Terms of Reference

Engagement Details:

Project/ Assignment Title:	ROSTER OF CONSULTANTS TO PROVIDE IT ASSURANCE AND ADVISORY SERVICES	
Responsible/Project Manager:	ANTONIO VILLAMOR/ MADINA BAZAROVA	
Business Unit	CGIAR INTERNAL AUDIT FUNCTION	
Location of Assignment:	☒ Remotely	☐ On Site ______________
Duration:	Start Date: 01/05/2022	End Date: 30/12/2022
Estimated Budget (if known)	Click or tap here to enter text.	
Budget Code	BU10007	

Objective and Scope of Work:

The CGIAR System Internal Audit Function (IAF) is seeking the services of individual consultants to provide technical assistance for its planned 2022 assurance and advisory engagements:

1. Key IT controls review
2. Quarterly assessment of management actions to mitigate IT security risks
3. Up-front advice on project management of the Performance and Results Management System (**PRMS)** and the Global Information Business System (**GIBS)** design and implementation

CGIAR System Internal Audit will lead the engagement planning, gathering the required engagement information, including preparing and issuing the engagement's terms of reference to the stakeholders. They will also be present at all meetings (e.g., start-up, status-update, and exit meetings) and are responsible for report (draft and final) circulation. Together with the CGIAR's Independent Evaluation function under CGIAR Advisory Services (CAS), CGIAR Internal Audit collaborates to provide combined assurance on the design and implementation of the PRMS and PRMS products. We detailed the individual consultants' roles and responsibilities on page 3.

The nature, timing, and extent of the **review of PRMS and GIBS implementation projects** will be to identify and assess risk and provide advice or recommendations for management focus.

Overview

1. The increasing adoption of IT solutions to automate business processes and controls causes an increased focus on the effective operation of controls around IT assets and services. The CGIAR Digital Services group periodically conducts IT control self-assessments, with the last assessment conducted in 2019. CGIAR Internal Audit review seeks to confirm the existence, adequacy, and effectiveness of the key IT controls at each CGIAR entity.
2. The CGIAR Digital Services group maintains an action tracker used for logging security-related recommendations and monitoring the extent of their resolution at respective CGIAR Centers. CGIAR Internal Audit seeks to provide continuous assurance on the timely installation of cross-cutting security measures recommended and detailed in the One CGIAR Security Improvement Plan that was commissioned in February 2022.
3. In 2020, CGIAR embarked on an ambitious reformulation of its partnerships, knowledge, assets, and global presence to support the UN's Sustainable Development Goals: One CGIAR. The aim is to have greater integration by all CGIAR Centers to face the interdependent challenges facing today's world through unified governance, institutional convergence, more and better funding, aligned mission, and transformative research programs. In 2019, the CGIAR System Council approved the Performance Results

& Monitoring Framework 2022-2030 (PRMF). In 2022, CGIAR's Strategic Impact, Monitoring, and Evaluation Committee (SIMEC) endorsed a Task Team to propose a set of standard reporting parameters that measure achievement against the Performance Results Management Framework (PRMF) and planned results of its various Research Initiatives. The PRMS, a mechanism to deliver on PRMF, aims to integrate management information from various systems to enable planning, monitoring and evaluation, and reporting on CGIAR's various Research Initiatives' progress. In collaboration with Accenture, CGIAR System Organisation conducted a fit-for-purpose assessment of its current PRMS. The assessment's key conclusions indicated the need for **integrated business applications, standard data model/definitions, and standardized data definitions to improve interoperability**. Internal Audit seeks to engage with management as the new PRMS is being designed and implemented, to provide up-front advice and input.

The institutional convergence within One CGIAR includes some aspects of harmonization of CGIAR's policies and internal business services in Human Resources, Information Technology, Finance, Procurement, Communications and Resource Mobilization. One CGIAR leadership envisions a standard Enterprise Resource Planning (ERP) System for core functions of Finance, Procurement, and Human Resources (i.e., GIBS). Internal Audit's involvement in this endeavor is to provide up-front input and advice.

Responsibilities:

Describe the key responsibilities, tasks, activities

1. **Key IT Controls Review – Workstream (H1/2022)**

a. Support engagement planning, including:
   - ➢ Propose scoping considerations for Key IT controls based on an understanding of CGIAR operations and developments in the IT sector
   - ➢ Prepare a detailed work plan and schedule of activities prior to commencement of fieldwork
   - ➢ Identify and prepare a request for information needed for the review
   - ➢ Develop an audit work program and audit procedures for select Key IT controls

b. Lead the engagement and, as a team member, execute fieldwork or provide technical guidance to internal auditors conducting the fieldwork to evaluate the design and effectiveness of prioritized IT controls for all CGIAR entities included in scope

c. Build capability through advice, training, and guidance to CGIAR assigned audit staff, delivering the Key IT controls engagement

d. Together with the CGIAR IAU Responsible/Project Manager, lead the start-up, fieldwork, and exit meetings with CGIAR Management

e. Appraise the CGIAR IAU Responsible/Project Manager on the work's progress through regular meetings/updates

f. Prepare a draft engagement report and deliver a presentation to identified CGIAR stakeholders and be available to address technical comments (if any)

2. **Assessment of the implementation of management actions to manage IT Security risks – Workstream (H2/2022)**

a. Support engagement planning, including:
   - ➢ Propose scoping considerations for security control areas to review using a risk-based approach.
   - ➢ Prepare a detailed work plan and schedule of activities prior to commencement of fieldwork
   - ➢ Identify and prepare a request for information needed for the review
   - ➢ Develop an audit work program and audit procedures relevant to the security area under review.

b. Through technical guidance of internal auditors conducting the fieldwork, validate the implementation of cross-cutting security measures recommended and detailed in the One CGIAR Security Improvement Plan

c. Build capability through advice, training, and guidance to CGIAR assigned audit staff, delivering the IT Security Reviews.

d. Together with the CGIAR IAU Responsible/Project Manager, lead the start-up, fieldwork, and exit meetings with CGIAR Management

e. Appraise the CGIAR IAU Responsible/Project Manager on the work's progress through regular meetings/updates

f. Prepare a draft engagement report and deliver a presentation to identified CGIAR stakeholders and be available to address technical comments (if any)

3. **Up-front advice on Project Management of PRMS and GIBS design and implementation**

The nature, timing, methodology and extent of the **reviews of PRMS and GIBS implementation projects** will be tailored to identify and assess risk and provide advice or focus recommendations. This engagement may include:

a. **Project risk assessment** at any phase of the project to identify project risks and areas or management focus

b. **Pre-implementation review** of resources, project plans, timelines, system design and implementation plans, data conversion approach, and techniques.

c. **Special purpose reviews** of functionality analysis against blueprint assumptions, independent testing of data migration for completeness and accuracy, review of interfaces and reports

d. **Go-Live assessment -** performance of a health check (pre-go-live) to determine whether project plans, testing, change management, training, and other key implementation project activities have been successfully completed prior to the roll-out of the new system.

e. **Post-implementation review and verification** that the intended project objectives have been attained

Expected Outcomes/Deliverables:

Workstreams 1 and 2
1. Memo reports for each Sprint of Key IT Control Review stream
2. Quartey update reports on the extent of implementation of the Security Improvement Plan and IT security-related recommendations
3. Consolidated system-wide report on the existence, adequacy, and effectiveness of Key IT controls
4. Presentation of the report to the Global Director of Digital Services and other concerned stakeholders as deemed relevant

Workstream 3
1. Status update reports from an independent perspective on relevant risks at each phase of the project
2. Consolidated independent quality assurance report on the PRMS and GIBS implementation project activities
3. Presentation of the report to project Sponsor and other concerned stakeholders as deemed necessary

Consultant Profile:

Type of Consultancy (Check where applicable)	☒ Individual Consultants (IC) ☐ Firm ☐ Consortium of Firms
Knowledge and Experience (Firm)	▪ The consultant must demonstrate prior experience and technical knowledge in providing advice on planning, implementing, and controlling the full life cycle management of digitally organized information and records aligned to an organization with distributed structures. This prior experience should include aligning an organization's technology strategy with its business mission, strategy, and processes and documenting these using architectural models. ▪ The consultant must demonstrate technical understanding and relevant knowledge spanning different IT domains, including defining and operating a framework of security controls and security management strategies related to protecting against risks managed on the use, storage, and transmission of data and information systems. ▪ The consultant must demonstrate the ability to investigate business situations to define recommendations for improvement activities and has a proven ability to influence stakeholder attitudes, decisions, and actions for mutual benefits.
Qualification Skills & Experience (IC or Project Team:)	Essential: ▪ Membership and accreditation with professional bodies such as the Information Systems Audit and Control Association (ISACA), Institute of Internal Auditors (IIA), Project Management Institute (PMI), International Institute of Business Analysis (IIBA), International Information System Security Certification Consortium (ISC2), and among others The Open Group. ▪ 10 - 15 years of progressive experience in delivering an independent, risk-based assessment of the effectiveness of processes, the controls, and the compliance environment of an organization. ▪ Able to apply and mix the various bodies of knowledge related to strategy and architecture, change and transformation, development and implementation, delivery and operation, people and skills, and relationships and engagement. ▪ Possess excellent written and oral communication and reporting skills (in succinct English). ▪ Able to apply mathematics, statistics, and data mining (predictive modeling is desirable) techniques to gain insights, predict behaviors, and generate value from data. ▪ Experience in providing support to transition an organization and its people to achieve its required future state. ▪ Experience in presenting to senior executives in a succinct and effective manner

Additional Information:

Different consultants may conduct specified workstreams dependent on their demonstrated qualifications, skills, and experience.