	ORGANIZATIONAL DEVELOPMENT UNIT	CODE: PO-14-ODU
		VERSION: 03
	RISK MANAGEMENT AND INTERNAL CONTROLS POLICY	Page 1 of 19

Contents

1. INTRODUCTION 3

2. POLICY OVERVIEW 4

3. OBJECTIVES..... 4

4. SCOPE 6

5. DEFINITIONS AND ACRONYMS 6

6. POLICY STATEMENTS..... 7

7. RISK MANAGEMENT AND INTERNAL CONTROLS STRATEGY 7

7.1. RISK MANAGEMENT STRATEGY..... 8

7.1.1. Alliance-Wide Risk Assessments..... 8

7.1.2. Risk Assessment for Alliance Projects, Programs and Initiatives 8

7.1.3. Regional and Country Risk Assessments 8

7.1.4. Unit and functional risk assessment..... 8

7.1.5. Risk Appetite 9

7.2. INTERNAL CONTROL STRATEGY..... 9

8. REPORTING MECHANISMS 10

9. ROLES AND RESPONSIBILITIES..... 10


10. IMPLEMENTATION 15

11. REVIEW AND APPROVAL 16

12. RELATED POLICIES/REFERENCES FOR MORE INFORMATION 16

13. VERSION CONTROL..... 16

Annex 1. Risk appetite statement relevant to the Alliance's objectives..... 17

	ORGANIZATIONAL DEVELOPMENT UNIT	CODE: PO-14-ODU
		VERSION: 03
	RISK MANAGEMENT AND INTERNAL CONTROLS POLICY	Page 2 of 19

1. INTRODUCTION

The Alliance as part of the CGIAR Integrated Partnership (IP) recognizes that risk taking and risk management are an integral part of delivering on its strategy. As an innovation-driven partnership, the Alliance cannot succeed without embracing risks and pursuing opportunities.

The purpose of this policy is to embed a culture of risk management, supported by capabilities, and best practices that the Alliance integrates with strategy and performance. By integrating risk management into decision-making processes, this policy ensures that risks are proactively identified, assessed, and managed, while maintaining full compliance with regulatory and donor requirements. It also establishes a consistent risk language, a shared understanding of risk management principles, and clear roles and responsibilities at all levels.

The policy provides a mechanism to foster the adoption of risk management practices as part of routine management for programs and operational activities aimed at managing risks and opportunities in alignment with the Alliance’s strategy and business planning, giving confidence to stakeholders, including funders and partners.


The policy sets forth the principles and requirements for developing, implementing, and maintaining a strong internal control system across the Alliance. This system is designed to:

- Enhance operational integrity and efficiency.
- Ensure compliance with regulatory and Donor expectations.
- Ensure the accuracy and reliability of financial and operational reporting.

By integrating internal controls within the Alliance’s broader risk management framework, the policy provides a foundation for risk-informed decision-making. It also aims to prevent and detect fraud, misconduct, and control failures, reinforcing a culture of accountability and transparency. Furthermore, the Policy promotes continuous improvement through ongoing monitoring, evaluation, and adaptation of internal control mechanisms.

This Policy is designed to provide guidance to all staff on implementing an Alliance-wide risk management framework. Risk Management principles and approaches are based on the International Organization for Standardization (ISO) 31000:2018 (Risk Management-Guidelines), the 2017 Committee of Sponsoring Organizations of the Treadway Commission (COSO)¹ Enterprise Risk Management Framework, and the CGIAR IP Risk Management Framework.

¹The Committee of Sponsoring Organizations of the Treadway Commission (COSO) document Enterprise Risk Management – Integrating with Strategy and Performance (www.coso.org). COSO is sponsored by five major professional associations in the United States: the American Accounting Association, the American Institute of Certified Public Accountants, the Financial Executives Institute, the Institute of Internal Auditors, and the Institute of Management Accountants. COSO first published its Enterprise Risk Management Integrated Framework in September 2004. A revised version of this Framework was published in June 2017.² Review the detailed Risk Appetite statement relevant to the Alliance’s objectives in the Annex 1.

	ORGANIZATIONAL DEVELOPMENT UNIT	CODE: PO-14-ODU
		VERSION: 03
	RISK MANAGEMENT AND INTERNAL CONTROLS POLICY	Page 3 of 19

2. POLICY OVERVIEW

Outlined in the following diagram are the essential components of the Alliance’s comprehensive risk management and internal controls Policy. Each element plays a crucial role in safeguarding the Alliance against potential threats and maximizing opportunities for success.

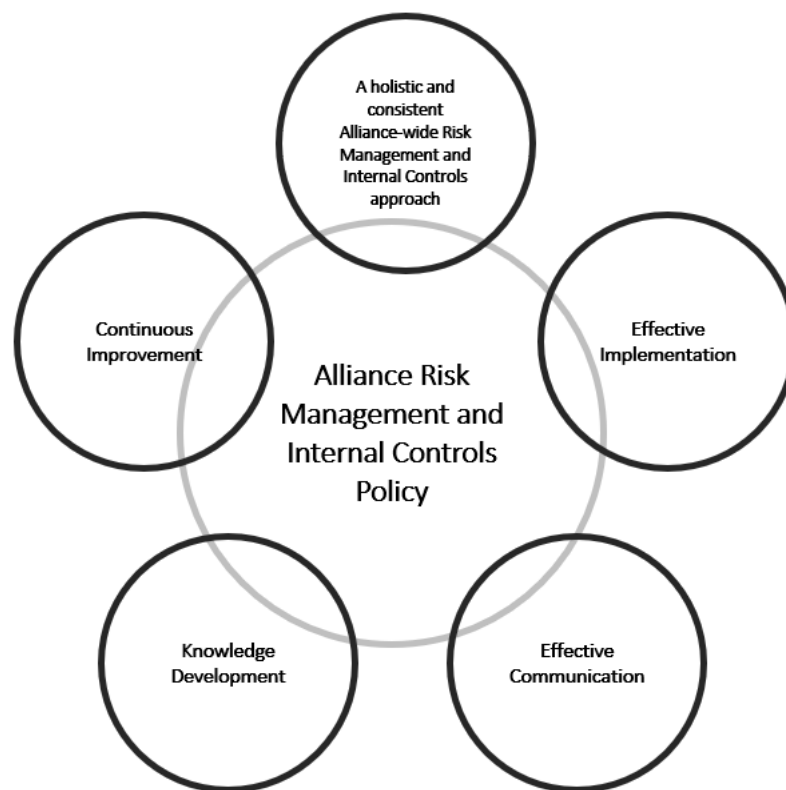


Image No. 1. Policy Overview


3. OBJECTIVES

1. A holistic and consistent Alliance-wide risk management approach

The Alliance as part of the CGIAR IP is committed to following a holistic and consistent Alliance-wide risk management approach that follows the Alliance’s risk management principles set out in the Risk Management Framework of the Integrated Partnership.

2. Effective implementation

The Alliance as part of the CGIAR IP is committed to the achievement of its strategy and objectives, including the overall management of risks and opportunities. The Alliance is committed to identifying

	ORGANIZATIONAL DEVELOPMENT UNIT	CODE: PO-14-ODU
		VERSION: 03
	RISK MANAGEMENT AND INTERNAL CONTROLS POLICY	Page 4 of 19

new and emerging risks and opportunities and responding appropriately and timely by carrying out planned risk assessments according to the annual risk plan but also unplanned assessments as changes of the internal or external environment require. Assessments as part of the annual plan include:

- Principal risks for the Alliance (top risks)
- Alliance-wide risks, including regional and country risks
- Selected (criteria-based) science programs and projects
- Operational controls – Strengthening efficiency, effectiveness, and governance across the Alliance’s activities.
- Compliance controls – Ensuring adherence to legal, regulatory, and donor requirements.
- Fraud prevention and detection – Establishing mechanisms to identify and mitigate fraud risks.
- Monitoring and evaluation – Enabling continuous assessment and improvement of the internal control environment

The Alliance’s decision-making and risk management strategies will be informed by CGIAR IP and Alliance’s Risk Appetite. The Alliance Board of Trustees is expected to confirm its Risk Appetite annually.

3. Knowledge development

The Alliance as part of the CGIAR IP is committed to ensuring that all staff, particularly those with management, advisory and decision-making responsibilities, obtain a sound understanding of the principles of risk management and the skills required to implement risk management effectively through common mandatory training.


4. Continuous improvement

The Alliance as part of the CGIAR IP will regularly monitor and review the progress being made in developing the CGIAR IP and Alliance’s risk management culture, capabilities and practices and the effective implementation of risk management as a basis for continuous improvement.

5. Effective communication

The Alliance has an obligation to communicate risks and principal risks and escalate events in a timely, transparent, and consistent manner. This ensures that decision-makers and oversight bodies at all levels are equipped with the necessary information to respond effectively and maintain the integrity and resilience of operations.

The Alliance as part of the Integrated Partnership is responsible for identifying and sharing key risks within the IP. Risk communication must flow through the appropriate management levels to ensure that material risks are elevated to the relevant governance and oversight bodies, such as the Audit, Finance, and Risk Committee (AFRC), the Board of Trustees, and the Senior Management Team, as applicable.

	ORGANIZATIONAL DEVELOPMENT UNIT	CODE: PO-14-ODU
		VERSION: 03
	RISK MANAGEMENT AND INTERNAL CONTROLS POLICY	Page 5 of 19

4. SCOPE

The CGIAR IP and Alliance risk management and internal controls policy aims to foster practices, capabilities, and a culture of effective risk management aligned with strategy-setting and performance objectives. It aims to support the Alliance's SMT, the Board of Trustees and Departments, Regions and Project Leaders in making more informed decisions, monitoring risks and related activities across the Alliance, and guiding initiatives to help the Alliance in preserving and creating value.

5. DEFINITIONS AND ACRONYMS

Risk: A potential event that, if it materializes, may have a positive or negative impact on the achievement of the Alliance's objectives. Risk is as much a potential threat as a missed opportunity. A risk can have consequences beyond failure to deliver on results. It may negatively affect reputation, integrity, credibility, and trust from funders and stakeholders. Risk has a cause and effect.

Principal risks: Principal risks should include, but are not necessarily limited to, those that could result in events or circumstances that might threaten the business model, future performance, solvency or liquidity and reputation. In deciding which risks are principal risks organizations should consider the potential impact and probability of the related events or circumstances, and the timescale over which they may occur.

Risk Management: coordinated activities to direct and control an organization regarding risk, in an enterprise-wide and holistic approach. It includes culture, capabilities, and practices, integrated with strategy-setting and performance, that organizations rely on to manage risk in creating, preserving, and realizing value.

Risk assessment: the overall process of risk identification, risk analysis, and risk evaluation.

Risk owner: A risk owner is a person or unit that has been given the authority to manage a particular risk and is accountable for doing so.


Event: Occurrence or change of a particular set of circumstances. An event can have one or more occurrences, and can have several causes and several consequences, an event can also be expected to not happen, or something that is not expected which does happen, an event can also be a risk source.

Consequence: The outcome of an event affecting objectives A consequence can be certain or uncertain and can have positive or negative direct or indirect effects on objective Consequences can be expressed qualitatively or quantitatively. Any consequence can escalate through cascading and cumulative effects

Current level: Inherent risk considering existing controls which may be incomplete

Target level: Residual risk within an agreed time horizon, guided by the risk appetite

Risk register/risk catalogue: A risk register, or risk catalogue is used as a risk management tool and acts as a repository for all risks identified and includes additional information about each risk, for example, the nature

	ORGANIZATIONAL DEVELOPMENT UNIT	CODE: PO-14-ODU
		VERSION: 03
	RISK MANAGEMENT AND INTERNAL CONTROLS POLICY	Page 6 of 19

of the risk, reference and owner, and mitigation measures. The register should be on a biannual basis to assess risks and update mitigation measures.

Risk category: The risks faced by an organization should be categorized according to the organization's needs. In the Alliance's case, we have defined the following as the main categories: change management, research innovation, partners and partnerships, scaling impacts, business continuity, talent management, data management, health, safety and well-being, ethics and integrity, legal and regulatory compliance, intellectual property, infrastructure, funding and financial risk.

Impact: The effect/severity of the risk relative to the achievement of the objective.

Likelihood: The probability that a risk will occur.

Control: An activity or measure that may be part of the risk response. A control may diminish the likelihood of the risk occurring or its impact or both and can be either preventive or detective.

Risk appetite: The degree of risk that the Alliance is willing to accept in pursuit of its mission and objectives. The risk appetite could be divided according to the categories of risks.

Risk tolerance: Degree, amount, or volume of risk the organization resists.

Risk management: Risk management is the process of systematically identifying, quantifying, and managing risks that can affect the achievement of an organization's strategic and financial goals.


6. POLICY STATEMENTS

Risk Management and Internal Controls Strategy: The Alliance as part of the CGIAR IP will conduct comprehensive risk assessments across all levels, including organization-wide, project-specific, and regional risk assessments, to proactively manage risks and align with the CGIAR IP risk appetite. CGIAR IP is committed to maintaining a strong internal control environment that supports effective operations, safeguards resources, and ensures compliance with policies, regulations, and donor requirements.

Reporting Mechanisms: Risks, including emerging risks and principal threats, will be communicated regularly to relevant stakeholders through defined reporting and escalation channels.

7. RISK MANAGEMENT AND INTERNAL CONTROLS STRATEGY

The Alliance as part of the CGIAR IP is committed to maintaining a strong internal control environment that supports effective operations, safeguards resources, and ensures compliance with policies, regulations, and donor requirements. To strengthen risk governance and foster strategic alignment, the Alliance will define a common risk management and internal controls strategy, including priority areas for risk assessment such as organization-wide, project-specific, and regional risks. The Organizational Development Unit (ODU) will

	ORGANIZATIONAL DEVELOPMENT UNIT	CODE: PO-14-ODU
		VERSION: 03
	RISK MANAGEMENT AND INTERNAL CONTROLS POLICY	Page 7 of 19

facilitate alignment across the Alliance by providing guidance and aggregating insights, enabling a more consistent understanding of risk exposure and supporting decision-making.

7.1. RISK MANAGEMENT STRATEGY

The Alliance as part of the CGIAR IP employs a structured risk management strategy to proactively identify, assess, and mitigate risks across its operations. This approach ensures alignment with the CGIAR IP’s strategic objectives as well as the Alliance institutional and strategic priorities while fostering resilience and informed decision-making.

7.1.1. Alliance-Wide Risk Assessments

The Alliance conducts comprehensive risk assessments to identify systemic risks and emerging threats. Biannually, both "top-down" and "bottom-up" evaluations are carried out with input from Directors, Managers, and key staff across Headquarters, Hubs, and activity locations. These assessments are updated as needed to reflect changes in the internal and external environment. Their purpose is to inform and refine the Alliance’s approach to managing risks and opportunities that may impact its objectives. As part of this process, trends in previously identified risks—as well as significant contextual developments—are analyzed to surface emerging or evolving risks.

7.1.2. Risk Assessment for Alliance Projects, Programs and Initiatives


All proposals for new initiatives such as partnerships with other institutions (USD 5 million or above), the largest research projects (USD 5 million or above), and capital projects, among others, should include an assessment of the risks that they will bring to the Alliance. In the case of Research projects this assessment will be implemented upon proposal submission and approval (when applicable) or upon Grant opening in the system. This assessment should consider our different categories of risks and incorporate the mitigation measures that will be put in place and all relevant information that could help in the decision-making process for accepting the project/program initiative or not. These assessments help identify potential challenges early, enabling proactive risk mitigation strategies.

7.1.3. Regional and Country Risk Assessments

Given the Alliance’s global presence, regional risk assessments are proposed to address location-specific risks, including geopolitical, environmental, and operational challenges. These assessments inform tailored risk responses and strengthen local resilience. In doing so, the Alliance can determine how much those risks might affect its operations and what steps they can take to manage or mitigate those risks. The review should be conducted at least once a year.

7.1.4. Unit and functional risk assessment

Functional areas of the organization have specific policies, procedures, processes, key performance indicators (KPIs), and key risk indicators (KRIs) as enablers to achieve short-term performance objectives and longer-term

	ORGANIZATIONAL DEVELOPMENT UNIT	CODE: PO-14-ODU
		VERSION: 03
	RISK MANAGEMENT AND INTERNAL CONTROLS POLICY	Page 8 of 19

organizational resilience. Through an effective risk review, continuous improvement can be achieved and improved internal controls applied.

7.1.5. Risk Appetite

The Alliance as part of the CGIAR Integrated Partnership recognizes that risk-taking is an integral part of delivering on its strategy. As an innovation-driven organization, the Alliance cannot succeed without taking risks and pursuing opportunities. In this context, risk appetite refers to the level and type of risk an organization is willing to accept, mitigate, or avoid in pursuit of its long-term strategic objectives. Given that the Alliance as part of the CGIAR IP operates within an extended enterprise environment, it brings together multiple stakeholders and partners, each with their own risk appetites and priorities. Therefore, this risk appetite statement provides necessary guidance to these stakeholders and partners, ensuring a common understanding of how risk should be managed to achieve the Alliance’s goals, and how risk should be maximized or minimized depending on the circumstances.

To maintain its relevance and effectiveness, this statement is reviewed annually.²


7.2. INTERNAL CONTROL STRATEGY

The Internal Control Strategy complements the Alliance’s risk management approach by establishing a structured system of checks, balances, and procedures that safeguard resources, ensure regulatory compliance, and promote operational efficiency. While risk management identifies and assesses potential threats, internal controls are the mechanisms that help prevent, detect, and respond to those risks identified.

The Alliance’s internal control system is designed based on the principles of the COSO Internal Control–Integrated Framework, emphasizing five key components:

1. **Control Environment:** Establishing a strong organizational culture that supports ethical behavior, accountability, and integrity. This includes clearly defined roles and responsibilities across different functions, a consistent tone from the top, and alignment with organizational values.
2. **Risk Assessment:** Integrating risk identification into business processes at all levels, supporting the proactive evaluation of operational, financial, compliance, and strategic risks.
3. **Control Activities:** Implementing preventive and detective control measures embedded in day-to-day operations (e.g., approvals, verifications, reconciliations, segregation of duties) to reduce the likelihood and impact of risks.
4. **Information and Communication:** Ensuring relevant information flows efficiently across all levels of the organization to support timely decision-making, issue resolution, and control execution.

² Review the detailed Risk Appetite statement relevant to the Alliance’s objectives in the Annex 1.

	ORGANIZATIONAL DEVELOPMENT UNIT	CODE: PO-14-ODU
		VERSION: 03
	RISK MANAGEMENT AND INTERNAL CONTROLS POLICY	Page 9 of 19

5. Monitoring Activities: Regularly reviewing and evaluating the performance of internal controls through audits, management reviews, and feedback loops, ensuring that the system adapts to changes in the internal and external environment.

In addition, the Internal Controls Strategy prioritizes:

- Control Mapping and Documentation: Standardizing Policies, Processes, Guidelines and documenting internal controls linked to key risk areas across business units and regions.
- Capacity Building and Awareness: Training staff in internal controls and their role in maintaining compliance and accountability.
- Technology and Automation: Leveraging digital tools and systems such as the institutional ERP to strengthen control efficiency, reduce manual error, and enhance transparency.
- Incident and Issue Management: Establishing clear procedures for escalating and remediating control failures or breaches. (documented in the institutional Policies and Procedures)

Together, the Internal Controls and Risk Management Strategies form a coherent, adaptive framework that enables the Alliance to protect its mission, optimize resource use, and meet its obligations to partners and stakeholders with integrity.

8. REPORTING MECHANISMS


The Alliance is responsible for identifying and communicating risks that may have a broader impact. This includes emerging risks, principal threats, and any significant operational, strategic, financial, or reputational risks to the Alliance Audit, Finance, & Risk Committee (A-AFRC) and the Board of Trustees.

The Alliance is also responsible for identifying and communicating risks that have the potential to affect the broader Integrated Partnership. Risks identified at the partnership level, which could have an impact on the Alliance will be communicated to all entities.

In cases where risks escalate beyond a certain threshold or require urgent attention, the relevant risks must be escalated. The escalation process helps ensure that risks are managed in accordance with the Alliance risk appetite and that the necessary corrective actions are taken to mitigate risks before they become larger threats.

9. ROLES AND RESPONSIBILITIES

The risk management framework at the Alliance and CGIAR IP is structured around the Institute of Internal Auditors (IIA) Three Lines Model, ensuring effective risk oversight, accountability, and governance. This model


	ORGANIZATIONAL DEVELOPMENT UNIT	CODE: PO-14-ODU
		VERSION: 03
	RISK MANAGEMENT AND INTERNAL CONTROLS POLICY	Page 10 of 19

will be implemented within the CGIAR Integrated Partnership (IP) and the Alliance management structures to strengthen risk management practices.

1. First Line: Operational Management
 - The SMT is responsible for identifying and managing risks across the Alliance, embedding risk awareness into day-to-day decision-making.
 - The SMT is accountable for Identifying and managing risks across the organization, embedding risk awareness into day-to-day decision-making; and ensuring that risk and control owners implement, maintain, and regularly review effective internal controls. In doing so, the SMT promotes a risk-aware culture and ensures that risk is actively managed at all operational levels.

2. Second Line: Risk Management & Compliance Functions
 - The Alliance Risk lead and Team, represented by the Organizational Development Unit head and team oversee risk management activities, providing expert guidance, best practices, methodologies, and tools.
 - These functions serve as advisors and facilitators, ensuring that risk management processes are standardized, integrated, and continuously improved across the Alliance.

3. Third Line: Internal Audit & Independent Assurance
 - The Internal Audit provides independent, objective assurance and advisory services, ensuring risk controls are effective and aligned with strategic objectives.
 - Key governing bodies receiving audit oversight include:
 - ✓ The Alliance Board
 - ✓ Integrated Partnership Audit, Finance, and Risk Committee (IP-AFRC)
 - ✓ Alliance Audit, Finance, and Risk Committees (AFRCs)

	ORGANIZATIONAL DEVELOPMENT UNIT	CODE: PO-14-ODU
		VERSION: 03
	RISK MANAGEMENT AND INTERNAL CONTROLS POLICY	Page 11 of 19

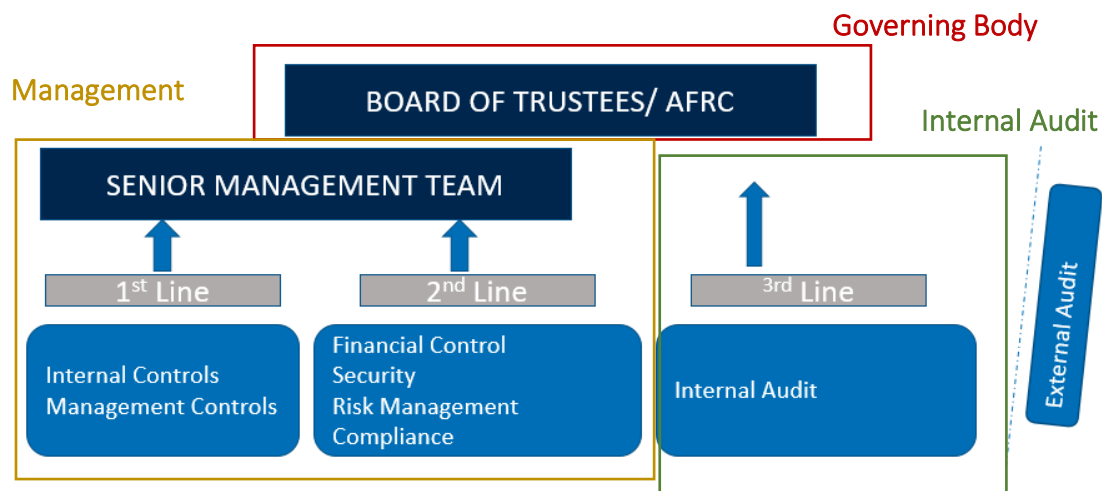


Image No. 2. The Three Lines Model


Governing Bodies

The Board of Trustees guides in developing the organizational strategic directions, including the appetite and capacity for risk. It approves the Alliance's Strategy and Business Plans, considering related risks that potentially affect the achievement of the objectives. The Board of Trustees approves the Risk Management and Internal Controls Policy and the Risk Appetite. It has the overall responsibility for ensuring that a risk management process is in place to identify significant risks to the Alliance with procedures to monitor, mitigate, and manage risks. The BOT will take prompt action on risks that have the potential to impact the CGIAR Integrated Partnership, including escalating relevant risks to the AFRC and IPB when deemed appropriate.

The Audit, Finance, and Risk Committee (AFRC) is responsible for providing assurance to the Board of Trustees that the Alliance effectively manages risk, maintains robust internal controls, and adheres to sound financial and operational practices. It oversees the effectiveness of management's responsibilities in these areas and ensures compliance with approved policies, directives, systems, and procedures.

The AFRC's responsibilities include:

- Reviewing and monitoring the adequacy and effectiveness of the Alliance's risk management and internal control systems, including financial, operational, strategic, and reputational risks.
- Ensuring that the control framework clearly defines roles and responsibilities, aligns with risk tolerance limits, and operates effectively and in compliance with institutional policies.
- Overseeing the work of internal Audit Unit and external auditors, including the scope, results, and follow-up of risk-based audits and assurance activities.
- Receiving and evaluating management's assurances on the effectiveness of risk management and internal controls and monitoring how significant risks and changes to the risk profile are reported and addressed.

	ORGANIZATIONAL DEVELOPMENT UNIT	CODE: PO-14-ODU
		VERSION: 03
	RISK MANAGEMENT AND INTERNAL CONTROLS POLICY	Page 12 of 19


- Identifying and escalating significant risk exposures, emerging threats, or management gaps to the Board, and providing actionable recommendations to mitigate and manage risks effectively.
- Ensuring that all risk events and assessments are addressed thoroughly, independently, and in alignment with legal, regulatory, and ethical standards.
- Advising the Board on key emerging risk trends, significant audit findings, and the outcomes of management’s risk mitigation efforts, including necessary corrective actions or strategic adjustments.
- Ensuring that any material risk issues requiring the attention of the Integrated Partnership AFRC are communicated clearly, documented appropriately, and escalated in a timely manner.
- Overseeing effective risk management within the Center for Center-related risks, and for those CGIAR IP-wide risks where the Center is identified as a risk owner within the CGIAR IP risk register (whether individually, or together with the IPB and System Council); Taking prompt action on risks that have the potential to impact the CGIAR System, including escalating relevant risks to the IPB in line with agreed procedures.

Management

The Director General has the overall responsibility for promoting an appropriate risk management culture and for implementing an effective risk management system. The DG is supported in these responsibilities by the Senior Management Team, the Head of the Organizational Development Unit, the General Counsel, the IAU, and other independent review activities commissioned by the Board of Trustees or the Senior Management Team who report to the DG on these matters at least annually.

The Senior Management Team, assisted by the Head of the Organizational Development Unit, develops risk management principles and approaches. Also, its specific responsibilities include the following:

- Development and achievement of the Alliance’s strategy and objectives
- Overall Management of Risk and Internal Controls and ensuring compliance with the Policy.
- Identifying risks and developing and implementing risk management and internal control practices, including mitigation strategies, systems, controls, and a business continuity plan specific to their respective research areas, regions, or units, which are aligned with and complementary to the Policy.
- Promoting risk and internal control awareness and monitoring the environment at the Alliance level for open communications on risks.
- Maintaining the Risk Management Catalogue and reports detailing the principal risks for their research areas, regions, and units.
- Overseeing risks reported by the internal stakeholders including projects, processes, systems, and research activities undertaken by or on behalf of the Alliance.
- Providing timely risk and control reporting to entity management and Boards, and supporting their oversight responsibilities through insights, recommendations, and updates.
- This includes ensuring the implementation, effectiveness, and continuous improvement of internal control systems that support the achievement of objectives, compliance and safeguarding of assets.

	ORGANIZATIONAL DEVELOPMENT UNIT	CODE: PO-14-ODU
		VERSION: 03
	RISK MANAGEMENT AND INTERNAL CONTROLS POLICY	Page 13 of 19

Risk Management Committee: This Committee is responsible for oversight of the risk management framework and monitors the processes and systems for identifying and reporting risks and risk management deficiencies. It ensures that the necessary processes are in place to achieve compliance with the Risk Management Strategy and duties assigned to the Organizational Development Unit.

The Associate Director General for Research, Strategy, and Innovation oversees and monitors risk assessment of projects, programs, and new initiatives having a value of USD 5 million or above that fall under the Research Division. The risk assessment should be conducted upon proposal acceptance or upon grant reception.


The Head of the Organizational Development Unit supports the Director General and the Senior Management Team in the development, implementation, and continuous improvement of the Risk Management and Internal Controls (RM&IC) framework. This includes:

- Promoting a strong risk and internal control culture across the Alliance.
- Overseeing the maintenance and operation of the compliance monitoring system to ensure that risk mitigation measures are effectively implemented.
- Conducting annual reviews of the RM&IC approach and policy, and recommending updates as needed.
- Preparing reports and statements for the Director General, Senior Management Team, and the Alliance Finance and Risk Committee (AFRC).
- Providing timely risk and control information to management and governance bodies to support oversight, decision-making, and strategic direction.
- Acting as the primary liaison with the RM&IC function of the Integrated Partnership to ensure consistency and alignment.
- Facilitating training, awareness, and capacity building on risk management and internal controls within the organization.
- Participate in the Risk and Internal Controls functions, which aim to enhance risk management within their entities and across the partnership.

Staff: In alignment with the values and principles of the Alliance and its mission, this Policy commits all staff to consistently apply and consider risk assessment and management processes in daily activities, including identifying risks in their area of work. If risks fall within the scope of the Whistleblower Policy, staff members are encouraged to follow it.

Principal investigator or project leader: For projects, programs, and new initiatives with proposals having a value of USD 5 million or above, the principal researcher should inform the Head of the Organizational Development Unit, who will co-lead, together with the principal researcher, an assessment of the risks that the project, program, or initiative could bring to the Alliance, this assessment should be carried out upon proposal submission and approval (when applicable) or upon Grant opening in the system. This assessment should consider our different categories of risks (see Annex 2) and incorporate the mitigation measures that will be put in place.

Risk Owners are responsible for identifying, overseeing, and managing risks within their remit, including development and monitoring of required controls and/or mitigating actions, and the timely reporting and communication of risks to management, as appropriate Risk Owners are typically members of the SMT or

	ORGANIZATIONAL DEVELOPMENT UNIT	CODE: PO-14-ODU
	RISK MANAGEMENT AND INTERNAL CONTROLS POLICY	VERSION: 03
		Page 14 of 19

leaders of functional areas. Risk ownership is assigned based on the alignment between the risk and the strategic or operational responsibility of the individual or function within the Alliance.

Internal Audit Unit-and Ethics Unit: The IAU and EBC Units report administratively to the Director General and functionally to the AFRC.

- Provide risk-based, independent assurance, advice, insight, and foresight on the adequacy and effectiveness of governance, risk management, and internal control systems.
- Deliver assurance services in accordance with the International Standards for the Professional Practice of Internal Auditing.
- Support the implementation of ethical standards and business conduct policies, promote a culture of integrity and accountability, and address potential misconduct.

External Audit: The External Audit function reports operationally to the Director General and functionally to the AFRC. Its scope includes reviewing aspects of the Alliance’s risk and quality management systems as part of the annual financial statement audit. The audit approach extends beyond accounting risks to consider broader business risks that may impact on the Alliance’s financial position and long-term viability. It also evaluates the adequacy of management’s responses and mitigation measures to address these risks.


10. IMPLEMENTATION

This policy will be implemented through the integration of risk management and internal controls practices into management activities. Staff will be trained in risk management and internal controls principles, and resources will be allocated to ensure risks are monitored and managed effectively across all operations.

The policy mandates mapping significant business processes that impact financial reporting to identify key risks and corresponding controls, thereby informing the development of Minimum Control Standards. These standards, which cover essential areas such as governance, compliance, fixed assets, revenue, HR, inventory, expenditure, IT, accounting, consolidation, tax, treasury, and sustainability, provide the Alliance with clear, adaptable guidance to meet its operational objectives.

As the risk management and internal controls framework matures, the Alliance is expected to integrate self-assessment tools—such as checklists, dashboards, and scorecards—to facilitate the ongoing evaluation of control efficiency and effectiveness. This will ensure that internal controls remain dynamic, proactive, and continuously enhanced through regular training, robust communication, and benchmarking against industry best practices.

The Alliance is responsible for conducting periodic internal controls self-assessment checks using established tools such as checklists, dashboards, and scorecards. These self-assessments enable it to monitor the effectiveness of its internal controls continually, promptly identify areas for improvement, and ensure that the control environment remains dynamic and aligned with best practices.

	ORGANIZATIONAL DEVELOPMENT UNIT	CODE: PO-14-ODU
		VERSION: 03
	RISK MANAGEMENT AND INTERNAL CONTROLS POLICY	Page 15 of 19

11. REVIEW AND APPROVAL

The AFRC on behalf of the Board of Trustees will review the Risk Management and Internal Control Policy as needed. The effective date of this revised Policy is 18 September 2020. This Policy supersedes previous policies regarding this subject matter, and previous policies are considered rescinded.


The effectiveness of this policy will be reviewed regularly to ensure it remains relevant and responsive to changing risks. Feedback from risk management and internal controls activities and the outcomes of periodic risk and internal controls assessments will inform us of continuous improvements to the policy and its implementation.

12. RELATED POLICIES/REFERENCES FOR MORE INFORMATION

- Fraud Policy
- Whistleblower Policy
- Code of Ethics/Conduct
- Risk Management Guide
- CGIAR Integrated Partnership: Risk Management and Internal Controls Policy
- CGIAR Integrated Partnership: Risk Management and Internal Controls Framework

13. VERSION CONTROL

VERSION	DATE OF APPROVAL OF THE NEWEST VERSION	DESCRIPTION OF CHANGE	PREPARED BY
00	09-18-2020	First Alliance Enterprise Risk Management Policy	Carlos Paredes Vanessa Riveros
01	06-24-2021	Changed “Organizational Management Unit” references to “Organizational Development Unit” and “Organizational Management Manager” to “Organizational Development Manager”.	Nicole Demers
02	11-22-2023	Section No. 5.2: Adjusted Wording in to clarify that the risk assessment should be conducted in the pre-award stage and that this will influence the decision of accepting or not the grant. Section No. 7: Roles and Responsibilities of the RMC, ADG and Principal Researcher/ Project Leader were added. Wording on R&R of the AFRC was amended for greater clarity.	Carlos Paredes Nicole Demers Vanessa Riveros


	ORGANIZATIONAL DEVELOPMENT UNIT	CODE: PO-14-ODU
		VERSION: 03
	RISK MANAGEMENT AND INTERNAL CONTROLS POLICY	Page 16 of 19

VERSION	DATE OF APPROVAL OF THE NEWEST VERSION	DESCRIPTION OF CHANGE	PREPARED BY
		Section No. 10 Review and Approval: Modifications to the Risk Management Policy were reviewed by the Governance Committee (30.10.2023) and presented to the Executive Committee for approval and subsequent presentation to the whole Board.	
03	06-12-2025	General modifications to the document to adapt CGIAR Integrated Partnership: Risk Management and Internal Controls Policy	Carlos Paredes Daniel Bastidas Reviewed by the AFRC and approved by the Board of Trustees on 12 June 2025

Reviewed by:

Approved by:

Audit, Finance, and Risk Committee (AFRC)	Whole Board on 18 September 2020
Nancy Andrews Chair AFR Committee	

	ORGANIZATIONAL DEVELOPMENT UNIT	CODE: PO-14-ODU
		VERSION: 03
	RISK MANAGEMENT AND INTERNAL CONTROLS POLICY	Page 17 of 19

Annex 1. Risk appetite statement relevant to the Alliance's objectives


The Alliance as part of the Integrated Partnership categorizes its risk appetite into three levels based on its willingness to pursue opportunities and manage threats to achieve its objectives.

Appetite Level	Definition	Implications on actions to manage risk	Implications on decision taking	Implications on risk communication/escalation
Low	The Alliance seeks to minimize or eliminate risk.	Strong and reasonable preventive controls are prioritized within the operating environment, even if the cost of mitigation actions may exceed potential event materiality.	Risk is minimized due to potential downside impacts.	Increased visibility and communication to appropriate governing bodies.
Medium	The Alliance seeks a balanced approach between opportunities and threats	Actions and controls are proportional value driven, ensuring efficiency without unnecessary rigidity.	Decisions consider both potential upside and downside risks, and benefits versus costs	Risk visibility is provided as needed to the appropriate governing bodies.
High	The Alliance encourages evidence-based and disciplined risk taking	Risk-return tradeoffs are actively managed, and flexibility is maintained for innovation.	Risk taking is strategic and intentional to maximize opportunities and tolerate failure to be innovative.	Visibility and communication to the governing bodies on a case-by-case basis


This approach ensures that risk management and internal controls in the Alliance are aligned with the CGIAR IP's strategic risk appetite, guiding decision-making and prioritization of controls.

Risk Appetite Across Key Risk Categories

- The Alliance's Risk Appetite is structured across 14 key risk categories, ensuring alignment with its mission, operations, and financial sustainability:

	ORGANIZATIONAL DEVELOPMENT UNIT	CODE: PO-14-ODU
		VERSION: 03
	RISK MANAGEMENT AND INTERNAL CONTROLS POLICY	Page 18 of 19

Common Risk Areas	Risk Category	Risk Appetite Level	Rationale
Strategic	Change Management	Medium	The Alliance acknowledges that organizational transformation is essential. It accepts moderate risks to balance innovation with structured implementation.
	Research Innovation	High	As a research-driven organization, the Alliance embraces high-risk, high reward innovation while maintaining ethical and responsible research practices.
	Partners & Partnerships	Medium	Collaboration is central to the Alliance's mission. While partnerships carry risks, due diligence safeguards its reputation and strategic objectives.
	Scaling Impacts	Medium	The Alliance aims to maximize the reach of its innovations while ensuring program viability, sustainability, and alignment with long-term goals.
Operational	Business Continuity	Medium	Operational resilience is a priority. The Alliance accepts moderate risks to enhance flexibility while mitigating disruptions.
	Talent Management	Medium	Attracting and retaining talent is critical. The Alliance takes calculated risks in HR matters to foster an inclusive and dynamic workforce.
	Data Management	Low	Security, integrity, and compliance are prioritized. Risks such as data breaches and misuse are minimized through strict controls.
	Health, Safety & Well-being*	Low	The safety and well-being of the Alliance's workforce and stakeholders are non-negotiable, with strict adherence to regulations.
	Ethics & Integrity*	Low	The Alliance maintains zero tolerance for unethical behavior and strong governance mechanisms to ensure transparency and accountability.
	Legal & Regulatory Compliance	Low	Strict adherence to global and local regulations is a priority, minimizing risks related to non-compliance.

	ORGANIZATIONAL DEVELOPMENT UNIT	CODE: PO-14-ODU
		VERSION: 03
	RISK MANAGEMENT AND INTERNAL CONTROLS POLICY	Page 19 of 19

	Intellectual Property	Low	The Alliance aims to maximize global access to innovations while also protecting the integrity, attribution, and misuse of IP.
	Infrastructure	Medium	The Alliance takes measured risks in infrastructure investment, balancing efficiency, sustainability, and innovation.
Financial	Funding	Medium	The Alliance actively explores diversified funding opportunities, accepting moderate risks while ensuring financial stability.
	Financial Risk	Medium	A prudent but flexible approach allows the Alliance to seek financial growth while maintaining strong financial oversight.

Note: Risk categories marked with an asterisk (e.g., Ethics, Health & Safety) have an aspirational risk.

Risk appetite statement

- The Alliance's risk appetite statement is summarized below:

Low	Medium	High
*Health, safety and well-being Legal and regulatory compliance *Ethics Data Intellectual Property <i>*Categories for which the aspirational risk appetite is zero</i>	Change management Partners and partnerships Scaling impact Funding Talent Business continuity Financial Infrastructure	Research innovation

Low

We aim to minimize or eliminate risks within our areas of operations to effectively maintain a robust control environment. It is essential to exercise caution when exploring opportunities in these areas.

Medium

We are willing to accept some risk in certain areas in which we seek a balanced approach to risk-return trade off.

High

To achieve success and effectively deliver on our strategy, we actively promote and encourage evidence-based and disciplined risk taking.