CGIAR

SCIENCE FOR A FOOD-SECURE FUTURE

Risk Assurance Tool

REQUEST FOR PROPOSAL

CGIAR SYSTEM ORGANIZATION

Contents

1. Introduction and Background

CGIAR System Organization aims to improve risk management, compliance, internal audits, and assurance processes by procuring a risk and assurance tool, i.e., a Governance, Risk, and Compliance (GRC) solution. The objective is to enhance collaboration, streamline operations, and align with industry standards. The tool will replace the existing Internal Audit tool while bringing functionalities for risk management and internal controls monitoring and management.
Current manual methods are insufficient for managing evolving risks efficiently. A risk and assurance solution is urgently needed to automate processes, provide insights, and support compliance.

CGIAR is a global research partnership whose mission is to deliver science and innovation to advance the transformation of food, land, and water systems in a climate crisis. CGIAR envisions a world with sustainable and resilient food, land and water systems that deliver diverse, healthy, safe, sufficient and affordable diets and ensures improved livelihoods and greater social equality within planetary and regional environmental boundaries. Its research is carried out by independent CGIAR Centers in close collaboration with hundreds of partners, including national and regional research institutes, civil society organizations, academia, development organizations and the private sector.

2. Scope of Software as a Service (SaaS) Solution:

Risk Management sought to deliver a centralized platform for systematically identifying, documenting, assessing, and managing risks across an organization. It enables comprehensive risk tracking, including risk types, likelihood, impact, mitigation measures, and responsible parties. Additionally, it facilitates ongoing monitoring, reporting, and analysis to support informed decision-making and ensure proactive risk management strategies are in place. The tool aims to enhance risk awareness, promote accountability, and strengthen the organization's ability to mitigate and respond to risks effectively.

Internal Controls sought to deliver a comprehensive framework for managing and overseeing the organization's internal (including financial) processes and operations. The tool should enhance reporting capabilities for financial quality assurance on a global level.

It should provide functionalities for documenting, assessing, and monitoring internal controls across various functions and departments. The tool should enable automated workflows for control testing, issue identification, and remediation tracking and offer real-time visibility into control effectiveness and compliance status. It aims to enhance risk management, strengthen governance practices, and ensure regulatory compliance by promoting organizational accountability and transparency.

Internal Audit: The objective of audit management software for the CGIAR internal audit function is to provide insight into the CGIAR and Center Risk and Assurance landscape, identifying gaps and enabling better-informed decision-making. The tool must support continuous risk-based audit

planning to prioritize areas of high risk, allocate resources to the most needed areas, and facilitate effective planning, scheduling, execution, and reporting of agreed engagements. This includes documentation of work and tasks performed by the various teams and enabling collaboration between team members who are not physically located in the exact location. It must measure performance on agreed KPIs, and it is essential that the user interface with the business on performance, status of work, findings, and recommendations is simple and accessible. Lastly, the application must ensure compliance with internal audit standards.

See detailed criteria – **Risk assurance tool criteria appendix 1**

Stakeholders that will interact with the solution:

Risk users	Audit Users	IC Users	Stakeholders	Other
Risk & Internal Controls Teams	CAE	Control Owners	Board	Advisory & evaluation
Risk Owners	Audit Team	Control Implementer	Audit Committee	Ethics Business Conduct
			DG	Legal
			Senior management	
			Governance team	
There will be a need for people's time of approximately one week from all 3 functions at the Center, Risk, Internal (financial) Controls and Internal Audit. Centers have not already committed to those resources until a more concrete proposal is made to them.				

3. Technical Specifications

Overview

The Integrated solution SaaS tool must be a web-based platform to streamline and automate processes. The tool must be available offline to accommodate users who do not have access to the Internet.

Architecture:

- **Frontend:** The application uses modern web technologies and supports responsive and interactive user interfaces.
- **Backend:** The backend is built using scalable and reliable technologies. Data storage is managed using a robust database management system.
- **Infrastructure:** The application is hosted on cloud infrastructure providers to ensure scalability, availability, and security.
- **Document Management:** Offers a centralized repository for storing and managing compliance-related documents, including policies, procedures, guidelines, and audit reports.

- **Workflow Automation:** Supports workflow automation for streamlining approval processes, notifications, and task assignments related to governance, risk, and compliance activities.
- **Reporting and Analytics:** Provides customizable dashboards, reports, and analytics to gain insights into risk exposure, compliance status, and performance metrics. Integration with business intelligence tools may be supported.
- **Alert Tools:** Allows notifications to end users over email for different reminders, escalations, and other incidents.

Security:

- **Data Encryption:** All data transmission and storage are encrypted using industry-standard encryption protocols.
- **Incident Alert:** Any incident that may impact integrity or security of data must reported to clients with full transparency and with minimal delay.
- **Access Control:** Role-based access control (RBAC) mechanisms are implemented to restrict access to sensitive information based on user roles and permissions.
- **Authentication and Authorization:** Users are authenticated CGIAR SSO (based on MS Entra). Multi-factor authentication (MFA) may be supported for enhanced security.
- **Audit Trails:** Comprehensive audit trails are maintained to track user activities, system changes, and access to sensitive data for compliance and forensic purposes.
- **Compliance Certifications:** The platform complies with industry regulations and standards such as GDPR, SOC 2, ISO 27001, etc., and undergoes regular security audits and assessments.

Integration:

- **APIs:** Provides well-documented two-way RESTful APIs for seamless integration with other enterprise systems such as ERP, CRM, HRIS, and SIEM.
- **Third-party Integrations:** Supports integrations with third-party tools and services for functionalities such as threat intelligence, vulnerability scanning, and identity management.

Scalability and Performance:

- **Elastic Scalability:** The architecture is designed to scale horizontally and vertically to accommodate growing data volumes, user loads, and feature enhancements.
- **Performance Optimization:** Utilizes caching mechanisms, database indexing, and query optimization techniques to ensure optimal performance for user interactions and data processing.

Support and Training:

- **User Documentation:** Comprehensive user documentation, tutorials, and help resources are provided to assist users in onboarding and utilizing the platform effectively.

- **Training Programs:** Training programs, workshops, and webinars are offered to educate users on best practices, new features, and compliance requirements.
- **Technical Support: Dedicated technical support channels such as ticketing systems, email support, and community forums are available to address user inquiries, issues, and feedback promptly.** CGIAR operates in all time zones and with different weekend/holiday schedules. CGIAR expects true 24/7 support to address any support requests.

4. Performance Measurement

In this section of the Request for Proposal (RFP), we delineate the framework for performance measurement and review for the prospective service provider. It is imperative that prospective Service Providers meticulously review the outlined performance structure and KPIs, as adherence to these will be mandatory in the execution of the project.

4.1 Key Performance Indicators (KPIs)

- Uptime and Availability: The SaaS provider's commitment to uptime and availability is typically expressed as a percentage.
- Response Time: The average response time for system queries or actions.
- Scalability: The ability of the SaaS solution to scale to accommodate growing user or data demands.
- Data Security: The security measures in place to protect sensitive data.
- Customer Support Response Time: The response time of the SaaS provider's customer support team.
- User Adoption.

4.2 Performance Review

Performance evaluation is a fundamental aspect of ensuring this project's success and timely completion. The outlined Key Performance Indicators (KPIs) will serve as the backbone for this continuous evaluation process, ensuring the vendor alignment with the project's goals and expectations. The comprehensive and structured performance evaluation process, built on stakeholder feedback, project progress reports, and reviews, will ensure the constant alignment of the vendor performance with the project's objectives.

The SaaS will provide monthly reports on the following:

1- Number of active users.
2- Number of user activities.
3- Number of support tickets raised, with their status and SLA compliance.
4- System up time.
5- Features/modules updates for the coming two months.
6- Average Time to Remediate Risks: The average time taken to resolve identified risks.

7- Incident Response Time: The time taken to respond to and address security incidents.
8- Number of Open Critical/High Findings: The count of significant issues identified through risk assessment that are yet to be addressed.

The reports will be reviewed by the CGIAR SaaS account administrator.

Communicating any performance issues will be communicated over the standard support channels.

5. Data Ownership and Security

By submitting a proposal, the service provider agrees to the following:

- Ownership: All data provided by CGIAR is sole ownership.
- Encryption: All data transmitted or at rest will be encrypted using current industry-standard encryption protocols (e.g., TLS/SSL) to prevent unauthorized access or interception.
- Access Controls: Role-based access controls (RBAC) will be implemented to restrict access to sensitive data based on user roles and permissions. Access to customer data will be granted only to authorized personnel on a need-to-know basis.
- Data Segregation: Data will be logically segregated to ensure that CGIAR data is isolated from other clients.
- Unauthorized Access: SaaS is responsible for preventing unauthorized access or accidental exposure of sensitive information.
- Authentication: SaaS will enable Single Sign On authentication using CGIAR Entra Active Directory.
- Regular Security Audits: The SaaS provider will conduct regular security audits and assessments to identify and address potential vulnerabilities in the platform. Reports such as SOC2 Type 2 will be provided to CGIAR to confirm compliance.
- Data Residency and Compliance: Customer data will be stored in data centers that comply with relevant data protection regulations and industry standards. Measures will be in place to ensure compliance with regulations such as GDPR, and others, including data residency requirements and data access controls.
- Logging: The SaaS will provide tools to report on all activities with their details.
- The SaaS platform includes a SIEM (Security information and event management) module that enables the tracking of security events for threat detection, investigation, and response.

6. Service Level Agreement (SLA)

- Support
    - The SaaS will provide a single support channel (help desk) that is available over the internet to all CGIAR staff.
- Availability
    - The SaaS will provide online tools to monitor service(s) health.
    - The SaaS will maintain a minimum uptime of 99.9% over any calendar month, excluding scheduled maintenance windows.

  - Scheduled maintenance windows will be communicated to customers at least 48 hours in advance, and efforts will be made to schedule them during off-peak hours.
- Enhancements
  - Any changes to the SaaS that affect end users (code, layout, features, modules, and other areas in terms of addition, modification, or removal) will be communicated to subscription administration at least 2 months before the change, with a clear indication of the purpose, impact, and workarounds.
- Support Response Time
  - CGIAR works globally across all time zones, 24/7 support model is required.
  - The support team will acknowledge all support requests within 1 hour of receipt during.
  - For critical issues affecting system functionality or security, a response will be provided within 30 minutes of receipt, regardless of the time of day.
- Issue Resolution Time
  - The support team will make all reasonable efforts to resolve non-critical issues within 1 business day.
  - Critical issues affecting system functionality or security will be prioritized, and resolution efforts will be made on a 24/7 basis until the issue is resolved.
- Data Security and Confidentiality
  - The GRC SaaS platform will implement industry-standard security measures to protect customer data from unauthorized access, loss, or disclosure.
  - Customer data will be treated as confidential and will not be shared with third parties without explicit consent, except as required by law.
- Data Backup and Recovery
  - All data will be backed up daily with a retention period of 1 year.
- Escalation
  - Clear escalation procedures will be provided to CGIAR.
- Penalties for non-compliance
  - Subscription discounts that are prorated according to SLA breaches / non compliance will be provided by the SaaS provider.

7. Technical Proposal Structure

(a) Executive Summary
(b) Company Profile and Relevant Experience
(c) Implementation plan and Timelines: The vendor is required to provide a detailed project proposal including estimated timelines with clear milestones
(d) Detailed response to each Scope of Service area (use excel spreadsheet provided in appendix 1)
- Risk Management criteria
- Internal (Financial) controls criteria
- Internal Audit
- Digital and Data Criteria D&D
- Common Criteria

(e) Include Case Studies / Sample Use Cases for each area

(f) Service Level of Agreements and KPI's for each area
(g) References from similar projects.
(h) Commercial proposal: Pricing and fees should be presented in US$ excluding taxes
    - Assumptions, dependencies, or exclusions.
(i) Annexes (for any additional information)

8. Pricing and Payment Terms

Specify the pricing structure for the SaaS subscription, including any recurring fees, payment schedule, and payment terms. Please be specific and define subscription fees, interaction customization and configuration, data migration, training and onboarding, support and maintenance, add-ons and Modules, scaling costs, License management (if across centers), and Total Cost of Ownership (ongoing subscription fees, maintenance, and support cost)]

- The SaaS platform should follow a clear subscription model (by tenant or by user).
- The SaaS should provide free tools for data import/export/migration/interfacing.
- Subscription must be possible to be paid monthly or annually as some users may require temporary access.
- Adding new licensing before subscription anniversary should be prorated.
- Any pricing changes must be notified to CGIAR 1 year before.
- The SaaS should be scalable in terms of users and data without incurring infrastructure costs to CGIAR.
- Cancellation Policy: Outline the terms for subscription cancellation, including any notice periods and potential penalties or fees.

CGIAR reserves the right to accept or reject any application, and to annul the selection process and reject all submissions at any time, without thereby incurring any liability to the affected Service Providers.

9. Proposal Evaluation

The purpose of this section is to outline the evaluation criteria and process that will be used to assess the best tool.

Technical Criteria	**Weight (100)**
Functional fit	(40%)
Technical Compliance	(20%)
Vendor experience and References	(10%)
Support and Training	(10%)

Cost competitiveness – Value for price] Provide a clear and detailed cost breakdown, assumptions, and any contingencies will be critical to evaluating the total cost of ownership	(20%)

10. Bid Schedule and Timelines

The following schedule includes key milestones and their associated completion dates and is provided primarily for planning purposes. CGIAR System Organization may modify the project timeline at its discretion.

Dates	Milestones
24 November 2025	**Issuance of Request for Quote**
26 November 2025	Last day to submit clarification Questions
28 November 2025	Responses to questions shared with bidders
08 December 2025	**Deadline for submission of proposal.**
15– 20 December 2025	Product Demonstrations (Demos)
5-12 January 2026	Summary report with conclusion and preferred option
12-19 January 2026	Presentation to different stakeholders
20-27 January 2026	Final clarifications with potential stakeholders' points
February 2026	**Decision & Endorsement**
February 2026	• Endorsement by CA FAC
February 2026	• Endorsement by GLT
February 2026	• Approval by EMD
March 2026	**Contract Finalization**
April – June 2026	**Platform Configuration**
July 2026	**Data Migration & Integration**
August 2026	**Training & Onboarding**
September 2026	**Go-Live**

Dates	Milestones
Q3 and Q4 2026	**Center-Level Fine-Tuning**

11. Communication during RFP period

CGIAR intends to run a fair bidding process where all respondents are given equal opportunity to put forward their best proposal. As such, any material questions asked by bidders will be collated, answered, and shared with all bidders before the RFP closes.

Submit your questions through the email smo-bidding@cgiar.org

12. How to submit a proposal

Please submit a cover letter expressing your interest together with a proposal to smo-bidding@cgiar.org no later than **December 08, 2025, at 17h00 (CET)**, Paris time. Only electronically submitted applications will be considered.

13. Confidentiality

The vendor agrees not to communicate or disclose to a third party any papers, documents, correspondence, books, films, tape recordings, files, registers, ciphers, or codes provided by the CGIAR System or any of its participating Centers in participating in this open tender process . The vendor will treat all information they receive as confidential and will exert diligent efforts to safeguard and avoid disclosing to third parties without written consent. They will also not make any press announcement, publicize their engagement or any part thereof, or use CGIAR or its participating Centers' name, acronym, or logo in publicity releases or advertisements, except with prior written consent.

14. Conflict of Interest

The vendor represents that they are unaware of any real or potential conflict of interest. During this open tender process, the vendor shall disclose any real or potential conflicts of interest that may arise concerning this open tender process. Should a real or potential conflict arise during this open tender process, the contact/responsible persons will discuss it with you and decide, at its sole discretion, the best course of action.

15. Standard Payment Terms

Standard payment terms are net-30 days from the date of invoice receipt. The invoicing schedule may vary based on the pricing structure outlined in the prospective vendor commercial proposal.

16. Annexes

Appendix 1 – **Risk assurance tool detailed criteria**