
	ORGANIZATIONAL DEVELOPMENT UNIT	CODE: PO-14-ODU
		VERSION: 02
	ENTERPRISE RISK MANAGEMENT POLICY	Page 1 of 22

Contents

1.	INTRODUCTION.....	2
2.	PURPOSE & OVERARCHING PRINCIPLES	2
3.	SCOPE	4
4.	DEFINITIONS AND ACRONYMS.....	4
5.	RISK MANAGEMENT STRATEGY	5
5.1	Alliance-wide risk assessments	5
5.2	Risk assessment for projects, programs, and new initiatives.....	5
5.3	Regional and country risk assessment	6
5.4	Unit and functional risk assessment	6
5.5	Risk appetite	6
6.	RISK ANALYSIS AND ASSESSMENT.....	7
6.1	Risk categories/factors.....	7
6.2	Risk analysis	7
6.3	Risk response	8
6.4	Risk communication and escalation.....	9
7.	ROLES AND RESPONSIBILITIES	10
8.	REVIEW AND APPROVAL	13
9.	RELATED POLICIES/REFERENCES FOR MORE INFORMATION.....	13
10.	VERSION CONTROL	13
	Annex 1. Reference framework ISO 31000:2018 Standards & COSO ERM	15
	Annex 2. Risk appetite statement relevant to the Alliance's objectives	17
	Annex 3. Risk categories/factors for impact and likelihood	19
	Annex 4. Acceptability Matrix and risk profile	22

	ORGANIZATIONAL DEVELOPMENT UNIT	CODE: PO-14-ODU
		VERSION: 02
	ENTERPRISE RISK MANAGEMENT POLICY	Page 2 of 22

1. INTRODUCTION

The Board of Trustees (BoT) and the Senior Management Team (SMT) acknowledge that effective risk management (RM) practices are essential to good governance and to develop the Alliance's overall strategic direction, set priorities, and enhance decision-making processes. The Alliance has a challenging mission that makes its operational environment and its work become more diverse, complex, and uncertain. The risks faced by the Alliance are intrinsic to the nature, modus operandi, and location of its activities, and are as dynamic as the environment in which it operates. The sources of risks faced by the organization include operational, financial, legal, human, and reputational factors. Effective risk management helps the Alliance deal with uncertainty and respond proactively to risks and opportunities.

This Policy is a mechanism to foster the adoption of risk management practices as part of routine management for all units and programs aimed at minimizing risks while taking advantage of opportunities to align with the Strategic Plan and the Business Plan, giving confidence to funders, partners, and general stakeholders.


The Alliance's 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 ONE CGIAR Risk Management Framework.¹

2. PURPOSE & OVERARCHING PRINCIPLES

This Policy establishes a pragmatic, systematic, and disciplined approach to identify and manage risks throughout the Alliance and is linked to the achievement of the strategic objectives. It promotes a strong risk management system that supports decision making, in particular when setting objectives, prioritizing strategic alternatives, selecting and managing a course of action, and evaluating results. A robust risk management system helps diminish the uncertainty of events and their related costs or losses while pursuing potential opportunities. The positive connotation identified in the content of the risk contributes to the generation of opportunities for the Alliance. Thus, risk management becomes an essential practice of the Alliance, contributing to the objectives of the enterprise to increase competitive advantage and generate opportunities.

This Policy also provides guidance to all staff on implementing the risk management process, including principles, strategy, and the Alliance risk appetite. It maintains a consistent risk management framework through which risks are identified, analyzed, addressed, and escalated, and for which accountability is assigned. This Policy serves to improve the quality of management and internal controls, operational processes, instructions, guidance, tools, and management information systems. The goal is to achieve a common understanding of the Alliance's risk exposure with its risk appetite, to be able to articulate its risk profile

¹ The 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.

	ORGANIZATIONAL DEVELOPMENT UNIT	CODE: PO-14-ODU
	ENTERPRISE RISK MANAGEMENT POLICY	VERSION: 02
		Page 3 of 22

coherently internally and externally to funders and external stakeholders. Furthermore, the idea is to establish a culture that links risk management to implementing the Alliance’s Strategic Plan and be considered proactively in decision making.

These principles provide guidance to the Alliance on the characteristics of effective and efficient risk management, communicating its value, and explaining its intention and purpose. The principles of the Alliance take ISO 31000:2018 principles as a benchmark and are the backbone of risk management that should be considered when establishing the Alliance's risk management framework and processes. These principles should enable an organization to manage the effects of uncertainty on its objectives.

The core principles of risk management are the following:

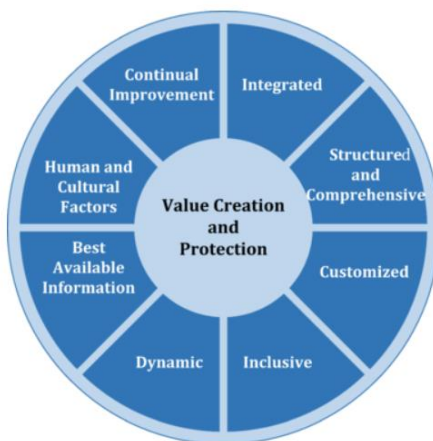



Image No. 1. Principles

- a) **Integrated:** Risk management is an integral part of all the activities in the Alliance.
- b) **Structured and comprehensive:** A structured and comprehensive approach to risk management contributes to consistent and comparable results.
- c) **Customized:** The risk management framework and processes are customized and proportionate to the Alliance’s external and internal context related to its objectives.
- d) **Inclusive:** The adequate and timely involvement of stakeholders allows for their knowledge, views, and perceptions to be considered. This results in better awareness and informed risk management.

	ORGANIZATIONAL DEVELOPMENT UNIT	CODE: PO-14-ODU
		VERSION: 02
	ENTERPRISE RISK MANAGEMENT POLICY	Page 4 of 22

- e) **Dynamic:** Risks may arise, change, or disappear with changes in the Alliance's external and internal context. Risk management anticipates, detects, recognizes, and responds to those changes and events in an adequate and timely manner.
- f) **Best information available:** Risk management inflows are based on historical and updated information, and on future expectations. Risk management explicitly takes into account any limitation and uncertainty associated with such information and expectations. The information should be timely, transparent, and available for the relevant stakeholders.
- g) **Human and cultural factors:** Human behavior and culture have a considerable influence on all risk management aspects, at all levels and in all stages.
- h) **Continual improvement:** Risk management is continuously improving through learning and experience.

3. SCOPE

This is a broad Policy of the Alliance, and it encompasses all operations in all countries where the Alliance operates. The Policy will operate with other business and operating/administrative policies.

4. 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. A risk has a cause and effect.


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.

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 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: financial, legal, image, operational, and people (as the main categories).

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

Likelihood: The probability that a risk will occur.

	ORGANIZATIONAL DEVELOPMENT UNIT	CODE: PO-14-ODU
		VERSION: 02
	ENTERPRISE RISK MANAGEMENT POLICY	Page 5 of 22

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 matrix: A graphical representation of key risks or risk categories with each other, reflecting their particular significance with regard to objectives and defined risk tolerance levels.

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.

Value of risk/level of risk: The magnitude of a risk or combination of risks, expressed in terms of the combination of impact and likelihood (probability).

5. RISK MANAGEMENT STRATEGY


Annex 1. Reference Framework

5.1 Alliance-wide risk assessments

The Alliance will conduct on a biannual basis "top-down" and "bottom-up" assessments with the input of directors, managers, and key staff, at headquarters, hubs, and locations of activities. These types of assessments aim to identify or update the approach that the Alliance is using to manage opportunities and risks affecting its objectives. As part of this work, these assessments will consider trends/tendencies identified in risks previously identified and significant trends of the context to identify risks not previously considered. These assessments will follow a formal methodology of risk management and will be consolidated and reported.

5.2 Risk assessment for projects, programs, and new 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, to be implemented during the pre-award stage. This assessment should consider our different categories of risks (financial, reputational, legal/compliance and regulatory, operational, and human factors – see Section 6.1) 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 grant or not.

	ORGANIZATIONAL DEVELOPMENT UNIT	CODE: PO-14-ODU
		VERSION: 02
	ENTERPRISE RISK MANAGEMENT POLICY	Page 6 of 22

5.3 Regional and country risk assessment

A country/regional risk assessment can help an organization identify and evaluate country-/region-specific risks. In doing so, organizations can determine how much those risks might affect their business and what steps they can take to manage or mitigate those risks. The review should be conducted at least once a year.

5.4 Unit and functional risk assessment

Functional areas of an organization have specific policies, procedures, processes, key performance indicators (KPIs), and key risk indicators (KRIs) as enablers to achieve near-term performance objectives and longer-term organizational resilience. Through an effective risk review, continuous improvement can be achieved and improved internal controls applied.


5.5 Risk appetite

Risk appetite is the amount of risk, on a broad level, that the Alliance will accept in pursuit of value. Each organization pursues various objectives to add value and should broadly understand the risk it is ready to undertake in doing so. The Alliance seeks to take advantage of opportunities that will contribute to achieving its mission in an effective and efficient manner. The Alliance recognizes that all risks cannot be eliminated, but must be managed, maximized, or minimized depending on the circumstances.

The Alliance uses four categories to describe its willingness to take opportunities and manage risks (based on the CGIAR Risk Management Framework and adapted to the Alliance):

No.	Categories	Opportunity	Tolerance for uncertainty
3	Open	The Alliance accepts and encourages opportunities presenting a risk of failure if the likelihood of inherent risks materializing combined with their potential impact results in the potential benefits outweighing the combined risk level.	Fully anticipate uncertain outcomes or period-to-period variations.
2	Flexible	The Alliance accepts opportunities presenting a risk of limited underachievement if the likelihood of risks materializing combined with their potential impact means benefits more than offset losses.	Expect some level of uncertainty, but will proactively manage potential impact.
1	Cautious	The Alliance is willing to accept risks only if they are essential in delivery, and there is a limited possibility of failure in achieving its objectives.	Limited tolerance for uncertainty, with a preference for safe delivery.
0	Averse	The Alliance is not willing to accept any level of risk; avoidance of risk is a core objective in decision making.	Extremely low tolerance or none for uncertainty.

Annex 2. Risk Appetite Statement relevant to the Alliance's objectives

	ORGANIZATIONAL DEVELOPMENT UNIT	CODE: PO-14-ODU
	ENTERPRISE RISK MANAGEMENT POLICY	VERSION: 02
		Page 7 of 22

6. RISK ANALYSIS AND ASSESSMENT

6.1 Risk categories/factors

Risks and opportunities should be considered with the institutional objectives. For implementing this Policy, the Alliance established the following factors to use during the risk assessment process:

- Financial factor
- Reputational/image factor
- Legal/compliance/regulatory factor
- Operational factor
- Human factor

6.2 Risk analysis

The purpose of risk analysis is to understand the risk and its characteristics, including, when appropriate, its level. An event may have multiple causes and consequences, and it may affect various objectives. The risk is analyzed through a combination of likelihood estimates and the impact of the occurrence of such an event, in the context of the control measures in place for that event. The assessment or measurement of the risk with control will follow a semi-quantitative method, in which the value of the risk will result from multiplying Likelihood by Impact, according to the following formula:

$$\text{Value of Risk} = \text{Likelihood} \times \text{Impact}$$


Annex 2. Risk categories/factors for impact & likelihood

A risk level will be assigned to each risk based on the combination of assessment of the likelihood and impact provided by risk owners according to a five-level risk matrix.

Annex 3. Acceptability Matrix of the Alliance and risk profile

Each risk will be assessed and classified in terms of the dimensions as mentioned earlier. A Risk Management Catalogue will record inherent risks for the Alliance, including risk analysis, and will include the following items:

- Clear and concrete definitions (cause and consequence(s) should be properly captured).
- The risk owner is responsible for ensuring the effectiveness of the procedures and systems.
- Controls (procedures and systems employed to manage risks, including internal policies, directives, and most recent risk mitigation achievements or plans), and the control owners.
- Actions (areas flagged as requiring further focused attention to risk mitigation) and action owners with clear implementation timelines.
- Adequacy of existing controls and mitigation activities.
- Risk impact assessment.
- Risk likelihood assessment.

	ORGANIZATIONAL DEVELOPMENT UNIT	CODE: PO-14-ODU
		VERSION: 02
	ENTERPRISE RISK MANAGEMENT POLICY	Page 8 of 22


- Risk level rating.
- Target risk rating.

6.3 Risk response

Risk response will identify a range of options to treat the risk, the evaluation of options, preparing plans for risk treatment, and their implementation. The selection of the most appropriate options for risk treatment means balancing potential benefits resulting from the accomplishment of objectives against the cost, effort, or disadvantages of implementation.

Risk response can take different forms that are not necessarily mutually exclusive (except for eliminate-avoid and accept-retain). The different treatments or responses that can be applied to the risk fall into the following categories:

Type of response	Opportunity
Avoid or eliminate the source of risk	<p>Entails deciding whether to conduct the activity that will probably generate the risk. Avoiding means quitting activities that create risks. Examples of elimination measures follow:</p> <ul style="list-style-type: none"> • Remove the source of risk. • Dispose of a unit, line of product, or geographic segment. • Decide whether to pursue new initiatives/activities that could lead to risks.
Prevention	<p>This involves a modification or change (reduction) in the risk's likelihood of occurrence. This includes actions on the "causes of risk." Examples of prevention measures follow:</p> <ul style="list-style-type: none"> • Formal reviews of requirements, specifications, engineering, and operational design. • Inspection and process control. • Verifications and tests. • Preventive maintenance. • Quality assurance, administration, and standards. • Establishment of operational limits. • Structured training.
Protection	<p>Entails modifying (reducing) the consequences. Examples of protection measures follow:</p> <ul style="list-style-type: none"> • Design features. • Engineering and structural barriers. • Fraud control approach. • Minimizing exposure to sources of risk.

	ORGANIZATIONAL DEVELOPMENT UNIT	CODE: PO-14-ODU
		VERSION: 02
	ENTERPRISE RISK MANAGEMENT POLICY	Page 9 of 22

Sharing	<p>Risk likelihood or impact is diminished by transferring or otherwise sharing the risk with one or several parties (stakeholders). Examples of sharing measures follow:</p> <ul style="list-style-type: none"> • Acquiring insurance against unexpected and significant losses. • Entering into a joint venture. • Entering into agreements with other organizations. • Entering into service, production, or tolling agreements with third parties. • Being protected against risks using capital market instruments. • Outsourcing business processes.
Accept or retain	<p>This consists of accepting the risk within the organization to pursue an opportunity and establishing an appropriate risk financing plan or retaining the risk based on an informed decision. Examples of retention measures follow:</p> <ul style="list-style-type: none"> • Allocating for possible losses. • Trusting in the natural compensations existing within a portfolio. • Accepting risk if it adapts to the existing risk tolerance.

6.4 Risk communication and escalation


The purpose of communication and consultation is to aid relevant stakeholders in understanding the risk, the basis upon which decisions are made, and the reasons specific actions are needed.

Communication seeks to raise the level of awareness and risk-understanding, while consultation involves obtaining feedback and information to support the decision-making process. Close coordination between both should facilitate information exchange based on timely, relevant, accurate, and understandable facts, with due regard to the confidentiality and integrity of the information and an individual's right to privacy. Communication and consultation with appropriate external and internal stakeholders will be applied in every stage of the risk management process.

The Alliance will provide specific communications that clearly explain its philosophy, its risk management approach, and its delegation and authority. Communications about processes and procedures will be aligned with the desired culture, which will be reinforced at all times. The Alliance will provide a top-bottom flow of information. The communication channels will also allow staff to communicate information about risks encountered in their areas.

To accomplish this, the Alliance will introduce overtime communications about risk administration at all levels, employing an adequate training strategy.

The training strategy is based on the communication and consultation plan for each step of the risk management process. It comprises both external and internal stakeholders. The plan is based on bilateral communication and consultation between these stakeholders.

	ORGANIZATIONAL DEVELOPMENT UNIT	CODE: PO-14-ODU
		VERSION: 02
	ENTERPRISE RISK MANAGEMENT POLICY	Page 10 of 22

Information obtained about incidents in the monitoring process will be combined to produce information from claims by type of risk (year after year, at the operational level, or by unit).

Similarly, since Management cannot fulfill its responsibilities of "good governance" if it is not informed about the critical risks faced by the organization, this will include the information on critical risks in biannual reports, in reports concerning important projects, or in other vital decisions. This information would contain controls undertaken to mitigate such risks.

7. ROLES AND RESPONSIBILITIES

The three Lines model provides a simple and effective way to enhance communications on risk management and control by clarifying essential roles and duties. It provides a fresh look at operations, helping to assure the ongoing success of risk management initiatives, and it is appropriate for any organization — regardless of size or complexity. It clarifies the separation of roles as between relevant bodies to provide a clear structure that best assists in the achievement of objectives and facilitates strong governance and risk management.

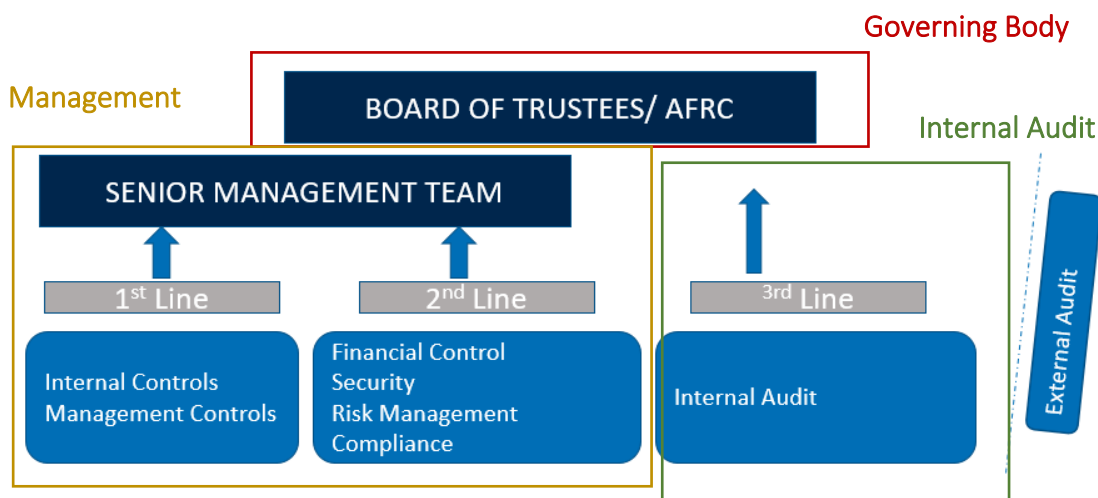



Image No. 2. The Three Lines Model

- The first line consists of functions that own and manage risk: the Alliance’s Senior Management Team (SMT): to ensure security through a sound control and risk framework. Directly aligned with the delivery of products and/or services, it includes the roles of support functions and has responsibility for managing risk remaining.
- The second line aids with managing risk by ensuring a focus on specific objectives of risk management, such as compliance with laws, regulations, and acceptable ethical behavior; internal control; information and technology security; sustainability; and quality assurance.
- The third line represents functions that provide independent assurance such as those provided by the internal audit. This line involves objective assurance and advice on the adequacy and

	ORGANIZATIONAL DEVELOPMENT UNIT	CODE: PO-14-ODU
		VERSION: 02
	ENTERPRISE RISK MANAGEMENT POLICY	Page 11 of 22

effectiveness of governance and risk management. It achieves this through the competent application of systematic and disciplined processes, expertise, and insight. It reports its findings to Management and the governing body to promote and facilitate continuous improvement.

- External assurance: independent external assurance comes through external audits.

Governing body

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 Policy. 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 Audit, Finance, and Risk Committee (AFRC) is responsible for overseeing the effectiveness of Management's responsibility to manage risk and maintain a proper system of internal control for financial and operational purposes and monitoring adherence to the Alliance's approved management policies, directives, systems, and procedures.

The AFRC assures the Board of Trustees that the Alliance manages risk effectively, has efficient and effective systems of internal control, and has independent audit arrangements (Trans-Regional Audit and external auditors) as well as other mechanisms to guarantee sound practices across operations. Those mechanisms include (i) a review of the Alliance's policies and control framework to ensure that roles and responsibilities for proper risk and control are defined, current, and operating effectively within agreed risk tolerance limits and in compliance with the Alliance's policies and directives; (ii) a review of the effectiveness of Management's efforts to identify, assess, and control risk, and how it monitors exposures and reports risk issues, events, and changes to the risk profile to the Director General, the AFRC and the Board of Trustees; and (iii) receiving Management's assurances on the status and effectiveness of risk management and from the external auditor and the Trans-Regional Audit (TRA) Group on the results of their risk-based audit work.

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 TRA, 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:

	ORGANIZATIONAL DEVELOPMENT UNIT	CODE: PO-14-ODU
		VERSION: 02
	ENTERPRISE RISK MANAGEMENT POLICY	Page 12 of 22

- Developing, implementing, and monitoring overall compliance with the Policy.
- Identifying risks and developing and implementing risk management 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 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 Director/Project Manager of activities, including projects, processes, systems, and research activities undertaken by or on behalf of the Alliance.


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 implemented at the pre-award stage to ensure that all risks are taken into account before a decision is made to sign an agreement.

The Head of the Organizational Development Unit supports the DG and Senior Management Team in developing an RM framework and overseeing its implementation, promoting a risk management culture, ensuring maintenance of the compliance monitoring system to verify that risk mitigation measures are being implemented as intended, reviewing annually the risk management approach and Policy and proposing changes as needed, and preparing reports and statements for the DG, SMT, and AFRC.

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 researcher 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, during the pre-award stage. This assessment should consider our different categories of risks (financial, reputational, legal, compliance and regulatory, operational, and human factors – see Section 6.1) 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 grant or not.

	ORGANIZATIONAL DEVELOPMENT UNIT	CODE: PO-14-ODU
		VERSION: 02
	ENTERPRISE RISK MANAGEMENT POLICY	Page 13 of 22

Internal Audit - Trans-Regional Audit (TRA) Group: The TRA reports administratively to the Director General and functionally to the AFRC. It conducts risk-based reviews on the effectiveness of the Alliance's Risk Management Practices and internal controls in line with the AFRC-approved risk-based medium-term Audit Plan. An Annual Report that includes an assurance opinion based on work done throughout the year will be shared with the Director General and presented to the AFRC, which will report the results to the full Board of Trustees.

External Audit: These reports operationally to the Director General and functionally to the AFRC on the operation of those aspects of the Alliance's risk and quality management system that are reviewed as part of the annual financial statement audit. The External Audit's approach focuses not just on accounting risks but also on other business risks that affect the Alliance's financial position and ongoing financial viability. It assesses the measures taken by Management to address those risks.

8. REVIEW AND APPROVAL


The AFRC on behalf of the Board of Trustees will review the Enterprise Risk Management Policy as needed. The effective date of this updated Policy is **January 1ST, 2024**. This Policy supersedes previous policies regarding this subject matter, and previous policies are considered rescinded.

9. RELATED POLICIES/REFERENCES FOR MORE INFORMATION

- Fraud Policy
- Whistleblower Policy
- Code of Ethics/Conduct
- Risk Management Guide
- CGIAR Risk Management Guidelines

10. 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


	ORGANIZATIONAL DEVELOPMENT UNIT	CODE: PO-14-ODU
		VERSION: 02
	ENTERPRISE RISK MANAGEMENT POLICY	Page 14 of 22

VERSION	DATE OF APPROVAL OF THE NEWEST VERSION	DESCRIPTION OF CHANGE	PREPARED BY
02	11-28-2023	<p>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.</p> <p>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.</p> <p>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.</p>	<p>Carlos Paredes Nicole Demers Vanessa Riveros Approved by the whole Board of Trustees</p>

Reviewed by:

Approved by:

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

	ORGANIZATIONAL DEVELOPMENT UNIT	CODE: PO-14-ODU
		VERSION: 02
	ENTERPRISE RISK MANAGEMENT POLICY	Page 15 of 22

Annex 1. Reference framework ISO 31000:2018 Standards & COSO ERM

The purpose of the risk management reference framework is to help the Alliance to mainstream risk management in all its significant activities and operations. Its effectiveness depends on its integration into the Alliance's governance, including decision making. This requires support from stakeholders, particularly the Alliance's Senior Management. The development of a reference framework entails the integration, implementation, assessment, and improvement of risk management across the Alliance. Below are the components of the reference framework.

- a) Leadership and commitment
- b) Integration
- c) Design
- d) Articulation of the commitment to risk management
- e) Assignment of roles, authorities, responsibilities, and accountability in the Alliance
- f) Allocation of resources
- g) Establishing communication and consultation
- h) Implementation
- i) Assessment

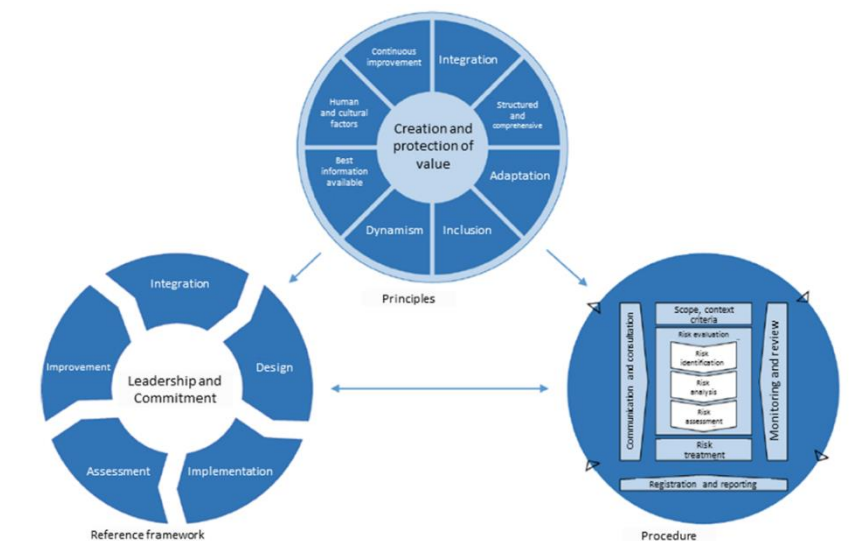



Image No. 3. Principles, reference framework, and process. ISO 31000:2018 STANDARD

Controls are the existing practices or devices that may operate to minimize the risk under analysis. The description of existing controls should be entered in the field "Controls." All the controls existing on the date of the analysis should be detailed in this field (current controls).

The evaluation of the controls' strength will depend on the score of two variables:

1. The effectiveness of the controls' design.

	ORGANIZATIONAL DEVELOPMENT UNIT	CODE: PO-14-ODU
		VERSION: 02
	ENTERPRISE RISK MANAGEMENT POLICY	Page 16 of 22

2. The effectiveness in the implementation of the controls (operational effectiveness or implementation of a set of controls).

The effectiveness of the controls’ design is assessed through an objective analysis using the following criteria or characteristics to be met by a suitable design. The suggested attributes to be considered include the existence of

- o An individual responsible for the implementation of the controls.
- o An adequate frequency of implementation of the controls.
- o Controls (manual or automatic) suitable to the type of risk.
- o The existence of suitable types of controls (to prevent or to detect).
- o The existence of documentation about controls.
- o The existence of a detailed description of the component activities.

The effectiveness of the controls’ design is ranked at one of the following levels or categories:

1. Strong
2. Moderate
3. Weak


The implementation or application of the controls will also be ranked according to the following levels or categories:

1. Strong
2. Moderate
3. Weak

Ranking the controls’ strength is the result of multiplying the controls’ design by their implementation, according to the following matrix:

	Strong	Inadequate	Opportunities for improvement	Adequate
Control design	Moderate	Inadequate	Opportunities for improvement	Opportunities for improvement
	Weak	Inadequate	Inadequate	Inadequate
		Weak	Moderate	Strong

Image No. 4. Implementation of controls. COSO ERM.

	ORGANIZATIONAL DEVELOPMENT UNIT	CODE: PO-14-ODU
		VERSION: 02
	ENTERPRISE RISK MANAGEMENT POLICY	Page 17 of 22

The table below shows the controls' strength and the type of ranking with one of the following levels or categories:

- Adequate
- With opportunities for improvement
- Inadequate


DESCRIPTOR	CONTROL STATUS
ADEQUATE	The controls are adequate and operate correctly. Policies and procedures are properly established and documented. The controls are constantly reviewed. No further action is required, except for reviewing and monitoring existing controls.
OPPORTUNITIES FOR IMPROVEMENT	There are still some weaknesses. The controls implemented are insufficient to fully prevent or mitigate risk.
INADEQUATE	The controls do not show an acceptable level. There are some informal actions with limited procedures, or they are not systematic.

Note: Current controls existing are separated from future action plans designed by risk owners intended to decrease risk exposure and to maintain an appropriate risk appetite. (This differentiation is clearly defined in the RM processes.)

Annex 2. Risk appetite statement relevant to the Alliance's objectives


Risk appetite is the amount of risk, on a broad level, an organization will accept in pursuit of value. Each organization pursues various objectives to add value and should broadly understand the risk it will undertake in doing so.

Risk appetite statements serve as guiding principles for managers and (a) allow analysis of, response to, and monitoring of their risks; (b) inform their day-to-day decisions and prioritization of resources; (c) support the establishment of performance targets for their areas of responsibility; and (d) enable them to carry out the Alliance's mission within the boundaries for risk management and regarding its core values.

	ORGANIZATIONAL DEVELOPMENT UNIT	CODE: PO-14-ODU
		VERSION: 02
	ENTERPRISE RISK MANAGEMENT POLICY	Page 18 of 22

RISK CATEGORY	TOP RISKS CGIAR	ALLIANCE–RISK APPETITE	JUSTIFICATION
Strategic	ONE CGIAR	Flexible	The strategy requires ongoing development and innovation in its operations through strategic initiatives that often carry significant risk. In order to achieve its objectives, the Alliance must be willing to take and accept risk.
	Impact Delivery		
Technology	Data Management	Flexible	Unscheduled system downtime affects our service delivery, causing reputational damage and financial loss.
			Financial loss and reputational damage due to a breach of data or technology disruption caused by internal/external attack.
Legal	Intellectual Assets	Cautious	Failure to adhere to legal, regulatory, and financial crime requirements leads to financial and reputational damage.
			Any issue with Host Country Agreements will affect the Alliance's operation.
Operational	Business Continuity	Flexible	No major effect on operations/ongoing activities (physical security, business continuity).
	Infrastructure		
People	Health & Safety	Cautious	Staff are one of the biggest assets of the Alliance; therefore, the risk appetite for this category is low.
			The Alliance takes any breaches of its Code of Conduct very seriously.
Financial	Liquidity	Cautious	The Alliance needs to remain financially sustainable to continue to serve its purpose and achieve its aspirations. The Alliance has a low-risk appetite for irresponsible use of resources and unnecessary liabilities. It operates in a world of grants with restricted funds. Any deviation from original budgets will affect reserves and the financial health of the Alliance.
	Funding		
Image	Reputation	Cautious	No major negative public/media attention (communications strategy, issue escalation).
Ethics	Fraud/Corruption Harassment/Bullying	Averse	The Alliance has no appetite for any dishonest or fraudulent behavior and is committed to deterring and preventing such behavior. It takes a very serious approach to cases, or suspected cases, of fraud or corruption perpetrated by its staff, and responds fully and fairly in accordance with provisions of the Code of Conduct.

Note: The One CGIAR is still in the process of developing an encompassing risk management framework. The Alliance will adjust this Annex 2 later to better align it with the One CGIAR risk framework and categories.

	ORGANIZATIONAL DEVELOPMENT UNIT	CODE: PO-14-ODU
	ENTERPRISE RISK MANAGEMENT POLICY	VERSION: 02
		Page 19 of 22

Annex 3. Risk categories/factors for impact and likelihood

The level of impact of risks will be evaluated according to the "vulnerability factor" that the analysis group deems more relevant or significant for the Alliance.

The impact tables to use according to the vulnerability factor are the following:


Level	Descriptor	Human factor
16	Critical	<ul style="list-style-type: none"> > One or more deaths of in-house and/or third-party staff (clients, contractors, and/or visitors). > Serious, progressive, and possibly fatal occupational disease. > Downtime of more than 40% of critical positions.
8	Higher	<ul style="list-style-type: none"> > Non-fatal occupational disease. > Injuries that result in disability for more than 3 days. Injuries with sequels but without disability. > Downtime from 20% to 40% of critical positions or more than 40% of non-critical staff.
4	Moderate	<ul style="list-style-type: none"> > Injuries that result in disability for 3 days or less, without sequels. > Downtime of less than 20% of critical positions or from 20% to 40% of non-critical staff.
2	Minor	<ul style="list-style-type: none"> > Wounded with superficial injuries, minor injuries, not disabling. > Downtime from 10% to 20% of non-critical staff.
1	Negligible	<ul style="list-style-type: none"> > First aid, no injuries. > Downtime of less than 10% of non-critical staff.

Level	Descriptor	Economic factor
16	Critical	Losses of more than US\$150,000
8	Higher	Losses equal to or more than US\$90,000 up to US\$150,000
4	Moderate	Losses equal to or more than US\$50,000 up to US\$90,000
2	Minor	Losses equal to or more than US\$25,000 up to US\$50,000
1	Negligible	Losses below US\$25,000



Level	Descriptor	Image factor – reputation
16	Critical	Negative effect on the reputation of the organization, its brand, its services, and/or processes, originated by any cause, made known by any means of communication, and with a global impact. > Effect repairable in the long term (more than 1 year). > Restriction or total loss (veto) of support from the interest group and/or strategic allies globally.
8	Higher	Negative effect on the reputation of the organization, its brand, its services, and/or processes, originated by any cause, made known by any means of communication, and with a regional impact (the Americas, Europe, Asia, and Africa are considered as regions). > Effect repairable in the long term (from 6 to 12 months). > Serious loss of support (condemnation) from the interest group and/or strategic allies regionally (the Americas, Europe, Asia, and Africa are considered as regions).
4	Moderate	Negative effect on the reputation of the organization, its brand, its services, and/or processes, originated by any cause, made known by any means of communication, and with a national impact (country where the Alliance operates). > Effect repairable in the short term (from 2 to 6 months). > Loss of support from one member of the interest group nationally.
2	Minor	Negative effect on the reputation of the organization, its brand, its services, and/or processes, originated by any cause, made known by any means of communication, and with a local impact (city where the Alliance is based). > Effect on the brand repairable in the short term (less than 2 months). > Partial veto by one member of the interest group locally.
1	Negligible	> Effect generated by a complaint or call/concern on the part of employees or members of the community (individually). > The situation is known only within the organization.

Level	Descriptor	Operational factor
16	Critical	> Total or partial interruption with limitations on support operations for more than 15 days. > Suspension of IT operations for more than 15 days. > Total or partial interruption with limitations on the project portfolio for more than 6 months.
8	Higher	> Total or partial interruption with limitations on support operations for more than 7 days and less than 15 days. > Suspension of IT operations for more than 8 days and less than 15 days. > Total or partial interruption with limitations on the project portfolio for more than 4 months and less than 6 months.
4	Moderate	> Total or partial interruption with limitations on support operations for more than 3 days and less than 7 days. > Suspension of IT operations for more than 72 hours and less than 8 days. > Total or partial interruption with limitations on the project portfolio for more than 2 months and less than 4 months.
2	Minor	> Total or partial interruption with limitations on support operations for more than 1 day and less than 3 days.

	ORGANIZATIONAL DEVELOPMENT UNIT	CODE: PO-14-ODU
		VERSION: 02
	ENTERPRISE RISK MANAGEMENT POLICY	Page 21 of 22

Level	Descriptor	Operational factor
		> Suspension of IT operations for more than 24 hours and less than 72 hours. > Total or partial interruption with limitations on the project portfolio for more than 1 month and less than 2 months.
1	Negligible	> Total or partial interruption with limitations on support operations (Finance, Legal, Partnerships & Communications, etc.) at the Alliance for less than 1 day. > Suspension of IT operations for less than 24 hours. > Total or partial interruption with limitations on the project portfolio for less than 1 month.

Level	Descriptor	Legal factor
16	Critical	Issuance of administrative and/or legal resolutions for failure to comply with the rules, regulations, or obligations, which result in the Alliance's > Definitive closure of processes or operations.
8	Higher	Issuance of administrative and/or legal resolutions for failure to comply with the rules, regulations, or obligations, which result in the Alliance's > Partial cancellation of permits and/or licenses of one part of its processes or operations. > (And/or) obligation to compensate for damages incurred.
4	Moderate	Issuance of administrative and/or legal resolutions for failure to comply with the rules, regulations, or obligations, which result in the Alliance's > Temporary suspension of permits and/or licenses of one part of its processes or operations. > Imposition of fines.
2	Minor	Issuance of administrative and/or legal resolutions for failure to comply with the rules, regulations, or obligations, which penalize the Alliance with > Imposition of fines.
1	Negligible	Issuance of administrative and/or legal resolutions for failure to comply with the rules, regulations, or obligations, which instruct the Alliance to > Adopt corrective measures in the organization's processes or operations.

The likelihood of occurrence refers to the possibility that potential sources of risk materialize. The likelihood of occurrence can be described as per the table below. Each scale level has been assigned an average number of events per year (frequency). Each likelihood descriptor is associated with a relative value from 1 to 5, which corresponds to its level. Ranking is done gradually on a decreasing basis, from the top score to the lowest, that is, the highest level (Almost Certain) will have a score of 5, while the lowest level (Rare) will have a score of 1.

Likelihood description			
Index	Likelihood	Description	Frequency
5	Almost Certain	The event is expected to occur in most circumstances	May occur frequently during the year
4	Likely	The event is expected to occur in some circumstances	May occur once a year
3	Possible	Might occur at some time	May occur once every 2 years
2	Unlikely	Could occur only at some future time	May occur once every 4 years
1	Rare	Only in exceptional circumstances	May occur once every 5 years or more

Annex 4. Acceptability Matrix and Risk Profile

The set of all scenarios contained in an Acceptability Matrix shapes the so-called Risk Profile of the Alliance. The Risk Profile is built locating in the matrix the reference code assigned to each risk scenario and entered into the Risk Catalogue.

LIKELIHOOD	Almost sure	5	MODERATE	MODERATE	HIGH	VERY HIGH	VERY HIGH
	Likely	4	LOW	MODERATE	HIGH	VERY HIGH	VERY HIGH
	Possible	3	LOW	MODERATE	HIGH	HIGH	VERY HIGH
	Unlikely	2	LOW	LOW	MODERATE	HIGH	VERY HIGH
	Rare	1	LOW	LOW	LOW	MODERATE	HIGH
				1	2	4	8
			Negligible	Minor	Moderate	Higher	Critical
IMPACT							

Image No. 4. Example of an Acceptability Matrix shaping the Risk Profile of the Alliance.