



ශ්‍රී ලංකා මහ බැංකුව
இலங்கை மத்திய வங்கி
CENTRAL BANK OF SRI LANKA

ලේකම් දෙපාර්තමේන්තුව
செயலகத் திணைக்களம்
SECRETARIAT DEPARTMENT

අංක 30, ජනාධිපති මාවත, කොළඹ 01, ශ්‍රී ලංකාව
இல. 30, சனாதிபதி மாவத்தை, கொழும்பு - 01, இலங்கை
No. 30, Janadhipathi Mawatha, Colombo 01, Sri Lanka

09/04/135/2023/001

07 March 2024

REQUEST FOR EXPRESSION OF INTEREST PROCUREMENT OF GOVERNANCE, RISK, AND COMPLIANCE (GRC) SYSTEM

The Central Bank of Sri Lanka (CBSL) invites Expressions of Interest (EOIs) from reputed and experienced vendors to provide a comprehensive commercial off-the-shelf (COTS) system as a Governance, Risk, and Compliance (GRC) solution. CBSL seeks to implement an integrated GRC solution that addresses multifaceted requirements in Risk Management, Incident Management, Compliance, Internal Audit, and Strategic Planning.

1. Introduction

As the monetary authority and the apex financial sector regulator in Sri Lanka, CBSL plays a pivotal role in ensuring price stability and financial system stability. With the commitment to maintain the highest standards of governance and risk oversight in its affairs, CBSL recognizes the need to adopt a robust and unified GRC solution to streamline and enhance its risk management practices across various operational domains.

Accordingly, the CBSL endeavours to automate its risk management framework, which is built upon the Three Lines model, where the first line consists of all business units, second line consists of risk management, compliance and information security functions and the third line consists of the internal audit function.

Currently the operations are handled in a disintegrated manner using a blend of manual and semi-automated processes with in-house developed software.

2. Requirements

The envisioned GRC system should encompass comprehensive functionalities across the following key areas, which need to be automated and integrated:

- 2.1. **Risk Management:** Facilitating risk identification, assessment, mitigation, and monitoring across diverse risk categories by following ISO 31000 standards. Further, the module should facilitate incident management.
- 2.2. **Compliance:** Supporting regulatory compliance adherence by providing tools for tracking regulatory requirements, monitoring compliance activities, and managing compliance-related data.
- 2.3. **Internal Audit:** Offering capabilities for conducting internal audit assignments, developing and monitoring of audit plans, automating audit processes, and generating audit reports efficiently in accordance with International Professional Practices Framework (IPPF) of the Institute of Internal Auditors (IIA).
- 2.4. **Cyber Security Incident Response:** Facilitating to automate cyber incident response process with reporting, monitoring and ability to integrate with other tools such as Security Information and Event Management (SIEM)s.
- 2.5. **Strategic Planning:** Supporting strategic planning initiatives by providing tools for strategic risk assessment, scenario analysis, and aligning risk management with organizational objectives.

The proposed GRC system should comprise modules covering above key areas. However, systems which cater one or more of the above key areas that can be integrated to other GRC solutions are encouraged to submit their proposals with details of integrating mechanism.

Further, the system should facilitate a centralized data repository and real-time monitoring, reporting including advanced data visualisations dashboards for managerial and compliance functions facilitating automated alerts.

3. Objectives of the EOIs

Through this Request for EOIs, CBSL aims to:

- 3.1. Identify suitably experienced and qualified vendors who are capable of providing a comprehensive GRC solution as a COTS product that is aligned with the above requirements.
- 3.2. Obtain information of GRC solutions available in the market, vendor capabilities, and implementation methodologies.
- 3.3. Initiate a competitive procurement process for the selection and implementation of a suitable GRC system.

4. Key Deliverables of the Prospective Vendor

- 4.1. **Comprehensive GRC Platform:** Provide a robust and scalable GRC platform that has the capability of integrating modules for Risk Management, Incident

Management, Compliance, Internal Audit, Cyber Security Incident Management, and Strategic Planning into a unified system. Also, the capability of generating user specific and dynamic reports/dash boards to meet specific requirements of stakeholders across the CBSL hierarchy.

- 4.2. **Advanced Functionality:** Showcase advanced functionalities, innovative features, and best practices within the GRC domain, ensuring the solution meets international standards and promotes efficiency, transparency, and compliance.
- 4.3. **Customization and Configuration:** Describe the degree of customization allowed in the proposed GRC solution through configuration changes.
- 4.4. **Implementation Services:** Offer comprehensive implementation services including project management, system configuration, data migration, integration with existing systems and/or any modules purchased from different vendors relating to GRC platforms through suitable interfaces, user training, and post-implementation support.
- 4.5. **Documentation and Training:** Provide comprehensive documentation, user manuals, guides, and commit to conduct frequent training sessions for administrators and end-users on utilizing the GRC solution effectively to familiarize with the solution and keep up with the modifications.
- 4.6. **Ongoing Support and Maintenance:** Commit to providing comprehensive post-implementation support, helpdesk assistance to cover Sri Lankan business hours, periodical updates/upgrades, maintenance, and addressing any issues or concerns in a timely manner.
- 4.7. **Data Security and Privacy:** Provide detailed information about data security measures, encryption protocols, access controls, and measures to safeguard sensitive information within the GRC application.
- 4.8. **Compliance:** The vendor must ensure that the proposed solution complies with regulatory standards, data privacy regulations, security standards, and industry best practices.

5. Eligibility Criteria

- 5.1. **Industry Recognition:** The CBSL invites EOIs from vendors for the proposed system from the vendors included in the "Chartis RiskTech Quadrant – Category Leader for EGRC solutions 2023". Vendors are expected to provide evidence of industry recognition, certifications, awards, or accreditations validating their expertise.

- 5.2. **The Vendor:** EOI shall be forwarded by a registered company or a firm or a joint venture of companies and/or firms who individually or jointly have offered GRC solutions. No third parties will be considered as prospective vendors.
- 5.3. **Experience:** The vendor, or in the case of a joint venture at least one party to the joint venture, should have at least three implementations of the proposed GRC solution over the last five years. Additional experience will be an added advantage and the vendors are encouraged to disclose such information.
- 5.4. **Contract with CBSL:** The vendor who submits the EOI should have the legal authority to enter into a contract with CBSL on all terms and conditions that are required to be mutually agreed upon.

6. Submission of EOI and selection of vendors

- 6.1. The following information shall be provided with the EOI:
 - 6.1.1. A comprehensive description on the functionalities available in the system related to risk, compliance, internal audit, and strategic planning and technical specifications.
 - 6.1.2. A comprehensive corporate profile of the party responding to this Request for EOI with contact details, (Refer to the Annex – I: Form - Corporate Profile).
 - 6.1.3. General information about the GRC Solution (Refer to the Annex – II: Form – Product Information).
 - 6.1.4. Details of experience in similar assignments with contact details of references (Refer to the Annex – III: Form – Client Information).
 - 6.1.5. The personnel serving on the proposed assignment, qualifications, and experience in similar assignments.
 - 6.1.6. Proposed activity schedule, estimated timeline, for delivery of the work specified in Section 4 – Key Deliverables of the Prospective Vendor above.
- 6.2. Vendors shortlisted based on information provided under 6.1 will be invited to demonstrate the functionalities of the proposed GRC solution to the Evaluation Committee, using sample data, at their own expenses.
- 6.3. Only those vendors who have been shortlisted based on EOIs submitted and completion of demonstration would be invited to respond to the Request for Proposal (RFP).
- 6.4. CBSL expressly stipulates that the shortlisting of the vendors under the EOIs is done on the understanding that this Request for EOI contains only the principal provisions of the assignment and that the scope of work set out in Section 4 – Key Deliverables of the Vendor is not exhaustive.

- 6.5. The EOI and all other relevant documents must be submitted in pdf format via email. The subject of the email should be “EOI FOR THE PROCUREMENT OF GOVERNANCE, RISK, AND COMPLIANCE (GRC) SYSTEM”. The maximum file size should be less than 8MB and if the EOI documents exceed this size, separate emails could be sent with the relevant name of the EOI followed by the version of the email.
- 6.6. All EOIs addressed to the Secretary, Central Bank of Sri Lanka No. 30, Janadhipathi Mawatha, Colombo 01 should be sent via email to procsec@cbsl.lk with a copy to sec@cbsl.lk not later than **1430 hrs on 28 March 2024**.
- 6.7. In the event the EOI and other relevant documents cannot be submitted via email, hard copies of EOIs addressed to the Secretary, Central Bank of Sri Lanka No. 30, Janadhipathi Mawatha, Colombo 01, should be submitted to reach the Secretary/Central Bank of Sri Lanka, not later than **1430 hrs on 28 March 2024**.
- 6.8. CBSL reserves the right to accept any or reject any or all EOIs received in response to this Request for EOIs.

7. Additional Information

- 7.1. Further information on the proposed assignment can be obtained by forwarding a request to the email address procsec@cbsl.lk or via the following contact persons.

Assistant Director (for Technical Information): - Tel. 011-2477404

Senior Assistant Secretary, Secretariat Department: - Tel. 011-2477312

Secretary
Central Bank of Sri Lanka

Corporate Profile			
Name of the Vendor (list all parties in a consortium or a joint venture)			
Brief overview of the Vendor			
Business Registration			
	Principal Vendor	Consortium or joint venture partner	
Registration Number			
Country of Registration			
Date of Registration			
Mailing Addresses			
Global Address		Local Office Address (if any)	
No. and Street		No. and Street	
City		City	
Province - Zip Code			
Country		Country	Sri Lanka
Contact Information			
Authorized Officer			
Name			
Job Title			
Mailing Address			Phone
			email
Single point of Contact (Local Representative if any)			
Name			
Job Title			
Mailing Address			Phone
			email

Product Information		
Details of the GRC Solution		
Name of the GRC Solution		
Mode of Implementation (Mark with 'x' sign)	<input type="checkbox"/> Cloud Deployment <input type="checkbox"/> On - Premises	
Available Licensing Model (Mark with 'x' sign)	<input type="checkbox"/> Per User <input type="checkbox"/> Per Core <input type="checkbox"/> Annual Subscription <input type="checkbox"/> Perpetual	
GRC Modules Supported in the Solution		
List the modules in the base product and add-ons (expand the table as required).	Modules in Base Product	Add-on Modules
Ability to interface with other GRC solutions		Yes/No
Business Areas Supported by the GRC Solution		
List the Areas of Industries your GRC Solution is used.		
Refer https://www.ilo.org/global/industries-and-sectors/lang-en/index.htm for list of industries.		

Note: Please provide comprehensive description about the proposed product

EXPERIENCE ON GRC SOLUTIONS IMPLEMENTATION

Provide details of experiences on implementing GRC solutions, in similar nature to this assignment, that are completed by The Vendor during past five (05) years.

Client Information		1
Name of Client		
Country		
Client's Area of Business		
Number of employees in the client institution		
Implementation Details		
Name of the vendor/partner in a joint venture		
Year which GRC Solution is purchased by the Client		
Year of commencement of live operations		
Briefly explain the work done by the Bidder		
Remarks (if any)		
Client's Contact Details		
Name		
Job Title		
email		
Phone		
Mailing Address		

Client Information		2
Name of Client		
Country		
Client's Area of Business		
Number of employees in the client institution		
Implementation Details		
Name of the Vendor/partner in a joint venture		
Year which GRC Solution is purchased by the Client		
Year of commencement of live operations		
Briefly explain the work done by the Vendor		
Remarks (if any)		
Client's Contact Details		
Name		
Job Title		
email		
Phone		
Mailing Address		

Client Information		3
Name of Client		
Country		
Client's Area of Business		
Number of employees in the client institution		
Implementation Details		
Name of the Vendor/partner in a joint venture		
Year which GRC Solution is purchased by the Client		
Year of commencement of live operations		
Briefly explain the work done by the Vendor		
Remarks (if any)		
Client's Contact Details		
Name		
Job Title		
email		
Phone		
Mailing Address		

Note: Please include details of additional experience in the above format.