CGIAR
Science for a food-secure future

SMB-ARC-08
Risk Management
Good Practice Note

Version: July 2017

RISK MANAGEMENT
Good Practice Note

Prepared by: CGIAR Internal Audit Unit

Table of Contents

FOREWORD

What is a GPN

A Good Practice Note (GPN) is a document themed around a specific risk or control-related area. It is developed by the CGIAR IAU with contributions of subject-matter specialists, leveraging knowledge accumulated within the System and reflecting good practices suggested by professional bodies or standard setters, and implemented by Centers and/or other external organizations.

GPNs aim to summarize, circulate and promote existing knowledge around the CGIAR System Organization and can be used to benchmark existing arrangements against good practices and to improve knowledge, processes and operations at Center and System levels.

What it is not

GPNs are not and should not be interpreted as minimum standards, policies, guidelines or requirements, as practices mentioned in the GPN may not be relevant to or applicable in all Centers.

Ownership

GPNs are the ownership of the CGIAR System Organization.

1. INTRODUCTION

There are opportunities that Centers could take to generate breakthroughs in many of the scientific problems, or that could help Centers better manage their human, physical and financial resources in support of their research objectives. However, like two sides of a coin, the pursuit of opportunities is always accompanied by the possibility of failure.

In the recent past CGIAR has faced challenges which include, among others:

- Uncertainty in funding for the Consortium Research Projects (CRPs) in its first phase of CRPs.
- Exponential increase in administrative/transaction costs across the system following the roll out of the CRPs.
- Misappropriation of funding in one location which resulted in a temporary hold-back of funds by donors to the system as a whole.
- Loss of key staff in the advent of funding uncertainty.
- Geo-political implications such as the war in Syria, Brexit, US General elections.
- Increasing challenges from cyber-security risks.

Risk management is all about getting better at grasping the opportunities, understanding the possible causes of failure, and managing them to minimize or at least mitigate their impact on a Center when they occur.

CGIAR Centers already have risk management processes in place. The key difference is the current levels of maturity of these processes across the Centers. As per COSO (2011), '*Any entity that is currently operational has some form of risk management activities in place. However, these risk management activities are often ad hoc, informal and uncoordinated. And, they are often focused on operational or compliance-related risks and fail to focus systematically on strategic and emerging risks, which are most likely to affect an organization's success. As a result, they fall short of constituting a complete, robust risk management process*.'

It goes further to state that '*existing risk management activities often lack transparency. What's more, existing risk management processes often are not providing boards and senior management with an enterprise-wide view of risks, especially, emerging risks. Unfortunately, many organizational leaders are struggling with how to begin in their efforts to obtain strategic benefit from a more robust enterprise-wide approach to risk management.*' Moreover, as the Chartered Institute of Internal Auditors (2016) notes, '*there is no universally recognized definition or approach to risk management…*'

This GPN therefore does not prescribe a formula for risk management nor purport to provide a one size fit all solution. Its purpose is to explore the existing best practices in risk management to help the Centers implement their selected approach in an effective manner in order to, among others:

- Encourage proactive rather than reactive management
- Improve the identification of opportunities and threats
- Improve corporate governance
- Strengthen controls
- Assist in decision making.

2. FRAMEWORKS FOR MANAGING RISK

2.1 What is a risk?

ISO Guide 73 'Risk Management Vocabulary' defines a risk as '*an effect of an uncertainty on objectives*'. The effect, in this context is a deviation from the expected, either positive or negative. The uncertainty is a state of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood. The objectives in turn may include a wide range of aims and goals at strategic, operational or tactical levels, that an organization or units/functions within it are striving to achieve. For example, an objective might be a certain target of funding level which a Center wants to reach within a period. The achievement of this objective will be uncertain considering funding environment and Center's capabilities; therefore, potential underachievement or overachievement of the set target will represent a risk.

Per ISO 31000, '*All activities of an organization involve risks'* implying that risk is something that should be on top of mind for boards, management and all staff.

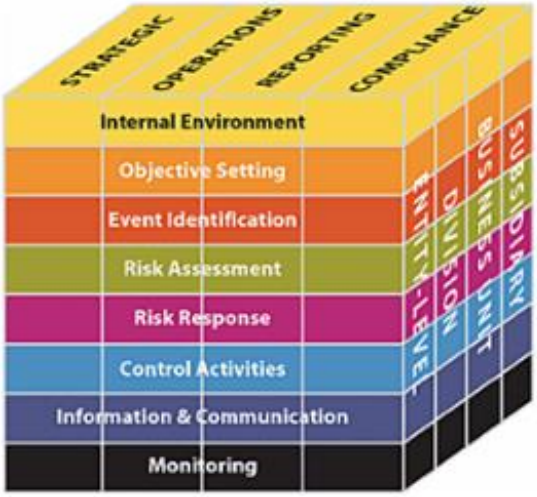
2.2 What is risk management?

The Enterprise Risk Management (ERM) Framework issued in 2004, by the Committee of Sponsoring Organizations of the Treadway Commission[1] (COSO) in the United States, defines enterprise risk management as: "*a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives*."

The COSO ERM framework is a widely used and referenced risk management framework. It identifies eight components of enterprise risk management.

A) Internal environment
B) Objective setting
C) Event identification
D) Risk Assessment
E) Risk response
F) Control activities
G) Information and Communication
H) Monitoring

COSO's guidance reflected the above eight components in a cube also illustrating the link between the components, and organizational objectives and organizational units.



COSO Cube

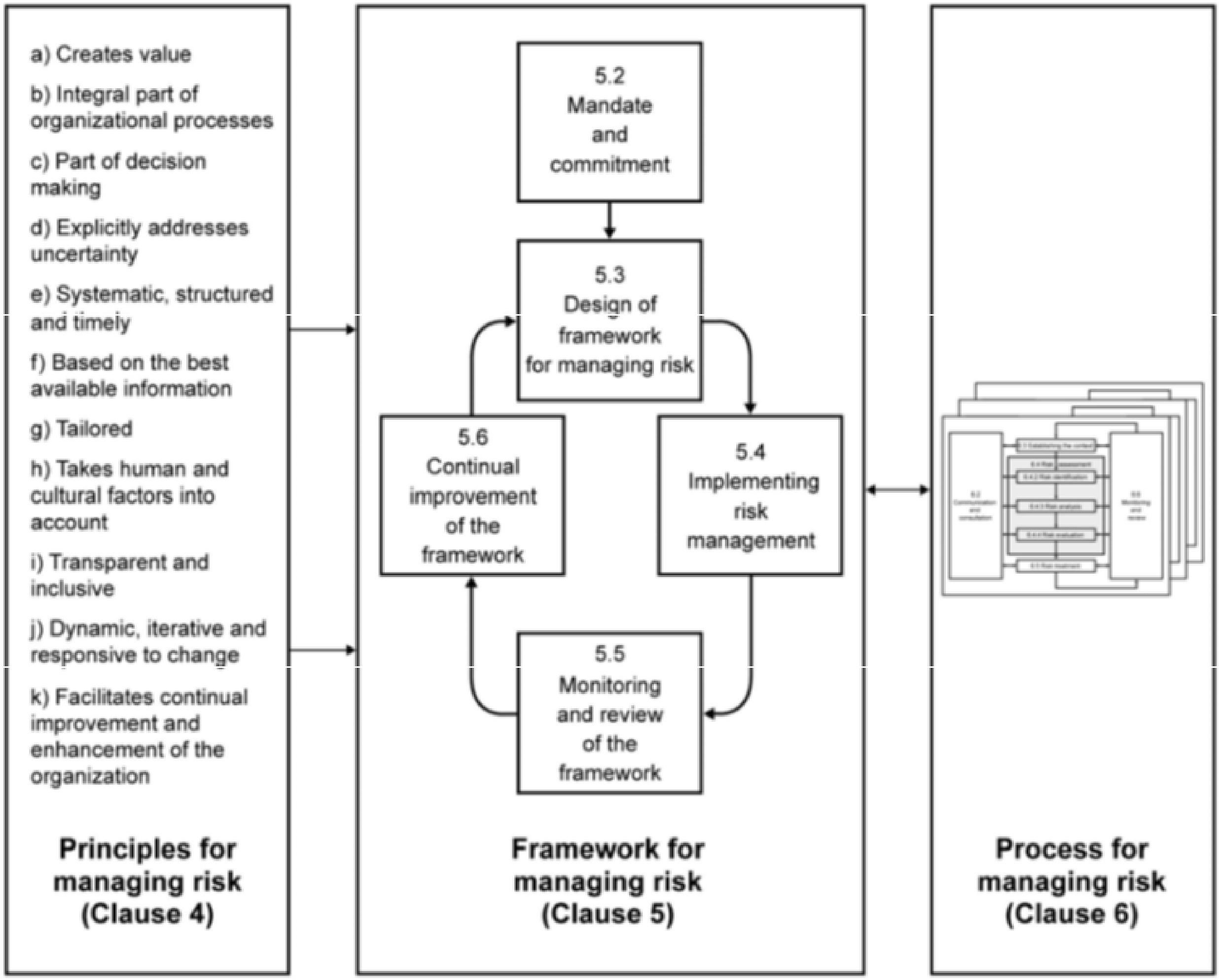
[1] This comprises representatives of the major US management, accounting, and auditing professional bodies.

At the time when the first CGIAR Enterprise-Wide Risk Management Good Practice Note (GPN 10) was developed in 2004, the International Standards Organization (ISO) had not yet developed a standard on risk management.

ISO31000 Risk Management standards published in 2010 include three major components of risk management:

- The Principles
- The Framework, and
- The Process.

Al three components (see in the chart below) are important and necessary for the effective risk management to operate in an organization.


a) Creates value
b) Integral part of organizational processes
c) Part of decision making
d) Explicitly addresses uncertainty
e) Systematic, structured and timely
f) Based on the best available information
g) Tailored
h) Takes human and cultural factors into account
i) Transparent and inclusive
j) Dynamic, iterative and responsive to change
k) Facilitates continual improvement and enhancement of the organization
Principles for managing risk (Clause 4)
5.2 Mandate and commitment
5.3 Design of framework for managing risk
5.4 Implementing risk management
5.5 Monitoring and review of the framework
5.6 Continual improvement of the framework
Framework for managing risk (Clause 5)
Process for managing risk (Clause 6)

Source: ISO31000 (2009)

The guiding principles constitute a set of expectations underpinning the design and implementation of the risk management framework and processes.

The framework refers to risk management as a control that needs to be designed, implemented, periodically reviewed and adjusted if needed according to the principles.

The process of risk management are the steps that are taken for:
A) Communication and Consultation
B) Establishing the context
C) Risk Assessment (which incorporates risk identification, risk analysis and risk evaluation)
D) Risk Treatment
E) Monitoring and review.

In the table below, the two standard frameworks have been mapped side by side with the key aspects and the related processes identified in the last column.

Table 1: COSO ERM and ISO31000 compared:

COSO Framework	**ISO31000 Framework**	**Related processes/aspects**
General overview		
Has been developed as a response to corporate governance failures and aims to mandate ERM in an organization. COSO includes more detailed discussion on risk appetite and more focussed on governance and control.	Is a more practical and user-friendly guide on how to design and implement an ERM. It is better structured separating risk management framework from risk management process.	Overall scope and structure.
Principles		
Not specifically defined	Eleven principles to provide foundation for design and implementation of the risk management framework and process.	Overall structure.
Framework		
• Internal environment • Objective setting	5.2 Mandate and Commitment 5.3 Design of framework 5.5 Monitoring and review 5.6 Continual improvement of the framework	• Getting board and management involvement and oversight • Policies and guidelines • Assigning risk management responsibilities and accountabilities

COSO Framework	ISO31000 Framework	Related processes/aspects
		• Performance measurement • Risk appetite
Process		
	6.3 Establishing the context	• Defining the scope and limitations of the risk assessment exercise
• Event identification • Risk Assessment	6.4 Risk Assessment (which incorporates risk identification, risk analysis and risk evaluation)	• Definition of risk identification process • Recording of risks • Scoring and assessment
• Risk response	6.5 Risk Treatment	• Action plan; implementation and follow up • Internal and external reporting
• Control activities		
• Information and Communication	6.2 Communication and Consultation	• Consultation and communication with internal and external stakeholders throughout the risk management process
• Monitoring	6.6 Monitoring and review	• Regular review of risks • Reporting to management and the board • Assurance over the effectiveness of risk management process

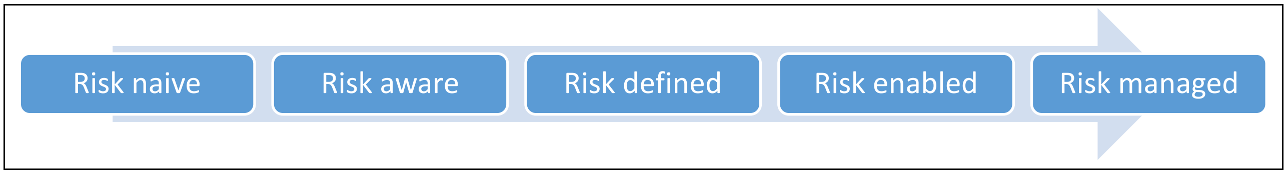
In the next section, the two key frameworks (COSO ERM and ISO31000) discussed above are referenced within the recommended practices.

3. RECOMMENDED PRACTICES

So, where do you start in finding a solution that will work best for your organization and make sure that the risk management process is effective? How do you know if your approach falls within the ‘good’ risk management practices?

A good place to start is to take stock of your current risk management approach and see how this compares to what is considered as best practice.

The Institute of Internal Auditors provides a guide for risk maturity assessment which has a 5-level rating, starting from ‘risk naïve’ to ‘risk managed’ as summarized below.



The design and implementation of a risk management process in an organization is a journey. While the principles of continuous improvements call for aiming for the best, each organization’s governing body should decide which level of maturity of risk management processes they expect the organization to be at in any moment of time.

Once implemented appropriately, risk management will, among others:

- Encourage proactive rather than reactive management. This will reduce time and effort spent on addressing crisis and help to achieve research results in a more efficient way.
- Strengthen corporate governance. Risk management creates framework for consistent decision-making supported by agreed definitions of risk appetite.
- Enhance controls. Design and implementation of controls will be directly linked to risks to be managed helping to eliminate inefficiencies and redundant processes.

Provided in Annex 1 is a comprehensive self-assessment metric based on the IIA model which has been tailored to CGIAR Centers. Internal audit, has also, within the same document, provided an overall assessment of where CGIAR Centers lie within the continuum for different processes and listed out key observations made for each process.

Based on the above self-assessment (Annex I) and ISO31000 on risk management, the following are key attributes of enhanced risk management (which would result in a ‘risk managed’ rating), and which provides a good target in terms of where the Centers may aim to get to:

A) Where risk management is viewed as integral to the organization's management processes at all levels.

B) Effective risk management is regarded by managers as essential for the achievement of the organization’s objectives.

C) Decision making within the organization, whatever the level of importance and significance, involves the explicit consideration of risks.

D) The organization’s governance structure and process incorporate considerations of supporting robust management of risk.

E) Comprehensive and fully defined accountability for risks, risk controls and risk treatment.

F) Designated individuals fully accept, are appropriately skilled and have adequate resources to check risk controls, monitor risks, improve risk controls and communicate effectively about risks and their management.

G) An emphasis on continual improvement in risk management through the setting of organizational performance goals, measurement, review and the subsequent modification of processes, systems, resources, capability and skills.

H) Continual communications with internal and external stakeholders including comprehensive and frequent reporting of risk management performance as part of good governance.

In the rest of this document, the key processes identified in the Table 1 above and those listed in the Assessment Matrix in Annex 1 are discussed in further detail to provide guidance on practice that would help a Center move towards the ‘risk managed’ status.

3.1 Tone at the Top

3.1.1 Mandate and commitment

An effective risk management process requires a strong commitment by Center boards and management, which should be reflected not only in words but also in actions. The COSO ERM Framework notes that the entity’s internal environment is the foundation for all other components of risk management, providing discipline and structure. The governing board is seen as a critical part of the internal environment and significantly influences its other elements. It further notes that championship by board members of risk management initiatives is a critical success factor for their implementation.

How can this be done practically?

A) Plan for the Center board and senior management to discuss risk management and its benefits with all staff. The board and management should make clear their interest in it and what is expected of all staff in the process.

B) Develop clear and comprehensive policies and guidelines and ensure that these are implemented and updated on a regular basis. Articulate and endorse these expressly to all staff.

C) Allocate resources for and assign clear responsibilities for risk management across the organization. Ensure that the same is reflected in job descriptions and that the respective staff are effectively assessed on their performance in risk management.

D) Include risk management as a standing agenda item at regular meetings, to inculcate it into every day processes and elevate its significance.
E) Publish the annual certification that the board is making regarding risk management for all staff to understand the commitment and the role that each one plays in the process.

3.1.2 Policies and guidelines

As part of the internal environment, management establishes a risk management philosophy – the entity's beliefs about risk and how is chooses to conduct its activities and deal with opportunities and potential failures. An enterprise risk management philosophy that is understood by all personnel facilitates employees' ability to recognize and effectively manage risk. Management communicates its enterprise risk management philosophy to employees through policy statements and other special communications, but also – importantly – through the regular planning, operations and reporting processes of the organization. Management reinforces the philosophy not only with words but with everyday actions as well.

The risk management policies and guidelines should describe the risk management strategy, including:

- the attention and commitment of the Board and management of the Center
- the link between the risk management strategy and the organization's objectives and other policies
- the scope of risk management activities
- approach to risk appetite
- risk management framework, processes and procedures applicable to all risk management activities in the Center
- roles and responsibilities for managing risk including 'risk ownership'
- communication channels for management and staff to discuss risks, report concerns and lessons learned about specific risks and opportunities
- the way risk management performance will be measured and reported
- commitment to the periodic review and verification of the risk management policy and framework and its continual improvement.

The Center should have a clear plan to ensure that the risk management policy, as articulated is implemented. This would include making risk management a key component in all the organization's activities such as policy development, strategic planning, change management etc.

3.1.3 Assigning accountabilities and responsibilities for risk management

The organization should ensure that there is accountability and authority for managing risks. Some centres have appointed a risk management coordinator or staff committee which provides a focal point within the Center for integrating the results of risk management activities throughout the Center and which also supports management and the Board in the preparation of Center-wide assessments and reporting. The majority of the Centers have a risk management committee which has representatives from different units within the organization.

COSO (2011) suggests that a Center should identify and position a leader to drive the risk management initiative. Specifically, it suggests to:

A) Identify a person with the right attributes to serve as the risk management leader. This does not have to be a dedicated staff position e.g. of a Chief Risk Officer but may instead aim to utilize existing resources.
B) Set objectives and expectations for the leader
C) Allocate appropriate resources to enable success.

It further suggests the establishment of a management working group, such a risk management committee to support the risk leader and to drive the risk management efforts across the organization. This group should have key people with sufficient stature and represent all key functions of the organization. This group should have clear objectives/terms of reference.

In addition to the risk leader and the risk management committee, it is agreed that all key employees (mainly managers and above) have a role to play in risk management. To ensure that this is clearly understood by all, the same should be embedded within their respective job descriptions, specifying the roles that they will play individually towards the overall objectives of the organization. Clear performance measures should also be defined and performance assessed of the same.

3.1.4 Risk Appetite

Risk appetite is the amount of risk an organization is prepared to be exposed to before it judges action to be necessary. This can vary by topic. For example, the risk appetite of CGIAR Centers concerning investment of surplus funds is (through policies set by the Boards) generally very low. The risk appetite for outsourcing research to partner institutions with limited capacity may be high where capacity building or partnership objectives are prominent in Center/program strategies. Similarly, the risk appetite for investing in research with uncertain returns, but which has the potential to produce valuable scientific breakthroughs, can be quite high.

Rittenburg L. and Martens F. (2012) in a COSO paper on risk appetite state that '*An organization's risk appetite should be articulated and communicated so that personnel understand that they need to pursue objectives within acceptable limits. Without some articulation and communication, it is difficult for management to introduce operational policies that assure the board and themselves that they are pursuing objectives within reasonable risk limits. A risk appetite statement effectively sets the tone for risk management. The organization is also more likely to meet its strategic goals when its appetite for risk is linked to operational, compliance, and reporting objectives.*'

It is the responsibility of the Board to clarify to management the extent to which it is authorized to take risks. COSO (2012) recommends the following three steps be applied to effectively adopting risk appetite.

A) Management develops, with board review and concurrence, a view of the organization's overall risk appetite.
B) This view of risk appetite is translated into a written or oral form that can be shared across the organization.
C) Management monitors the risk appetite over time, adjusting how it is expressed as business and operational conditions warrant.

Herein below, is a proposed four level scale for risk appetite which can be used to define appetite for different families of risk e.g. governance, funding and donor relations, research, operations, human resources etc. Centers are encouraged to refine this further to meet their respective needs.

Level	**Definition**
High	We accept and encourage opportunities presenting risks of failure if the likelihood of risks materializing combined with their potential impact make benefits greater than potential losses
Significant	We accept opportunities presenting a risk of limited under-achievement if the likelihood of risks materializing combined with their potential impact make benefits greater than potential losses
Moderate	While accepting the possibility of under-achievement in some circumstances, we seek safe operations and program/project delivery options despite lower potential rewards.
Low	We are not willing to accept risks under any circumstances that would significantly impact achievement of our objectives

3.2 Risk Identification

In risk identification, the aim should be '*to generate a comprehensive list of risks based on those events that might enhance, prevent, degrade or delay the achievement of the objectives. It is also important to identify the risks associated with not pursuing an opportunity*.' (ISO31000, 2010)

It is important that Centers integrate into their regular business processes steps whereby the key risks and opportunities at process, unit, regional, country office and Center levels are considered, and are inventoried for assessment and monitoring. This is crucial as risks which are not identified in this stage would not be available for further analysis.

For the risk identification to be effective, strategic and operational contexts should be established. This will allow the risk considerations be constrained within the environment which the organization operates in. To establish the context external and internal factors will need to be considered. These may include political, social and economic situation, security issues, taxation, legal and regulatory requirements, environmental and technological aspects as well as internal and external stakeholder expectations, organizational capabilities, strategies and culture.

The process for risk identification requires engagement with people with the right knowledge or information to identity these risks. Various methods may be employed to identify risks and opportunities.

At a "process level" risk identification (and analysis) is ideally embedded in standard business processes: e.g. in the logical framework or similar analysis prepared for new project proposals; and in business plans for new initiatives or renewed operations.

At a unit or Center level, the more common methods are (and they are not mutually exclusive):

- control and risk self-assessment exercises;
- interviews and surveys of stakeholders;
- the use of checklists of standard risks, SWOT analysis;
- brainstorming in group workshops, focusing on different levels (process/ unit/ Center-wide);
- review of results of internal monitoring activities such as project quality assurance reviews, impact assessments, financial projections, occupational health and safety reviews, and security reviews;
- continuous improvement efforts such as quality management and business process re-engineering. This includes such techniques as process mapping, and benchmarking with other organizations in similar environments or with similar characteristics;
- ongoing update of an automated risk management tracking system;
- internal audits, Center-commissioned reviews, external audits and external program reviews;
- CGIAR-wide and donor discussions;
- confidential reporting ("whistle blowing") processes.

Given the nature of the CGIAR System, Centers have many risks in common with other Centers and there is a great deal of scope for each Center to refine its own analysis by exchanging information about the types of risks that are being identified. This is being done through:

- the IAU, drawing on its work across the Centers to facilitate and evaluate risk identification;
- Communities of Good Practice across the system.

There are also risks that are shared collectively with other Centers, with the System Management Office or with other entities closely associated with the CGIAR. Collaborative processes are needed to inventory these risks, as a first step before assessing how well they are being managed through joint activities.

Examples where risks are shared include:

- Common donor funding channels – a large proportion of donor funds are channeled to Centers through the System Management Office;
- Consortium Research Projects (CRPs);
- Joint outsourcing of the administration of internationally recruited staff salaries and benefits payments, retirement funds and insurance administration;
- Linked information technology networks, through the implementation of Active Directory;
- Joint outsourcing of electronic mail, web hosting and other information and communications technology services;

- Common financial information systems, such as the Agresso Business World.

The risk identification process, if conducted at all levels of the organization, is expected to generate a comprehensive list of risks. These risks will be of varying importance throughout the organization. For example, while some risks may be considered as important at the functional or unit level, when considered at the Center level, it may not be considered as a priority or necessary for the attention of senior management or the board. The risks identified therefore require prioritization, which is done through risk analysis and evaluation.

IAU has put together, in Annex II a listing of typical enterprise risks of CGIAR Centers. The input of the Heads of Internal Audit of Centers was sought in putting together this list of risks. It should however be noted that this is not a comprehensive list but a guide to the risk identification process. It is important for each of the Centers to make their own listing and interpretation of risks.

3.3 Risk Assessment

3.3.1 Risk Assessment Criteria

COSO (2012) argues that '*The first activity within the risk assessment process is to develop a common set of assessment criteria to be deployed across business units, corporate functions, and large…projects*.'
It also states that '*Some form of measurement of risk is necessary. Without a standard of comparison, it's simply not possible to compare and aggregate risks across the organization*.'

'Impact' and 'likelihood' are the most common criteria for rating risk and opportunities (COSO, 2011), which is also what the majority of CGIAR Centers use.

"Impact" (or consequence) represents the effect on the organization or unit should failure occur, while "likelihood" represents the possibility that a given event will occur after considering the risk mitigating actions of the organization as they are currently designed and operating.

However, other organizations are expanding the assessment criteria to include other dimensions such as the velocity of the risk/speed of its onset, the organizations vulnerability/preparedness, among others to manage the limitations of the 'impact' and 'likelihood' criteria. While this may be used for more advanced risk management processes, the CGIAR IAU does not presently recommend this for CGIAR Centers.

The analysis of impact and likelihood may be done qualitatively (e.g. using the "high", "medium" and "low" rankings) or quantitatively (e.g. assigning numeric scores or financial effects). Whichever approach is selected, the same should be done consistently within the Center to permit comparisons.

Qualitative analysis is probably the most practical approach for Centers to implement, and given their non-profit character, the appropriateness of incorporating a financial analysis in the scoring is debatable.

So far, most Centers have opted for a 3-part “high”, “medium” and “low” qualitative scale in their risk assessments. Five point scales are however known to yield better dispersions than three point scales (COSO, 2011). Scales any higher than 5 would likely increase precision but would more likely be more time consuming to analyze, without generating much in the way of incremental benefits.

Provided herein below are illustrations of 5 level impact and likelihood scales provided in the COSO ERM, Risk Assessment in Practice (October 2012)

A. **Illustrative 5 level Impact Scale:**

Rating	Descriptor	Definition
5	Extreme	• Financial loss of $X million or more • International long-term negative media coverage; game-changing loss of market share • Significant prosecution and fines, litigation including class actions, incarceration of leadership • Significant injuries or fatalities to employees or third parties, such as visitors • Multiple senior leaders leave
4	Major	• Financial loss of $X million up to $X million • National long-term negative media coverage; significant loss of market share • Report to regulator requiring major project for corrective action • Limited in-patient care required for employees or third parties, such as visitors • Some senior managers leave, high turnover of experienced staff, not perceived as employer of choice
3	Moderate	• Financial loss of $X million up to $X million • National short-term negative media coverage • Report of breach to regulator with immediate correction to be implemented • Out-patient medical treatment required for employees or third parties, such as visitors • Widespread staff morale problems and high turnover
2	Minor	• Financial loss of $X million up to $X million • Local reputational damage • Reportable incident to regulator, no follow-up • No or minor injuries to employees or third parties, such as customers or vendors • General staff morale problems and increase in turnover
1	Incidental	• Financial loss up to $X million • Local media attention quickly remedied • Not reportable to regulator • No injuries to employees or third parties, such as visitors

		• Isolated staff dissatisfaction

(COSO-ERM, Risk Assessment in Practice, October 2012)

B. **Illustrative Likelihood Scale:**

	Annual Frequency		**Probability**	
Rating	**Descriptor**	**Definition**	**Descriptor**	**Definition**
5	Frequent	Up to once in 2 years or more	Almost certain	90% or greater chance of certain occurrence over life of asset or project
4	Likely	Once in 2 years up to once in 25 years	Likely	65% up to 90% chance of occurrence over life of asset or project
3	Possible	Once in 25 years up to once in 50 years	Possible	35% up to 65% chance of occurrence over life of asset or project
2	Unlikely	Once in 50 years up to once in 100 years	Unlikely	10% up to 35% chance of occurrence over life of asset or project
1	Rare	Once in 100 years or less	Rare	<10% chance of occurrence over life of asset or project

(COSO-ERM, Risk Assessment in Practice, October 2012)

3.3.2 Risk Analysis and Evaluation

Risk analysis is all about assigning values to each of the risks identified using the risk criteria. The causes and sources of risk, their consequences - positive and negative – and likelihood of occurrence. The assessment process should help identify the appropriate level of effort that should be made to put in place preventive or corrective internal controls.

Risk evaluation is about identifying the risks that need treatment in order to prioritize treatment implementation. In some cases, the risk evaluation may result in a decision to do further analysis or even not to treat a risk in any other way over and above the existing controls. This is determined by the organization's risk appetite.

It is also important to assess how events correlate, where sequences of events combine and interact to create significantly different probabilities or impacts. While the impact of a single event might be slight, a sequence of events might have more significant impact.

The positive and negative consequences of potential events, individually or by category, across the entity should be considered. Further, having identified shared risks, there is a need for Centers to evaluate the significance of these in the same manner as other risks. This is most efficiently done through a collaborative effort.

3.4 Risk Treatment

The COSO Framework notes that effective enterprise risk management requires that management select a response that is expected to bring risk likelihood and impact within the entity's risk tolerance.

Risk responses fall within the categories of risk avoidance, reduction, sharing and acceptance. Avoidance responses include taking action to exit the activities that give rise to the risks. Reduction responses (through implementation of preventive and corrective controls) reduce the risk likelihood, impact, or both. Sharing responses, such as taking out insurance coverage, reduce risk likelihood or impact by transferring or otherwise sharing a portion of the risk. Acceptance responses take no action to affect likelihood or impact.

In selecting the most appropriate risk treatment option, the key deciding factor is the cost verses the benefit e.g. where risk treatment may not be economically justifiable when considered against the probability of occurrence.

Communication is also key in selecting risk treatment options. For instance, where risk treatment options may affect risks in other parts of the organization, then staff in those other areas should be involved in the decision. Though equally effective, some risk treatments can be more acceptable to stakeholders than others.

It should also be noted that some level of residual risk will always exist, not only because resources are limited, but also because of future uncertainty and limitations inherent in all activities.

Where there may be limited resources available for risk treatment, it is important to prioritise these. Risk treatments on the other hand have the potential to introduce risks and a significant risk can be the failure or ineffectiveness of the risk treatment measures. Effective monitoring of the risk treatment options is therefore a necessary and integral part of the risk treatment plan.

Once identified, risk treatments should be documented in a risk treatment plan i.e. risk implementation plan. Information to be included in the risk treatment plan, as outlined in ISO31000 are:

A) expected benefit to be gained;
B) performance measures and constraints;
C) persons who are accountable for approving the plan and those responsible for implementing the plan;
D) proposed actions;
E) reporting and monitoring requirements;
F) resource requirements; and
G) timing and schedule.

3.5 Recording the risk management process

Recording allows for traceability and facilitates continuous improvement in the risk management process. Documentation in standard format across a Center may be facilitated by the adoption of:

- Risk management software, that automates the rolling up of results of risk identification, analysis and evaluation activities across the Center.
- Risk registers – document formats that facilitate a summary of risk inventory and analysis by unit or activity. Risk registers may be maintained manually or via the risk management software referred to above. An example of a simple risk register is provided in Annex III.

Many of the off-the-shelf software tools currently available in the market are mainly designed for large organizations. They can be very demanding in terms of maintenance and update. CGIAR Centers would need to weigh the pros and cons of investing in an automated system vs. the manual systems that are currently used widely in CGIAR.

The CGIAR Internal Audit Unit has an audit management software which offers an option for a risk management module. However, separate license would need to be obtained to use it.

The fact that elements of a Center-wide risk management process may not be fully documented does not mean that they are not effective or that they cannot be evaluated. However, an appropriate level of documentation usually makes monitoring more effective and efficient, and supports the dissemination of lessons learned. With the requirement for Center Boards of Trustees to make statements to external parties regarding enterprise risk management, it is essential that documentation is developed and retained to support the statements

3.6 Communication and Consultation

There should be a clear plan on how risk management related communication will be managed for both internal and external stakeholders. It is also important to take note that judgements on risk and risk management are dependent of perceptions, which are likely to vary depending on individual values, needs, assumptions and concerns of different stakeholders. Effective communication should facilitate the identification of the specific risks, potential impact and also possible mitigation measures.

Build internal communication systems for the risk management process that will ensure that:

- the risk management framework, and changes made to it are communicated appropriately;
- there is sufficient consultation of internal stakeholders;
- there is an effective feedback system on the effectiveness and outcomes of the framework and;

- relevant information from the risk management process is relayed in a timely fashion and at the appropriate levels.

External communication should also be planned and managed effectively such as legally required disclosures, external reporting required to comply with regulatory and legal requirements, communicating with stakeholders in the event of crisis etc. This communication should be managed to ensure effective and accurate exchange of information.

3.7 Monitoring and review

This is also a very important part of the risk management process which requires clear assignment of responsibility. Monitoring ensures that enterprise risk management continues to be applied at all levels and across the entity. The monitoring and review process, according to ISO31000 should enable the Centers to:

a) analyse and learn lessons from events, changes and trends;
b) detect changes in the external and internal operating environment including changes to the risks which may require revision of risk treatments and priorities;
c) ensure that the risk control and treatment measures are effective in both design and operation; and
d) identify emerging risks.

This monitoring may be periodic or ad hoc. Either way, this should be clearly planned, recorded and reported both internally and externally as required. Ongoing monitoring is built into the normal, recurring operating activities of the Center. Since separate evaluations take place after the fact, problems often will be identified more quickly by ongoing monitoring routines.

Risk assessment and reporting are cyclical processes which take place at different levels of an organization. At a senior management level, normally only key entity risks (10-15) will be reviewed and reported on periodically. Key risks and measures to manage them will be reported to a Center's governing body. Lower level risks which might be high at a unit level will be periodically e.g. at least annually reviewed by a business unit/departmental teams. Centers may need to develop a process whereby emerging high risks at a unit level are escalated to senior management. It may be done through a risk management committee.

Separate evaluations of the robustness of risk management processes themselves include periodic internal and external audits and Center-commissioned external reviews. Shortcomings in risk management detected through monitoring mechanisms, which affect the Center's ability to develop and implement its strategy, should be reported to those positioned to take necessary action.

This review process should also feed into the organization's performance management system.

4. ROLES AND RESPONSIBILITIES

A) **Board of Trustees (BoT)**

The IIA position paper (2009) states that '*The board has overall responsibility for ensuring that risks are managed. 1. Ensuring that there is a rigorous risk management process in place 2. Approve the risk management policy'.*

The OCED principles of Corporate Governance identifies that reviewing and guiding the risk policy is a key function of governing boards. According to the principles, such policy will involve specifying the types and degree of risk that a company is willing to accept in pursuit of its goals i.e. the risk appetite of the organization.

B) **Senior Management (SM)**

IIA position paper (2009) states that '*In practice, the board will delegate the operation of the risk management framework to the management team… There may be a separate function that co-ordinates and project-manages these activities and brings to bear specialist skills and knowledge… Everyone in the organization plays a role in ensuring successful enterprise-wide risk management but the primary responsibility for identifying risks and managing them lies with management*.'

Key duties of senior management in the risk management process therefore include:

- Review the risk management framework regularly.
- Manage the risk management process.
- Consider risk as part of all decisions.

C) **Risk Management Committee (RMC)**

Key duties of a risk management committee include to:

- Develop risk management policy and guidelines and communicate to staff
- Identify strategic risks affecting the organization and make recommendations to the Board as to the ways in which these will be managed.
- Ensure risks are managed effectively through the risk management framework and report to management and the board regularly.

D) **Managers (M)**

Key duties of organizational managers include to:

- Ensure risk is managed effectively in each function within the agreed strategy and report to risk management committee regularly.
- Identify individual risks affecting their activities, ensure that these are recorded in the Unit's risk register and that appropriate control measures are in place for managing those risks.
- Continually monitor the adequacy and effectiveness of all control measures and report to their RM committee
- Formally review all arrangements for risk management affecting their activity as part of regular organizational planning.

E) **All Employees (E)**

All staff should, among others:

- Undertake their job within risk management guidelines including compliance with all control measures that have been identified
- Report hazards/risks to their managers.

F) **Internal Audit (IA)**

Internal audits role is to:

- Comment on the adequacy of the process in place to identify risk and effectiveness of the control measures in place
- Make recommendations to management and the board as necessary.

It is useful to document responsibilities in a RACI matrix based on ISO:31000 to understand to what extent different parties are involved in the risk management processes.

Area	**Responsible**[2]	**Accountable**	**Support**	**Consulted**	**Informed**
5.2 Mandate and commitment	SM	BoT	M	M	E, IA
5.3 Design of framework for managing risk	SM, RMC	SM	M	M, IA	BoT, E, IA
5.4 Implementing risk management	RMC, M, E	SM	BoT		
6.2 Communication and consultation	RMC, M	SM	E	External stakeholders	BoT
6.3 Establishing context	RMC, M	SM	E	External stakeholders	BoT

[2] Responsible: Those who do the work to achieve the task. There is at least one role with a participation type of responsible, although others can be delegated to assist in the work required.
Accountable (final approving authority): The one ultimately answerable for the correct and thorough completion of the deliverable or task, and the one who delegates the work to those responsible. In other words, an accountable must sign off (approve) work that "responsible" provides. There must be only one "accountable" specified for each task or deliverable.
Support: Resources allocated to "responsible". Unlike "consulted", who may provide input to the task, "support" helps complete the task.
Consulted: Those whose opinions are sought, typically subject matter experts; and with whom there is two-way communication.
Informed: Those who are kept up-to-date on progress, often only on completion of the task or deliverable; and with whom there is just one-way communication.

6.4 Risk assessment	RMC, M	SM	E	External stakeholders	BoT
6.5 Risk treatment	RMC, M	SM	E	External stakeholders	BoT
6.6 Monitoring and review	RMC, M	SM	E		BoT
5.5 Monitoring and review of the framework	RMC	SM	IA	M	E, BoT
5.6 Continual improvement of the framework	RMC	SM	M, IA	BoT	E, IA

5. BIBLIOGRAPHY AND CREDITS

This GPN was developed under the leadership of Pierre Pradal, CGIAR IAU Director, by Alison Ngeny-Otieno, CGIAR IAU Internal Audit Manager and Madina Bazarova, CGIAR IAU Associate Director, with kind contributions of Bioversity, CIAT, CIFOR, CIP, IITA, ILRI, IWMI, IRRI, ICRAF and CIMMYT whose risk management policies were used in the appendix D.

It was based on the following materials:

- Chartered Institute of Internal Auditors (2016) '*Defining risk, risk management and ERM*' [ONLINE]. Available at: https://www.iia.org.uk/resources/risk-management. [Accessed 8 November 2016]

- COSO (2004) '*Enterprise Risk Management - Integrated Framework*' 1st ed. AICPA

- COSO (2011) '*Embracing Enterprise Risk Management, Practical Approaches to getting started*' http://www.coso.org/documents/EmbracingERM-GettingStartedforWebPostingDec110_000.pdf (Accessed 8 November 2016)

- COSO (2012) '*Risk Assessment in Practice*' http://www.coso.org/documents/COSOAnncsOnlineSurvy2GainInpt4Updt2IntrnlCntrlIntgratdFrmwrk%20-%20for%20merge_files/COSO-ERM%20Risk%20Assessment%20inPractice%20Thought%20Paper%20OCtober%202012.pdf (Accessed 10 November 2016)

- Institute of Internal Auditors (2009) '*IIA Position Paper: The Role of Internal Auditing in Enterprise-Wide Risk Management' https://na.theiia.org/standards-guidance/Public%20Documents/PP%20The%20Role%20of%20Internal%20Auditing%20in%20Enterprise%20Risk%20Management.pdf* (Accessed 24 January 2017*)*

- ISO (2009) 'ISO Guide 73 Risk Management Vocabulary'. 1st ed. Switzerland: ISO

- ISO 31000 (2009) '*Risk management – Principles and guidelines'* 1st ed. ISO

- Rittenburg L. and Martens F. (2012) '*Enterprise Risk Management – Understanding and Communicating Risk Appetite*' COSO https://www.coso.org/Documents/ERM-Understanding-and-Communicating-Risk-Appetite.pdf (Accessed 25 January 2017

APPENDIX A: RISK MATURITY ASSESSMENT MATRIX

Criteria	Risk naive	Risk aware	Risk defined	Risk managed	Risk enabled	
Key characteristics	**No formal approach developed for risk management**	**Scattered silo based approach to risk management**	**Strategy and policies in place and communicated.** **Risk appetite defined**	**Enterprise approach to risk management developed and communicated**	**Risk management and internal controls fully embedded into the operations**	**Observations from recent audits of Centre risk management processes**
1. Tone at the top						
The Board and senior management make statement demonstrating clear commitment to implementation of robust risk management system and set expectations as to how this will be achieved	No	Yes - but this is done as part of the board processes including preparing a statement on risk management. However, no further action beyond this.	Yes - Publish board papers e.g. (board statement on risk management and risk management policy) and alert staff.	Yes - Risk Management is embedded in the strategy, is in place and implemented.	Yes – There are clear accountability structures in place.	1. Risk Management policies developed. 2. Board statements produced annually, but not published internally and externally (other than in the audited financial statements) 3. Staff are not aware of them nor of the expectations set 4. Regional and country management responsibilities for risk management are not clearly stipulated. 5. No clear plans to improve risk management 6. The responsibility to lead and manage the risk management

Criteria	Risk naive	Risk aware	Risk defined	Risk managed	Risk enabled	
Key characteristics	**No formal approach developed for risk management**	**Scattered silo based approach to risk management**	**Strategy and policies in place and communicated.** **Risk appetite defined**	**Enterprise approach to risk management developed and communicated**	**Risk management and internal controls fully embedded into the operations**	**Observations from recent audits of Centre risk management processes**
						framework mainly sits with the CSEs 7. The RMC is inactive and only meet to review the risk register in time for BOT meetings. 8. Staff are not held accountable for managing risks well. 9. Low level of awareness of the Risk management policy although available on Centre intranets. 10. The RM policies have not been updated since they were first prepared.
The risk appetite of the organization has been defined	No	No	Risk appetite may have been defined but is not communicated nor used	Risk appetite has been defined well and communicated	Risk appetite is used for all decision making.	1. Risk appetite defined in the RM policy but not used for decision-making 2. Staff are not generally aware of the risk appetite and decisions are made based on individual experience and sometimes

Criteria	Risk naive	Risk aware	Risk defined	Risk managed	Risk enabled	
Key characteristics	**No formal approach developed for risk management**	**Scattered silo based approach to risk management**	**Strategy and policies in place and communicated.** **Risk appetite defined**	**Enterprise approach to risk management developed and communicated**	**Risk management and internal controls fully embedded into the operations**	**Observations from recent audits of Centre risk management processes**
			in decision making.			without involving staff with relevant expertise.
Responsibility for the determination, assessment, and management of risks is included in job descriptions	No	No	Limited - Key staff JDs refer to Risk Management	Most staff JDs refer to RM	All JDs refer to RM	JDs do not clearly define responsibilities for managing risk.
Management have been trained to understand what risks are, and their responsibility for them	No	Limited training	Training planned, provided to key staff	Training provided to all managers	Training provided to all managers	1. No structured training provided 2. No induction.
Managers are assessed on their	No	No	Only primary risk managers	Senior managers	All managers	No formal assessment of risk management performance.

Criteria	Risk naive	Risk aware	Risk defined	Risk managed	Risk enabled	
Key characteristics	**No formal approach developed for risk management**	**Scattered silo based approach to risk management**	**Strategy and policies in place and communicated.** **Risk appetite defined**	**Enterprise approach to risk management developed and communicated**	**Risk management and internal controls fully embedded into the operations**	**Observations from recent audits of Centre risk management processes**
risk management performance						
Internal Audit approach	Promotes risk management and relies on alternative audit methods	Promotes enterprise wide approach to risk management and relies on alternative audit planning method.	Facilitates risk management / liaises with risk management and uses management assessment of risk where appropriate.	Audits risk management process and uses management assessment of risk as appropriate.	Audits risk management processes and uses management assessment of risk as appropriate.	1. IA initiated the risk management process in the Centres. 2. IA introduced the risk register, the annual review templates and process 3. IA initiated the RMC and in some instances led it. 4. IA identifies new risks and key risks 5. IA reviews the RM processes on annual basis and reports to the Finance/Audit (and risk) Committee 6. Real or perceived conflict of interest in IA's involvement.
2. Objective setting						

Criteria	Risk naive	Risk aware	Risk defined	Risk managed	Risk enabled	
Key characteristics	**No formal approach developed for risk management**	**Scattered silo based approach to risk management**	**Strategy and policies in place and communicated.** **Risk appetite defined**	**Enterprise approach to risk management developed and communicated**	**Risk management and internal controls fully embedded into the operations**	**Observations from recent audits of Centre risk management processes**
The organization's objectives are defined	Possibly	Yes – but there may be no consistent approach	Yes - strategic and operational objectives are defined but not consistently aligned; there is no alignment to the centre's risk appetite	Yes - Strategic and operational objectives are defined and aligned, but not consistently aligned with risk appetite	Yes - Strategic and operational objectives are aligned and aligned with risk appetite	1. Strategies are not reviewed for alignment with the centre's risk appetite. 2. There is no guidance how risks should be assessed. 3. The annual risk review cycle not tied with major business cycles which makes it hard to include any costs for new risk mitigating actions into the budget.
3. Risk identification						
Processes have been defined to determine risks, and these have been followed	No	Unlikely	Yes, but may not apply to the whole organization	Organization - wide risk identification	Organization -wide risk identification	1. Many risks in risk registers have not changed significantly relative to the first risk register. 2. IA has been an initiator to raise new risks based on

Criteria	Risk naive	Risk aware	Risk defined	Risk managed	Risk enabled	
Key characteristics	**No formal approach developed for risk management**	**Scattered silo based approach to risk management**	**Strategy and policies in place and communicated. Risk appetite defined**	**Enterprise approach to risk management developed and communicated**	**Risk management and internal controls fully embedded into the operations**	**Observations from recent audits of Centre risk management processes**
						conversations with management. 3. No structured way to raise risks from units, regional and country offices. 4. No criteria to define key risks e.g. in terms of scoring or the gap between the residual risk scoring and risk appetite
All risks have been collected into one list. Risks have been allocated to specific job titles.	No	Some incomplete lists may exit.	Yes, but may not apply to the whole organization	Majority of business units record risks	All business units record risks	1. Risks consolidated at the centre level, but none at operational level, regional/country office level. 2. Risk information is generic. These should be SMART.
All significant new projects/strategies are routinely assessed for risk	No	No	Some projects	All major projects	All projects	1. Not formally and consistently done. 2. Key staff are not involved
4. Risk assessment						

Criteria	Risk naive	Risk aware	Risk defined	Risk managed	Risk enabled	
Key characteristics	**No formal approach developed for risk management**	**Scattered silo based approach to risk management**	**Strategy and policies in place and communicated. Risk appetite defined**	**Enterprise approach to risk management developed and communicated**	**Risk management and internal controls fully embedded into the operations**	**Observations from recent audits of Centre risk management processes**
A scoring system for assessing risks has been defined	No	Unlikely with no consistent approach defined	Yes, but may not be applied consistently	Consistently applied	Consistently applied	1. There is a scoring system but inconsistently applied/not communicated 2. It is not clear which risks are assessed, what is considered as 'inherent' and what is 'residual'. 3. It may result in different scoring of the level of risk.
All risks have been assessed in accordance with the defined scoring system	No	Some incomplete lists may exist	Yes, but may not be applied consistently	Consistently applied	Consistently applied	
5. Risk response and control activities						
Responses to the risks have been selected and implemented	No	Some responses identified	Responses identified for limited number of risks	Responses identified and implemented for all key risks	Responses identified and implemented for all risks	1. Responses to manage risks have not been consistently documented. 2. Some responses are too generic to follow up on. 3. No due dates have been set for implementing additional measures.
Management have set up methods to	No	Monitoring is seldom done	Monitoring done only	Monitoring is done for all	Monitoring is done for all	1. Monitoring activities seldom done.

Criteria	Risk naive	Risk aware	Risk defined	Risk managed	Risk enabled	
Key characteristics	**No formal approach developed for risk management**	**Scattered silo based approach to risk management**	**Strategy and policies in place and communicated.** **Risk appetite defined**	**Enterprise approach to risk management developed and communicated**	**Risk management and internal controls fully embedded into the operations**	**Observations from recent audits of Centre risk management processes**
monitor the proper operation of key processes, responses and action plans (‘monitoring controls')			covers selected processes	key processes across the organization	key processes across the organization	2. Some risk mitigating activities might be assessed and some not, meaning that risks which may be perceived to be well managed may not be. 3. Misunderstanding that IA is responsible for checking the robustness of mitigating actions.
6. Communication						
Risk information is shared with managers and staff to help align with the risk mitigating activities	No	Limited information sharing	Information is shared with key staff	Information is consistently shared	Information is consistently shared and staff are alerted to it	1. Information on key risks/risk registers is not shared across the organization e.g. units, regions and countries to inform their activities. 2. Risk tolerance levels are not documented.
Internal and external risk related communication is planned and	No	Limited, mostly for internal audience	Sometimes, for both internal and external audience	Planned in most instances	Well planned	1. No clear plans for meeting external legal disclosure requirements

Criteria	Risk naive	Risk aware	Risk defined	Risk managed	Risk enabled	
Key characteristics	**No formal approach developed for risk management**	**Scattered silo based approach to risk management**	**Strategy and policies in place and communicated.** **Risk appetite defined**	**Enterprise approach to risk management developed and communicated**	**Risk management and internal controls fully embedded into the operations**	**Observations from recent audits of Centre risk management processes**
managed effectively						2. Limited plans for communication with stakeholders in the event of crisis.
7. Monitoring and reporting						
Risks are regularly reviewed by the organization	No	Some risks are reviewed but infrequently	Yes, but on an annual basis	Quarterly reviews	Quarterly or monthly reviews	1. In many cases, IAU facilitates review on an annual basis. 2. Progress updates are generic or reflect no real action. 3. Only done for key risks. 4. The risk owner's reviews/comments are not validated or challenged.
Management report risks to directors where responses have not managed the risks to a level acceptable to the board	No	No	Yes, but seldom and may not be a formal process	Reporting mechanisms in place but not consistently used	Reporting mechanisms in place and used consistently	1. In most cases, this is not reported as there is no process, other than the annual review, to identify whether there is risk reduction. 2. The annual process is not validated.

Criteria	Risk naive	Risk aware	Risk defined	Risk managed	Risk enabled	
Key characteristics	**No formal approach developed for risk management**	**Scattered silo based approach to risk management**	**Strategy and policies in place and communicated.** **Risk appetite defined**	**Enterprise approach to risk management developed and communicated**	**Risk management and internal controls fully embedded into the operations**	**Observations from recent audits of Centre risk management processes**
Managers provide assurance on the effectiveness of their risk management	No	No	No	Management assurance on key risks	Management assurance on all risks	Managers are not formally required to explain what assurance mechanisms they used to understand the robustness of risk mitigating actions.

APPENDIX B: TYPICAL ENTERPRISE LEVEL RISKS FOR CGIAR CENTERS

STRATEGIC	COMPLIANCE	FINANCIAL	OPERATIONAL
Funding	**Legal**	**Financial**	**Human Resource Management**
Lack of continuity/visibility of funding	Penalties and fines from non-compliance e.g. legal, environmental, health and safety	Donor restrictions on full cost recovery resulting in funding short falls	Mismatch of skills and business needs
Reduced funding due to changing donor priorities	Failure to meet contractual obligations to partners.	Significant loss of funds due to poor investment decisions	Erosion of professional staff scientific skills
No strategy on resource mobilization	Sanctions from inadvertent financing of terrorist organizations or individuals	Mismatch between research priorities and budgets.	Inability to attract and retain appropriate staff
Over-reliance on one or few key donor	Use of illegal software	Center paying more for external goods and services than it requires or can get in the market	Inadequate staff capability/capacity to deliver scientific results/conduct projects
Lack of coordination	Center fails to observe internationally accepted and contractually binding ethical research standards (e.g. informed consent, handing of traditional knowledge)	Inefficient financial systems	Loss of institutional knowledge due to inadequate handover processes
Inability to raise sufficient funding to achieve objectives	**Donor**	Inadequate reserves for medium term liquidity	Poor management or mismanagement of payroll and staff benefits.
Changes in the CGIAR may impact the Centers negatively in terms of funding	Non-compliance with donor agreements	Cashflow problems: inability to pay debts on time	**Station/country operations**

STRATEGIC	COMPLIANCE	FINANCIAL	OPERATIONAL
Missed funding opportunities/insufficient proposal pipeline	Donor technical requirements as reflected in grant agreements may not be met i.e. quality, and timelines	Inadequate financing of institutional costs from restricted projects	Ineffective and inefficient operations due to decentralized structures and limited/ineffective oversight.
Political	**Host Country**	Surprise significant over/under expenditure	**Procurement and asset management**
Government instability	Sanctions/Expulsion from failure to comply with host country agreement	Significant foreign exchange losses	Procuring goods & services with inflated prices leading to Center financial loss
Governance & organizational culture	Non-compliance with national and international undertakings on germplasm transfer	Unauthorized/inaccurate disbursements	Misuse, loss or lack of maintenance of Center property
Ineffective leadership	**Policies/procedures**	Opportunity cost of long outstanding receivables	Misuse of IT resources
No clear structure	Ineffectiveness due to undeterred non-compliance		**General operations**
Lack of Accountability	Non-compliance due to ignorance/lack of awareness		Inefficient farm operations
Lack of oversight (Board)	**Financial reporting**		Inefficient food and housing operations.
Ineffective collaboration	Financial disclosures not in accordance with International Financial Reporting Standards		Inefficient transport operations
Uncertainty surrounding the future and governance of CRP system	Financial reporting is materially incorrect		Inefficient and unfavorable contracting process
Micro-management by the board			**Fraud**

STRATEGIC	COMPLIANCE	FINANCIAL	OPERATIONAL
Senior Management resisting oversight from the board			Fraud/Corruption at management level
Science & Strategic Research			Scientific fraud
Research focus and priorities are not consistent with the organization strategy			Misappropriation or misuse of Center funds
Strategic research and capacity building are directed to activities which have limited or no impact			Loss of assets through theft or damage
No consistent/proper scientific strategy at institute level			**Safety and security**
Poor quality of research activities and/or publication			Disaster disrupts operations
Not delivering scientific results			Staff caught up in civil disruption
Duplication of research activities			Hazardous working conditions
Loss of genebank accessions due to poor handing, environmental or physical security or contamination.			Staff exposed to dangerous travel conditions
Research partner failure to deliver requirements			
Knowledge Management			
Research data lost or difficult to access			
Inadequate dissemination of research results			
Intellectual property disputes			

APPENDIX C: ILLUSTRATIVE MANUAL RISK REGISTER

			Inherent risk data					Residual risk data				Required Mitigation			
Risk ID	Category	Description	Likelihood	Impact	Score	Inherent risk level	Key controls/mitigating factors in place	Likelihood	Impact	Score	Residual risk level	Response	Description	Timeline	Accountability
1	Research	Poor quality of research activities and/or publication	3	4	12	🟧	Peer review of publications	2	4	8	🟨	Reduce	1. Verification of base data on scientific publications 2. Progressive quality assessment in life of project	Jun-17	Science leader

APPENDIX D: EXAMPLE OF RISK MANAGEMENT PRACTICES AT CGIAR[3]

Center	Last Updated	Introduction	Roles and Responsibilities	Approach	Others
A	Sept 2004	Provides the purpose of the policy, objectives and definitions.	Defines responsibilities for the board, DG, risk management team and internal audit.	Provides limited information on the risk management framework.	
B	Mar 2015	Provides the purpose, scope and risk management principles	Defines responsibilities of the board, audit and risk committee, the DG, the management team, the general counsel, risk management coordinator, all staff, internal and external audit.	i) Defines risk appetite. ii) Risk identified classified into 3 categories. iii) Provides a 4-level risk analysis matrix, showing impact against likelihood. iv) Provides risk response options (4). v) Defines approach for risk monitoring, review, communication, escalation and reporting.	
C	Oct 2016	Provides the purpose of the policy and its scope	Defines responsibilities of the board, executive team, risk owners, all managers, all staff, functions/hubs, risk	i) Defines risk appetite. ii) Risk identified classified into 4 categories, split between external and internal drivers. iii) Provides a 4-level risk analysis matrix, showing impact against	Provides; i) Definitions ii) templates for recording risks iii) a project/activity risk assessment checklist.

[3] The names of the Centers were anonymized

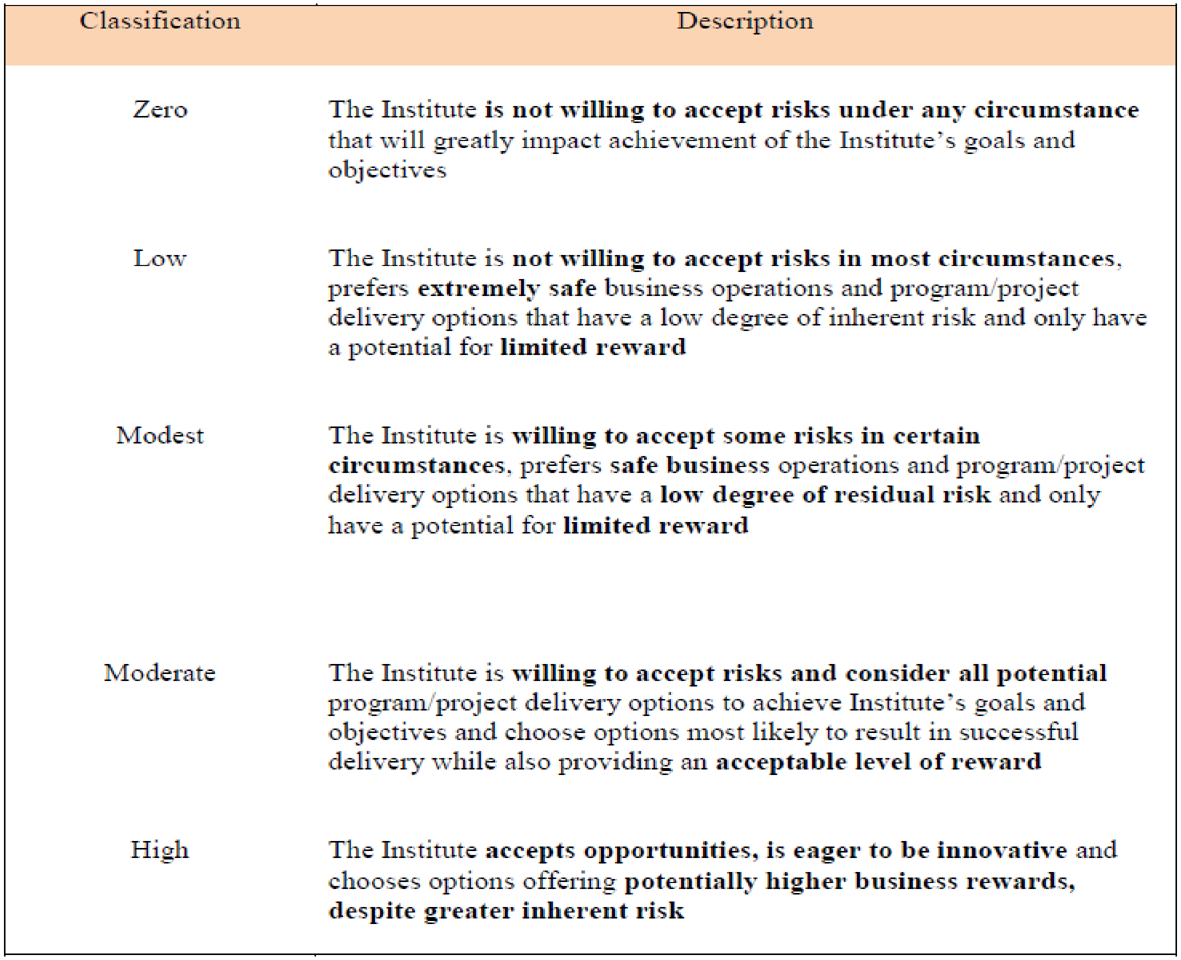
Center	Last Updated	Introduction	Roles and Responsibilities	Approach	Others
			coordinator, internal and external audit.	likelihood. It also gives scores (in 4 level matrix) for impact and likelihood. iv) Provides risk response options (4). v) Defines approach for risk monitoring, communication and reporting.	iv) Executive committee TOR
D	Jan 2015	Provides the purpose and scope of the policy	Defines responsibility of the RM committee, the DG and all staff.	i) References a policy framework previously approved by the board. ii) For implementation, identifies the RM committee as the key driver of monitoring and reviewing the implementation and effectiveness of the risk management program. iii) Provides that risks shall be recorded in a risk management matrix. iv) Defines status update frequency for senior management and the board	
E	Nov 2015	Defines risk management and provides its purpose and objectives.	Defines responsibilities of the audit committee (board), DG, top management, RM committee, unit heads, budget holders and project managers and internal audit.	i) Defines acceptable risk ii) That guidance, directives, procedures & documentation for use in risk identification, assessment and development of mitigation action plan and its execution shall be developed and issued by the Risk Management Committee.	Reflects that it applies to all units, hubs, stations, projects and all staff across the organization.

Center	Last Updated	Introduction	Roles and Responsibilities	Approach	Others
				iii) Risk monitoring and benchmarking	
F	2012	Provides an introduction including the purpose of the policy and its objectives	Defines responsibilities of the board, DG, risk coordinator, all staff and internal audit.	i) Defines risk appetite ii) Outlines the risk management framework which includes risk identification, risk analysis and evaluation (3 level impact and likelihood scale used – High, Moderate, Limited) iii) Defines the data to be recorded in the risk analysis iv) Defines risk treatment options (4 options) v) Monitoring, review and reporting	Provides appendix with sample

Center	Last Updated	Introduction	Roles and Responsibilities	Approach	Others
G	May 2004	Provides an introduction including the purpose of the policy and its objectives	Defines responsibilities of the board, DG, risk coordinator, all staff and internal audit.	i) Defines risk appetite ii) Outlines the risk management framework which includes risk identification, risk analysis and evaluation (3 level impact and likelihood scale used – High, Moderate, Limited) iii) Defines the data to be recorded in the risk analysis iv) Defines risk treatment options (4 options) v) Monitoring, review and reporting	Provides appendix with sample
H	Oct 2008	Provides an introduction including the purpose of the policy and its objectives and scope	Defines responsibilities of the board, DG, directors, risk coordinator, risk management and quality assurance (RMQA) steering committee, RMQA Senior Manager and RMQA officers, organizational unit heads', all staff and internal audit.	i) Sets out reporting requirements ii) Refers to ISO standards iii) Establishes that risk assessments shall be conducted on new ventures and activities, including projects, processes, systems, and research activities iv) Defines the data to be recorded in the risk analysis v) Requires each unit to appoint a RMQA officer who would coordinate regular risk assessments within a unit. The results are then reviewed, collated and reported on by RMQA Senior Manager.	Risk appetite is defined in a separate document approved by the BoT.

Center	Last Updated	Introduction	Roles and Responsibilities	Approach	Others
I	Nov 2014	Provides an introduction including the purpose of the policy and its objectives	Defines responsibilities of the board, DG, risk coordinator, risk management committee, all staff and internal audit.	i) Defines risk appetite ii) Outlines the risk management framework which includes risk identification, risk analysis and evaluation (3 level impact and likelihood scale used – High, Medium, Low) iii) Defines the data to be recorded in the risk analysis iv) Defines risk treatment options (4 options) v) Monitoring, review and reporting	Incorporates suggestions from ISO 31000 on risk management principles and guidelines Identifies policies related to the RM policy. Provides definitions.
J	Nov 2016	Provides purpose of the policy and key definitions	Defines responsibilities of the board, AFC, DG, management committee, all staff, risk support officer, external and internal audit.	i) Defines risk appetite ii) Defines risk management principles iii) Defines risk management framework and components of the process	

Example of risk appetite scales (IRRI):



Classification	Description
Zero	The Institute **is not willing to accept risks under any circumstance** that will greatly impact achievement of the Institute's goals and objectives
Low	The Institute is **not willing to accept risks in most circumstances**, prefers **extremely safe** business operations and program/project delivery options that have a low degree of inherent risk and only have a potential for **limited reward**
Modest	The Institute is **willing to accept some risks in certain circumstances**, prefers **safe business** operations and program/project delivery options that have a **low degree of residual risk** and only have a potential for **limited reward**
Moderate	The Institute is **willing to accept risks and consider all potential** program/project delivery options to achieve Institute's goals and objectives and choose options most likely to result in successful delivery while also providing an **acceptable level of reward**
High	The Institute **accepts opportunities, is eager to be innovative** and chooses options offering **potentially higher business rewards, despite greater inherent risk**