ANNEX B.1

SYSTEM COUNCIL NOVEMBER 2017 PAPER

# DRAFT- CGIAR System Risk Management Guidelines
(for SMB approval in December 2017 after System Council inputs)

## Purpose

**These guidelines are proposed as a companion document to the Risk Management Framework of the CGIAR System to support the attainment of a common standard regarding risk management practices across CGIAR's Centers, and for the CGIAR System Organization**.

The Guidelines are not intended to be exhaustive or prescriptive. Rather, the Guidelines emphasize key elements that are identified as important to ensure an adequate foundation for effective risk management for the CGIAR System, whilst leaving flexibility as to how the Guidelines are implemented within each organization in CGIAR's extended enterprise environment.[1]

The System Council is invited to provide input on the Guidelines, by 17 November 2017 to support the System Management Board's deliberations at its 8th meeting on 11-12 December 2017.

[1] UK Institute of Risk Management, 'Managing risk in complex 21st century organizations – Executive Summary', 2014

# Risk Management Guidelines of the CGIAR System

(Draft for inputs, 25 October 2017)

Approved by the System Management Board
[Date]

## A. Context

1. The System Council and System Management Board have certain oversight responsibilities for risk management[2] and assurance for the CGIAR System under the System's governing instruments.[3]

2. To support the System's adoption of the principle of subsidiarity within the Risk Management Framework of the CGIAR System, these Guidelines set out those elements that are identified as minimum standards to provide reasonable assurance that the risk management practices of CGIAR's Centers[4] and the CGIAR System Organization ('System Organization') are sufficient to ensure that System risks are being effectively monitored, and there is appropriate within-System communication and consultation on opportunities and risks.

3. Internationally, there is growing support towards combined assurance being a preferred means of ensuring that a coordinated approach is applied in receiving reasonable assurance on whether key risks are being managed appropriately.

4. In recognition of the international nature of CGIAR's operations, 'combined assurance' is a preferred model for risk management across the System. CGIAR System entities are strongly encouraged to move towards this model over forthcoming years.

## B. Minimum standards for effective risk management practices

5. To provide for a solid foundation for effective risk management across the System, the System Organization and each Center must have in place, and be actively utilizing, a risk management policy[5] 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. It is the responsibility of management to deliver effective risk management and the respective Boards to ensure effective oversight.[6]

6. The contents of each risk management policy should be grounded in risk management best practice and aligned to the extent relevant with the approved Risk Management Framework of the CGIAR System.

7. Following risk management best practice, each risk management policy should cover as a minimum the following concepts:

---

[2] Common risk terminology is set out in Appendix A of these Guidelines.

[3] Relevant provisions of the CGIAR System Framework and the Charter of the CGIAR System Organization are set out in Appendix B to these Guidelines.

[4] In these Guidelines, unless otherwise stated, a reference to a CGIAR Center includes any non-CGIAR Center that serves as a "Lead Center" for a CGIAR Research Program or Platform.

[5] Nomenclature naturally differs across the System, and so the risk management arrangements may be called a policy, framework or other.

[6] Approval of these Guidelines repeals with immediate effect the former 'CGIAR Consortium Financial Governance Framework' approved in June 2013, and amended in March 2015 by the Consortium Board.

a. Risk management principles, processes and reporting;
b. Categories of risk;
c. Risk register that considers likelihood and consequences of potential events;
d. Roles and responsibilities;
e. Risk appetite statement; and
f. Communication and escalation principles.

8. The System Organization and each Center are also responsible for ensuring that relevant and cost-effective controls are in place, and that appropriate internal arrangements are in place for management to provide assurance to their respective Board that:

a. There is an up to date list of the key risks and opportunities;
b. There is an appropriate action plan to manage the risks that considers likelihood and severity, and the agreed appetite for risk;
c. Actions are being followed up on a timely basis relevant to priority; and
d. There has been full disclosure on a matter that is a System risk.

9. Building on the *CGIAR Financial Guidelines Series, No.3 - Auditing Guidelines* regarding membership of Audit Committees[7] and international best practices, the System Management Board and each of the Center Boards are responsible for ensuring that within their respective committee structures, at least one of the Board's Committees has responsibility to support the Board in the discharge of its role regarding effective risk management, and that there is adequate financial, audit and risk management literacy held by the members of the Committee(s) designated to provide that support. Board member transition planning should be undertaken in a way to ensure that minimum financial, audit and risk management competency is always maintained.

10. Respectively, the Directors General of each Center and the Executive Director of the System Organization are required to ensure compliance with their organization's risk management policy. The Director General/Executive Director as applicable will provide attestation of compliance through an annual letter of assurance submitted to the CGIAR System Organization in a format approved by the System Management Board considering periodic advice from the Assurance Oversight Committee of the System Council.

## C. Review of System-wide opportunity and risk indicators

11. Based on consultations with Centers, the System Management Board will perform an annual review of the CGIAR System's operational and risk indicators as set out in the CGIAR System risk register. This may result in revisiting the nature and level of priority of risks relevant to the CGIAR System. The System Council, thought its Assurance Oversight Committee, will be apprised of the outcome of this interactive process.

[7] Refer Article 1.3 in the Financial Guidelines Series, No.3: https://cgspace.cgiar.org/bitstream/handle/10947/4483/FG%203%20-%20Auditing.pdf?sequence=1

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

    a. Structures (governance, roles and accountabilities), considering the CGIAR System Framework and the Charter of the CGIAR System Organization;
    b. Risk management frameworks and policies;
    c. Opportunity and risk perceptions, values and culture;
    d. Information systems, information flows, and decision-making processes (both formal and informal);
    e. The cultural, political, legal, regulatory, financial, technological, economic, natural and "competitive" environment, whether international, national, regional or local; and
    f. Key drivers and trends that impact on CGIAR's objectives.

## D. Linkage to ongoing CGIAR System policies and guidelines

13. The following policies and guidelines of the CGIAR System, amongst others, include information relevant to the CGIAR System maintaining an overall adequate risk management and combined assurance framework:

    a. CGIAR Principles on the Management of Intellectual Assets;
    b. CGIAR Open Access and Data Management Policy; and
    c. CGIAR's Financial Guidelines Series (No. 1, 2, 3, 5 and 6).

14. The status of ongoing System-wide operational conformity with such policies and guidelines will be considered periodically by the System Management Board's Audit and Risk Committee in the discharge of the Committee's responsibility to provide the System Management Board with independent assurance of adequate internal audit capacity, system-wide governance, risk management and internal controls.[8]

## E. Increasing coordination and sharing of best practices

15. As a means of continuous learning and sharing of best practices in the CGIAR extended enterprise environment, the Audit and Risk[9] Committee Chairs of CGIAR's Centers will meet annually with the System Management Board's Audit and Risk Committee to:

    a. Review the status and ongoing relevance of the 'top risks' and the opportunity and risk indicators;
    b. Reflect upon the risk management practices and lessons learned across the System during the prior year;

[8] Mandate of the Audit and Risk Committee is as stated in Article 9.11(a) of the Charter of the CGIAR System Organization

[9] Term is used to include a reference to the committee(s) charged with responsibility for audit and risk management matters, recognizing that nomenclature and committee mandates differ amongst the Centers.

c. Consider emerging international good practices and the possible adoption of additional best practices across the Centers;
d. Share information as relevant to the preparation of annual work plans for internal and external audit assurance providers between Centers and for the System as a whole;
e. Identify areas of priority work for the Internal Audit Support Service[10], based on inputs from the Heads of Internal Audit and Risk Management Communities of Practice; and
f. Discuss the content of annual reporting to the System Council's Assurance Oversight Committee on the overall state of risk management practices and capacity across the System.

16. CGIAR's Centers and the System Organization will share the following materials, and any updates or revisions from time to time, to keep an up to date repository of key risk management documents, information and capacities, to inform annual discussions with the System Management Board's Audit and Risk Committee on the adequacy of System-wide risk management practices, and to support the System Council and System Management Board in discharging their oversight responsibilities[11]:

a. Audit and Risk Committee Terms of Reference (or other relevant committee);
b. Board membership and skills list and Committee assignments;
c. Risk management policy (or other documents depending on nomenclature);
d. Risk appetite statement;
e. Risk register – updated at least annually;
f. Whistleblower policy and/or guidelines;
g. Charter for the Internal Audit provider (in-house, regional or out-sourced); and
h. Identity of the External Auditor, the number of successive years of engagement, and the balance of annual fees between assurance and advisory work.

## F. Communication on opportunities and risks between risk owners

17. CGIAR's Centers are responsible for the effective management of all Center-own risks and each Center may define their own risk categories for internal Center-own risk management purposes.

18. To deliver on the principle of subsidiarity in the CGIAR System Framework, to the largest extent possible, CGIAR's Centers will be identified as the risk owners for CGIAR System-wide opportunities and risks, or at a minimum, one of the risk owners in circumstances where the opportunities and risks need to be managed to some extent by the System Management Board also, and in more limited contexts, by the System Council in addition to the System Management Board.

[10] Terms of Reference for the Internal Audit Support Service are to be approved by the System Management Board based on the recommendation of the Centers.
[11] Article 11(e) of the Charter of the CGIAR System Organization

19. Risks managed by Centers and the System Organization that are also relevant to CGIAR System-wide opportunities and risks will be mapped up on an annual basis.

20. When mapping to and communicating about System-wide risks, as relevant, the following three CGIAR System categories will be used, to facilitate the effective exchange of risk analysis and to provide visibility on the appropriateness of any planned risk response:

    a. Institutional risks: Internal risks that can be controlled through compliance with established policies.

    b. Programmatic risks: Strategic risks that are taken on in the pursuit of value and relating to program objectives and interventions.

    c. 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 should occur in the future.

## G. Periodic self-assessment of risk maturity

21. CGIAR Centers' Audit and Risk Committee Chairs have identified the value of an annual self-assessment of overall risk maturity in agreed areas, as a basis to review and strengthen risk maturity over time.

22. Facilitated by the CGIAR System Organization, in the first quarter of each calendar year, Center Board Chairs, Audit and Risk Committee Chairs, Directors General, Heads of Internal Audit, and staff responsible for risk will complete a self-assessment according to the model set out on Table 1 (following), according to the categories below.[12]

| Level of maturity | Descriptor |
|---|---|
| Level 5**: Excellence.** | Risk discussion is embedded in strategic planning, capital allocation, and other processes and in daily decision-making. Early warning system is used to notify board and management to risks outside of established thresholds. |

[12] Supplied by Bob Semple, Chair of the Audit, Finance and Risk Committee of the CIMMYT Board of Trustees, and member of the System Management Board's Audit and Risk Committee at the date of approval of these Guidelines.

Level 4: **Managed.** Risk management activities are coordinated across areas. Common risk management tools and processes are used where appropriate, with entity-wide risk monitoring, measurement and reporting. Consequences of opportunities are measured again specific risk appetite statements. Alternative responses are analyzed using scenario planning. Process metrics are in place.

Level 3: **Repeatable.** Common framework risk assessment/response framework is in place. Entity-wide view of risk is provided to executive leadership. Risk appetite is defined in general terms. Action plans are implemented in response to high priority risks.

Level 2: **Initial.** Risk is defined in different ways and managed in silos with uneven levels of management commitment. Risk appetite is not defined. Rigor of the process discipline cannot be ascertained.

Level 1: **Ad hoc.** Risk management process is not documented; Activities react to changing circumstances and depend on individual initiatives.

23. Collectively, CGIAR Centers agree to work towards an overall maturity of "Repeatable" by end-2019, with the aspiration to work towards "Managed" over the longer-term.

24. A consolidated and anonymized report on self-perceived risk maturity across the CGIAR Centers will be presented at each annual meeting of the General Assembly of the Centers in addition to being a standing agenda item of the annual meeting of the Audit and Risk Committee Chairs of the Centers and the Audit and Risk Committee of the System Management Board. Post-discussion with the Centers, the consolidated and anonymized report will be presented to the System Council's Assurance Oversight Committee as part of the provision of assurance materials relevant to the discharge of the System Council's responsibilities in respect of risk management. This practice aims at obtaining alignment within Centers and across the CGIAR System.

Table 1: Risk Maturity Model Regarding Operational Areas for Risk Management

| | Operational Area | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Level of Maturity** | **Framework** | **Commitment** | **Ownership** | **Processes** | **Communication & Training** | **Measurement** | **HR Support** | **Oversight** |
| **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 |
| **Managed** | Managers confirm compliance | Risk management embedded | Center 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 organization |
| **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 |
| **Initial** | Policy/ process defined | Rules-based approach | Partially defined roles | Risk management champion drives implementation | Risk management materials circulated | One-off requirements announced | New staff trained | Monitored by exception |
| **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 |

# Appendix A- 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 Owner.** The person or entity with the responsibility to manage a risk.
- **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 several organizations come together in a joint endeavor in order to achieve outcomes that none of them could have achieved on their own.

# Appendix B: 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)<br>• 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)<br>• 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)<br>• **[*Review findings and follow-up emanating from the Internal Audit Function* 6.1(j)]<br><br>** Based on consultations with Centers to date, the proposal to be made to the System Council at its 5th meeting to move this responsibility to the System Management Board | • Approve TOR and process for fulfilling, considering System Council input and the audit arrangements of Centers 8.1(i)<br>• 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)<br>• Approve an annual internal audit plan and appropriate funding 8.1(k)<br>• 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)<br>• 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)<br>• 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) |