and uses of each.				
IMP	IMPLEMENTATION	A / U / P	1 / 2	Additional Module	DESCRIBE THE SYSTEM'S FEATURE
GEN	GENERAL				
IMP-GEN-01	Provide an estimate of the duration of the project given the number and nature of transactions assuming a limited number of customizations to the product.				
IMP-GEN-02	From prior experience, are there any factors, internal and external, that you think are likely to affect the implementation schedule of this project? If "Yes" provide a list and suggestions of how best to overcome them.				

<p>IMP-GEN-03</p>	<p>Describe your proposed project implementation framework, including details on technical services required, as well as a short description of how the following deliverables below will be achieved:</p> <p>Include a sample project plan, proposed project plan, project team requirements and methodology to be used to perform and complete tasks, as well as the system development life cycle; inclusive of customization and configurations. Mark this clearly as IMP-GEN-03.</p>				
<p>IMP-GEN-03.1</p>	<p>a) Implementation services of the proposed software solution for all items outlined in the attachments to this RFP</p>				
<p>IMP-GEN-03.2</p>	<p>b) Completion of business requirements/system specifications, including client specific configurations or customizations based on a cost/benefit analysis and the availability of workarounds</p>				
<p>IMP-GEN-03.3</p>	<p>c) Completion of development and configuration</p>				
<p>IMP-GEN-03.4</p>	<p>d) Development and installation of interfaces to internal and external systems utilized by the CBL</p>				
<p>IMP-GEN-03.5</p>	<p>e) Documentation detailing all environment specific configurations and interface maintenance</p>				
<p>IMP-GEN-03.6</p>	<p>f) Documentation detailing all customizations required for the software solution in order to meet CBL requirements</p>				

IMP-GEN-03.7	g) Data migration plan from the existing manual systems into the new system				
IMP-GEN-03.8	h) User and technical training, including elements that are tailored to incorporate environment specific configurations				
IMP-GEN-03.9	i) Completion of User Acceptance Testing (UAT)				
IMP-GEN-03.10	j) Parallel and go live				
IMP-GEN-03.11	k) Post implementation services				
IMP-GEN-03.12	l) Maintenance and support				
IMP-GEN-04	CBL requires that the potential vendor/supplier describes the organization of the implementation team (Project Manager and specialists). Also explain how the potential vendor/supplier proposes to supply an appropriately qualified organization team, including subcontractors, to deliver the primary tasks identified.				
IMP-GEN-05	How many days of the week will the identified team members be available throughout the implementation period?				
IMP-GEN-06	Will the project manager and team be dedicated to CBL (onsite/virtually) for the entire implementation period?				

IMP-GEN-07	Clearly list all the obligations and responsibilities of CBL and proposed vendor, preferably using onsite/virtual model.				
IMP-GEN-08	Describe the standard communication channels with the CBL team and describe, clearly, the proposed escalation process and procedures for any potential challenges in the implementation period.				
IMP-GEN-09	Describe the reporting procedures that you will use to report progress to the CBL, along with the timing of meetings for discussing progress and specify the change and quality control procedures that will be used during the project.				
IMP-GEN-10	What communications processes and procedures does the potential vendor/supplier recommend to ensure that the project teams, project board and user populations are kept up to date with decisions and progress? Describe other aspects of stakeholder management that the potential vendor/supplier has found to be useful similar projects in the past.				
IMP-GEN-11	Describe the process controls to be put in place to set agreed milestones with the CBL, to ensure the work required throughout the project is performed and deliverables and milestones are achieved while staying within budget. Include sample Program				

	deliverables, weekly & executive status reports, progress/success metrics, etc. and mark these IMP-GEN-11				
IMP-GEN-12	What matrices do you propose to measure progress and measure success? Include sample progress/success metrics and mark them IMP-GEN-12				
IMP-GEN-13	Describe your proposed methodology for data conversion and migration from manual to the RM and CM system? Include in your proposal, tools and techniques for data reconciliation.				
IMP-GEN-14	Describe on how the vendor/supplier will support system integration testing and UAT for the RM and CM system.				
TD	TRAINING AND DOCUMENTATION	A / U / P	1 / 2	Additional Module	DESCRIBE THE SYSTEM'S FEATURE
TRN	TRAINING				
TD-TRN-01	Describe your knowledge transfer methodology.				
TD-TRN-02	Provide details on the nature and schedule of functional, technical and infrastructure related training that will be provided upon taking the systems live.				

TD-TRN-03	The vendor/supplier must provide Executive and Management training. Please describe your standard executive training program, its duration and content.				
TD-TRN-04	The vendor/supplier must provide Functional End User Training. Please describe your standard end-user training programme, its duration and content.				
TD-TRN-05	The vendor/supplier must provide Computer Operations Training, including details on computer operation requirements, computer operation security mechanism, backup, disaster recovery, contingency plan and business continuity. Describe how vendor/supplier would provide this kind of training, including timelines and content.				
TD-TRN-06	The vendor/supplier must provide Technical Training, including system maintenance and operating procedures, including any specific enhancements for the CBL. Describe how vendor/supplier would provide this kind of training, including timelines and content.				
TD-TRN-07	The vendor/supplier must provide training on use of post implementation technical support alternatives, including virtual support. Describe how vendor/supplier would provide this kind of training, including timelines and content.				

TD-TRN-08	The winning vendor/supplier must provide to the CBL all training material used in the training sessions for use in subsequent post-implementation training sessions. These materials may include handouts, slides, speaker notes, videotapes, etc. Provide details of when and how vendor/supplier plans to make these available				
TD-TRN-09	The vendor/supplier must conduct all training sessions on-site at the CBL/ virtually. Provide details of how vendor/supplier plans implement these.				
DOC	DOCUMENTATION				
TD-DOC-01	Confirm availability of the following security documentation and whether this is system generated or manually produced. Provide an exhibit and mark it IT-DOC-01				
TD-DOC-01.1	a) Recovery programs.				
TD-DOC-01.2	b) Security schemes.				
TD-DOC-01.3	c) Audit/control techniques descriptions.				
TD-DOC-01.4	d) Disk space usage estimation.				
TD-DOC-01.5	e) Systems Narratives/Glossary of terms.				
TD-DOC-01.6	f) File structures/Data Dictionary.				

TD-DOC-01.7	g) Please confirm availability of the following documentation and whether this is system generated or manually produced:				
TD-DOC-01.8	h) Provision of Application Manuals.				
TD-DOC-01.9	i) Provision of Standard Operating Procedures.				
TD-DOC-02	What is your documentation policy? Example documentation on methodology or algorithm used in the system should be shared with CBL.				
TD-DOC-03	The platform should be accompanied with detailed documentation on the implementation of the proposed platform/solution.				
TD-DOC-04	What are the documentation delivery mechanisms that your system supports? For example: online/on-screen help, tool tips, white papers and others.				
TD-DOC-05	Are the following documents available? Briefly describe how they will be made available to CBL:				
TD-DOC-05.1	a) User manual				
TD-DOC-05.2	b) Operations manual				
TD-DOC-05.3	c) Technical documentation				

TD-DOC-05.4	d) Data modeling Documentation				
TD-DOC-05.5	e) System Configuration				
TD-DOC-05.6	f) And other relevant documents				
TD-DOC-06	Does the solution provide online context sensitive help?				
TD-DOC-07	Does the solution provide the system administrator the capability to modify the original user help menu and contents?				
TD-DOC-08	Does the solution have a complete Online Help system explaining the solution features and functions?				
TD-DOC-09	Is the Help system fully integrated with the solution? Describe the capabilities.				
TD-DOC-10	Do you provide additional user training on a need basis and following completion of system upgrades?				
TD-DOC-11	Will the vendor/prospective supplier document all customizations made to the software for the CBL environments? Please confirm this and confirm that these documents will be made available to the CBL.				
	SUPPORT AND MAINTENANCE	A / U / P	1 / 2	Additional Module	DESCRIBE THE SYSTEM'S FEATURE

SM	SUPPORT AND MAINTENANCE				
SM-SM-01	Indicate the location of the office that will be responsible for providing technical support to the CBL in case your company wins the bid.				
SM-SM-02	Describe the relevant experience of your staff that will be dedicated to this project, particularly on the risk and compliance operations of a central bank.				
SM-SM-03	CBL will require onsite/virtual support for two (2) weeks after go live. Will the vendor/supplier adequately provide the required services as required?				
SM-SM-03.1	a) Work with the project team to execute the cut over plan.				
SM-SM-03.2	b) Prepare a checklist for readiness to go live and verify status and work with the project team to address any lack of readiness identified. (The vendor implementation team should provide the plan for going live in the initial phases of the project to avoid late surprises.)				
SM-SM-03.3	c) Advise and work with the project team to address issues before going live.				
SM-SM-03.4	d) Post go-live, assign issues the highest priority for resolution and escalate issues quickly and to the right party within the vendor company.				

SM-SM-03.5	e) What type of post-implementation technical support services and facilities will be provided by the vendor/supplier? Describe the technical support services and facilities that will be provided – including e-mail, dedicated telephone lines within CBL operating hours (0800hrs to 1700hrs) Minimum 24x7 production support is required.				
SM-SM-03.6	f) Can the system problems be diagnosed remotely? If so, explain how the vendor/supplier proposes to access the system remotely and securely.				
SM-SM-03.7	g) Provide an indication of your guaranteed and average response times during and outside standard hours for technical support based on company SLAs.				
SM-SM-03.8	h) Describe special support that will be provided during production cut-over and go live.				
SM-SM-03.9	i) Describe the procedures and schedules for installations or upgrades of software modules and changes relating to upgrades of operating systems and database engines.				
SM-SM-03.10	j) Describe proposed change control process and corresponding procedures and standards of				

	service (by problem type/severity, as appropriate).				
SM-SM-03.11	k) Describe proposed escalation process and procedures to be used in this project.				
SM-SM-03.12	l) Provide clearly defined and detailed Service Level Agreement (SLA) components pertinent to the support and maintenance of the integrated Risk and Compliance management system. The SLA components should be defined and formalized for user expectations with regard to the system availability, system performance, and support.				
SM-SM-03.13	m) Please include your standard SLA as part of the proposed solution package.				
SM-SM-03.14	n) What period of post-rollout warranty support does the vendor/supplier provide?				
SM-SM-03.15	o) Does your company have international presence/support? If so, specify where?				
SM-SM-03.16	p) Are there additional charges for the support? Provide details.				
SM-SM-03.17	q) Which legal jurisdiction is applied in case of disputes?				
SM-SM-03.18	r) What is your company's source code policy?				

SM-SM-04	Does the system provide built-in end-user online support functions listed below? Provide details and attach an exhibit labeled IT-SM-01				
SM-SM-04.1	a) Online documentation.				
SM-SM-04.2	b) Online help.				
SM-SM-04.3	c) Online search facilities.				
SM-SM-04.4	d) Online procedures.				
SM-SM-05	Do you have an arrangement for source code escrow? Provide full details.				
RM	RELEASE MANAGEMENT				
SM-RM-01	Any new version (major or minor or patch) release of the product by the vendor/supplier can be optimally opted by CBL to be implemented in their installations. During that, all required technical, functional, documentation support/training should be provided. Describe how this process will be managed.				
SM-RM-02	Are there any known schedules of known future or planned upgrades/releases? Provide details, along with a description of functionality and changes scheduled to be included in each.				

SM-RM-03	With every new release, does an existing implementation need to be compulsorily upgraded?				
SM-RM-04	For how long are outdated product versions supported?				
SM-RM-05	As a matter of policy, it is imperative that version upgrades and patches are tested in Test, UAT and SIT environments prior to release into PRODUCTION. The two (2) lower environments (typically Test and UAT) should have the capability to replicate production in all aspects for day-to-day testing needs. Elaborate on the whole process, including licensing implications.				
SM-RM-06	Does the system have the capability to run system/batch/real-time processes across all environments?				

12.2 FINANCIAL PROPOSAL

The financial proposals shall be invited at the later stage from only vendors/prospective suppliers that have satisfactorily met the technical requirements.

13 REQUEST FOR PROPOSAL PROCESS

13.1 CONTACT PERSONS

Enquiries arising from this RFP should be directed, in writing, to;

Name: Mrs. Matsepo Lechela

Title: Secretary, Tender Committee

Tel: (266) 22232126

Fax: (266) 22310051

E-mail: mlechela@centralbank.org.ls

13.2 CLARIFICATION

Any queries relating to this RFP must be addressed in writing to the relevant person designated in 13.1 above. Responses will be sent to the enquirer and will also be posted on the website. The closing date for requests of clarifications is 19th August 2022.

13.3 ELIGIBILITY

Proposals will not be evaluated if the prospective supplier's current or past corporate or other interests may, in the Bank's opinion, give rise to a conflict of interest in connection with this project. Only proposals that comply with all the requirements of this RFP will be considered.

13.4 DELIVERY OF PROPOSALS

13.4.1 Technical Proposal

Technical Proposals must be submitted electronically and provided as attachments to an email and should be emailed to mlechela@centralbank.org.ls. The subject of the email should read **“Technical Proposal for Risk and Compliance Management System”**.

Proposals must be provided as a PDF attachment to the email in a compressed folder.
Only electronic proposals will be accepted.

13.4.2 Financial Proposal

Financial proposal shall be invited only from vendors/prospective suppliers that have satisfactorily met the technical requirements of the Bank and have scored an overall of 80% under technical requirements.

13.5 DEADLINE FOR THE SUBMISSION OF TECHNICAL PROPOSALS

Proposals should be received on or before **Friday, 02nd September 2022, between 14:30hrs and 16:30hrs** (recipient time). Proposals received after the above-specified date and time shall not be considered.

13.6 OPENING OF TECHNICAL PROPOSALS

Proposals shall be opened on the same day. As a health measure, no bidders will be allowed to attend the opening session. All proponents will be emailed the tender register.

13.7 EVALUATION OF PROPOSALS AND SELECTION

Proposals compliant with the requirements for submissions described above shall be evaluated. Technical evaluation shall involve both submission analysis and pitch evaluation.

14 EVALUATION CRITERIA

14.1 MANDATORY EVALUATION CRITERIA

Proponents will receive a Pass/Fail rating on the Mandatory Criteria, depending on the fulfillment of the requirements listed below. Proponents missing any of the requirements below will not be considered for the next stage of evaluation. The next stage is the technical evaluation.

REQUIREMENT	YES	NO	REMARKS
Valid copy of the trader's license or company registration certificate issued by each proponent's inland registrar of companies.			
Valid copy of the tax clearance certificate or Tax Compliance Certificate issued by each proponent's Inland tax authority. E.g SARS or LRA.			
Signed letter of introduction.			

14.2 TECHNICAL EVALUATION CRITERIA

Technical evaluation shall comprise of technical proposal evaluation and the "pitch"

Technical proposal evaluation criterion is divided in two parts as follows:

14.2.1 TECHNICAL PROPOSAL EVALUATION CRITERIA

Technical proposal evaluation criterion is divided in two parts as follows:

a) FUNCTIONAL REQUIREMENTS EVALUATION CRITERIA

Evaluation under this area will be on the basis of the following criteria, scored as indicated

THE PROPOSED SYSTEM FUNCTIONAL REQUIREMENTS EVALUATION CRITERIA	
Key Functional Area	Allocated Score
Risk Management Process (risk identification, analysis, evaluation, as well as responses with timelines and notifications given to responsible officers)	10
Incident Management	10
Compliance Management	10
Reporting requirements (notifications, alerts, Interactive dashboards)	5

General and Technical Requirements	10
TOTAL	45

b) OTHER EVALUATION CRITERIA

Evaluation under this area will be on the basis of the following criteria, scored as indicated

PROJECT IMPLEMENTATION PLAN AND APPROACH EVALUATION CRITERIA	
Implementation Area	Allocated Score
Project Implementation Framework (approach and high level plan)	4
Implementation Team Composition and qualifications	3
Training and Support Framework	5
Proponent Experience (Market Perception and Product Exposure)	3
Proponent financial capability	20
TOTAL	35

To qualify for pitch evaluation, the proponents should score a minimum score of 80% under technical proposal evaluation.)

14.2.2 PITCH EVALUATION CRITERIA

The purpose of pitch session (oral presentation) is to validate the information provided by the proponent in their proposal and to test the proponent's understanding of the requirements as detailed in the RFP. The pitch is evaluated and it involves question and answer session. Only proponents that have scored the minimum score of 80% and above shall be invited for the pitch and shall be evaluated based on the criteria as follows:

Evaluation Area	Allocated score
Clarity of the presenter and ability to answer questions appropriately	10
Demonstrated knowledge and understanding of CBL requirements	10
Consistency with the RFP	10
TOTAL	30

(To qualify for financial evaluation the proponents should score a total weighted score of 80% under both submission evaluation and pitch.)

14.3 FINANCIAL EVALUATION

Financial proposals will be evaluated following completion of the technical evaluation and oral presentations. Proponents that have scored a combined weighted score of 80% under technical evaluation will be invited to submit their financial proposals.

Financial proposals will be evaluated based on the predetermined criteria as below. Proponents will receive a Pass/Fail rating depending on the fulfillment of the requirements listed below. Proponents missing any of the requirements below shall be disqualified.

EVALUATION AREA	YES	NO	REMARKS
Accuracy-100% accuracy			
Compliance- Full compliance to the requirements (taxes, all costs categories as per the RFFP).			
Completeness- Complete financial proposal covering all the requirements.			

14.4 SELECTION FOR AWARD (Least cost based selection)

The proposal that meets all the requirements under Technical and Financial evaluation and is found to be the lowest priced proposal shall be selected.

15 TERMS AND CONDITIONS OF THE RFP

15.1 PROPOSAL VALIDITY & FIRM PRICING

Proposals should be valid for at least 90 days after the closing date and prices shall be “locked” for the entire contract period.

15.2 CURRENCY

All responses to this RFP should be expressed in LSL Loti or ZAR Rands. Proposals in other currencies shall not be permitted.

15.3 TAXES

15.3.1 Value Added Tax

Prices quoted should be:

- a) Exclusive of 15% Value Added Tax; and
- b) In accordance to applicable Lesotho laws.

15.3.2 Withholding Tax

In effecting payments, the applicable withholding taxes shall apply: 10% for foreign companies and 5% for local companies. This is not an added tax. Proponents that include an added amount to their proposed fee as the withholding tax shall be disqualified.

15.4 OWNERSHIP OF PROPOSALS

All proposals, including supporting documents, submitted to the Bank become the property of the Bank.

15.5 CONFIDENTIALITY OF INFORMATION

All proposals submitted by prospective suppliers shall be held in strict confidence and will not be revealed to any other party. All Information pertaining to the Bank obtained by the prospective suppliers as a result of participation in this project is confidential and must not be disclosed without written authorization from the Bank. The successful prospective suppliers shall be required to:

- Sign a confidentiality clause.
- Hand over all the design documentation raised over to CBL

15.6 AMENDMENT OF RFP DOCUMENT

At any time prior to the deadline for submission of responses, CBL, for any reason, whether at its own initiative or in response to a clarification requested by a prospective respondent, may modify the RFP documents by amendment.

All prospective respondents that have received the RFP documents will be notified of the amendment in writing, and such amendment will be binding on them. To allow prospective respondents reasonable time to take any amendments into account in preparing their responses, CBL may at its sole discretion extend the deadline for the submission of responses based on the nature of the amendments.

15.7 TECHNICAL FACILITIES

The Bank will provide working space, where necessary. However, the Bank may not provide other technical facilities; hence prospective suppliers should provide own requisite facilities.

15.8 COSTS OF RESPONDING

Prospective suppliers are solely responsible for their own expenses incurred during the preparation of the proposal and for subsequent negotiations with the Bank including the “pitch” sessions.

If the Bank rejects all or any proposal, it shall not be liable to any prospective supplier for any claims, whether for costs or damages incurred by the prospective suppliers in preparing the proposal, loss of anticipated profit in connection with any final contract, or any other matter whatsoever.

15.9 BACKGROUND CHECK

The Bank reserves the right to check and verify the background of all or any persons (firms, directors, partners, technical staff, etc.) involved in the Bid and reserves the sole right to determine whether or not to accept or reject any such Bid on any grounds.

15.10 PERFORMANCE BOND

The Bank **may** require a performance bond of not less than 10% of the bid amount from the preferred prospective suppliers before entering into the contract.

15.11 HEALTH AND SAFETY

The Bank adheres to Occupational Health and Safety (OHS) requirements under the Lesotho Labour Code Order No.24 of 1992 and as amended; International Organization for Standardization (ISO) 45001:2018 and other international best practices on OHS. As such, all its service providers shall also be required to comply with applicable Lesotho Legislation on Occupational Health and Safety including Public Health Order No.12 of 1970 as amended and adhere to the Bank's OHS policy.

15.12 LANGUAGE OF THE PROPOSAL

The proposal shall be written in the English Language. All correspondence and other documents pertaining to the proposal and its implementation shall also be in English.

15.13 JOINT VENTURE

If a bidding firm does not have all the expertise for the assignment, there is no objection to the firm associating with another firm to enable a full range of expertise to be

presented. The joint venture shall be accompanied with full documented details of the proposed association.

In the case of a joint venture or association, all the firms constituting the joint venture or association will be jointly and severally liable and at least one firm, preferably the lead entity in the joint venture or association shall be financially capable of meeting the contract requirements and potential liabilities on its own and shall assume contracting responsibility and liability for satisfactory execution of the assignment.

15.14 WITHDRAWAL, SUBSTITUTION AND MODIFICATION OF BIDS

Tenderers may modify or withdraw the tender prior to the submission deadline. The modification or notice of withdrawal shall be effective if it is received by the Bank prior to the Proposal Submission Deadline.

15.15 ACCEPTANCE AND/OR REJECTION OF PROPOSALS

- The Bank is not bound to give reasons for declining any or all of the proposals.
- The Bank is not bound to accept the lowest or any bid and may cancel the bidding process at any stage prior to the award of contract and is not bound to provide reasons for cancellation.