DRAFT 0 - SYSTEM COUNCIL NOVEMBER 2017 PAPER

IDENTIFYING CGIAR'S TOP RISKS
AND THE ASSURANCE FRAMEWORK AROUND IT

Purpose

Based on the discussions set out in this paper, this document:

1. **Presents for discussion and, if considered appropriate, decision at SC5**:

    Appendix A.1   **Strategic Operational Objectives to delivery on CGIAR SLOs**

    Appendix A.2   **CGIAR System 'top risks'** (re strategic objectives)

    Appendix A.3   **Inaugural 'CGIAR System' Risk Appetite Statement**

    Appendix A.4   **Inaugural 'Risk Management Framework of CGIAR System'**

    Appendix A.5   **TOR System Council's 'Assurance Oversight Committee'**

2. **Presents for System Council input at SC5**, **in advance of proposed final approval by the System Management Board at its 8th meeting** (11-12 December 2017):

    Appendix B.1   **Draft Risk Management Guidelines of the CGIAR System**

    Appendix B.2   **Draft TOR CGIAR System internal audit function**

Distribution notice: **Restricted circulation -** This document is part of an internal deliberative process of the System Management Board and is not for release. The outcomes of the Board's deliberations will be provided in the meeting summary.

Prepared by: CGIAR System Management Office

Discussion points to support System Council deliberations

Background

1. **On risk and assurance matters,** CGIAR's Centers and Funders agreed in the CGIAR System's revised governing instruments to distribute roles in a way that confirms[1]:

    a. <u>**For the System Council**</u>: **a high-level oversight role** – with a focus on being comfortable that there is sufficient System-wide assurance based on a shared vision regarding System-wide risks; and

    b. <u>**For the System Management Board**</u>: **the role of defining and managing operational aspects of System-wide risk and assurance process**, together with the responsibility for ensuring, as required, any "corrective action is taken in accordance … with the risk management framework", informing the System Council accordingly.

2. **CGIAR's Centers and Funders also accepted[2] that the principle of subsidiarity should guide frameworks, policies and guidelines**. In elaborating this principle, there was joint acknowledgement that:

    a. **Centers should be responsible for System functions that can be more efficiently and effectively executed by them**; and

    b. **System Council decisions should allow Centers and their Boards flexibly to adapt guidelines** appropriate to the needs and conditions of individual Centers while achieving the goals and expected results of cross-cutting and system-wide guidance.

3. **The materials presented for discussion and input embody these principles**, proposing that the <u>System Council</u> sets the overall approach for deciding how System-wide risks are managed and opportunities are appropriately exploited, and the <u>System Management Board</u> puts in place and oversees the machinery that can give the Council confidence that appropriate assurance arrangements in place.

4. **The materials build on the strengths of what is already in place at Centers**. Using the first half of 2017 to take stock of what is already in place, the material presented avoids duplication, looks for cost-efficiency, and meets international standards. Periodic reviews are also built into the proposed Risk Management Framework of the CGIAR System, to ensure that the System's operational framework is adequate, without imposing unnecessary cost and process.

Putting in place essential building blocks for risk-based cost-effective assurance

---

[1] **Appendix C to this paper** collates the text of the various elements of the CGIAR System Framework, and the Charter of the CGIAR System Organization, which forms the basis for the summarized position as presented.

[2] The 'Guiding Principles for the Governance of the CGIAR System' were agreed between the Centers and Funders in February 2016, and incorporated into the *CGIAR System Framework* at Article 1.

5. Building on international best practice, the key elements required to deliver an appropriate risk management and assurance framework across the CGIAR are summarized below, noting approval bodies. Items for review at SC5 are in red text.

ELEMENT	STATUS	ACTION REQUIRED (as relevant)
Appropriate governing arrangements - allocate clears roles and responsibilities	APPROVED	**Council** – CGIAR System Framework **SMB** – Charter of CGIAR System Organization
Express (i) **operational objectives** to deliver on the SRF; (ii) related '**top risks**'; and (iii) overall **System appetite** for opportunity and risk	DRAFT	**For System Council approval** **Proposed objectives set out at Appendix A.1**
	DRAFT	**For System Council approval** **Proposed 'top risks' set out in Appendix A.2**
	DRAFT	**For System Council approval** **Set out in proposed 'Risk Appetite Statement' at Appendix A.3**
Allocate **roles and responsibilities** for the oversight of System risks	DRAFT	**For System Council approval** **Set out in proposed 'Risk Management Framework' at Appendix A.4**
Institutional mechanism(s) to oversee System risk management and quality of assurance	APPROVED	**For SMB approval – TOR for Audit and Risk Committee and membership appointed** 2016 (Robust oversight of assurance requirements)
	DRAFT	**For System Council approval** **Proposed TOR for System Council's Assurance Oversight Committee" at A.5**
Assurance providers mandated to deliver combined assurance on opportunity and risk taking for System matters	Work in Progress	**For System Council approval** ** TOR for science advisory and evaluation functions (not covered in this paper)*
	FOR INPUT	**For SMB approval after SC5 input** **TOR for 'Internal Audit Function arrangements' draft at Appendix B.1**
Reporting and escalation mechanisms that ensure the right body is overseeing the right opportunity and risk taking, and there are effective communication channels	FOR INPUT	**For SMB approval after SC5 input** **Draft 'Risk Management Framework Implementation Guidelines' Appendix B.2**
	To Do...	**For SMB development and management after SC approval** of risk framework 1. System opportunities and risk register 2. Escalation Procedures to SMB + SC

(side labels: *Differing roles*; *Part of broader combined assurance*)

Justification for proposed formal adjustments to the *CGIAR System Framework*

6. **To give overall effect to the package of materials presented for System Council review,** the System Management Board makes the following proposals for formal changes to the CGIAR System Framework, shown in track changes below:

    8.2(a)   an <u>Assurance Oversight Committee</u> ~~Audit and Risk Committee~~, with a majority of independent members, the purpose of which shall be to provide: The System Council with assurance of the completeness and effectiveness of the Internal Audit Function and the independence of external audit functions; a structured reporting line between internal and external auditors and the System Council; and oversight of system-wide governance, risk management and internal controls

    6.1(j)   ~~Review findings and follow-up emanating from the Internal Audit Function~~

7. **Justification to retitle the System Council's standing committee:**
   <u>Rationale</u>: *Remove confusion from the System Council and System Management Board having identically named Committees, yet with different mandates.* <u>Explanation</u>: The Council's committee is envisaged to have strategic oversight of the adequacy of assurance across the System. This change better reflects the nature of the role.

8. **Justification to delete article 6.1(j):**
   <u>Rationale</u>: *Put the 'management' of System-wide internal audit findings correctly in the hands of the System Management Board to escalate to the System Council as relevant to System-risks.* <u>Explanation</u>: Reviewing the detailed findings and follow up emanating from the work of the Internal Audit Function is a detailed task that more naturally falls in the remit of the System Management Board's Audit and Risk Committee. Summarized strategic reporting and recommendations will come to the System Council annually out of that work, or more frequently in the case of an issue requiring early escalation.

9. To facilitate timely implementation of these formal changes to the CGIAR System Framework, subject to System Council discussion and, if considered appropriate, approval, both the General Assembly of the Centers and the System Management Board have agreed to these changes. The agreement of all three is required pursuant to Article 16 (Amendment) of the CGIAR System Framework.

Timetable for next steps

10. Approval of the inaugural Risk Management Framework of the CGIAR System is an important facilitative action to take other elements forward. The table below summarizes major follow up actions, subject to direction from SC5 deliberations.

Item	Title	Decision body	Timing and rationale

2017 Ongoing actions			
1	**Launch nominations** process for **System Council AOC** *(majority independent members required in the CGIAR System Framework)*	SC	November 2017 post SC5: TOR requires approval to communicate clearly the appropriate mandate. SC to approve member nominations in line with TOR. Expected February 2018 appointment decisions.
2	**Approve** Risk Management **Guidelines of the CGIAR System**	SMB	SMB8 - December 2017: Need B.1 in place to take this forward, and inputs from SC5 will help to shape this operational guidance for Centers
3	**Approve TOR CGIAR System Internal Audit Function**	SMB	SMB8 - December 2017: same as for B.4, so appropriate scope is agreed
4	**Establish CGIAR System risk register for SMB oversight in consultation with SC AOC**	SMB	SMB8 – December 2017: same as for B.4
5	**Resource the Internal Audit Function arrangements**	SMB Audit Committee	January 2018: Preliminary work will be done in advance of final SMB8 decision on the TOR
6	**Approve the System escalation & communication procedures for System risks**	SMB, consulting with SC and Centers	By March 2018: Preliminary material will be presented to SMB8 but will required SC5 decisions before further drafting and ongoing consultation can take place. * *In the interim, the Financial Framework Agreements all have interim escalation processes included to address this topic*
7	**Reporting on status of follow up actions**	SC - AOC	SC6 May 2018: preliminary assurance view
8	**Instituting inaugural annual report to System Council on the overall status of System-wide assurance**	SC – AOC	SC7 – (Nov) 2018: implementing annual status of assurance report, and annual thereafter

DRAFT 0 - SYSTEM COUNCIL NOVEMBER 2017 PAPER

APPENDICES A.1 – A.5

Purpose

This Appendix A sets out the following materials, for review, and if considered appropriate, approval by the System Council at its November 2017 meeting

Item	Title	Decision maker	Timing and rationale	Pages
A.1	CGIAR strategic operational objectives for CGIAR as a system	SC	November 2017: forms the basis of risk identification in a way that connects CGIAR System actions to potential to deliver against the three System Level Outcomes (or SLOs)	
A.2	CGIAR System 'top' risks	SC	November 2017: establishes shared understanding of operational basis of CGIAR System – to inform risk appetite and risk management practices	
A.3	Risk Appetite Statement of the CGIAR System	SC	November 2017: Takes the strategic objectives and identifies the scope of action that CGIAR is prepared to take to achieve the SLOs, by strategic operational objective category (A.1)	
A.4	Risk Management Framework of the CGIAR System	SC	November 2017: Sets the overarching approach for risk management as a System – but recognizes the independence of the various operating bodies – including Funders and Centers.	
A.5	TOR for Assurance Oversight Committee of the System Council	SC	November 2017: Delivers on the action under the 'CGIAR System Framework´ to have small, specialized committee to comment on the quality and overall effectiveness of assurance providers across the System, drawing heavily on the work of the SMB but who must be independent of the SMB to give the overall view of that state of assurance.	

Prepared by: CGIAR System Management Office

TRANSLATING CGIAR'S SYSTEM LEVEL OUTCOMES INTO STRATEGIC OPERATIONAL OBJECTIVES TO SET 'TOP RISKS'

Considering that the "Strategy and Results Framework 2016-2030" does not provide system-wide strategic objectives for CGIAR's *'extended enterprise'* system, the following are proposed as strategic operational objectives that can be used to measure the System's actions towards delivery on the System Level Outcomes.

Proposed 5 key objectives of CGIAR's extended enterprise System	Objective's name
A. Deliver good science, partnerships and other research outputs that provide critical improvements for food security, nutrition and resilience to climate change	**"Delivery"**
B. Establish and maintain CGIAR as a relevant and sustainable tool for agricultural research for development	**"Relevance"**
C. Make the association with CGIAR a rewarding and rational decision	**"Reputation"**
D. Fulfill formal commitments	**"Reliability"**
E. Generate all benefits mentioned above efficiently and provide "value for money"	**"Efficiency"**

APPENDIX – A.2 - CGIAR SYSTEM 'TOP RISKS' AND OPPORTUNITY AND RISK TRIGGERS (PROPOSED)

5 'Top' System Risks	Opportunities and Risk indicators	Sources of assurance taking a System perspective
CGIAR is no longer a front runner	Adequate financial resources enable CGIAR's ability to keep up with competitors' leading edge technologies	SMB ARC
	CGIAR's adequate exposure and ability to share the sense of urgency reinforce Funders' commitment to CGIAR	SC SIMEC
	Relevance and/or cutting-edge of CGIAR science	SC SIMEC
	Sustainable competitive advantage as a result of identifying and seizing the "next thing"	Scientific advisory body
	CGIAR seizes opportunities to revisit its priorities and rebalance the portfolio	Scientific advisory + Evaluation processes
CGIAR loses its central role in R4D	Efficient use of intellectual property: Data produced by CGIAR are leveraged by the scientific and development communities	Evaluation & review processes (Center initiated and/or System)
	CGIAR is seen as a desirable potential partner and is able to support existing partners	Scientific advisory + Evaluation processes (Center initiated and/or System)
	CGIAR's diversity of funding sources enables it to be seen as a multilateral institution -and a global player	SC SIMEC and SMB
	CGIAR's research activities are deployed with adequate coordination in target countries, generating efficiencies, supporting delivery and projecting an image of consistency.	Evaluation processes (Center initiated and/or System)
	All components of the CRPs and Platforms contribute toward achieving the objectives of the SRF	Evaluation processes (Center initiated and/or System)
Non adherence to appropriate values	Ethical research practices are used to achieve research results	Internal audit processes (Center and/or System)
	CGIAR values or behaviors support and strengthen its credibility and attractiveness	Internal audit processes (Center and/or System)
	Adequate processes are in place to prevent or detect inappropriate use of funds	Internal audit processes (Center and/or System)
	Components of the portfolio are financed in a clear and segregated manner	Internal audit processes (Center and/or System)
Unsatisfactory evidence and assurance received	Evidence of impact based on hard data	Scientific advisory/ Impact assessment (Center/CRP initiated and/or System)
	SC receives reliable information that funds were used in accordance with approved annual work programs and budgets	Internal Audit process (Center and/or System) and/or External Audit providers
	Implementation of activities and related use of funds are allocated to CRPs, platforms and flagships according to priorities defined by Funders	Evaluation processes (Center initiated and/or System)
	SMB is provided the required visibility over the level of delivery of programs and projects of the portfolio	Internal Audit + Evaluation processes (Center initiated and/or System)
	Project assessment and lifecycle management are effective	Internal audit processes (Center and/or System)
Poor execution	Genebanks are effectively managed and implementing the expected quality level in their operations and demonstrating their unique role	Internal Audit + Evaluation processes
	The benefits drawn from of the CGIAR System more than outweigh its cost and constraints	SMB ARC
	Adequate use of intellectual property or decisions use preserving the "Global Public Goods" nature of the research	Evaluation processes (Center initiated and/or System)
	CGIAR's attractiveness to top talent is supported by all Centers' ability to attract and retain staff	Internal Audit + External benchmarking
	All Centers meet minimum requirements for financial stability	Escalation from Center Board

Draft 0
CGIAR System risk appetite statement[1]

Introduction

In delivery of the goals of its ambitious Strategy and Results Framework 2016-2030, CGIAR strives to identify and measure an optimum balance between leveraging opportunities and managing risks.

CGIAR recognizes that its 'extended enterprise' structure, in which a number of organizations come together in a joint endeavor in order to achieve outcomes that none of them could have achieved on their own,[2] brings together a number of stakeholders and partners, each with their own risk appetites and priorities. As these stakeholders and partners work together to deliver on CGIAR's mission, they are asked to make decisions guided by a common overarching understanding of to what extent risk-taking in pursuit of CGIAR's goals should be maximized or minimized in the relevant circumstance.

Risk appetite categories

CGIAR's Risk Management Guidelines set out the strategic operational objectives that the System has identified to facilitate delivery of the wider strategic mission, and against which opportunities and risks are identified and monitored. CGIAR uses 4 categories to describe its willingness to take risk to achieve its objectives – with each area being indicative rather than exhaustive.

	Level	Definition
3	**High**	CGIAR accepts and encourages opportunities presenting risks of failure if the likelihood of risks materializing combined with their potential impact make benefits more than offset losses
2	**Moderate**	CGIAR accepts opportunities presenting a risk of limited underachievement if the likelihood of risks materializing combined with their potential impact make benefits more than offset losses
1	**Low**	CGIAR is not willing to accept excessive risks that would significantly impact achievement of its objectives
0	**Not tolerated**	CGIAR is not willing to accept any level of risk

---

[1] This statement draws on practices across partner and comparator organizations, as well as recognized international standards, including but not limited to: The Gavi Alliance, IIA, COSO. Several Center risk appetite statements were also used as input to the development of this Statement.

[2] UK Institute of Risk Management definition; for details see https://www.theirm.org/media/1155369/IRM-Extended-Enterprise_A5_AW.pdf

Risk appetite statement relevant to CGIAR's strategic operational objectives

1. In **delivering good science, partnerships and other research outputs that provide critical improvements for food security, nutrition and resilience to climate change,** CGIAR has a <u>high</u> risk appetite as it seeks to maximize research opportunities in pursuit of its goals, or System-Level Outcomes ('SLO's): Within that:
    a. CGIAR has a <u>low</u> risk appetite with regard to research practices and research data management, recognizing that high ethical and evidence-based standards are essential for delivery of high-quality science.

2. In **establishing and maintaining CGIAR as a relevant and sustainable tool for agricultural research for development**, CGIAR has a <u>high</u> risk appetite as it develops its research in a complex and competitive setting, recognizing the competitive nature of the funding landscape and the need to maintain CGIAR's comparative advantage. Within that:
    a. CGIAR has a <u>low</u> risk appetite with regard to the implementation of effective management of quality systems.

3. In **ensuring that the association with CGIAR is a rewarding and rational decision**, CGIAR has a <u>low</u> risk appetite, recognizing that deviation from adherence to positive values and behaviors and potential negative public image would have a high adverse effect on the achievement of CGIAR's goals. Within that:
    a. CGIAR has a <u>moderate</u> risk appetite in the communication of the outputs and outcomes of its activities to be innovative in keeping agricultural research for development high on the global agenda.

4. In **fulfilling formal commitments**, CGIAR has a <u>low</u> risk appetite, as it seeks to ensure that relationships with research partners, suppliers and target households and consumers are respected and based on trust. Within that:
    a. CGIAR has <u>no tolerance</u> with regard to the misuse of funds and scientific fraud.

5. To **generate all benefits mentioned above efficiently and provide 'value for money'**, CGIAR has a <u>moderate</u> risk appetite, as it seeks to maximize research and organizational synergies and retain top talent, but recognizing the need to ensure that efficiency gains in one area do not engender them in another.

<u>Agreed: [date]</u>

INITIAL WORKING DRAFT

RISK MANAGEMENT FRAMEWORK OF THE CGIAR SYSTEM[3]

Introduction

1. The scope of CGIAR's operations is significant - involving multiple national, regional and international partnerships, a geographic footprint that extends across the globe, and the involvement of thousands of individuals working towards achievement of our strategic goals. CGIAR cannot deliver on its mission without collective awareness that as opportunities are exploited to deliver against our strategic goals, we face many risks.

2. The nature of the CGIAR System – comprised of fifteen independent Centers, a broad and diverse range of Funders, the System Council and its strategic advisory bodies, and the CGIAR System Organization – brings a unique challenge to the identification of a shared vision of CGIAR's risk universe and how an appropriate balance between related risks is achieved. CGIAR's overarching goal is to have an overall risk culture of being risk aware, not risk adverse.

3. CGIAR's risk management framework is thus developed on the basis that CGIAR operates as an '*extended enterprise - where a number of organizations come together in a joint endeavor in order to achieve outcomes that none of them could have achieved on their own'.*[4]

4. While each stakeholder in the CGIAR System defines its own internal risk management processes, CGIAR acknowledges the importance of adopting a set of common risk management concepts and principles to facilitate the taking of risk-informed decisions to further our shared goals. The objective of this framework is to provide such principles and describe how risks relevant to the System and the flow of information around them will be managed.

---

[3] As adopted by the System Council at its 5th meeting (November 2017), Decision SC/M5/DPX.
[4] UK Institute of Risk Management, 'Managing risk in complex 21stcentury organizations – Executive Summary', 2014

Why effective risk management is important

5.   CGIAR recognizes that effective risk management is critical to the success of any enterprise and is a key element to good governance. In CGIAR's extended enterprise environment, effective risk management practices will provide CGIAR's many stakeholders with adequate assurance that, as a System:

    a.   We embrace strategically relevant opportunities – current and new – in the way that best leverages our capabilities, with awareness of the potential trade-offs involved.

    b.   Where the exploitation of an opportunity nevertheless involves downside aspects which cannot be fully mitigated, we are monitoring and continually evolving our actions to minimize or prevent loss of key assets.

6.   This risk management framework draws upon risk management approaches and recommended practices under ISO 31000 and COSO's September 2017 revised framework, as adapted to CGIAR's extended enterprise context.[5]

CGIAR's overarching risk management principles as a System

7.   Building on the *Guiding Principles for the Governance of the CGIAR System*[6] the *CGIAR System Framework*[7] and the *Charter of the CGIAR System Organization*[8], CGIAR collaborates on risk management across the System according to the following principles:

- **Responsibility for an entity's own internal risk management rests with its own management:** Risk management must be tailored, embedded across each entity taking human and cultural factors into account, and under the exclusive responsibility of management, who must ensure that it has capacity to meet expected standards. Management must seize opportunities, address identified risks, assess the impact of its action on the residual level of risk, and ensure effective overall risk management oversight.

- **Risk management is performed closest to the risk to maximize effectiveness**: Aligning with the concepts incorporated into CGIAR's performance-based management system, Centers, the System Management Board and the System Council each have certain areas that fall within their direct sphere of control –

---

[5] (i) The Committee of Sponsoring Organizations of the Treadway Commission (COSO), 6 September 2017 revised risk management framework titled '*ERM Framework: Enterprise Risk Management–Integrating with Strategy and Performance';* and (ii) The 2009 standard of the International Organization for Standardizaton titled '*ISO 31000 - Risk Management: Principles and Guidelines'*

[6] Agreed between CGIAR's Funders and Centers in February 2016, and incorporated into the CGIAR System Framework at Article 1, with the intent to guide the development of policies, procedures, guidelines and operations of the CGIAR System.

[7] http://library.cgiar.org/bitstream/handle/10947/4371/CGIAR%20System%20Framework%20-%20WEB.pdf?sequence=4

[8] https://library.cgiar.org/bitstream/handle/10947/4370/Charter%20CGIAR%20Organization.pdf?sequence=4
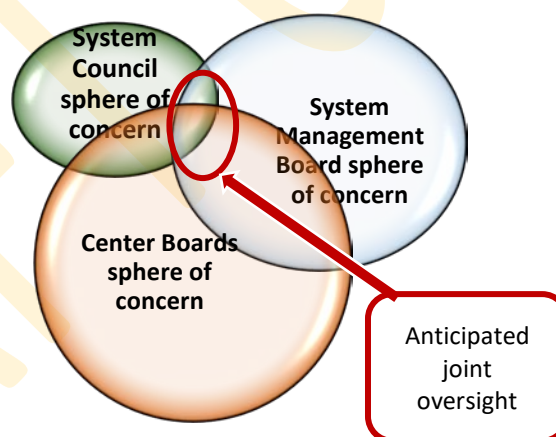
where they are the System-wide stakeholder that can take direct action in respect of any given risk or series of related risks.

Table 1 – Spheres of control, influence and interest

Sphere of control	Where entities can and must assume the responsibility of managing risks that are in their area of control
Sphere of Influence	Where entities are to be engaged in matters where they can support identification, assessment and mitigation but do not own the risk
Sphere of Interest	Where entities are informed regularly in areas that may help them to adjusting their own practices

- **Effective risk management in CGIAR's extended enterprise environment will require CGIAR's main governing bodies to also take into consideration risks that arise from the very nature of CGIAR's collaborative model.**

In CGIAR's multi-dimensional extended setting it is accepted that a subset of CGIAR's key risks will need to be overseen by multiple stakeholders. Considering the Guiding Principle of Subsidiarity – CGIAR anticipates that to the extent appropriate, some System-level risks will be managed by the Centers and/or the System Management Board

- **Effective risk management is dynamic, iterative and responsive to change.** As an innovation-driven System, CGIAR needs to adopt and implement strategic actions that are the most likely to support the achievement of its System-Level Outcomes. We seek to obtain the best and most current balance of available opportunities against the most acceptable level of potential issues. We are committed to identify and measure key risks on a regular basis, revisit our formerly agreed attitude to risk and formulate strategies to address significant risks as they arise.

- **Risk management is transparent and inclusive:** Some risks will require joint management because of the inherent nature of those risks in a multi-dimensional extended enterprise setting. Management of the respective entities involved will exchange the information needed to ensure that potential consequences of risk management action on the entire System are always considered.

- **Opportunities and risks are considered individually and in their aggregate**: CGIAR recognizes that several types of risks and opportunities may have the potential to influence the delivery of the same objective. Potential System risk events will be assessed according to the System's risk appetite, possible response strategies, and which entity or function is most appropriate to take responsibility for that response (the "owner").

- **We ensure appropriately mandated and resourced assurance providers and promote 'combined assurance' across the System**: CGIAR encourages and supports the coordination of multiple assurance processes to ensure that each risk is monitored and managed at the appropriate level, through:

    i.   a common understanding of risks (the risk universe),
    ii. a coordinated plan, based on respective skillsets, to provide assurance on these (the assurance map and coverage strategy), and
    iii. a shared information (the overall opinion) to governance bodies.

    To the largest possible extent, duplication between sources of assurances to the Center Boards, the System Management Board and the System Council is to be avoided. Any System-wide assurance needs and approaches should complement and support assurance obtained at Center level. Each source of assurance refers to its own professional framework, and seeks to comply with a generally accepted set of requirements.

- **We are risk aware and routinely take stock of our risk management capability**: Regular self-assessment of risk maturity, and periodic formal assessment of the capabilities of CGIAR's combined assurance providers according to international standards will be used to inform evolution of CGIAR's risk management practices.

- **We share information as needed and take decisions promptly**: As risks are managed by multiple stakeholders across the CGIAR System, we value clear, transparent and timely communications to avoid missing opportunities, or the risk that an existing problem grows. Our aim is to foster a pro-active communications culture across the System, which is underpinned with communications strategies and plans for incident response.

CGIAR System-wide operational objectives and associated 'top' risks

8. **System-level outcomes**: CGIAR's "Strategy and Results Framework 2016-2030" presents three System Level Outcomes (SLOs) – being the strategic goals through which CGIAR aims to reduce poverty, improve food and nutrition security and improve natural resources and ecosystem services.

9. **Setting strategic System-wide operational objectives to achieve our goals**: To provide an essential link between CGIAR's SLOs and actions of CGIAR System stakeholders to

deliver against those outcomes, CGIAR has adopted the following five operational objectives in the context of its extended enterprise environment:

- **Delivery**: Deliver good science, partnerships and other research outputs that provide critical improvements for food security, nutrition and resilience to climate change.
- **Relevance**: Establish and maintain CGIAR as a relevant and sustainable tool for agricultural research for development.
- **Reputation**: Make the association with CGIAR a rewarding and rational decision for partners and funders.
- **Reliability**: Fulfill our formal commitments.
- **Efficiency:** Generate all benefits mentioned above efficiently and generate value for money.

10.   **Linking operational objectives and key System risks**: The attainment of each operational objective depends on key success factors – thereby giving rise to inherent System-wide risks. These risks and their corresponding opportunity and risk indicators are identified from analysis of the objectives.

11.   Some System-level risks have operational implications throughout the System, and thus will involve the Centers mapping their risks up, with the System Management Board providing oversight. Others, because of their highly strategic nature, will be particularly relevant to the System Council.

12.   The CGIAR System Risk Management Guidelines, approved by the System Management Board from time to time, will provide a basis for common language and define the top risks relevant for the System based on international best practices. It is the responsibility of the System Management Board to oversee the maintenance of a risk register to set out these risks and their status from time to time.

13.   The CGIAR System Risk Management Guidelines do not supersede any individual entities own definition risk categories. Rather, on an action-oriented basis, where a risk is in the sphere of control of a CGIAR System stakeholder, they would communicate within the System on that risk in a manner consistent with the Guidelines

14.   The System Management Board has responsibility for periodically reviewing the appropriateness of top risks, in consultation with the System Council's [Assurance Oversight Committee.]

System-level risk appetite statement

15.   While the risk appetite of individual CGIAR System stakeholders will vary, consensus in decision-making is reached through the System Council and the System Management Board, as guided by CGIAR's mission, Strategy and Results Framework, the agreed System-level outcomes or goals, and the operational objectives agreed by the System Council from to time to time.

16.   The CGIAR System risk appetite statement is approved and periodically reviewed by the CGIAR System Council for appropriateness.

17.   The objective of the CGIAR System's risk appetite statement is to clarify the System's willingness to take risk in pursuit of its goals. This requires:

- agreement on the parameters of what is broadly acceptable;
- effective communication within the System as to how much risk the System Council believes is appropriate to take to maximize CGIAR's impact; and
- monitoring and reporting on how much risk is being taken, to inform whether adjustments are required.

Roles and responsibilities across the System

18.   **Centers' Boards** are ultimately responsible for the oversight of the entire risk management process and its outcomes for their respective Centers. Center Boards approve their respective risk appetite statements.

19.   **The System Management Board** is responsible for overseeing the process of identification of System-wide risks and opportunities, and for obtaining adequate assurance that these risks and opportunities are being acted upon. In practice, the ongoing performance of this oversight is delegated to its Audit and Risk Committee. The System Management Board also approves the System-wide escalation policy, risk management guidelines, maturity model and arrangements for the internal audit function, after receiving inputs from the System Council. It develops the CGIAR System Risk Management Framework and Risk Appetite Statement and drafts their updates for System Council approval.

20.   **The System Council** reviews and approves the current Risk Management Framework, the CGIAR System's Risk Appetite Statement and their further updates, on the recommendation of the System Management Board. To the extent possible, the System Council and its members provide timely information on budgetary outlook and anticipated changes in funding levels for the CGIAR Trust Fund. It is the role of the System Council to ensure that its advisory bodies have risk-focused terms of reference that help them deliver against the combined assurance model. The System Council's [Assurance Oversight Committee][9], through an effective protocol with the System Management Board's Audit and Risk Committee, provides an effective communication bridge between the System Council and the System Management Board.

21.   **CGIAR System Partners** represented at the System Council inform the System Council about significant issues and opportunities relevant to the CGIAR System or likely to impact it.

---

[9] Requires System Council agreement to change this name

CGIAR System communication and escalation principles

22. CGIAR's extended enterprise environment necessitates a common framework to guide communication and escalation/de-escalation on risk. The System Management Board's responsibility is to oversee the development by the System Management Office of an escalation process which incorporates a proactive communication protocol for specific incidents.

23. The following principles guide development of that process:

    a. The information needed to act on any risk or opportunity should be escalated or de-escalated to the most relevant place in the System, and the originator should be informed of the outcome of related management action.

    b. It is the responsibility of each Center's Board to identify and inform the System Management Board of the existence of a risk or an opportunity that should be placed under its ownership or would potentially impact the System as a whole.

    c. In a situation where the System Council should be appraised of a significant risk-related event, it is the responsibility of the Chair of the System Management Board, or if relevant, of the Chair of the System Management Board's Audit and Risk Committee to alert the Chair of the System Council.

Continuous Learning

24. CGIAR accepts that change is constant. Not only are the internal and external environments we operate in continually evolving, but also the field of risk management and the maturity of each of our entities in their risk management approaches.

25. CGIAR commits to taking the lessons we learn while implementing this initial framework and the developments in the risk management field and to improve and transform our extended enterprise risk management framework and approaches to ensure success in changing economic conditions. This commitment to constant improvement will be supported by a formal assessment being performed on a regular basis, leading to actionable recommendations.

APPENDIX A.5

Draft Terms of Reference
Assurance Oversight Committee of the System Council

Purpose

These draft Terms of Reference focus on ensuring that duplication of the respective mandates of this Committee and of the Audit and Risk Committee of the System Management Board is avoided and that the level of oversight demanded from the System Council's Standing Committee is at the right, strategic level, maximizing reliance on the principle of subsidiarity. This draft includes the proposal that the System Council's standing committee be re-titled to 'Assurance Oversight Committee': to avoid confusion; and to better position the System Council's Committee in our 'extended enterprise' environment.

Terms of Reference

A.   Committee Purpose and System-wide context

1.   **The Assurance Oversight Committee ("AOC"), a standing committee of the System Council ("Council") composed of a majority of independent members[10].**

2.   **Its purpose**[11] is to provide:

   a.   **The Council with assurance of the completeness and effectiveness of the Internal Audit Function and the independence of external audit functions**, and a structured reporting line between internal and external auditors and the System Council; and

   b.   **Oversight of system-wide governance, risk management and internal controls**.

3.   **The AOC operates within the following context as agreed between CGIAR's Funders and Centers in June 2016**:

   a.   The Council's principal role is to keep under review the strategy, mission, impact and continued relevancy of the CGIAR System[12];

---

[10] As stated in Article 8.2 of the CGIAR System Framework
[11] As stated in Article 8.2(a) of the CGIAR System Framework
[12] As stated in Article 2(b) of the CGIAR System Framework

b.   CGIAR's Funders provide guidance and financial resources for CGIAR Research and for the agreed operations of the CGIAR System Organization, which is governed by the CGIAR System Management Board ("Board");

c.   CGIAR's Centers are autonomous organizations with their own Board of Trustees comprised of a majority of independent trustees, and supported by their respective Center's management, risk and assurance structures and processes, including Center-specific finance, risk and/or audit committee;

d.   The Board's system-level oversight role is supported by a Board-appointed Audit and Risk Committee with a broad mandate in respect of system-level finance and risk and assurance matters;

e.   Between the Council and Board, it is the Council's responsibility to approve a risk management framework of the CGIAR System, and it is for the Board to approve System-focused internal audit function arrangements that are aligned to the risk management framework and which arrangements take into consideration the existence of the internal audit arrangements of each Center;

f.   Agreed Guiding Principles[13] are intended to guide the development of policies, procedures and guidelines of the CGIAR System. These principles include (numbered 12), that "the principle of subsidiarity should guide policies and implementation, and overreach must be avoided. The Centers should be responsible for system functions that can be more efficiently and effectively executed by them and by CGIAR Research Programs and for the use of funds provided to them…"

4.   The AOC serves the Council in all matters covered by this Terms of Reference. In so doing, it shall be the responsibility of the AOC Chair to:

a.   Maintain regular and open communication among AOC members and with the Council; and

b.   Establish and maintain an effective consultation model with the System Organization via the Board's Audit and Risk Committee, to facilitate delivery on the respective mandates of the two committees, thus ensuring open and transparent communications, and the appropriate escalation and de-escalation of matters as relevant to the differing oversight responsibilities within the CGIAR System.

---

[13] The Guiding Principles are recognized in Article 2 of the Framework and set out in full text in Annex 1, as agreed at the meeting of Centers and Contributors in February 2016.

B.   Committee roles and responsibilities

5.   Pursuant to the purpose set out in Article 2(a) above, the AOC's responsibilities comprise the following:

Assurance functions related to internal and external audit

a.   Provision of input on behalf of the Council into the Board's approval and periodic review of terms of reference and process for fulfilling the Internal Audit Function arrangements for the CGIAR System;[14]

b.   Provision of advice on the System's Internal Audit Function arrangements; whether they provide sufficient-system wide assurance consistent with the risk management framework of the CGIAR System and whether such arrangements are appropriately funded; and

c.   Consideration of consolidated lessons learned and prioritized recommendations relating to system-wide risks arising from the Board's review of findings and follow-up emanating from the Internal Audit Function, and providing advice to the Council on the appropriateness of planned actions;

d.   Consideration of consolidated metrics on the quality and independence of internal audit arrangements and external audit providers throughout the System, and offer recommendations to the Council regarding any system-wide assurance risks or gaps which may arise;

e.   Serving as the conduit for a structured reporting line between the internal audit function arrangements and external auditors, and the Council; including providing recommendations to the Council on appropriate escalation and de-escalation processes are in place to respect the principle of subsidiary to the extent possible having regard to the nature of the risk or assurance questions arising.

Oversight of system-wide governance, risk management and internal controls

f.   Provision of advice and recommendations to the Council regarding its approval and periodic review of the risk management framework of the CGIAR System and an appropriate risk appetite statement related to System-level risks[15];

g.   Review of strategic-level risk exposures and the steps taken by the System Organization to monitor and control such exposures, and report to the Council on such matters and any recommendations arising therefrom;

---

[14] Article 6.1(h) of the CGIAR System Framework. The review cycle would typically be each 3-5 years.
[15] Article 6.1(l) of the CGIAR System Framework. The review cycle would typically be every 3-5 years.

h.   Review of consolidated information on corrective actions taken by the System Management Board under funding agreements with Centers and the risk management framework of the CGIAR System, providing observations to the Council on the adequacy and relevance of those actions;

i.   Provision of advice to the System Management Board on the reasonableness of business plans and budget projections for the Council's advisory functions to inform the Board's submission to the Council of consolidated System entity multi-year and/or annual work programs and budgets;

j.   Review of key recommendations from the CGIAR System Organization arising from their review of consolidated system-level annual financial reports, providing feedback to the Council in line with the risk management framework of the CGIAR System;

k.   Provision of advice to the Council regarding its approval of CGIAR policies relating to system-wide governance and risk management; and

l.   Upon request, provision of input into the System Management Board's commissioning of governance and management reviews of CGIAR Centers to complement the evaluations of the CGIAR Portfolio.

C.   Composition and Chair

6.   <u>Composition</u>. Membership of the AOC shall be composed of a maximum of five (5) persons, three (3) of whom are independent members[16], and two (2) of whom shall be selected from amongst the Council's voting member constituencies. In line with good governance practices, independent members shall not have been involved in any capacity with the CGIAR System in the 3 years prior to their appointment date.

7.   <u>Appointment process</u>. AOC members are appointed by the System Council. As required, the System Council [Chair] shall appoint an ad hoc nominating committee to undertake a search for membership candidates and make appointment recommendations. The CGIAR System Management Office shall serve in a secretariat capacity to the nominating committee.

8.   <u>Skills and experience</u>. Persons serving as members of the AOC who are not System Council voting member constituency representatives shall have one or several of the following experience and skills:
a.   Corporate Governance
b.   Financial and programmatic performance management
c.   Internal audit and risk management
d.   Ethics and investigation

---

[16] In line with the requirement in Article 8.2(a) of the CGIAR System Framework, the Committee shall have a majority of independent members.

9. Term of members. Each AOC member (including the Chair) shall serve on the committee for up to three-years, and shall serve until their successors shall be duly designated or until such member's earlier resignation or removal by decision of the Council. AOC members may be renewed. Renewal of terms shall be determined by the Council.

10. Chair. The members of the AOC shall elect a Chair from amongst their members, using a simple majority vote, for a term of three years. The Chair may be re-appointed for one additional three-year term if supported by all other members of the AOC and endorsed by the Council. Whenever possible, the AOC Chair should be drawn from the independent members of the AOC.

11. Delegation of Authority. The AOC shall have the power to delegate on an exceptional basis its authority and duties to the AOC Chair.

D. Operations

12. Meetings. The AOC shall meet at least twice per year, preferably prior to Council meetings. Meeting dates shall be determined by the Chair in consultation with the other members.

13. Quorum. A majority of members, one of whom is the Chair (or a temporary Chair nominated by the Chair should circumstances required), shall constitute a quorum for the transaction of business.

14. Agenda. The AOC Chair shall develop an annual rolling agenda, and for each meeting a draft Agenda, and distribute that draft to committee members not less than 14 days before the meeting.

15. Meeting documents. Documents for each meeting will, to the extent practicable, be posted on a dedicated System Council AOC meeting site by the System Management Office not less than 7 days prior to each meeting so as to permit meaningful review in advance of the meeting.

16. Observers and other invitees. The AOC Chair will ensure that relevant stakeholders from across the System are invited to participate in meetings relevant to the agreed agenda.

17. Authority. The AOC may seek any information it considers necessary to fulfil its responsibilities.

18. Access to expertise, including consultants. The AOC in fulfilling its duties under these Terms of Reference will draw on expertise from the System Organization, and subject to budget resources permitting, external consultants, individuals and institutions as appropriate.

19. <u>Decision-making on matters for recommendation to the Council.</u> The AOC Chair should aim for consensus on all decisions resulting in a recommendation being formally put to the Council. If consensus cannot be reached, both the majority and minority positions shall be reported to the Council.

20. <u>Reporting</u>. The AOC formally reports to the Council. The AOC shall provide the Council with each meeting summary and regularly report on its meetings and other activities to the Council. As such, AOC meeting summaries may form public record documents of the Council. The Executive Director of the System Organization shall designate a resource person to serve as the secretariat officer for all meetings.

21. <u>Participation in Council meetings.</u> The AOC Chair shall be invited to attend the System Council meetings, if that person is not otherwise a member of the System Council[17].

E. Declarations of interests and independence

22. <u>Register of interests and continuing disclosure requirements for potential conflicts.</u> All AOC members will be required to comply with the Council's policies on disclosure of interests, and a register of AOC member interests will be accessible to Council members. Where an AOC member has a perceived or actual conflict of interest on a specific topic under discussion, they will make the circumstances known to the AOC, to ensure that discussions proceed in an open and transparent manner.

23. <u>Declarations of independence</u>. All external independent members will be required to sign a declaration of independence in the format approved by the Council.

F. Remuneration and financial support to attended meetings

24. <u>Support.</u> The external independent members of the AOC may receive [an honorarium for service in accordance with any honorarium framework approved by the Council, in addition to] support for travel expenses and per diem according to the stipulations of the System Organization's travel and expenses policy.

G. Committee performance and changes to the Terms of Reference

25. <u>Performance</u>. The AOC will review its own performance on an annual basis having regard to the principles and the purpose of these Terms of Reference and report the outcome of such reviews to the Council.

26. <u>Amendment</u>. The AOC will review these Terms of Reference from time to time and recommend any proposed changes to the Council. The Council may amend these Terms of Reference in accordance with the provisions of the Framework.

---

[17] As stated in Article 3.3(a) of the CGIAR System Framework

APPENDICES B.1 – B.2

[SEPARATELY INCLUDED ON DILIGENT BOARD]

Appendix C: From footnote 1: Responsibilities from CGIAR governing documents – risk and internal audit

Functional areas of responsibility	CGIAR System Framework	Charter of the CGIAR System Organization	
	System Council	System Management Board	System Management Office
CGIAR System* Risk Management Framework	• Approve the integrated Risk Management Framework of the CGIAR System* 6.1(l)	• Recommend a proposal to the System Council (including financial, reputational, legal, regulatory, operational, and strategic risk) and escalation processes 8.1(t)	• Develop, in consultation with the Centers, the proposal 11(f) • Monitor & report on implementation of framework 11(ee)
Internal Audit Function	• Review and provide input into the TOR and process for fulfilling the Internal Audit Function 6.1(h) • Ensure, through the System Council's Audit and Risk Committee ('SC ARC'), that arrangements for the Internal Audit Function provide sufficient system-wide assurance consistent with the risk management framework of the CGIAR System* and those arrangements are appropriately funded 6.1(i) • **[*Review findings and follow-up emanating from the Internal Audit Function* 6.1(j) ** suggest this moves to SMB	• Approve TOR and process for fulfilling, considering System Council input and the audit arrangements of Centers 8.1(i) • Ensure completeness and effectiveness of arrangements for the Internal Audit Function, taking into account audit arrangements at the Centers and the risk management framework 8.1(j) • Approve an annual internal audit plan and appropriate funding 8.1(k) • Keep under review the capacity and quality standards for internal audits to be undertaken by the Centers in conformity with international audit standards and guidelines, including through external quality assurance carried out under the Internal Audit Function 8.1(l) • Provide periodic assurance to the Audit and Risk Committee of the System Council that an effective Internal Audit Function is in place that is consistent with the risk management framework of the CGIAR System 8.1(m) • Facilitate provision of guidance, technical assistance, and advisory support by the Internal Audit Function when requested by a Center 8.1(n)	• Coordinate the development of the proposal 11(g)

<u>APPENDIX B.1</u>

SYSTEM COUNCIL NOVEMBER 2017 PAPER

DRAFT 0- CGIAR System Risk Management Guidelines

Purpose: **The SMB is invited to provide overall observations at SMB7** - the SMB's Audit and Risk Committee will meet on the immediate following day, Thursday 28 September, to consider those inputs and the detailed drafting, and refine the proposal in this document before consultation across the System.

Purpose

These guidelines seek to support the attainment of a common standard regarding risk management practices. These guidelines apply to CGIAR Centers and the CGIAR System Organization and encompass all operations in all countries in which all Centers operate.

1.   Risk Categorization at CGIAR System level

When reviewed in detail, System-wide risks and opportunities can be classified using categories that should be comprehensive, common and stable. For its risk register, the CGIAR System has adopted the following broad risk categorization:

- Institutional risks: Internal risks that can be controlled (e.g. the risk of employee misconduct) through compliance with established rules or policies

- Programmatic risks: Strategic risks taken on in the pursuit of value and relating to program objectives and interventions

- Contextual risks: External risks that are largely beyond control (e.g. the risk of impact from geopolitical events or a natural disaster) but can still be managed by generating ideas about the type and magnitude of external events that could happen, and by developing a plan for mitigating the negative impact if such an event actually occurs in the future.

As a common language on risks is key for optimal coordination and efficient cooperation, the Centers are asked to map their system wide risks into the CGIAR categorization. Each Center is free to define their own risk categories and map their categories to the CGIAR System categories to verifying consistency and of allowing the exchange of risk analysis.

2.   Annual Review of System-wide Risks

The System Management Board will perform an annual review of the System-wide objectives, together with a review of internal and external matters that influence CGIAR's achievement of its objectives. This may result in revisiting the nature and level of priority of risks relevant to the CGIAR System, and the critical success factors supporting their achievement. The System Council will be appraised of the outcome of this interactive process involving Centers.

Aspects the CGIAR System's internal and external context that will be assessed on a regular basis include, but are not limited to System-wide:

- structures (governance, roles and accountabilities), considering the CGIAR System Framework and the Charter of the CGIAR System Organization;
- policies and frameworks;
- perceptions, values and culture;
- information systems, information flows, and decision-making processes (both formal and informal);
- the cultural, political, legal, regulatory, financial, technological, economic, natural and "competitive" environment, whether international, national, regional or local; and
- key drivers and trends that impact on CGIAR's objectives.

3.   Risk Management Framework and Policy to be established by Centers

While the System Council and System Management Board have been given certain oversight responsibility for risk management for the CGIAR System under the System's governing instruments, the primary responsibility for risk management rests with management and the Board of Trustees of each Center.

As such, each Center Board must have in place, and be actively utilizing, a risk management framework and policy which seeks to promote a culture of risk management and create a shared understanding of and promote a consistent approach to risk and risk management within the Center.

The contents of each Center's risk management framework and policy shall be grounded in risk management best practice and aligned with the approved CGIAR System risk management framework. Following risk management best practice, each Center's risk management framework and policy should cover the following concepts

- Risk management principles, processes and reporting
- Categories of risk
- Risk register
- Roles and responsibilities
- Risk appetite statement
- Communication and escalation principles

4.   Escalation and De-escalation

The information needed to act should be escalated or de-escalated to the most relevant place in the System through agreed mechanisms, described in the System-wide escalation policy. Depending on the severity (combining potential impact and likelihood) of each risk and its level of immediacy, an escalation or de-escalation process ensures that official ownership of risks is clarified and that all those who need to be informed or consulted are. As an outcome of this process, feedback is provided to the originator, and if appropriate to other parts of the System, that the right corrective action has been taken.

A specific escalation process regarding the requirement to inform in respect of financial irregularities is mentioned in Financial Framework Agreements, and will be replaced by the System-wide escalation policy when it is approved and implemented. The process requires entities to promptly inform the other System entities positioned closer to the funding source if there is a credible concern of financial irregularities and of the corrective measures initiated.

Where partners are involved, these should inform the relevant CGIAR Participating Center and the Lead Center. Participating and Lead Centers should inform the System Organization. And the System organization is responsible for alerting the System Council. The System-wide escalation policy will define conditions and, where relevant, thresholds for escalating any issue further.

5.   Reporting and Attestation

The Director General and the Chair of the Board are required to ensure compliance with the Center's risk management framework and policy and the Director General will provide attestation of compliance through an annual letter of assurance approved by the System Management Board and submitted to the CGIAR System Organization.

Pursuant to the Charter of the CGIAR System Organization[1], the following documents from each Center are to be included in the repository required to be maintained by the CGIAR System Organization as part of the System Council and System Management Board discharging their oversight responsibilities:

- Center Audit Committee Terms of Reference
- Center Audit Committee membership and skills list
- Risk management framework and policy
- Risk appetite statement
- Risk register – updated annually
- Annual mapping to the CGIAR Top Risks of any risks in the spheres of concern of the System Management Board and System Council

---

[1] Article 11(e) of the <u>Charter of the CGIAR System Organization</u>

6.   Periodic Assessment of Risk Maturity

A risk management maturity model provides a visual and analytical tool to assess the level of maturity of an entity in several agreed areas.

CGIAR Centers' Audit and Risk Committee Chairs have identified the value of an annual self-assessment of overall risk maturity. Facilitated by the CGIAR System Organization, in the first quarter of each calendar year Center Board Chairs, Audit Committee Chairs, Directors General Heads of Internal Audit and Risk Officers (or the role performing that function) are asked to complete a self-assessment according to the following model[2]:

Level of Maturity	Framework	Commitment	Ownership	Processes	Communication & Training	Measurement	HR Support	Oversight
Ad hoc	No structured approach	Risk management seen as unnecessary expense	No interest in using risk management	No tracking of risk management	No formal risk management training	No risk assessment performed	No HR support	No standard reporting
Initial	Policy/process defined	Rules-based approach	Partially defined roles	Risk management champion drives implementation	Risk management material circulated	One-off requirements announced	New staff trained	Monitored by exception
Repeatable	Practical guidance provided	Proactive approach	Clearly defined roles	Managers drive implementation	Co-ordinated training provided	Repeat measurements reported	Risk management integrated into all training	Business units monitor own risks
Managed	Managers confirm compliance	Risk management embedded	Centre of excellence model	Business units drive implementation	Business units drive tailored training	Risks measured consistently	Risk management ability impacts hire/ promote decisions	Single view of risk across organisation
Excellence	Risk management central to decision making	Risk management used for strategic advantage	Managers pursue risk unconsciously	Board and CEO drive risk agenda	Training focuses on best practice	Risk-adjusted performance measures used	Risk management seamlessly integrated into HR	Business driven with key risk indicators

Collectively, CGIAR Centers agree to work towards an overall maturity of "Repeatable" by 2019, with the aspiration to work towards "Managed" over the longer-term. A consolidated and anonymized feedback is presented at each annual General Assembly of the Centers. This process aims at obtaining alignment within Centers and across the organization.

---

[2] Supplied by Bob Semple, Chair of the Audit Committee of CIMMYT and members of the System Management Board's Audit and Risk Committee.

7.   Supporting ongoing consistency and professionalism in the delivery of Center Internal Audit services

Professional standards: The IIA Standards require that internal audit services have access to a quality assurance and improvement program, with a recommendation that professional tools are utilized by internal audit teams in the delivery of their services.

Access to a CGIAR quality assurance program: CGIAR's quality assurance program will be facilitated by a community of practice of the Heads of Internal Audit of the Centers/Regional teams, in consultation with the Audit Committee Chairs of the Centers. Respectively, one Head of Internal Audit and one Audit Committee Chair will be the focal points for the ARC.

Recognizing the benefit to the System of continuous learning and quality improvement, both the licensing costs of System-wide cost-effective professional tools, and funding for the quality assurance program will be provided by the CGIAR System Organization. Cost-efficiency considerations will determine the location for that small quality assurance program facilitation function.

Appendix to CGIAR System Risk Management Guidelines

Risk Terminology

- **Risk:** An event or circumstance that may affect the achievement of objectives. A risk has a cause and effect.
- **Threat**: An event or circumstance that may adversely affect the achievement of objectives.
- **Opportunity:** An event or circumstance that may positively affect the achievement of objectives.
- **Risk Impact:** In risk management terms, the effect of a risk relative to the achievement of the objective.
- **Risk Likelihood:** The possibility that a risk will occur.
- **Risk Severity:** The overall importance of a risk considering both the impact of the event and the likelihood of its occurrence. Risks can be ranked according to their level of severity.
- **Risk Appetite:** The degree of risk, on a broad-based level, that the organization is willing to accept in pursuit of its mission and objectives. For different types of risk, the organization may have different appetite levels.
- **Inherent Risk:** The risk without considering the application of any mitigating measures or any controls.
- **Residual Risk:** The risk after the application of mitigating measures or controls.
- **Risk Register:** Documents the organization's main risks by describing each risk, the likelihood of its occurrence, the likely impact should it occur, relevant internal and external development, mitigation action being undertaken, etc.
- **Risk Response:** Decisions made and actions taken to mitigate the risk, i.e. to bring the residual risk within the limits of an entity's risk appetite. The organization can make the decision to accept, reduce, avoid, or transfer/share the risk.
- **Risk Reduction:** An activity or measure that may be part of the risk response. A preventive or detective control may reduce the likelihood of the risk occurring, and a mitigating control may reduce its impact. Good controls enable assurance providers to provide reasonable assurance over the achievement of objectives.
- **Risk Tolerance:** The ability of the organization to withstand the actual occurrence of events impacting it, for instance its reputation and other assets.
- **Risk Universe:** All risks that could affect an organization.
- **Risk Profile:** An organization-wide or office-wide inventory of risk categories, from internal and external sources, assessed in terms of significance in relation to objectives and defined risk tolerance levels.
- **Risk Maturity Model:** A graphical and analytical representation of where an entity stands on the key criteria identified to define the possible levels of maturity in the risk management process.
- **Extended Enterprise:** is a structure where a number of organizations come together in a joint endeavor in order to achieve outcomes that none of them could have achieved on their own

<u>APPENDIX B.2</u>

<u>Draft 0 – System Council November 2017 paper</u>

Terms of Reference for the CGIAR System Internal Audit Function arrangements
<u>for approval by the SMB after considering inputs of the System Council</u>

<u>Purpose</u>: **The SMB is invited to provide overall observations at SMB7** - the SMB's Audit and Risk Committee will meet on the immediate following day, Thursday 28 September, to consider those inputs and the detailed drafting, and refine the proposal in this document before consultation across the System.

Definitions

1. **Internal Audit Function** means the arrangements agreed between the System Council and the System Management Board to provide independent and objective **assurance services** and **advisory and consultative services** to the System Council and the System Management Board ('**Board**').[1]

2. **Assurance services** involve a structured examination of a process, system or other; and **advisory and consultative services** take the form of preventative and supportive analysis and/or reviews.

3. **Audit and Risk Committee** ('**ARC**') as defined by the *Charter of the CGIAR System Organization* is a standing committee of the Board, the "purpose of which shall be to provide the System Management Board with independent assurance of adequate internal audit capacity, System-wide governance, risk management and internal controls." It operates according to detailed Terms of Reference approved by the Board. [2]

4. **Assurance Oversight Committee** ('**AOC**'), as defined by the *CGIAR System Framework,* is a standing committee of the System Council, with a majority of external independent members, the "purpose of which shall be to provide:

    a. The System Council with assurance of the completeness and effectiveness of the Internal Audit Function and the independence of external audit functions;
    b. A structured reporting line between internal and external auditors and the System Council; and
    c. Oversight of System-wide governance, risk management and internal controls."[3]

---

[1] Article 2(q) of the Charter of the CGIAR System Organization; and 'Definition' (o) of the CGIAR System Framework

[2] http://library.cgiar.org/bitstream/handle/10947/4641/SMB-ARC_TOR_approved17Dec2016.pdf?sequence=1

[3] Article 8.2(a) of the CGIAR System Framework

General principles

5.   The Internal Audit Function arrangements are established according to the following principles:

- CGIAR's Centers have the mandate and responsibility to ensure that Center-own internal audit needs are met and funded through appropriate arrangements, whether provided via in-house; regional teams; and/or third-party assurance providers;

- The CGIAR System Organization ('**System Organization**') has the mandate and responsibly to ensure that its own internal audit needs are met and funded through appropriate arrangements, whether in-sourced or out-sourced;

- The Internal Audit Function operates on a demand-driven not supply-led basis to ensure that cost-efficiency and value for money are fully embedded.

- The Guiding Principles of the CGIAR System, as set out Annex A of the *CGIAR System Framework*, including that responsibilities should be assigned to those entities that can most efficiently and effectively fulfil them, and duplication is to be avoided.

Purpose and client of the Internal Audit Function

6.   **Purpose:** The primary purpose of the Internal Audit Function is to identify strategic recommendations that add value and improve CGIAR System-wide operations, achievable only by reason that the Internal Audit Function arrangements take a cross-System view. Internal Audit Function recommendations may result from conducting engagements commissions by the ARC or from analysis undertaken at the request of the ARC but which draws upon pre-existing information.

7.   **Link to risk management framework of the CGIAR System:** The Internal Audit Function delivers part of the CGIAR System's assurance framework. The preferred model for CGIAR Center and CGIAR System Organization operations in respect of risk-taking is a combined assurance model, to provide visibility on whether the System is receiving adequate cost-effective reasonable assurance.

8.   **Clients -** The Internal Audit Function exists to assist the System Management Board in carrying out its oversight mandate.   The System Council or any other body may make request of the Internal Audit Function through the ARC of the Board.

Organizational arrangements

9. **The Internal Audit Function will be provided by the most appropriate and cost-effective means from amongst the following options as determined by the ARC in consultation with Assurance Oversight Committee of the System Council**, depending on the circumstances as assessed by the Board's ARC:

    a. **An outsourced model**, supported through a consultancy or retainer basis; or

    b. **A full or part time experienced 'staff' resource**, with cost-efficiency driving the location for that resource; or

    c. **An in-sourced model**, provided on a full or part-time by contracting part of the services of an existing Head of Internal Audit of one of the Centers/regional teams.

10. **Periodic review of arrangements**: The ARC will review the organizational arrangements each three years, or earlier should capacity needs or other circumstances require, to ensure ongoing optimal arrangements.

11. **Key competencies**: Without limiting the ARC's decision-making in respect of the person or persons who are engaged from time to time to support the Internal Audit Function, minimum competencies include:

    a. **Capacity to consolidate and filter the most relevant of information**: to identify the most strategic and relevant opportunities for value add, taking the organizational, political and institutional considerations into context.

    b. **Instill confidence**: based on a capacity to hold in-confidence and/or more detailed materials within the Internal Audit Function and the Board's ARC, with aggregated materials providing anonymized thoughtful analysis and System-wide strengthening recommendations.

    c. **Relationship builder and respectful communicator**: Capacity to understand CGIAR and support the System's efforts to achieve cost-effective appropriate results in the context of an ever-evolving dynamic environment. A crucial element includes demonstrating a sound understanding of the basis for differing views, and communicating alternate points in a way that brings out the respective merits of those views.

    d. **Solution focused**: a person who is skilled at synthesizing information and knowledge to present cost-effective pragmatic solutions in the context of an extended enterprise environment.

12. **Reporting line** – The Internal Audit Function provider is supervised by the Board through the ARC.

Implementation arrangements: assurance plans and funding

13. **Rolling multi-year plan informed by Center multi-year assurance plans:** Delivery of assurance engagements via the Internal Audit Function will be according to a System-wide multi-year assurance plan focused on System-wide opportunities and risks where internal audit is the most appropriate assurance mechanism. The Internal Audit Function's multi-year rolling work plan must be informed by the Centers' multi-year assurance plans.

14. **Linkages with System-wide evaluations:** The ARC will ensure that any proposed annual internal audit function activity plan takes into account System-wide assurance that is provided through the System Council's agreed evaluation arrangements.

15. **Approvals:** The Board approves the Internal Audit Function costed annual activity plan for System-required assurance engagements upon the recommendation of the ARC. The ARC oversees and guides the maintenance of an ongoing multi-year rolling Internal Audit work plan in line with the IIA Standards.

16. **Optimizing assurance engagement work planning:** By end-January of each year, the Centers' Audit Committee Chairs and the Heads of their respective Internal Audit arrangements will [meet][engage] with the Internal Audit Function and the SMB Audit and Risk Committee Chair to inform the ARC's advice to the Board on key areas of focus for the Internal Audit Function for the year ahead taking into account Center-own assurance plans for that same year. In some years, Board identified assurance requirements may require a range of System-focused engagements through the Internal Audit Function arrangements. In other years, the number may be small.

17. **Information needs:** The annual activity plan of the **Internal Audit Function** will include a summary of the nature of the information that will be required to deliver on the respective engagements over the year. Once endorsed by the Board, the ARC has delegated authority from the Board to develop and approve the Terms of Reference ('TOR') for each engagement that includes specific information needs to deliver an effective engagement will be included in each TOR.

18. **Revising the Internal Audit annual activity plan:** Any proposed major revisions to the approved Internal Audit Function activity plan during a calendar year must be approved by the Board, based on input from the CGIAR Center Audit Committee Chairs.

19. **Budget**: The annual budget for delivery of the Internal Audit Function is met from the CGIAR System Organization sub-group of System entity accounts. It will be paid from Unrestricted Funding as defined in the *Charter of the CGIAR System Organization.*

Types of assurance engagements

20.   Subject to paragraphs [13 and 15 above], assurance engagements to be conducted by the Internal Audit Function that may be requested by the Board periodically (not more frequently than each 3 years) include:

   a.   Verifying the integrity and effectiveness of shared information systems (active directory, OCS, hosting services): vulnerability, contractual arrangements and monitoring, and identifying systemic opportunities for cost-effective value-added improvements;
   b.   Providing a systemic view of the overall independence of external audit providers for the Centers and the CGIAR System Organization;
   c.   Analysis of information collected through each Center's whistleblowing process to assess the overall appropriateness of System-wide whistleblowing processes related to System opportunities and risk-taking (using anonymized information);
   d.   Considering the effectiveness and communications quality of the CGIAR System-wide escalation and de-escalation policy;
   e.   Effective implementation of agreed Performance-based Management systems (e.g. MARLO) System-wide;
   f.   Reporting process on the outputs and outcomes of country coordination: Reliability of information reported and value added.

21.   **Commissioning of investigations:** When necessary and mandated to do so by the Board due to the prevailing circumstances, investigate suspected fraudulent or unethical practices spanning several Centers or the CGIAR System Organization.

22.   **Assurance, advisory, or more limited investigation engagements related to System-wide risks are performed either by teams assembled from Center internal audit services or by external resources, dependent on availability and the subject matter**. Such teams are assembled by the Internal Audit Function at the direction of the ARC.

23.   **Center-specific matters which may be identified during System-wide engagements:** In the unlikely event that information comes to light during an Internal Audit Function engagement that is specific only to a particular Center, that information will be kept within the specific Center context and will not form part of the consolidated reporting.

24.   **Maintaining confidentiality:** Delivery of Internal Audit Function engagements will be supported by appropriate confidentiality arrangements to ensure that matters that are only relevant to a particular Center remain under the oversight of the relevant Center's Board.

25.   **Formal reporting on engagements**: Material presented for the Board, and, when relevant, the System Council, will be delivered in a way that provides a System-wide view on the subject matter of the report, with solution-based pragmatic recommendations for action when relevant. Material presented to the System Council

must be first reviewed and approved by the Board. In recognition that the purpose of the Internal Audit Function is to address systemic topics that can enhance the efficiency of the CGIAR System as a whole, recommendations will relate only to System-wide benefits. Individual Centers will not be identified in reporting to the System Council but rather the System-wide topic that requires attention.

Access to key stakeholders

26. **ARC**: The Internal Audit Function will attend relevant sessions of ARC and Board meetings.

27. **Center Audit Committee Chairs and internal audit assurance providers**: The Internal Audit Function requires effective communication channels with Center Audit Committee Chairs and Heads of Internal Audit. Communications will be required:

    a. To discuss the scope of specific engagements, to support the ARC's approval of appropriate TOR;
    b. To seek clarifications on information supplied to the Internal Audit Function to facilitate synthesis of information into System-focused cost-effective reporting;
    c. To ensure the appropriate formulation of pragmatic recommendations that add value and improve overall System effectiveness and efficiency.

28. **Engaging with the Heads of Internal Audit Community of Practice:** The Internal Audit Function works collaboratively with the Community of Practice through its Chair; the purpose of this engagement is to ensure effective cooperation, appropriate information-sharing and avoiding duplication in time and cost.