Request for Proposal

for the

Supply, Installation and Configuration of a

Governance, Risk and Compliance (GRC) Tool

for the Bank of Mauritius

RFP No.: *BOM/GRC/8-2023*
Services: *Supply, Installation and Configuration of a GRC Tool*
Client: *Bank of Mauritius*
Country: *Mauritius*
Issued on: *01/08/2023*

Table of Contents

1. Bid Information Sheet

Name of Bid	**Supply, Installation and Configuration of a Governance, Risk and Compliance (GRC) Tool for the Bank of Mauritius**
Name & Address of Issuer	Bank of Mauritius Sir William Newton Street Port Louis 11328 Mauritius
Addressee	Chairperson – Tender Committee Bank of Mauritius Sir William Newton Street Port Louis 11328 Mauritius Email: tender.committee@bom.mu
Date of commencement of Request for Proposal process	Tuesday 01 August 2023
Closing date of Bid	Tuesday 22 August 2023, 4pm, Mauritius Time
Validity Period	180 days from bid closing date
e-Tendering	Electronic copies of bids shall be encrypted and submitted by email to the following address: tender.committee@bom.mu
Bid currency	Mauritian Rupees (MUR)
Bid language	English
Deadline for sending queries	Friday 11 August 2023, 2pm., Mauritius Time
Sharing of responses to queries	Wednesday 16 August 2023

2. Introduction

2.1 The Bank of Mauritius, hereinafter referred to as “Bank”, is the central bank of the Republic of Mauritius and is established under the Bank of Mauritius Act 2004.[1]

2.2 The primary object of the Bank is to maintain price stability and to promote orderly and balanced economic development. Other objects of the Bank are to ensure the stability and soundness of the financial system of Mauritius. The Bank is the regulatory authority for financial institutions in Mauritius as defined in the Banking Act 2004.[2] It is responsible for the regulation and supervision of the operations and activities of financial institutions under its purview.

2.3 The Bank is also mandated, under the National Payment Systems Act 2018, to regulate, oversee and supervise the national payment systems and payment systems being operated in Mauritius primarily for the purpose of ensuring their safe, secure, efficient and effective operation and accessibility to the public.[3]

3. Purpose of RFP

3.1 The intent of this Request for Proposal (“RFP”) is to invite bids from experienced and reputable firms for the supply, installation and configuration of a Governance, Risk and Compliance (GRC) tool for the Bank.

3.2 The GRC Tool will assist the Bank to identify, assess, prioritise, and manage risks within its organisation. The GRC Tool must be user-friendly, comprehensive, and customisable to meet the unique needs of the central bank.

4. Invitation to Bid

4.1 The Bank invites eligible firms to submit their proposals in accordance with the details provided in this RFP for a GRC Tool, which can be on-premise or a hybrid model.

5. Instructions to Bidders

5.1 Bidders are required to carefully read the specifications and conditions in this RFP. Bidders may seek any clarification required from the Bank within the deadline for sending queries as set out in the Bid Information Sheet before submission of their bid.

[1] The Bank of Mauritius Act 2004 is accessible at https://www.bom.mu/about-bank/legislations/bank-mauritius-act-2004.

[2] The Banking Act 2004 is accessible at https://www.bom.mu/about-bank/legislations/banking-act-2004.

[3] The National Payment Systems Act 2018 is accessible at https://www.bom.mu/about-bank/legislations/national-payment-systems-act-2018.

5.2 Any act of collusion that may distort normal competitive conditions may cause the rejection of a bid by the Bank. By participating in this bid, bidders certify not to be involved in such acts of collusion. Counteroffers submitted with bids will not be considered. Letter of qualification accompanying bids may be ignored if they have the effect of modifying either the terms of a bid or the comparability of a bid with other bids.

5.3 Should a bidder, in good faith, wish to propose modifications to the terms, conditions and contents of its bid for the purpose of reducing the bid amount, then the bidder shall contact the Bank in writing well before the date of bid submission. Should the proposed modification be approved by the Bank, the bidder shall be advised in good time. No proposed modification shall be considered unless this procedure has been adopted.

5.4 All deletions, additions and corrections to figures inserted in the bid documents are to be countersigned by the bidder.

5.1 Eligible Bidders

5.1.1. Eligible bidders shall demonstrate that it meets the eligibility criteria set out in Annexure A of this RFP.

5.1.2 Eligible bidders must be already engaged in the provision of similar end-to-end systems and services, comprising of the supply, installation, and configuration of a GRC tool.

5.1.3 Eligible bidders shall provide the product and services for the stipulated duration from the date of commencement (hereinafter referred to as the "term") specified in the bid documents.

5.1.4 The Bank's employees, committee members, board members and their relatives (spouse and children) are not eligible to participate in the bidding exercise.

5.1.5 Bidders involved in corrupt or fraudulent practices or debarred from participating in public procurement or procurement with the Bank shall not be eligible.

5.2 Cost of Bidding

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

5.3 Content of RFP

5.3.1. The RFP includes the documents listed below and any addendum issued by the Bank in accordance with the Instructions to Bidders:

a. Eligibility Criteria (Annexure A),
b. Details of the GRC already set up by the Bidder (Annexure B),
c. Bid Form (Annexure C),
d. Information Security Requirements (Annexure D),
e. Request for Clarifications (Annexure E), and
f. Price Schedule of Services (Annexure F).

5.3.2 Bidders are expected to examine all instructions, forms, terms and specifications in the bid documents. Failure to provide all information required in the bid documents or to submit a bid not substantially responsive to the bid documents in any respect, may result in the rejection of the bid.

5.4 Clarification of Documents

5.4.1 Prospective bidders wishing to request for clarifications on the content, form and/or any other details contained in the RFP may write to the Bank as per format specified in Annexure E using the contact details below:

Chairperson – Tender Committee
Bank of Mauritius
Sir William Newton Street
Port Louis 11328
Mauritius
Email: tender.committee@bom.mu

5.4.2 All questions/queries should refer to specific sections of the RFP. If a change or explanation is deemed necessary for all potential bidders, the Bank shall notify all potential bidders by addendum to the RFP which shall be communicated to all prospective bidders.

5.4.3 If questions/queries are technical in nature, the Bank may identify the appropriate stakeholder and arrange for such questions to be answered. All questions, business or technical in nature, must be addressed to the **Chairperson – Tender Committee** or by email to tender.committee@bom.mu.

5.4.4 The deadline for submitting any question/query is as per the Bid Information Sheet. Bidders' questions, along with the Bank's responses, shall be aggregated in an anonymous manner and communicated to all bidders. Bidders are advised to consolidate their queries.

5.5 Amendment of Bid Documents

5.5.1 At any time prior to the deadline for submission of bids, the Bank may, for any reason, whether at its own initiative or in response to a clarification requested by a prospective bidder, modify the bid documents by issuing an addendum. Such addendum, if any, will be posted on the website of the Bank.

5.5.2 To allow prospective bidders reasonable time to take the said amendment into account in preparing their bids, the Bank may, at its discretion, extend the deadline for the submission of bids.

5.6 Language of Bid

5.6.1 The bid prepared by a bidder as well as all correspondences and documents relating to the bid exchanged by a bidder and the Bank, shall be in writing and in English language. Any printed literature submitted by a bidder may be written in another language provided they are accompanied by an accurate English translation of the relevant passages in which case, for purposes of interpretation of the bid, the English translation shall govern.

5.7 Documents Comprising the Bid

5.7.1 The bid submitted by a bidder shall comprise the following documents:

a. a Bid Form (Annexure C),

b. a Technical Proposal, to contain as a minimum the requirements listed at Section 6 (Technical Requirements) including duly completed Tables A-N, and

c. a Financial Proposal, which includes the Price Schedule as per Annexure F,

with all submissions prepared in accordance with the requirements laid down in this RPF, including section 7.

5.7.2 A bidder shall submit its Technical Proposal and a Financial Proposal in separate files attached to the email sent by the authorised signatory of the bidder. The name of the electronic file for the Technical Proposal must be "**Technical Proposal – Governance, Risk and Compliance (GRC) Tool**". The name of the electronic file for the Financial Proposal must be "**Financial Proposal – Governance, Risk and Compliance (GRC) Tool**".

5.8 Format and Submission of Bids

5.8.1 All the above documents shall be sent electronically, by email, from the email address of the authorised signatory of the bidder to tender.committee@bom.mu.

5.8.2 The electronic documents should be encrypted before being sent by email. The encryption procedures are detailed at Section 5.8.3. The Pretty Good Privacy ("PGP") tool shall be used for encryption. For that purpose, a cryptographic public key shall be made available by the Bank to all bidders.

5.8.3 Encryption procedures:

a. Download PGP Tool (or equivalent) from https://pgptool.github.io/

b. Download the public key from the Bank's website at https://www.bom.mu

c. Click on **Import** to import the key and select the public key downloaded above.

d. Click **Encrypt File**.

e. Select the file and choose the public key and then proceed to encrypt file.

Failure to comply with the above submission formats may entail rejection of the bid.

5.9 Form of Bid

5.9.1 A bidder shall complete and submit all the required documents as detailed at 5.7.1 and in accordance with Annexures A, B and C.

5.10 Bid Prices

5.10.1 The bidder shall indicate in its Financial Proposal on the Price Schedule (Annexure F) the unit prices where applicable and total bid prices of the services that it proposes to provide under the contract in accordance with Annexure F.

5.10.2 Prices indicated on the Price Schedule shall be the cost of the services quoted including all customs duties, VAT and any other taxes payable.

5.10.3 Prices quoted by the bidder shall remain fixed during the term of the contract, unless otherwise agreed by the parties. A bid submitted with an adjustable price quotation shall be treated as non-responsive and shall be rejected.

5.10.4 Contract price variations shall not be allowed for contracts not exceeding one year (12 months).

5.10.5 Where contract price variation is allowed for contracts exceeding one year (12 months), the variation shall not exceed 10% of the original contract price.

5.10.6 Price variation requests shall be processed by the Bank within 30 days of receiving a request.

5.11 Bid Currencies

5.11.1 Prices shall be quoted in MAURITIAN RUPEES (MUR), unless otherwise specified.

5.12 Bidders Eligibility and Qualifications

5.12.1 Pursuant to Section 5.1, a bidder shall provide, as part of its bid, documents establishing the bidder's eligibility to bid and its qualifications to perform the contract.

5.12.2 The documentary evidence, as set out in Annexure A, of a bidder's qualifications to perform the contract shall establish to the Bank's satisfaction that the bidder has the financial and technical capability necessary to perform the contract.

5.13 Validity of Bids

5.13.1 Bids shall remain valid for 180 days or as specified in the Invitation to Bid after the date of bid opening prescribed by the Bank. A bid valid for a shorter period shall be rejected by the Bank as nonresponsive.

5.13.2 In exceptional circumstances, the Bank may solicit the bidder's consent to an extension of the period of validity. The request and the responses thereto shall be made in writing. A bidder granting the request shall not be required nor permitted to modify its bid.

5.14 Deadline for Submission of Bids

5.14.1 Bids must be received by the Bank at the address given in the Invitation to Bid no later than **22 August at 3:00 pm (Mauritius time).**

5.14.2 The Bank may, at its discretion, extend this deadline for the submission of bids by amending the bid documents, in which case all rights and obligations of the Bank and bidders previously subject to the deadline will thereafter be subject to the deadline as extended.

5.15 Clarification of Bids

5.15.1 To assist in the examination, evaluation and comparison of bids, the Bank may, at its discretion, ask a bidder for a clarification on its bid. The request for clarification and the response shall be in writing, and no change in the prices or substance shall be sought, offered or permitted.

5.15.2 Any effort by a bidder to influence the Bank in its bid evaluation, bid comparison or contract award decisions may result in the rejection of the bidder’s bid.

5.16 Deadline for Evaluation

5.16.1 The bid evaluation committee shall evaluate the bid within 60 days from the date of opening of the bid.

5.17 Preliminary Examination and Responsiveness

5.17.1 All bids/proposals shall undergo a two-stage evaluation process, with the evaluation of technical proposal completed prior to any price proposal opened and compared. The financial proposal will be opened only for bids that pass the technical score. The Bank will then select the most cost-effective proposal.

5.17.2 The Bank will examine the bids to determine whether they are complete, no computational errors have been made, required securities have been provided, the documents have been properly signed, and whether the bids are generally in order.

5.17.3 The Bank may waive any minor informality or nonconformity or irregularity in a bid which does not constitute a material deviation, provided such waiver does not prejudice or affect the relative ranking of any bidder.

5.17.4 Prior to the detailed evaluation, the Bank shall determine the substantial responsiveness of each bid to the bid documents. For purposes of this RFP, a substantially responsive bid is one which conforms to all the terms and conditions of the bid documents without material deviations. The Bank’s determination of a bid’s responsiveness is to be based on the contents of the bid itself, without recourse to extrinsic evidence.

5.17.5 If a bid is not substantially responsive, it shall be rejected by the Bank and may not subsequently be made responsive by the bidder by correction of the nonconformity.

5.17.6 Substantially responsive proposals shall be reviewed by the evaluation committee and scored against the stated criteria. The evaluation committee may review references, request oral presentations, conduct on-site visit and use the results to score the proposals.

5.17.7 For price comparisons, mathematical 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 bidder does not accept the correction of the errors, its bid shall be rejected. If there is a discrepancy between words and figures, the amount in words will prevail.

5.17.8 The final bid outcome will be a combination of Technical score (making up to 70% of total score) and Financial score (making up for 30% of total score). The winning bid shall be the one which scores the highest of the combined Technical and Financial scores.

5.18 Contacting the Bank

5.18.1 No bidder shall contact the Bank on any matter relating to its bid, from the time of the bid opening to the time the contract is awarded.

5.18.2 Any effort by a bidder to influence the Bank in its decisions on bid evaluation, bid comparison or contract award may result in the rejection of the bidder's bid.

5.19 Award of the Contract

Post qualification

5.19.1 In the absence of pre-qualification, the Bank will determine to its satisfaction whether the selected bidder is qualified to perform the contract satisfactorily.

5.19.2 The assessment will consider both the bidder's financial and technical capabilities. It will be based upon an examination of the documentary evidence of the qualifications submitted by the bidder, as well as such other information as the Bank deems necessary and appropriate.

5.19.3 An affirmative determination of the bidder's capabilities to perform the contract satisfactorily will be a prerequisite for award of the contract to the bidder. A negative determination will result in rejection of the bidder's bid, in which event the Bank will proceed to the next preferred bid to make a similar determination of that bidder's capabilities to perform the contract satisfactorily.

Award Criteria

5.19.4 Subject to Section 5.19.2 of the RFP, the Bank shall award the contract to the successful bidder whose bid has obtained the highest bid score, provided further that the bidder is determined to be qualified to perform the contract satisfactorily.

5.19.5 The Bank reserves the right to accept or reject any bid, to annul the bidding process and reject all bids at any time prior to contract award, without thereby incurring any liability to the affected bidder or bidders or any obligation to inform the affected bidder or bidders of the grounds for the Bank's action. However, if the Bank determines that none of the bidders are responsive, the Bank shall notify each bidder who submitted a bid.

5.19.6 A bidder who gives incorrect information in the bid document about its qualification or who refuses to enter into a contract after notification of contract award shall be considered for debarment from participating in future procurement at the Bank.

5.20 Notification of Award

5.20.1 Prior to the expiration of the bid validity, the Bank shall notify the successful bidder in writing that its bid has been accepted.

5.20.2 The notification of award shall signify the formation of the contract subject to the signing of the contract between the bidder and the Bank pursuant to Section 5.21 of the RFP. Simultaneously the other bidders shall be notified by the Bank that their bids have not been successful.

5.21 Signing of Contract

5.21.1 Within fourteen (14) days of receipt of the contract, the successful bidder shall sign and date the contract and return it to the Bank.

5.22 Corrupt or Fraudulent Practices

5.22.1 The Bank requires that bidders observe the highest standard of ethics during the procurement process and execution of contracts. All bidders shall sign a declaration that they have not and shall not be involved in fraudulent practices.

5.22.2 The Bank will reject a proposal for award if it determines that the bidder recommended for the award has engaged in corrupt or fraudulent practices in competing for the contract in question.

5.22.3 Further, a bidder who is found to have indulged in corrupt or fraudulent practices, shall be debarred from participating in future procurement at the Bank.

5.23 Non-Disclosure and Confidentiality

5.23.1 All information contained in this RFP, unless the information is already in the public domain, are qualified as Confidential Information. All information contained in a bidder's bid, unless the information is already in the public domain, are deemed to be Confidential Information. Participants to this RFP are *de facto* under strict non-disclosure and confidentiality agreement with the Bank and each participant therefore mutually undertakes:

a. not to use or circulate the Confidential Information contained in this RFP or the bidder's bid within its own organisation except solely to the extent necessary for the purposes intended by its disclosure, and not to use the Confidential Information in any way which would or might be harmful to the other party;

b. to ensure that: (i) all persons such as, amongst others, its employees, to whom disclosure of the Confidential Information is necessary are made aware of the confidential nature of the disclosed Confidential Information, and (ii) these persons are subject to the same confidentiality obligations as the participant is subject to hereunder;

c. to effect and maintain adequate security measures to safeguard the Confidential Information from unauthorised access, use and misappropriation; and

d. to notify the other party of any unauthorised use, copying or disclosure of the Confidential Information of which it becomes aware and to provide all reasonable assistance to the party to terminate such unauthorised use and/or disclosure.

The above confidentiality obligations of the participants shall subsist during and after their relationship with the Bank.

5.24 Termination of Contract

Termination for Cause

5.24.1 Where the successful bidder fails to perform on the project or any separable part thereof in a timely or workmanlike manner in accordance with the contract, or otherwise fails, in the sole opinion of the Bank, to comply with any of the terms and conditions of the contract, or where the Bank is not satisfied with the works of the successful bidder, then the contract may be terminated by the Bank at any time within the contract period on giving ten (10) working days advance written notice to the successful bidder, who shall be liable to the Bank for any excess cost that may be incurred by the Bank. Default or breach of any clause of the contract shall constitute "cause" for termination.

5.24.2 Further, any act or omission by the successful bidder which is contrary to law or public policy shall be considered as a "cause" allowing for termination of the contract as provided herein. The Bank shall not be liable for any termination costs where termination is for cause. Whether or not the successful bidder's right to proceed with the project is terminated, it and its sureties shall be liable for any damage to the Bank resulting from the successful bidder's default/breach.

Termination for Convenience

5.24.3 The Bank shall have the right to terminate the contract for convenience upon giving ten (10) working days advance written notice to the successful bidder. In the event that the contract is terminated upon the request and for the convenience of the Bank, then the Bank shall pay the successful bidder for all materials purchased to date on the Bank's behalf and for the value of services rendered to date. The Bank shall not otherwise pay for costs of termination, opportunity costs or any costs or amounts of other description.

Excusable delays

5.24.4 The right of the successful bidder to proceed shall not be terminated for any delays in the completion of the work due:

a. to any acts of the Government, including controls or restrictions on requisitioning of materials, equipment, tools or labour by reason of war or any other national emergency;

b. to any acts of the Bank;

c. to causes not reasonably foreseeable by the parties to the contract and which are beyond the control and without the fault of negligence of the successful bidder, including, but not restricted to, acts of God or of the public enemy, acts of another successful bidder in the performance of some other contract with the Bank, fires, floods, epidemics, quarantine, restrictions, strikes, freight embargoes, and weather of unusual severity such as cyclones, and other extreme weather conditions;

d. to any delay of any subcontractor occasioned by any of the causes specified in subparagraphs (1), (2) and (3) of this paragraph, provided, however, the successful bidder promptly notifies the Bank in writing within ten (10) working days of the cause of the delay. Upon receipt of such notification, the Bank shall ascertain the facts and the cause and extent of delay. If upon the basis of the facts and the terms of the contract, the delay is properly excusable, the Bank shall extend the time for completing the project for a period of time commensurate with the period of excusable delay.

5.25 Commissioning

5.25.1 The successful bidder shall be required to prepare all necessary commissioning documents in duplicate and submit same to the Bank during the installation, configuration and testing period, for verification by staff of the Bank. Commissioning is deemed complete when the GRC solution is successfully installed, configured, tested, used successfully for a period of one-month, technical staff trained and commissioning documents signed.

5.26 Terms of payment

5.26.1 The term of payment shall be as follows:

20 % on allocation of contract;
50 % on delivery and installation of solution;
20 % on commissioning; and
10 % 3-month post commissioning, following satisfactory use of the tool.

5.27 Liquidated damages

5.27.1 The successful bidder shall pay liquidated damages for delays in delivery of the works up to a sum equal to 0.5 **%** of the value of the undelivered goods to the Bank for each day that delivery is delayed up to a maximum of 20 **%** of the contract amount.

6. Technical Requirements

6.1 Scope

6.1.1 The Bank is seeking qualified vendors capable of supplying, installing and configuring a GRC Tool. The Bank has a workforce of 400 staff.

6.1.2 A bidder must provide a detailed description of the proposed GRC Tool, including features, benefits and functionalities. The non-exhausting requirements of the GRC Tool are listed in Tables A to N below and in accordance with Annexure D. Any additional services offered – such as training, technical support and customisation – must be disclosed as well.

Table A: General/Platform

No	Requirements	Comply (Y/N)	Explanation or Reference to supporting document
A1	The tool should be able to provide customised dashboards and user interfaces based on the needs of different business units and stakeholders.		
A2	In respect of dashboards, can users drill down into the underlying data elements and to what level?		
A3	Does your system provide capabilities to create presentations using real-time data?		
A4	State the number of modules available in the system.		
A5	Automatic Notifications (GUI, emails and others) based new entries (e.g. new incidents, new actions etc) and/or based on a date (e.g. action due date)		
A6	Option to export data		
A7	Customised views/grids per user. Describe the system's graphing & charting capabilities.		
A8	Capability for Admin user to add new fields		
A9	Reporting functionality – generate customised reports based on data added in the system and the option to export the report in various formats (at least: PDF, Excel).		
A10	Schedule exporting of reports to specific recipients via email.		
A11	Information export options - All information about the Risk/Loss event can be exported as a separate report as well as in Excel or CSV.		
A12	Does the solution support the ability to import external data in support of advanced analytics and visualizations relative to risk data?		
A13	Does the system support presentation-ready reports and dashboards?		
A14	Document Management: Can workflow in manual of procedures be shown for each major task/function in each department/division?		
A15	Describe how workflows are created and modified		
A16	Does the system support configurable workflow that tracks the way tasks are carried out?		
A17	Prefix Suffix functionality		
A18	Option to send emails through the system		

Table B: User Accessibility

No	Requirements	Comply (Y/N)	Explanation or Reference to supporting document
B1	Admin User: Full access to all the information of the module, with ability to configure the system.		
B2	General User: Full access to all the information of the module, with no ability to configure the system.		
B3	Simple User: Access the system to perform RCSA, register signals, incidents and actions.		
B4	Review User: Access user role and conduct user auditing		

Table C: System

No	Requirements	Comply (Y/N)	Explanation or Reference to supporting document
C1	Capability to user Microsoft/Azure AD Single Sign-on.		
C2	Is the solution on-premise?		
C3	Integration: The system should integrate seamlessly with our existing IT systems, to allow for the exchange of data and information.		
C4	What is the maximum of staff that can be trained to use the tool and modules provided? Bidders to elaborate.		
C5	What is the package (cost per month/year) for the number of users who can access the platform?		
C6	User-friendly interface: The system should have a user-friendly interface that is easy to navigate and use and requires minimal training to operate.		
C7	Describe how the system leverages AI and machine learning.		
C8	Can a training module be implemented to facilitate use of the platform?		
C9	Can a training module be implemented to raise general awareness on risk areas and risk controls?		

Table D: Risks

In line with a framework following the Committee of Sponsoring Organizations (COSO) principles, with the functionality to:

No	Requirements	Comply (Y/N)	Explanation or Reference to supporting document
D1	The system should have a capability to identify and capture risks across different departments and business processes. The system should allow for the addition of new risks and modification of existing ones.		
D2	Provide with embedded comprehensive risk taxonomy.		
D3	The system should provide 4-eyes principle for approval of new risks and other related criteria taxonomies.		
D4	Single Risk Summary - Clicking on a risk in the risk register shows the complete details of the risk including: • inherent, residual risk assessments, • control assessments, • suggested and approved management actions, • linkage to processes and root cause categories, • financial actual and potential financial impact, • linked incidents, systems, vendors etc.		
D5	Define action plans with specific deadlines, action owners, follow-up actions, automated communication e.g. inform action owners of new assignment.		
D6	Provide build-in libraries for list fields, such as risk types, controls.		
D7	Apply various levels of pre-defined access rights.		
D8	The system should provide real-time monitoring of risks and allow for the generation of customisable risk reports, including heat maps and dashboards.		
D9	Ability to monitor risks and provide alerts when risk levels change.		
D10	Ability to track the progress of mitigation efforts.		
D11	Ability to generate reports and dashboards to provide management with a holistic view of risks and the status of mitigation efforts.		

D12	Describe how risks are managed in the system including creating, editing, categorising and assigning owners.		
D13	Describe the system's ability to correlate and integrate risk relationships within the Bank and how is it visualised and reported on?		
D14	Describe how risks can be linked to controls, processes and policies.		
D15	Does the platform have the ability to run business resilience tests (Business Continuity Plan)?		
D16	Does the system support Business Impact Analysis (BIA) data to be input on a platform in terms of: • Prioritised business activities, • Probability of impact and • Planning required		
D17	Does the system cater for calculation/input of: • Maximum Acceptable Outage (MAO) • Maximum Tolerable Period of Disruption • Recovery Time Objective (RTO) • Recovery Point Objective (RPO) – maximum data loss		
D18	Can checklists be uploaded or the implementation of Business Continuity Plan?		
D19	Perform qualitative and monetary assessments of inherent and residual risk.		
D20	Monitor risks against established tolerances and risk appetite.		
D21	Manage risk scenarios on a consolidated basis, performing risk assessments and relating them to the risk register.		
D22	Visibility into assessment progress, risk treatments and remediation activity via pre-defined reports and risk dashboards.		

Table E: Key Risk Indicators (KRIs)

No	Requirements	Comply (Y/N)	Explanation or Reference to supporting document
E1	Functionality to maintain a register of Key Risk Indicators (KRIs) and create new ones.		
E2	The system should provide that actual values of the KRIs automatically updated using various data in the system.		
E3	The system should have notification functionality of responsible employees in case the KRIs have reached the critical/red zone.		
E4	The configuration of KRIs thresholds should follow the traffic light principle.		
E5	The system should support manual registration of other values needed for KRIs values calculation.		
E6	The systems should support the storage of historical values of KRIs.		
E7	Ability to generate reports and dashboards to provide management with a holistic view of KRIs.		
E8	Describe how the solution supports relating KRIs to specific risks or risk categories.		
E9	Describe how the solution supports defining risk thresholds around risk appetite statements and KRIs.		
E10	Can we link specific KRIs to the inputted metrics of the risk appetite statement?		

Table F: Risk Assessment

No	Requirements	Comply (Y/N)	Explanation or Reference to supporting document
F1	Bottom-Up Risk Assessments - have the option to assess risks either by various units and/or by the risk unit by further option for consolidation.		
F2	Automatic reminder when the risk should be reviewed/assessed.		
F3	At least 3 assessment methodologies - the system should allow to conduct the Risk Control Self-Assessment (RCSA) using qualitative and quantitative risk assessments, as well as automatic or manual risk score calculations.		
F4	Ability to assess the impact and likelihood of identified risks, prioritise them based on their potential impact, and assign risk owners.		
F5	Risk response planning: The system should allow for planning and tracking of risk response plans, including risk mitigation, risk transfer, risk acceptance and risk avoidance strategies.		
F6	What functionality exists to quantify risk factors related to GRC?		
F7	Can risk scores be weighted?		
F8	What calculations are available to quantify risk factors?		
F9	The system should create risk heat maps. Describe how heatmaps can be configured to display risks. Include how the heatmaps can be filtered.		
F10	Risk heatmaps by inherent and residual risk level.		
F11	The solution should provide the ability to map inherent and residual risk scores to qualitative risk assessment criteria (e.g., high, medium, low).		
F12	Multiple stakeholders make their own assessment of the risk. Explain how is this handled in the system.		
F13	Describe the forecasting capabilities.		
F14	Describe how the system can calculate the total cost of risk and facilitate the allocation of these costs within the Bank.		
F15	Efficient management of self- assessment campaigns by second line of defence stakeholders, including necessary workflow to vet and challenge first line of defence assessments.		
F16	Robust key risk and control indicator program management to provide early warning and remediation.		

Table G: Incidents Management

No	Requirements	Comply (Y/N)	Explanation or Reference to supporting document
G1	Must contain the following fields: • Impacted department, • Incident date, • Incident loss/potential loss, • Incident description, • Incident cause, • Control weakness/breach identified, • Actions taken to date, • Incident status following actions, • Incident review by Second line of Defence		
G2	Comprehensive classification - The losses recorded can be classified according to various loss event types, root cause categories and recovery options.		
G3	Related risks registration option (e.g. financial and non-financial risks)		
G4	Define action plans with specific deadlines, action owners, follow-up actions, automated communication e.g. inform action owners of new assignment		
G5	Ability to assess the type, severity, and impact of incidents and assign priority levels based on the criticality of the incident.		
G6	Ability to track incidents from the initial report to closure and document all activities related to the incident.		
G7	Ability to generate reports and dashboards to provide management with a holistic view of incidents and the status of response efforts.		
G8	Ability to assign incidents to the affected units (divisions/departments).		
G9	Option to add supporting documents.		
G10	The system should provide task-management capabilities for creating, assigning and tracking tasks. Please describe.		

Table H: Alerts/Signals Management

No	**Requirements**	**Comply (Y/N)**	**Explanation or Reference to supporting document**
H1	The system should have separate functionality for actual or potential risk event registration by any employee. Any user will be able to register an event related to a risk.		
H2	The system should support integration of the module with the organisation's other systems.		
H3	Automated feedback option on the status of loss event identified by the person.		
H4	Automated notifications/alerts functionality to responsible employees for registered signal's review.		
H5	The system should support the • conversion of signal in incidents and • the grouping signals in one incident by predefined common criteria into the system.		
H6	The system should support segmentation of users to differentiate: • the user level and • the corresponding categories of the Signals.		

Table I: IT and Security Risk Management

No	Requirements	Comply (Y/N)	Explanation or Reference to supporting document
I1	Repository and taxonomy for IT risks and controls.		
I2	Prebuilt risk and threat assessments to manage risk assessment processes.		
I3	Centralised tracking of gaps and remediation activities for compliance issues.		
I4	Comprehensive built-in governance framework and taxonomy (ISO 27000, NIST, COBIT, PCI-DSS)		
I5	Automated workflow and change management.		
I6	Catalogue resources related to ISMS, including information assets, applications, business processes, devices and facilities.		
I7	Document and maintain an information security risk register.		
I8	Establish policies and standards in support of the ISMS.		
I9	Identify, document, and manage Cybersecurity Maturity Model Certification (CMMC).		
I10	Identification, documentation, management, and resolution of deficiencies across security requirements.		
I11	Built-in risk calibration and analysis engine for cyber risk calculation.		
I12	Realtime status dashboarding.		

Internal Audit Management Module

The solution should include an Internal Audit management (IA) system that will eliminate manual processes and gain comprehensive real-time visibility into audit findings, as well as audit programs, issues and trends. The system should be user-friendly, easy to integrate with our existing systems, and scalable to accommodate our growing needs.

Table J: Internal Audit Features

No	Requirements	Comply (Y/N)	Explanation or Reference to supporting document
J1	The system should have the functionality of IA Universe creation in accordance with the requirements of International IA standards.		
J2	The user should be able to add and remove IA Universe elements as well as link them to Risk register and the Bank's Divisions/Departments/Units.		
J3	The system should have embedded IA Risk Assessment methodology that complies with the requirements of International IA standards.		
The IA Risk Assessment should be linked to IA Universe elements and should include the following qualitative and quantitative assessment elements:			
J4	The results of the performed RCSA of all risks (financial and non-financial, including compliance). The results should be automatically transferred from GRC module and included in the IA Risk assessment in accordance with the embedded methodology.		
J5	The results of risk assessment of Incidents registered in GRC. The results should be automatically transferred from GRC module and included in the IA Risk assessment in accordance with the embedded methodology.		
J6	Input of Internal Audit on the risks (i.e. risks known to Internal Audit, different opinion on the risks assessed by the other control units).		
J7	Date the area was last audited.		
J8	Past Internal Audit findings (from past audit reports).		
J9	Scope of the area audited		
J10	Mandatory/regulatory audits.		
J11	Complaints.		
J12	Financial information that could be used to provide an indication of the risks involved to also be included. The below are some examples of what can be included and preferably to be able to include comparative amounts		

	(i.e. 2 different periods and the %increase/decrease to be calculated and % to totals). • assets • Investments • Salaries • Directors remuneration separately • Expenses • NPL • Provisions		
13	Man days needed for defined auditable areas.		
J14	Comparison with the man days available.		
J15	The system should have IA Risk assessment review and approval work flow as well as report generation capability.		
J16	The system should have the functionality to create risk based Annual Internal Audit Plans in accordance with the requirements of International IA standards.		
J17	Annual Internal Audit Plan should be automatically generated in accordance with the performed IA Risk Assessment and should include separate entries for each planned internal audit engagement.		
J18	The system should have Annual Internal Audit Plan review and approval workflow as well as report generation capability.		
J19	Internal Audit Engagements should be created in accordance with the planned Internal audit engagements included in the Annual Internal Audit plan.		
J20	The functionality should include: Creation of Engagement plan, including the following details: • Engagement objectives • Engagement scope • Engagement planned resources • Engagement planned control tests • Engagement planned other tasks • review and approval work flow capability for Engagement plan		
J21	Sending information submission requests to different users with submission due dates.		
J22	Review and approval work flow capability for information submission.		
J23	Registration of working papers by internal auditors.		
J24	Review and approval work flow capability for working papers.		

J25	Registration and assessment of internal audit findings.		
J26	Storage of files separate in each section of the module.		
J27	Review and approval work flow capability for findings.		
J28	Capability of Engagement report creation with the following information to be included: • Engagement plan • Engagement conclusion • Engagement risk assessment • Findings and recommendations • review and approval workflow capability		
J29	The system should have the functionality of findings and related recommendations registration in accordance with the requirements of International IA standards.		
J30	The system should have review and approval workflow capability for findings.		
J31	The finding profile should include the following: - related engagement - related risks - risk assessment - related systems - related functions and or Bank's units - related business processes - responses and comments - files enclosed - automated status functionality considering the stage of the finding - related recommendations.		
J32	The recommendation profile should include the following: - recommended mitigating actions - approved recommendation with the link to recommended mitigating actions - register the approval and date - register responsible users and due dates - recommendation status control capability - review and approval work flow capability - follow-up plan capability for regular monitoring of recommendations' statuses - follow-up plan reporting capability.		
J33	The auditor should have the option to select the controls for testing and registration of testing results.		
J34	Testing results should be aggregated at the control level and test plan level.		
J35	Control test plans and testing results should be linked to:		

	- specific Engagement - risks - systems - vendors if applicable - working documents.		
J36	Review and approval workflow capability for control testing results should be available.		
J37	The system should have man days calculator that should include the following: - Separate planned and actual man days calculator for each internal auditor. - Functionality for reporting of actual man days spent on specific internal audits by the internal auditors. - Separate user rights for man days spent approval. - Man days spent summary functionality separately by internal auditors and internal audits - Widgets displaying real time status on planned and actually spent man days by internal auditors and internal audits.		
J38	The IA System should have the following technical requirements: • Web-based and accessible from desktop and mobile devices • Multi-factor authentication • Configurable workflows and business rules • Customizable dashboards and reports • Integration with third-party systems, including but not limited to, accounting, HR, and compliance systems • Strong security features, including role-based access control, encryption, and multi-factor authentication.		
J39	The system should be able to provide customized dashboards and user interfaces based on the needs of different Divisions/Departments/Units.		
J40	Automatic Notifications based on new entries (e.g. new incidents, new actions etc) and/or based on a date (e.g. action due date).		
J41	Option to export/import data.		
J42	Customized views/grids per user.		
J43	Capability for Admin user to add new fields.		

J44	Reporting functionality – generate reports based on data added in the system and the option to export the report in various formats (at least: pdf, word, excel).		
J45	Document Management.		
J46	Prefix Suffix functionality.		
J47	Option to send emails through the system.		
J48	Information export options - All information about the Risk/Loss event can be exported as a separate report as well as in excel.		
J49	Audit trail for all users' activities.		
J50	Audit trail for all users' activities		
	Report		
J51	The solution should generate report and release to the Auditee after completion of the Audit Execution phase.		
J52	Response of Auditees to each Observation/Recommendation through the portal.		
J53	Access of Auditee to the Portal, where they can record their responses/upload documents, timelines and action plans.		
J54	Once response is received from the auditee, it is reviewed and then incorporated in the Final Report.		
	Follow up and Tracking		
J55	Once the Final Report is released and approved, audit team should monitor and track the follow-ups of unresolved audit observations on a periodic basis.		
J56	Audit teams and auditees must be informed of the progress of outstanding observations through periodic alerts.		
J57	Auditees should be able to record their responses/upload documents, timeliness and action plans.		
J58	The response shall be reviewed by the auditors. If satisfied, the follow up will be closed.		
J59	Integration: The system should integrate seamlessly with our existing IT systems, including our enterprise resource planning (ERP) system, to allow for the exchange of data and information.		
J60	Security: The system should be secure and comply with the Bank's IT Security policies.		

Table K: Change Management

No	Requirements	Comply (Y/N)	Explanation or Reference to supporting document
K1	The system should have separate functionality for risk assessment of new products, markets, systems, vendors, services etc.		
K2	Option to show the risk profile of the organisation and dynamic heat maps considering the risk assessments of new products, markets, services etc.		
K3	The system should have a change management workflow module for the Bank's internal IT and other divisions (initial change request and several approval levels)		
K4	Please describe the solution's ability to provide workflows (e.g., any approval, assignment of corrective actions, etc).		
K5	Do workflow automations and approval processes execute immediately? Can they be scheduled and triggered?		

Table L: Other Requirements

The GRC Tool should have the following technical requirements:

No	Requirements	Comply (Y/N)	Explanation or Reference to supporting document
L1	Web-based and accessible from desktop and mobile devices using HTTPs.		
L2	Configurable workflows and business rules, dual control and approval levels.		
L3	Customisable dashboards and reports.		
L4	What reporting is available to present the risks and the likelihood of occurrence?		
L5	Integration with third-party systems, including but not limited to, accounting, HR, and compliance systems		
L6	Strong security features, including role-based access control, encryption (at rest and in transit), dual control and multi-factor authentication.		
L7	The solution should provide the ability to link records to each other throughout the application for reporting and reference.		
L8	Does the system allow for associations to be easily made across your organization in a visual manner? For example, linking risks to corporate objectives or controls.		
L9	What audit trails are available for fields, documents, or policies?		
L10	The solution should offer integration with standard email programs (i.e., Microsoft Outlook).		
L11	Describe the solution's ability to provide workflows specific to GRC.		

Table M: Information Security Requirement

No	Requirements	Comply (Y/N)	Explanation or Reference to supporting document
M1	A different platform should be provided for test which is distinct from production. Data on from the production environment should never be used on the test platform. Data to be used on any environment should be first authorised by the Bank.		
M2	Database proposed and implemented for the systems should allow for encryption of data, auditing of user access and transactions in the data base. Furthermore, it shall also provide data masking functionalities.		
M3	Unnecessary database users (e.g. root, admin), default passwords and stored procedures shall be eliminated and the principle of least privilege for the application database to defend against SQL query poisoning shall be followed.		
M4	During implementation, secured protocols shall be used to communicate with the database and efficient indexing shall be implemented for rapid data retrieval.		
M5	Application design should prevent Bank's IT support and admin resources to have access to or able to view live and production data as part of their normal day to day activity. Restricted administrative access should be implemented.		
M6	Solution provider shall apply the latest stable patches and updates available on all systems deployed. This shall not be done prior to testing on test environment at the Bank and shall be authorised by the Bank.		
M7	Applied firmware, updates and hotfixes shall be downloaded only from sites recommended by the suppliers.		
M8	OS Hardening shall be performed for all systems deployed for this solution especially on the production server prior to going live.		
M9	Application should provide user the functionality to setup complex passwords consisting of uppercase, lowercase and special characters. The application should have a separate user administration module for user access administration.		

M10	Proper mechanism shall be implemented to ensure that user access reviews are properly replicated to the DR site.		
M11	User Access to modules shall be on a least privilege and on a need to know basis.		
M12	Certificates to be used for HTTPs implementation shall not be self-generated and should be certified either by a certifying authority or by using an offline root CA. The existing certificate for the current website can be used.		
M13	The application should create session keys with lengthy strings or random number to prevent guessing of valid session key.		
M14	Application should regenerate session IDs after a successful login to prevent session fixation attack.		
M15	Application shall provide configurable session time-outs and account lockout with proper reset mechanism.		
M16	Encryption of data and session key that is transferred between the user and the web servers should be implemented. HTTPs or equivalent secured implementation will be required for all web-based applications.		
M17	As far as possible, the admin console port should be changed from the default and a new well documented port should be used.		
M18	Security and risk mitigation should be formal design criteria in any Software Development Life Cycle ("SDLC") process and start with threat and risk assessment of the proposed system, identification of controls, implementation of those controls, and testing and review. Security should not be an afterthought, and controls retrofitted in an ad hoc way only after security weaknesses are identified. Suppliers will be required to consider the OWASP and OWASP MAS Top Ten application security risks during the design and implementation of the systems.		

M19	Application controls for input, processing and output functions shall be implemented. They should include methods to help ensure data accuracy, completeness, validity, verifiability and consistency, thus achieving data integrity and data reliability. Also controls shall consist of edit tests; totals; reconciliations and identification; and reporting of incorrect, missing or exception data.		
M20	Automated controls should be coupled with manual procedures to ensure proper investigation of exceptions. Implementation of these controls helps ensure system integrity; that applicable system functions operate as intended; and that information contained by the system is relevant, reliable and secure.		
M21	Application shall be designed to capture all user access and activity in the system. Logs shall be kept for auditing purposes. Archiving and rapid retrieval of these logs shall be a mandatory feature.		
M22	User access to application shall be based on two-factor authentication. The solution provided shall be integrated seamlessly to prevent complexity and management overheads. The supplier may integrate their application with the Bank's existing two-factor authentication system which is based on Open OTP solutions.		
M23	Security controls shall be implemented based on the risk management process of the Bank and it should be documented to explain how the inherent risks have been mitigated and the residual risk after the application of the security controls. This shall also document the control risk.		

Table N: Server

Bidders should supply the Bank with two (2) servers [Head Office (1) and DR (1)] in case the solution is on-premise. No OS or software is required. The specification for the server is as follows:

No	**Server Quantity: 2**		
	Feature per server	**Type**	**Please specify**
N1	Processor Architecture		
N2	Processor Clock Speed		
N3	Number of physical CPU cores		
N4	Multi-threading support		
N5	Hyper-threading support		
N6	Virtualisation support		
N7	Memory		
N8	Hard Disk		
N9	Hard Disk (SSD)		
N10	Network Interface	4 x 1Gbps	
N11	Power Supply	Dual Power	
N12	Remote Console management	Net Management	
N13	Power Cords	C13, 2 x 3 Metres	
N14	Form Factor	Rack Mountable. Rail kits to be provided	

6.2 Project implementation plan

The bidder is required to provide a detailed implementation plan for the GRC project together with a timeline and project governance framework. The list all personnel involved in the project including their roles/functions has to be submitted.

Project Management Report (to be included as part of the Technical Proposal submission)

The bidder would be required to provide periodic reports on how the project is progressing.

The formats of the reports would be discussed and agreed upon prior to the commencement of the project. An indicative list of reports is provided below:

Table O: Implementation

No	Project Stage	Report	Frequency
O1	Implementation	Main Project Status Report: • Project progress vis-à-vis planned timelines. • Tasks completed during the week. • Issues and concerns (Prioritise - Low, Medium & High). • Current period's accomplishment compared to the Project timeline. • Pending action items from previous reporting period. • Next steps. • Interventions required.	• Weekly • Monthly
O2	Maintenance	Maintenance Status Report: • Periodic update on maintenance activities. • Periodic SLA performance reports.	As per SLA requirements and/or mutually agreed between the Bank and the successful bidder

7. Profile of the Bidder

7.1 Confidential Business Questionnaire

Bidders are advised that it is a serious offence to give false information under this section as it may render the bidder and its bid being automatically disqualified from the present tender exercise. The bidder may also be disqualified from participating in future tender exercise of the Bank.

7.1.1 Part I: General Information

- The questionnaire must be fully and comprehensively completed in all respects.
- Information given by the bidder shall be treated in strict confidence.
- Any information given and later found to be incorrect shall lead to disqualification of the bidder.
- Deliberately incorrect information leads to disqualification of the bidder's proposal.
- Canvassing will lead to automatic disqualification of the bidder.

7.1.2 Part II: Bidder Details

- The purpose of this section is to provide the required background information of the bidder.

  a. The bidder to provide documentary evidence of the registered name, number and date of registration of Company.

     Company Name
     Company Registration Number
     Country of Registration
     Registration Date

  b. The bidder to give full details of its bankers.

7.1.3 Part III: Details of Contact Person(s)

- The bidder to provide the contact person(s) name(s), addresses, phone numbers, etc.
  Contact Person Name
  Landline Telephone Number
  Cellular Telephone Number
  Facsimile Telephone Number
  E-mail
  Postal Address
  Permanent Address

- The bidder to provide evidence of its registered street and postal addresses
  Registered Street Address
  Registered Postal Address

- The bidder to provide evidence of current registration with relevant regulatory body within its industry, if any.

7.1.4 Part IV: Bidder’s Organisation Profile

- The bidder to provide details of the holding company and the main shareholders indicating percentage of shares held.
- The bidder to provide a list with the estimated percentage of revenue earned from each of the primary business activities of the bidding organisation.

7.1.5 Part V: Bidder’s Client Base

- The purpose of this section is to get a view of the number and profile of customers that the bidder has.

  The Bank intends to contact these customers when checking references. The bidder is expected to state any objections. If not stated, it shall be deemed that the Bidder has authorised the Bank to contact these customers.

- The bidder to provide references from its major clients where it has successfully carried out similar or comparable assignment.

7.1.6 Part VI: Bidder’s Standard Contracts

- The bidder to describe its approach to contracting and negotiation specifically relating to the availability and use of standard contracts and whether it considers any of the standard contracts or specific clause to be not negotiable.
- The bidder to provide details of the preferred payment plan if not contained in the standard contract supplied.

7.1.7 Part VII: Verification of Business Sustainability

- The bidder to provide certified audited financial statements for the last three (3) financial years. The supply of these financial statements will be mandatory for the bid to be considered responsive.

- The bidder to state whether it is currently involved in any litigation or arbitration (or any other legal process which may result in legal or financial liability).

  If yes, is the bidder to provide the financial exposure as a result of the litigation, arbitration or other legal process and on the basis on which this financial exposure has been calculated.

  If yes, the bidder to also state what other exposure could result from the litigation, arbitration or other legal process and whether this financial or other exposure will materially prejudice the bidder’s financial position or its ability to successfully and timely implement any contract which may be awarded to it pursuant to this bid.

- The bidder to confirm whether it has ever:

Question	***Response (Yes/No)***
Forfeited any payment on a contract?	
Been declared in default of a contract?	
Negotiated the premature termination of a contract?	
Had an uncompleted contract assigned to another solution provider?	

The Bidder authorises the Bank, as part of its bid evaluation exercise, to consult the Credit Profile Report of the bidder, if any, maintained on the Mauritius Credit Information Bureau (MCIB).

7.1.8 Part VIII: Technical Support & Capacity Building

- The bidder to state its policy on technological (maintenance) and operational support including capacity building (training) that it offers to its clients.

7.1.9 Part IX: Details on Previous or Current Blacklisting of the Company or the Shareholders and/or Directors of the Company, if any

- The bidder shall:
  a. certify to the Bank by way of a written undertaking that **none** of its shareholder(s)/director(s)/beneficial owner(s) have been involved or alleged to have been involved in any case of bribery, corrupt or fraudulent practices, money laundering and/or otherwise debarred from participating in any public procurement.
  b. inform the Bank whether any of its directors, shareholders or beneficial owners have ever made any arrangements or composition with creditors, filed for bankruptcy or adjudged bankrupt or been convicted with a criminal offence and if so, the nature thereof.
  c. where applicable, provide the Bank with the written consent of the bidder, shareholder(s)/director(s)/beneficial owner(s) allowing the Bank to request for their respective Credit Profile Reports, to be used solely for the purpose of this RFP exercise.

Certification

I/We do hereby certify that the above information is correct in all respects.

Full Name : ……..

Designation/Position : ……..

Signature : ……..

Date : ……..

Company Seal and/or Stamp:

8. Annexures

Annexure A: Eligibility Criteria

<Name of the bidder>

A-1	The bidder should provide a cover letter, duly signed by an authorised senior executive, specifying inter alia contact details of the company in the format specified at **Annexure C**.
A-2	The bidder should provide a comprehensive document describing the underlying concepts of the system and the technicalities.
A-3	The bidder must be already engaged in the supply and installation of a GRC solution. The following details should be provided as per **Annexure B**: - Entity name - Contact person - Telephone and email address of contact person - Project name and scope - Composition of implementation team (bidder, subcontractor's/system integrators) - Year of engagement - Project duration - Total cost of project (in MUR)
A-4	The bidder should be a standalone business entity and should have an annual turnover of at least MUR 40 million for the previous three (3) financial years. The bidder should provide audited financial statements (Balance Sheet, P&L, Cash Flow and Notes to Accounts) for the last three (3) financial years. The accounts must be audited by a reputable audit firm.
A-5	The bidder may provide current and potential contracts in hand and any other relevant information to enable the Bank to take a view of its future financial strength. The bidder may provide any additional information that can help in the evaluation of its financial health.

A-6	The Bank will reject any bidder who may have been involved or alleged to have been involved in any corrupt or fraudulent practices, money laundering and, debarred from participating in any public procurement. The bidder must provide a written undertaking for this purpose.
A-7	The bidder shall provide the details of proposed Project Management Team (Directors, Managers etc.) and Implementation Team members, with past experience in similar projects.
A-8	The bidder should provide the list of their directors, beneficial owners and executive management. The Bank will reject any bidder whose director or beneficial owner or member of executive management may have been involved or alleged to have been involved in any corrupt or fraudulent practices or money laundering.
A-9	The bidder should provide the shareholding structure of the company indicating majority shareholders. Refer to **Annexure C**.
A-10	The bidder shall not outsource the project to any other third-party company.

Annexure B: Details of the GRC Tool already set up by Bidder

B-1	Project Name	
B-2	Entity Name & Address	
B-3	Client Contact Person Name: Designation: Phone Number: Fax Number: Mobile Number: Email Address:	
B-4	Project Value in MUR	
B-5	Sector	
B-6	Project Schedule Start Date End Date (as per PO) End Date (actual)	
B-7	Composition of Implementation Team	

B-8	Detailed Scope of Project	
B-9	Geographical Spread of Client	City/Province/Country/Global
B-10	Bidder's Role in the Project (Project Management / Design/ Set up / Maintenance / Testing)	
B-11	Overall Client Satisfaction (Excellent/Good/Satisfactory/Below Average)	

Annexure C: Bid Form

The Chairperson - Tender Committee
Bank of Mauritius
Sir William Newton Street
Port Louis 11328
MAURITIUS

Dear Sir/Madam,

SUPPLY, INSTALLATION AND CONFIGURATION OF A GOVERNANCE, RISK AND COMPLIANCE (GRC) TOOL FOR THE BANK OF MAURITIUS (BANK)

In accordance with the Request for Proposal (RFP) bearing reference BOM/GRC/8-2023 dated 01 August 2023 for the execution of the above works, we, the undersigned, offer to undertake the above works to the entire satisfaction of the Bank.

We are hereby submitting our Proposal, which includes a Technical Proposal and a Financial Proposal, by email encrypted as per the requirements of the RFP.

1. We acknowledge that the Annexures to the Bid Form forms part of our bid.
2. We undertake, if our bid is accepted, to commence the works as soon as is reasonably possible after the receipt of the Letter of Acceptance.
3. We agree to abide by this bid for a period of 180 days from the date of bid opening and it shall remain binding upon us and may be accepted by the Bank at any time before the expiry of this period.
4. Unless and until a formal agreement is prepared and executed, this bid together with the Bank's written acceptance thereof shall constitute a binding Contract between us.
5. We understand that the Bank is not bound to accept the lowest bid or any bid that it may receive without giving any reason whatsoever. The Bank may also cancel the whole tendering exercise without giving any reason therefor and incurring any liability in that respect.
6. We also authorise the Bank, as part of its bid evaluation exercise, to consult the Credit Profile Report of the bidder, if any, maintained on the Mauritius Credit Information Bureau (MCIB).

Name of Contractor: ……………………………………………………………………………………………
Signature of the first Director …………………………………………………………………………….
Address………………………………………………………………………………
………………………………………………………………………………………….

Date……………………………………………………………………………….

Signature of the second Director ……………………………………………………………………………
Address………

…………………………………………………………………………………………..

Date……………………………………………………………………………..

Company Seal

Bidder's details

No.	Description	Details
C-1	Name of bidder	
C-2	Date of incorporation and/or commencement of business	
C-3	Certificate of incorporation and details of shareholders and directors.	
C-4	Brief description of the bidder including details of its main line of business	
C-5	Particulars of company	
C-5.a	Website URL	
C-5.b	Address	
C-5.c	Phone number (Landline)	
C-5.d	Mobile number	
C-5.e	Fax number	
C-5.f	Email address	
C-6	Particulars of the authorised signatory of the bidder	
C-6.a	Name	
C-6.b	Designation	
C-6.c	Address	
C-6.d	Phone number (Landline)	
C-6.e	Mobile number	
C-6.f	Fax number	
C-6.g	Email address	

Annexure D: Information Security Requirements

D-1	The database proposed and implemented for the systems should allow for encryption of sensitive data, auditing of user access and transactions in the data base. Furthermore, it shall also provide data masking functionalities.
D-2	Unnecessary database users (e.g. root, admin), default passwords and stored procedures shall be eliminated and the principle of least privilege for the application database to defend against SQL query poisoning shall be followed.
D-3	During implementation, secured protocols shall be used to communicate with the database and efficient indexing shall be implemented for rapid data retrieval.
D-4	Restricted administrative access should be implemented.
D-5	The solution provider shall apply the latest stable patches and updates available on all systems deployed.
D-6	OS Hardening shall be performed for all systems deployed for this solution.
D-7	The application should provide the user the functionality to setup complex passwords consisting of uppercase, lowercase and special characters. The application should have a separate user administration module for user access administration.
D-8	Proper mechanism shall be implemented to ensure that user access reviews are properly replicated to the DR site.
D-9	User Access to modules shall be on a least privilege and on a need-to-know basis.
D-10	The application should create session keys with lengthy strings or random number to prevent guessing of valid session key.
D-11	The application should regenerate session IDs after a successful login to prevent session fixation attack.
D-12	The application shall provide configurable session time-outs and account lockout with proper reset mechanism.
D-13	Encryption of data and session key that is transferred between the user and the web servers should be implemented. HTTPs or equivalent secured implementation will be required for all web-based applications.
D-14	Automated controls should be coupled with manual procedures to ensure proper investigation of exceptions. Implementation of these controls helps ensure system integrity; that applicable system functions operate as intended; and that information contained by the system is relevant, reliable, secure and available when needed.
D-15	Application shall be designed to capture all user access and activity in the system. Logs shall be kept for auditing purposes. Archiving and rapid retrieval of these logs shall be a mandatory feature.

Annexure E: Request for Clarifications

Bidders requiring specific points of clarification may communicate with the Bank during the specified deadline for sending queries in the Bid Information Sheet using the following format. The column Clarifications is reserved for the Bank to respond to bidder's queries.

Query No.	Requirement Number	Current Specification	Query (In terms of Clarification or Modification or Addition of New Clause)	Clarifications
1				
2				
3				
4				

Annexure F: Price Schedule of Services

A bidder shall make a Financial Proposal based on its Technical Proposal.

The tables below shall be used as format in responding to the Financial Proposal. The items in the table below are indicative and may be changed by the bidder.

Overall Cost for the whole Project

Bidders are required to provide overall cost for the project as well as a break down cost of all the different modules, options and licences as necessary. Prices should include all taxes and should be in Mauritian Rupees. Additional modules (or options) and breakdown costs may be included by bidders, if needed.

On premise***/hybrid*** solution

No.	Item	Total Cost
1	Software License	
2	Hardware	
3	License, Support (including training) &Maintenance for five (5) years	
	Total	

Maintenance Cost

Item	Year 1	Year 2	Year 3	Year 4	Year 5
Hardware (Head Office)					
Software License (Head Office)					
Hardware (DR Site)					
Total					

Maintenance cost for 5 years (excluding first year where the solution is expected to be under warranty for the first year).

Signature of bidder ____

Note: In case of discrepancy between unit price and total, the unit price shall prevail.