



Enterprise Risk Management

Part of a series of notes to help Centers and their internal auditors review their own Center internal management processes from the point of view of managing risks and promoting value for money, and to identify where improvement efforts could be focused. The good practices described in this series of notes should not be interpreted as minimum standards as not all may be applicable to every Center

SUMMARY

The purpose of this note is to provide a set of benchmarks to Centers for implementing an enterprise (Center-wide) risk management system. The note draws on the results of a survey of external good practice (national standards and guidance material from various CGIAR member countries) conducted by the CGIAR Internal Auditing Unit, as well as the results of recent work with CGIAR Centers.

Enterprise risk management is becoming widely implemented in both public and private sectors in many countries, including in some CGIAR donors. Various high profile events in recent years – ranging from large scale financial collapses to major failures in the provision of public services – have led to an explosion in regulatory requirements and professional guidelines on managing risks. These have focused on prevention or mitigation of losses. However, in an environment where organizations must evolve to stay relevant and attractive to investors, risk management is also concerned with how well the organization manages opportunities.

Taking a broader view then, enterprise risk management is concerned with how an organization assures itself, for the whole range of activities in which it is engaged, that the opportunities and risks associated with existing operations and with potential new activities are identified, evaluated and acted upon in a timely manner. Enterprise risk management is defined in the COSO Enterprise Risk Management Framework published in the United States, 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.”

Centers have always dealt with opportunities and risks in one way or another. However a more systematic, explicit, enterprise-wide risk management process – drawing on good practice from CGIAR member countries – should help Centers better deal with uncertainty and avoid unpleasant surprises. Reporting by management and Boards on the effectiveness of risk management will provide assurance



to current and potential donors and other stakeholders in the CGIAR system, and support requests for greater unrestricted funding.

The design of enterprise risk management should reflect a balanced (risks and opportunities) view of the nature of the underlying business activities. Intelligent risk management should also encourage management and staff to challenge existing ways of making sense of the external and internal environments, enabling a more proactive management approach.

The risks and opportunities that the CGIAR Centers manage are as complex as any found in any international public or private sector organization. However, the challenge for the Centers is to implement integrated risk management processes at a scale and cost that is commensurate with their size and the need to keep costs to a minimum.

Bearing these aspects in mind, the CGIAR Internal Auditing Unit has identified in this Note various good practices which can assist Centers to implement an effective and efficient enterprise risk management process. These are summarized below.

THE KEY ELEMENTS OF AN ENTERPRISE RISK MANAGEMENT PROCESS

Establish the context

- Consider risks and opportunities across all the activities of a Center, taking into account both the external and internal environment in which the Center operates
- Promote, through clear policies and procedures, awareness raising activities and senior management emphasis, an internal environment that supports proactive risk management at all levels
- Ensure that clear business objectives are set for all Center business units and programs, so that risks can be readily identified and assessed
- Identify a point of coordination within the Center, which can assist the Director General to integrate the results of various risk management activities across the Center

Identification of Risks

- Integrate, into the Center's regular business processes, steps whereby the key risks and opportunities at process, unit and Center level are considered and are inventoried for assessment and monitoring
- Identify, through collaborative processes with other Centers and System Office components, those risks that are common to or shared across the CGIAR System



Risk Analysis/Evaluation

- Consider how the identified risks might affect the achievement of business objectives from two perspectives: the impact of failure on the Center's objectives should it occur and the likelihood of occurrence and damage in such an event
- Evaluate the Center-wide significance of risks identified at unit / activity level
- Evaluate, through collaborative processes with other Centers and System Office components, common or shared risks
- Evaluate trends in risk impact and likelihood

Risk Treatment

- Establish an oversight process for ensuring that there are clear management responses for all identified risks where likelihood and impact are rated as significant
- Ensure that all risk responses are implemented through appropriate control activities
- Integrate risk management results into established Center policy and planning processes

Monitoring and Review

- Document the results of risk monitoring activities, including action taken to address shortcomings identified and progress with mitigation plans

REPORTING ON RISK MANAGEMENT

- Prepare periodic summary management reports on the status of Center-wide risk management activities
- Prepare Board statements on risk assessment and internal control that are supported by the Center's internal risk management system. A proposed format of Board statement has been developed based on research by the CGIAR Internal Auditing Unit and is documented in a separate Discussion Note.
- Implement, preferably through existing internal management reporting processes, reporting by unit / activity managers on the status of risk management at their level and actions proposed



Acknowledgement

This note has been prepared solely for use by CGIAR Centers and their internal auditors. We thank CGIAR Center managers and staff who provided input and advice on the preparation of this note. We also thank staff of the United Kingdom DFID Internal Audit Unit who provided material and advice helpful to the preparation of this note.

The note draws on a number of external frameworks and standards, in particular:

- *The Enterprise Risk Management Framework issued in 2004 by the Committee of Sponsoring Organizations of the Treadway Commission (US). This can be obtained (for a fee) from www.coso.org*
- *The Australia/New Zealand Risk Management Standard AS/NZS 4360: 1995. This can be obtained (for a fee) from www.standards.com.au*
- *The Japan Industrial Standard JIS Q 2001 - Guidelines for development and implementation of a risk management system. This can be obtained (for a fee) from www.jsa.or.jp*
- *British Standard BSI 6079-3: 2000 Project Management – Part 3: guide to the management of business related risk. This can be obtained (for a fee) from www.bsonline.techindex.co.uk*
- *The Integrated Risk Management Framework, Treasury Board of Canada, 2001 available at www.tbs-sct.gc.ca*
- *The DFID Risk Management Policy Framework, November 2002, available at www.dfid.gov.uk*
- *The Code of Corporate Practices and Conduct, King Report on Corporate Governance, Institute of Directors in Southern Africa, March 2002. A copy of the executive summary is available at www.eccg.org (codes and principles – country documents – South Africa)*





Enterprise Risk Management

THE NATURE OF OPPORTUNITIES AND RISKS

Because of the uncertainty that is intrinsic to any endeavor, all enterprises are presented with both opportunities and risks in the achievement of their objectives. CGIAR Centers, while relatively small entities by such measures as number of staff or size of budget, have challenging missions that must be delivered in an increasingly complex environment.

There are opportunities to be tapped which could produce breakthroughs in many of the scientific problems of being researched by the Centers, or which may 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. Risk management is all about getting better at grasping the opportunities, understanding the possible causes of failure, and managing them so as to minimize them or at least mitigate their impact on the Center when they occur.

Consider the following aspects of the environment in which CGIAR Centers operate, to appreciate the type of challenges management face and the importance of effective risk management to meet those challenges:

- scientific research needs to flourish in an environment that supports innovation and experimentation, as well as meeting a level of quality expected of an international scientific research institution;
- there are shifting views about what constitutes the particular global public goods that the Centers are best positioned to deliver, as the roles and capacities of national institutions and the private sector changes in different aspects of agricultural research, and as donor interests evolve.
- there are growing constraints on the ownership and use of intellectual property and biological materials;
- there are increasing concerns about biosafety and other health and safety issues associated with agricultural research activities;
- Centers are moving to decentralize more of their operations, in many cases to very widely dispersed locations around the world;
- there is political and social instability in many of the areas of the world in which Centers operate;
- there are variations in the privileges and immunities granted by host countries to the Centers in various locations
- Centers are now placing major reliance on information technology and global connectivity to operate effectively;



- The financial environment is becoming increasingly uncertain, wherein a major proportion of Center budgets are now financed from restricted grants, and the maintenance of long term unrestricted funding at historic levels is no longer a certainty.

Not only must CGIAR Centers be internationally recognized centers of scientific research excellence; they must be adept managers of as complex a set of continually evolving opportunities and risks as any faced by any major international enterprise.

RISK: A THREE-PART DEFINITION

One of the challenges of discussing risk management is that the term “risk” carries with it multiple meanings, relevant in different contexts. A 1999 study prepared by PricewaterhouseCoopers for the International Federation of Accountants provides a useful guide to the distinct senses of the term “risk” when used in a management context: risk as opportunity, risk as hazard or threat, and risk as uncertainty. The IFAC study’s definitions are reproduced below.

Risk as opportunity is implicit in the concept that a relationship exists between risk and return. The greater the risk, the greater the potential return, and, necessarily, the greater the potential for loss. In this context, managing risk means using techniques to maximize the upside within the constraints of the organization’s operating environment, given any limitations associated with having to minimize the downside.

Risk as hazard or threat is what managers most often mean by the term. They are referring to potential negative events such as financial loss, fraud, theft, damage to reputation, injury or death, systems failure, or a lawsuit: the downside. In this context, managing risk means installing management techniques to reduce the probability of the negative event without incurring excessive costs or paralyzing the organization.

A third view embraces the more academic notion of risk as uncertainty. This refers to the distribution of all possible outcomes, both positive and negative. In this context, risk management seeks to reduce the variance between anticipated outcomes and actual results.



Box 1. Opportunities: a CGIAR Center view

Just as Centers must be alert to existing or emerging hazards to their operations, so should they be alert to new opportunities that present themselves as the environment changes. Some examples to illustrate:

- Adopting new scientific approaches available through advances in biotechnology may result in major research breakthroughs.
- Political developments in the regions in which the Centers work may present new opportunities to assist with post-conflict reconstruction of national agricultural research systems and the agricultural genetic resource base.
- Broader connectivity and accessibility by outside parties to Center information resources may accelerate problem solving and dissemination of research results.
- Streamlining control procedures and decentralizing authority may produce significant cost savings, particularly where staff costs are rising.
- Greater collaboration with the private sector and advanced research institutions may provide low cost access to expensive research facilities and specific scientific expertise needed to tackle major problems.

The three-part definition of risk above implies that risk management, in the full sense, is therefore not just about “avoiding things that go wrong” but also about “helping to make things go right”. Or in the words of the IFAC study, it is about seeking the upside (“performance”) while managing the downside (“conformance”).

THE CONCEPT OF “ENTERPRISE-WIDE RISK MANAGEMENT”

While risk management has a dual aspect – managing opportunities as well as risks, it has been the series of spectacular private and public sector failures, in recent years and in a number of countries, that have spurred the latest efforts to develop more effective approaches to enterprise-wide risk management. These efforts complement the attention that has been given by professional and standard-setting organizations to risk management in specific areas such as biosafety, information technology security, electronic funds transfers, and occupation health and safety. As a result various risk management regulations, standards and guidelines which have emanated have tended to focus more on the management of hazards or uncertainties.



The Enterprise Risk Management (ERM) Framework issued in Exposure Draft form in July 2003, and subsequently issued in final form in 2004, by the Committee of Sponsoring Organizations of the Treadway Commission¹ (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 appetite², to provide reasonable assurance regarding the achievement of entity objectives.”

THE CASE FOR ENTERPRISE-WIDE RISK MANAGEMENT

The COSO ERM Framework makes a number of points that are pertinent to justifying and explaining the adoption of enterprise-wide risk management processes. These are summarized or modified below for a CGIAR Center context.

Value of an enterprise-wide risk management process

An effective enterprise-wide risk management process should help Centers deal with uncertainty and proactively respond to both risks and opportunities, by:

- Establishing a basis for more explicit consideration of the acceptable levels of risk (the “risk appetite”) in the Centers’ strategy and objective setting.
- Providing the rigor expected of an international public organization to identify and select among alternative risk responses – risk avoidance, reduction, sharing and acceptance.
- Enhancing the capability to identify potential events, assess opportunities and hazards and establish responses, thereby reducing the occurrence of surprises and related costs or losses.
- Understanding interrelated impacts of risks in different areas. Risks for individual units may be within the units’ risk tolerances, but taken together may exceed the risk appetite of the Center as a whole.
- Providing integrated solutions for managing the risks. An integrated approach uses a common language, shared tools and techniques.

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

² 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.



- Enabling management to gain an understanding of how certain events represent opportunities, which may be seized.
- Incorporating analysis of risks that are shared with other Centers and entities external to the CGIAR, whose management may be through joint mechanisms such as System Office components, System-wide Program and Challenge Program governance structures, and outsourcing (e.g. internationally recruited staff payroll and benefits administration, electronic mail services).
- more effectively assessing overall resource needs and improve resource allocation.

Relationship with corporate governance

Enterprise risk management is interrelated with corporate governance. Governing boards are responsible for ensuring that their organizations have adequate mechanisms to manage opportunities and risks. Enterprise risk management assists by providing information to Boards on the most significant risks and how they are being managed.

For public and private sector organizations in a number of CGIAR member countries, it is now becoming mandatory for their Boards to report publicly on the status of risk management and internal control measures in the organizations, and in some cases (especially as it relates to risks over financial reporting) to have this independently audited³. Donors are encouraging CGIAR Centers to implement public reporting on risk management. Options for Board/Center reporting on the management of risks and internal controls are discussed in a later section of this note and in more detail in a separate Discussion Note.

Taking a “portfolio” view of risk

Enterprise risk management requires an entity to take a *portfolio view* of risk. This might require that each manager who is responsible for a business unit, function, process or other activity within a Center should develop an assessment of risk for the unit. The assessment may be quantitative or qualitative. With a composite view at each succeeding level of the Center, senior management is positioned to make a determination whether the Center’s overall risk profile is commensurate with its risk appetite.

³ See for example, Section 404 of the United States Sarbanes-Oxley Act 2002



Reasonable assurance

Effective enterprise risk management can be expected to provide reasonable assurance of achieving objectives relating to the reliability of reporting and to compliance with laws and regulations. Achievement of those categories of objectives is within the Center's control and depends on how well the Center's related activities are performed. However, achievement of strategic and operational objectives is not always within the Center's control. For these objectives, enterprise risk management can provide reasonable assurance only that management, and the Board in its oversight role, is made aware, in a timely manner, of the extent to which the Center is moving toward achievement of the objectives.

Box 2 - The Case for "Integrated Risk Management" – A Canadian Perspective

Integrated risk management is a continuous, proactive and systematic process to understand, manage and communicate risk from an organization-wide perspective. It is about making strategic decisions that contribute to the achievement of an organization's overall corporate objectives.

Integrated risk management requires an ongoing assessment of potential risks for an organization at every level and then aggregating the results at the corporate level to facilitate priority setting and improved decision-making. Integrated risk management should become embedded in the organization's corporate strategy and shape the organization's risk management culture. The identification, assessment and management of risk across an organization help reveal the importance of the whole, the sum of the risks and the interdependence of the parts.

Integrated risk management does not focus only on the minimization or mitigation of risks, but also supports activities that foster innovation, so that the greatest returns can be achieved with acceptable results, costs and risks. Integrated risk management strives for the optimal balance at the corporate level.

Source: Integrated Risk Management Framework, Treasury Board of Canada, 2001 available at www.tbs-sct.gc.ca

THE KEY ELEMENTS OF A CENTER-WIDE INTEGRATED RISK MANAGEMENT PROCESS

The first technical standard on risk management is AS/NZS 4360:1995, issued jointly by the Australian and New Zealand national standards organizations. At this time there is no general ISO standard on this topic produced by the International Standards Organization, and the AS/NZ standard provides a useful and straightforward general framework for considering the elements of an integrated risk management system. The AS/NZ standard identifies six key elements of a risk management process:

- Establish the context
- Identification of risks



- Risk analysis
- Risk evaluation
- Risk treatment
- Monitoring and review

The COSO ERM Framework identifies eight components of enterprise risk management:

- Internal environment
- Objective setting
- Event identification
- Risk assessment
- Risk response
- Control activities
- Information and communication
- Monitoring

Frameworks and guidelines issued in Canada, the United Kingdom, Japan and South Africa⁴ identify variations of these. This section attempts to synthesize the information contained in these various sources, in a manner relevant to CGIAR Centers, using the A/NZS standard components as the overall organizing principle.

Establish the Context

Good practice

Consider risks and opportunities across all the activities of a Center, taking into account both the external and internal environment in which the Center operates

⁴ Since the AS/NZS standard was issued, the Canadian Standards Association has published CAN/CSA-Q850-97, the British Standards Institute has published BSI 6079-3:2000 and the Japanese Standards Association has published JIS Q 2001. Government Treasury Boards in Canada and the UK have also since issued guidelines on risk management.



An effective risk management process should identify the strategic and organizational context under which an organization operates, to ensure that it is applied comprehensively. A broad understanding of the operating environment is an important first step in developing the corporate risk profile.

A broad view of opportunities and risks should be taken by Centers, which includes such dimensions as:

- financial
- operational
- human resources
- environmental/physical
- host country
- donors
- partners
- suppliers
- impact
- safety
- legal
- reputational

External influences that can affect opportunities and risks for the Centers should be considered in a systematic way. The Canadian Treasury Framework recommends an external “environmental scan” as part of the risk management process. Key external and internal factors and risks that influence the organization’s policy and management agenda are identified. Identifying major trends and their variation over time is particularly relevant in providing potential early warnings. Some external factors that the Canadian Treasury Framework identifies for consideration of potential risks include:

- Political: the influence of international governments and other governing bodies;
- Economic: international and national markets, globalization;
- Social: major demographic and social trends; and
- Technological: new technologies.



Box 3. Context for Risk Management – Points to consider

Is the context in which risk is managed identified by considering the issues of

Stakeholders, including

Public interests?

Service user interests?

Wider societal interests?

Risk aspects of relationships inside and outside of [the Center] including key suppliers of goods and services), including:

Ways in which the behavior of “partners” affects [the Center]?

Ways in which the behavior of [the Center] affects the “partners”?

The risk priorities of “partners”?

Adapted from UK Treasury guidance material.

Good practice

Promote, through clear policies and procedures, awareness-raising activities, and senior management emphasis, an internal environment that supports proactive risk management at all levels

The COSO ERM Framework notes that the entity’s internal environment is the foundation for all other components of enterprise risk management, providing discipline and structure. The internal environment comprises many elements, including an entity’s ethical values, competence and development of personnel, management’s operating style and how it assigns authority and responsibility. The governing board (Board of Trustees in the CGIAR context) is seen as a critical part of the internal environment and significantly influences other internal environment elements. Championship of risk management initiatives by Board members is a critical success factor for their implementation.

As part of the internal environment, management establishes a risk management philosophy – the entity’s beliefs about risk and how it 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.



Management policies should describe the risk management strategy, including:

- the attention and commitment of the Board and management of the Center
- the scope of risk management activities
- approach to risk appetite
- risk management framework, processes and procedures applicable to all risk management and opportunity assessment activities in the Center
- roles and responsibilities for risk management, including “risk ownership”
- new staff orientation and methods for keeping staff aware of risk management responsibilities
- communication channels for management and staff to discuss risks, report concerns and lessons learned about specific risks and opportunities; and
- documentation and reporting requirements.

The policies should apply to all areas and entities within the organization and the implementation of the policies should be the responsibility of all managers and staff.

The OECD Principles of Corporate Governance⁵ identifies that reviewing and guiding 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.

Boxes 4-6 which follow provide some useful references from which a general Center policy on risk management can be drawn.

⁵ OECD Principles of Corporate Governance 2004, available from www.oecd.org



Box 4. Establishing the environment for risk management – a South African corporate perspective

The Code of Corporate Practices and Conduct contained in South Africa's 2002 King Report, which predates the COSO Exposure Draft, sets out a number of similar requirements relevant to creating an environment conducive to effective risk management:

- The board should set the risk strategy policies in liaison with senior management.
- These policies should be clearly communicated to all employees to ensure that the risk strategy is incorporated into the language and culture of the company.
- The board must decide the company's appetite or tolerance for risk.
- The board has the responsibility to ensure that the company has implemented an effective ongoing process to identify risk, to measure its potential impact against a broad set of assumptions, and then to activate what is necessary to proactively manage these risks.

The Code also envisages that a Board committee should assist the Board in reviewing the risk management process and the significant risks facing the company.

Source: The Code of Corporate Practices and Conduct, King Report on Corporate Governance, Institute of Directors in Southern Africa, March 2002.

Box 5 - Leadership and Strategy – Points to consider

Is there a risk strategy which:

- Is endorsed by the ... Board / Audit Committee / Risk Committee?
- Sets out the organization's attitudes to risk?
- Defines the structures for the management and ownership of risk and for the management of situations in which control failure leads to material realization of risks?
- Specifies the way in which risk issues are to be considered at each level of business planning ranging from the corporate process to the setting of individual staff's objectives?
- Specifies how new activities will be assessed for risk and incorporated into risk management structures?
- Ensures common understanding of terminology used in relation to risk issues?
- Defines the structures for gaining assurance about the management of risk?
- Defines the criteria which will inform assessment of risk and the definition of specific risks as "key"?
- Defines the way in which the risk register and risk evaluation criteria will be regularly reviewed?

Whether the strategy is set out in a single document or in a series of related documents or resources, is it easily available to all staff and reviewed at least annually to ensure it remains appropriate and current?

Adapted from UK Treasury guidance material



Box 6 - Example of the “strategy” component of a risk management policy document – from DFID

“1.3 Key elements of DFID's policy towards risk are:

- a) that we are averse to risks that would impact adversely on DFID's reputation or the quality of our financial management;
- b) that we are increasingly ready to allocate financial resources to activities which have a high risk of not achieving their objectives, provided that the potential benefits of success (e.g. in contributing to the achievement of the Millennium Development Goals) are proportionately high and that the risks are managed sensibly;
- c) that we want to encourage a greater risk appetite in some front line policy/spending departments, in particular to incentivise more innovation and experimentation
- d) that we consider it is important to enhance our capacity to both rigorously assess and manage risks.
- e) that we want to decentralize risk management as far as possible. So the Management Board focuses on risks to reputation and organizational capability to achieve our high level goals; Directors focus on risks to the achievement of the PSA and other targets for which they are responsible; and individual Departments/Offices on risks related to spending or policy they are responsible for.

1.4 Further work is planned to enable the Management Board to provide the Department with a clear statement on the levels of risk appetite that they expect to be tolerated in different parts of the Department to ensure delivery.”

Source: DFID Risk Management Policy Framework, November 2002, DFID Management Board, available at www.dfid.gov.uk

Drawing on the international guidance referred to in this Note, the CGIAR Internal Auditing Unit has developed templates for the Centers to use in preparing their own general risk management policy.

Good practice

Ensure that clear business objectives are set for Center business units and programs, so that risks can be readily identified and assessed

The COSO ERM Framework notes that objectives must exist before management can identify events potentially affecting their achievement. Effective enterprise risk management is predicated on organizations having a process to both set objectives and align the objectives with the entity's mission/vision and ensure these are consistent with the entity's risk appetite.



According to the COSO Framework, the Center's objectives can be viewed in the context of the following four categories:

- Strategic – relating to high-level goals of the Center and the types of business activities in which the Center chooses to engage. Strategic objectives include supporting business sustainability under normal and adverse operating conditions, and behaving responsibly towards all stakeholders (two key objectives separately flagged by South Africa's King Commission)
- Operations – relating to effectiveness and efficiency of the Center's operations, including performance and financial goals. They vary based on management's choices about structure and performance.
- Reporting – relating to the effectiveness of the Center's reporting. They include internal and external reporting and may involve financial or non-financial information.
- Compliance – relating to the Center's compliance with applicable laws and regulations.

To these four can be added a fifth (sometimes counted under either “operations” or “reporting”):

- Safeguarding of assets – viewed broadly, this deals with prevention of loss of a Center's assets or resources (including information assets), whether through theft, waste, inefficiency or what turns out to be simply bad business decisions.

The CGIAR Internal Auditing Unit has developed, with inputs from the Centers, a proposed analytical framework for thinking about a Center's business objectives. Using the framework, a set of high level common business objectives, applicable to all Centers, has been identified – see Exhibit 1 below.



Exhibit 1 – Business Objectives: A Proposed Analytical Framework for CGIAR Centers

A Center seeks to achieve its vision and mission through the application of various resources and in the context of an external environment. These resources can be classified for analytical purposes into those shown in the circular diagram below. In applying those resources and interacting with the external environment, the Center seeks to achieve various business objectives and manage the associated risks. These business objectives can be broadly classified for analytical purposes into the five categories shown in the boxes below the diagram.





Using the analytical framework, the following common high level Center business objectives have been identified. Each of these objectives can be broken down into more detailed objectives specific to each Center.

Effectiveness
Relevance of Center research mission
Achievement of Center research mission
Protection and effective use of germplasm collections
Integrity and security of information
Continued operations in the event of significant natural, political, social and other disruptions
Efficiency and Economy
Efficient and economical use of funds
Protection of Center physical property
Protection of Center data and intellectual property rights/ protection against third party restrictions on use
Financial Integrity and Compliance
Adequate funds to meet medium term plans and short term obligations
Compliance with financial obligations to staff
Compliance with external financial reporting obligations
Legal and other Compliance
Compliance with host country agreements
Compliance with donor agreements
Compliance with partnership and other third party legal obligations
Compliance with data privacy laws and standards
Integrity in the management of resources
Breaches of research ethics
Partnerships apply the same level of compliance
Safety and Security
Safe working environment for staff and visitors
Safe products (e.g. novel food products, transgenic varieties, farming technologies)
Staff and families adequately equipped to deal with health problems in Center locations
Safe staff travel
Avoid environmental damage from Center operations
Center premises secure against unauthorized intrusion



Good practice

Identify a point of coordination within the Center, which can assist the director general to integrate the results of various risk management activities across the Center

A risk management coordinator or staff committee provides a focal point within the Center for integrating the results of risk management activities throughout the Center and supports management and the Board in the preparation of Center-wide assessments and reporting (see box 8 below for suggestions for a terms of reference).

Box 7 – Risk Management Coordinator or Committee – Possible Items for a Term of Reference

- Develop for the Director General (DG), Management Team (MT) and Board approval, the center's risk management framework and formulate policies, procedures, and documentation related to risk management.
- Advise the DG and MT on risk management issues.
- Encourage the development of a culture of risk awareness and risk management in all staff and the integration into business processes of the identification, analysis and monitoring of key risks and opportunities at process/unit and center level through information and presentation to staff.
- Oversee a program of unit level risk assessment, whereby unit managers and staff review the principal areas of risk relating to their units, activities, and objectives and consider the likelihood and exposure of the center to these risks.
- From a center wide perspective, review with senior managers the principal areas of risk within the center and consider the likelihood and exposure of the center to these risks. Integrate into this analysis unit level risk assessments.
- Prepare for the DG/MT status reports on the implementation of the risk management system within the Center. These reports would support management reports to the Board and an annual board statement.

Either coordination approach, via an individual or committee, can be effective, and there has been some variety of practice across the Centers.

Identification of Risks

Good practice

Integrate into the Center's regular business processes steps whereby the key risks and opportunities at process, unit and Center levels are considered, and are inventoried for assessment and monitoring



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:

- control and risk self assessment exercises
- interviews and surveys of stakeholders;
- the use of checklists of standard risks, SWOT (Strengths/ Weaknesses/ Opportunities/ Threats) 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 reengineering. 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 and Management Reviews
- advice from CGIAR System Office units such as the Chief Information Officer, the Strategic Advisory Service on Human Resources, the Central Advisory Service for Intellectual Property or the Gender and Diversity Program, as well as the CGIAR Internal Auditing Unit
- CGIAR-wide and donor discussions
- Confidential reporting (“whistle blowing”) processes

The Japanese risk management standard makes the point that staff should be encouraged to be open in their discussions on risk and not be penalized for expressing their views. The standard also notes that preconceptions can be a barrier to effective risk identification and analysis. The approach (es) adopted by an organization to identify (and analyze) risks should encourage imagination and a willingness to overcome standard patterns of thought. As one commentator on risk management has put it, it should



be “capable of addressing uncomfortable uncertainties and deep seated working assumptions, overcoming the psychological and institutional need to fit recalcitrant phenomena into well tried, incrementally adjusted, linear frameworks of understanding”⁶. Managers and staff should feel empowered to raise questions about risk and propose solutions where they feel that opportunities and hazards are not being addressed adequately within the organization.

Box 8 - Internal audit risk identification and analysis

International internal auditing standards require that internal auditors prepare their audit engagement plans based on a risk assessment, undertaken at least annually. The standards also provide that the internal audit activity should assist the organization by identifying and evaluating significant exposures to risk.

In preparing and updating the medium term internal audit plans for Centers it works with, the CGIAR Internal Audit Unit undertakes:

- a series of interviews with key managers and staff to help identify the key areas where risks are felt to significant in terms of likelihood and impact, or where there appear to be significant opportunities to improve operations;
- follow up of past audits and
- examination of other reviews and analyses undertaken within the Centers.

Internal audit assessments at the work planning phase, as well as in audit reports issued during the year, are one source of risk management information for Centers. The IAU is reviewing the formats of the detailed documentation supporting its medium term audit plans to ensure that this documentation can support future Center-managed risk management efforts.

At the same time, once the first full Center-wide risk analyses are completed by management, these analyses and their future updates will form the basis for future internal audit work prioritization and audit work plans will need to show their linkage to the Center-wide risk assessments.

⁶ “The Risk Management of Everything: Rethinking the politics of uncertainty”, Michael Power, Demos 2004 (available from www.demos.co.uk)



Table 1. Typical enterprise-level risks for CGIAR Centers

Business objectives	Risk	Principal Related Business Activities/Processes
Effectiveness		
Relevance of Center research mission	Research has limited or no impact in addressing the problem or issue identified	Research planning and priority setting; Project activity management
	Poor quality of research activities	Project activity management
	Inadequate dissemination of research results	Project activity management
	Mismatch of skills with business needs	Human resources management
	Inability to attract or retain appropriate staff	Human resources management
	Erosion of professional staff scientific skills	Human resources management
	Research data lost or difficult to access	Management of research data
	Research partner's failure to deliver requirements	Management of research partner agreements
	Poor-quality research publication	Project activity management
	Scientific fraud	Project activity management
Protection and effective use of germplasm collections	Loss of genebank accessions due to poor handling, environment or physical security, or contamination during regeneration	Genebank operations
Continued operations in the event of significant natural, political, social and other disruptions	Disaster significantly disrupts Center's operations	Business continuity planning; IT management
Efficient and economical use of restricted and unrestricted funds	Duplication of research activities	Project Activity Management; Management of Research Data
	Mismatch between research priorities and budgets	Budgeting process



Business objectives	Risk	Principal Related Business Activities/Processes
	Inefficient farm operations	Farm labor management system; distribution/sale of farm production
	Inefficient food and housing operations	Food and housing services
	Inefficient transport operations	Transport services
	Inefficient and unfavorable contracting process	Private sector partnership; Management of research partner agreements
	Insufficient funds to meet operations	Donor fund raising and contracting; management of liquid assets; outreach offices (financial management)
	Institute paying more for external goods and services than it requires or can get in the market	Procurement (HQ and outreach offices); travel process
Efficient financial management	Inefficient financial systems	Financial systems renewal project
Protection of Center physical assets	Misuse, loss, or lack of maintenance of Center property	Management of tangible assets (HQ and outreach offices); management of Physical plant services; Distribution and sale of farm product
Protection of Center data and intellectual property rights / protection against third party restrictions on use	Intellectual Property disputes	Management of Research Data; Receipt, Storage and Distribution of Genetic Materials; Private Sector Partnerships; Management of Research Partner Agreements;
	Misuse of Center IT resources	IC T management



Business objectives	Risk	Principal Related Business Activities/Processes
Financial integrity and compliance		
Adequate funds to meet medium-term plans and short-term obligations	Missed funding opportunities/insufficient project pipeline	Donor fund raising and contracting
	Failure to tap funds (and research opportunities) from Challenge Programs and other System-Wide Programs	Donor fund raising and contracting
	Inadequate reserves for medium-term liquidity	Management of liquid assets
	Cash flow (liquidity) problems; inability to pay debts on time	Management of liquid assets
	Inadequate financing of institutional overhead items from restricted projects	Project cost allocation
	Surprise significant over-or under expenditures	Budgeting process
	Significant foreign exchange losses	Management of liquid assets
	Significant loss of funds due to poor investment decisions	Management of liquid assets
	Significant loss of funds due to bank failures	Management of liquid assets
	Misappropriation or misuse of Center cash funds	Management of liquid assets; Outreach offices (financial management)
	Unauthorized/inaccurate disbursements	Accounts payable/receivable; management of liquid assets
	Opportunity costs of long outstanding receivables	Accounts payable/receivable
Compliance with financial obligations to staff	Poor management or mismanagement of payroll and staff benefits	Human resources management



Business objectives	Risk	Principal Related Business Activities/Processes
Compliance with external financial reporting obligations	Financial reporting (restricted project and Center) is materially incorrect	Financial systems renewal project; Accounts payable/receivable; Financial statements
	Financial disclosures not in accordance with standards applying to international public sector organizations	Financial statements
Legal and other Compliance		
Compliance with host country agreements	Non-compliance with host country requirements	Human Resources management; Outreach Offices (administration)
	Loss of host country privileges and immunities	Host country relationship management
Compliance with donor agreements	Non compliance with donor agreements	Donor reporting; Project activity management
Compliance with partnership and other third part legal obligations	Failure to meet contractual obligations to partners	Management of Research Partner Agreements
	Use of illegal software	IT Management
	Non compliance with international undertakings on germplasm transfers	Receipt Storage and Distribution of Genetic Materials
Compliance with data privacy laws and standards	Breaches of privacy laws leading to institutional and personal penalties; data withheld due to lack of confidence in how it will be handled	IT Management, Management of Research Data
Breaches of research ethics	Center fails to observe internationally accepted or contractually binding ethical research standards (e.g. informed consent, handling of traditional knowledge)	Project Management



Business objectives	Risk	Principal Related Business Activities/Processes
Partnerships apply the same level of compliance	Center suffers reputation losses or has to spend resources as a result of partners associated with it in collaborative activities not complying with requirements to the same standard as expected of the Center (e.g., germplasm distribution, IP safeguarding, data privacy, host country requirements, research ethics standards)	Management of Research Partnership Agreements
Integrity in the management of resources	Transactions involving conflict of interest	Procurement; Accounts Payable/Receivable
Safety and Security		
Safe working environment for staff and visitors	Hazardous working conditions (farms, stores, workshops, laboratories, offices, official vehicles, sports facilities, campus grounds)	Occupational Health & Safety / Biosafety Processes
	Staff caught up in civil disruption	Security
Safe products (e.g. novel food products, transgenic varieties, farming technologies)	Litigation over research product performance (e.g. germplasm quality, health claims, farming technology)	Project Management; Biosafety management
Staff and families adequately equipped to deal with health problems in Center locations	Staff downtime due to preventable or treatable medical conditions	Occupational Health & Safety
Safe staff travel	Staff exposed to dangerous travel conditions	Travel, Security
Center operations are safe for the surrounding environment	Environmental damage impacts from chemicals, pesticides and GMO releases	Environmental / Biosafety management
Center premises secure against unauthorized intrusion	Damage or theft of Center property by intruders	Security



Table 1 above lists, for the main types of business objectives of a Center (see Exhibit 1 earlier in this Note), typical Center or unit level risks, and activities/processes through which the risks are managed. This list of risks has been prepared by the CGIAR Internal Auditing Unit based on experience to date in the Centers as well as drawing on its own research. Each of these risks can be broken down into multiple sub-risks for further analysis. Other IAU Good Practice Notes and risk analysis templates provide guidance to Centers on this more detailed analysis for selected risks, and good practices and lessons learned concerning their management.

Note that the Table does not show reputational risk as a separate risk. Rather, it is a by-product of other risks not being adequately controlled e.g. irrelevant research, scientific fraud, financial mismanagement, non compliance with donor or host country agreements. Reputational risk can render the concept of materiality obsolete: isolated or financially immaterial events may have a big significance to an organization's reputation, particularly if amplified by media attention. Reputational risk management should really be a by-product of the management of the primary risks of an organization and not become an end in itself⁷.

Good practice

Identify, through a collaborative process with other Centers and System Office components, those risks that are shared across the CGIAR System

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;
- System Office Unit collaborations, such as those between the IAU and the ICT-KM Program, the Gender & Diversity Program, the Strategic Advisory Service on Human Resources, and the Central Advisory Service on Intellectual Property
- Communities of practice such as the Information Technology Managers group and the System-Wide Group on Genetic resource Conservation, which have adopted common frameworks for the identification and analysis of ICT and genebank related risks respectively

⁷ Power, "The Risk Management of Everything"



There are also risks that are shared collectively with other Centers, with System Office components 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 CGIAR Secretariat using World Bank trust fund management processes;
- Joint ventures in the form of Challenge Programs and other System-wide research activities;
- 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; and
- Joint outsourcing of electronic mail, web hosting and other information and communications technology services.

Risk Analysis/Evaluation

Good practice

Consider how the identified risks might affect the achievement of business objectives from two perspectives: the impact of failure on the Center's objectives should it occur, and the likelihood of occurrence and damage in such an event

“Impact” (or consequence) represents the effect on the organization or unit should a 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.

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), but 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. In any case, the methods used at a Unit level should facilitate the Center's overall assessment of risks across the organization.

So far, most Centers have opted for a 3-part “high”, “medium” and “low” qualitative scale in their risk assessments. One Center has opted for a 5-part qualitative scale, but beyond a scale of 3 this requires that the initial qualitative assessment is then converted into a numeric score to prioritize the risk rankings. In either case the Centers have, with the encouragement of the CGIAR Internal Auditing Unit, kept their approaches relatively simple, so that the initial phase of introducing an explicit Center-



wide risk assessment does not get bogged down in complexity. Some external organizations use larger quantitative scales (such as 1-10), and the usefulness of this may be considered by Centers once the risk management has been adequately bedded down in their organizations.

Box 9 – Suggested definitions for a 3-part Qualitative Ranking of “Impact”

High – failure has the potential to significantly damage or destroy the effective functioning of the Center or its future viability, particularly through loss of important donors’ confidence or major financial or reputational loss. Also could include potentially significant employee health and safety hazards

Medium – failure has the potential to damage important aspects of the Center’s functions or future viability, which would require significant management effort and time to recover

Limited – failure has the potential to damage particular aspects of the Center’s functions, drawing on significant management effort if an adverse event occurred, but not expected to damage the overall medium-long term operations of the Center.

Box 10 – Suggested definitions for a 3-part Qualitative Ranking of “Likelihood”

High – The risk mitigating actions taken by the Center – in terms of (i) avoidance of certain activities, (ii) controls (such as policies, procedures, clarity of responsibilities, training, management monitoring and information), and/or (iii) insurance arrangements – are not considered sufficient or controls are not yet operating effectively, and the probability of occurrence of adverse events for the Center is therefore considered high (>50% probability i.e. more likely than not) over the short-medium term.

Medium – The risk mitigating actions taken by the Center are partial and there are further opportunities in terms of action the Center should take, or are planned but not yet fully implemented. As a result probability of occurrence of adverse events for the Center is therefore considered moderate (25%-50% probability) over the short-medium term.

Low – The risk mitigating actions taken by the Center are sufficiently designed and operating effectively to reasonably protect the Center against foreseen adverse events.

Ranking according to impact and likelihood may be done participatively using polling methods in control and risk self-assessment workshops, where staff (and possibly other stakeholders) are asked to rank according to a numeric scale.

Thinking about risk in terms of impact and likelihood helps identify the appropriate level of effort that should be made to put in place preventive or corrective internal controls, as illustrated in the matrix below taken from the Canadian Treasury Framework:



Impact	Risk Management Actions		
Significant	Considerable management required	Must manage and monitor risks	Extensive management essential
Moderate	Risks may be worth accepting with monitoring	Management effort worthwhile	Management effort required
Minor	Accept risks	Accept, but monitor risks	Manage and monitor risks
	Low	Medium	High
	Likelihood		

The analysis of likelihood may be further refined. One Center has broken down its likelihood analysis into two parts: (a) likelihood of occurrence after considering preventive controls as designed and operating and (b) likelihood of damage if a failure still occurs, after considering impact mitigating actions (such as insurance, contingency planning, and backup and recovery mechanisms).

Some Centers have suggested that it would be useful to distinguish, in the likelihood analysis, between:

- those risks where failure would be sudden or quickly apparent; and
- those risks where failure might arise gradually, from a build up of a steady occurrence of small failures (e.g. quality failures within the research portfolio or partnerships), or a steady decline in such factors as donor confidence or host country relations.

This distinction is seen as helpful to the process for prioritizing management attention.

Good practice

Evaluate the Center-wide significance of risks identified at unit/activity level

While many Centers, in the initial phase of implementing a Center-wide risk management system, have opted to start with a “top down” approach – i.e. having individuals or committees undertake the initial identification of those risks most relevant to the Center as a whole – some have implemented more “bottom up” approaches wherein individual Units prepare risk assessments which address both Unit-level and institutional risks. Both approaches have their merits, though eventually Centers should implement a combination of both in order to get the full benefit of investing in a formalized and



systematic risk management framework. These assessments need to be reviewed to ascertain the significance of these risks for the institution.

Evaluation takes the initial analysis and reviews it against the Center's known priorities and requirements. Management may 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.

Management should consider the positive and negative consequences of potential events, individually or by category, across the entity.

Good practice

Evaluate, through a collaborative process with other Centers and System Office components, identified shared risks

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.

Good practice

Evaluate trends in risk impact and likelihood

As Centers move from initial Center-wide assessments to a regular cycle of updates, Board and management will be interested in trends. Impact assessments may change due to changing business conditions. Likelihood trends will be of particular interest as it will signal progress in implementing mitigation plans. So far, many Center Boards have indicated that they expect to see trend information on the major, identified risks in future risk assessment reports.

Risk Treatment

Good practice

Establish an oversight process for ensuring that there are clear management responses for all identified risks where likelihood and impact are rated as significant

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.

Box 11 - Risk Analysis – Points to consider

- [Are risks analyzed] using defined criteria which are applied consistently?
- [Is there an] evaluation of inherent risk (before any control implemented) and residual risk (risk remaining after planned controls are implemented)?
- [Does the analysis take] account of both
 - the likelihood of the realization of the risk, and
 - the impact of the realization of the risk?
- [Does the risk analysis identify] assigned ownership of the risk at a level or grade with sufficient authority to assign appropriate resources to control the risk?
- [Does the analysis record], in as far as it can be defined,
 - the acceptable level of exposure in relation to each risk?
 - why it is considered that the defined acceptable level of exposure can be justified?
- Do specific criteria for evaluating risk encompass a range of factors, including:
 - Financial / value-for-money issues?
 - Service delivery / quality of service issues?
 - Reversibility or otherwise of the realization of the risk?
 - The quality or reliability of evidence surrounding the risk?
 - The impact of the risk on the organization / stakeholders / partners / others?

Adapted from UK Treasury guidance material

Business continuity planning (BCP) is a form of corrective control, designed to minimize the impact of continuity risks should they materialize. BCP includes insurance (to minimize financial impacts), safety backup of physical assets such as germplasm collections and vital physical documents, and disaster recovery for electronic systems and data. A separate IAU Good Practice Note has been prepared on BCP.



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

Good practice

Ensure that all risk responses are implemented through appropriate control activities

An effective risk management process requires that appropriate steps (control activities) are implemented to ensure that all risk responses are implemented. These typically include:

- Processes for approving and implementing adjustment to business activities, or objectives of particular units or activities in response to assessments
- Processes for approving and implementing new or revised control activities proposed by relevant units / activity centers of the Center
- Internal review and/or internal audit of implementation measures.

Box 12 - Risk Control – Points to consider

Are controls in place in relation to each risk which are:

- Based on active consideration of the options for controlling that risk to an acceptable level of residual exposure?
- Promulgated to all those who need to know about the controls?
- Regularly reviewed to consider whether they continue to be
 - Effective?
 - The best value for money response to the risk?
- Documented by the relevant managers?

In respect of key risks, including those that lie beyond the control of the organization, are plans developed and documented contingent against the risk being materially realized despite the controls that are in place?

Adapted from UK Treasury guidance material

Good practice

Integrate risk management results into established Center policy and planning processes



The Canadian Treasury Framework makes the useful point that the results of risk management should be integrated both horizontally and vertically into organizational policies, plans and practices.

Horizontally, it is important that results be considered in developing organization-wide policies, plans and priorities. Vertically, functional units, such as branches and divisions, need to incorporate these results into programs and major initiatives.

South Africa's King Commission Code of Corporate Practice and Conduct also makes the point that risk management and internal control should be embedded in day-to-day activities.

The Canadian Treasury Framework notes that, in practice, the risk assessment and response to risk should be considered in developing local business plans at the activity, division or regional level. These plans would then be considered at the corporate level, and significant risks (horizontal or high-impact risks) would be incorporated into the appropriate corporate business, functional or operational plan.

Monitoring and Review

Good practice

Document the results of risk monitoring activities, including action taken to address shortcomings identified, and progress with mitigation plans

The COSO ERM Framework notes that monitoring can be done in two ways: through ongoing activities or separate evaluations. Monitoring ensures that enterprise risk management continues to be applied at all levels and across the entity.

Ongoing monitoring is built into the normal, recurring operating activities of an entity. Since separate evaluations take place after the fact, problems often will be identified more quickly by ongoing monitoring routines.

Separate evaluations include periodic internal and external audits, Center-commissioned external reviews, and External Program and Management 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.

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 will be essential that documentation is developed and retained to support the statements.

Documentation in standard format across a Center may be facilitated by the adoption of:

- Risk management software, which automates the rolling up of results of risk identification, analysis and evaluation activities across the Center.
- Risk registers – document formats which facilitate a summary of risk inventory and analysis by unit / activity. In the United Kingdom all Departments are required to have a corporate risk register that is regularly reviewed by the Management Board. South Africa’s King Commission also promotes the use of registers of key risks in their Code of Corporate Practice and Conduct. Risk registers may be maintained manually or via the risk management software referred to above.

Box 13 - Risk Registers – Points to consider

Does a risk register exist which:

- Records identified risks in a structured way
- Records dependencies between risks?
- Records linkages between lower level risks and higher level risks?
- Identifies key risks?
- Facilitates assignment of ownership at a level which has authority to assign resources to the management of the relevant risk?

Adapted from UK Treasury guidance material

Many of the off-the-shelf software tools currently available in the market are designed for large organizations. They can be very demanding in terms of maintenance and update. All CGIAR Centers would find it difficult to devote significant resources to maintenance of elaborate documentation systems. An in-house solution, which draws on the principles of risk management software packages but is suitably scaled to the Centers’ needs, is currently being developed by IRRI. This Center has offered to share its system software with other Centers (on an as-is basis) once it is fully tested and operational.



Box 14 - Risk Review and Assurance – Points to consider

Are review and assurance mechanisms in place to ensure that:

- Each level of management, including the Board, regularly reviews the risks and controls for which it is responsible?
- Are these reviews monitored by / reported to the next level of management?
- Is any need to change priorities or controls clearly recorded and either actioned or reported to those with authority to take action?
- Are lessons that can be learned from both successes and failures identified and promulgated to those who can gain from them?
- Is an appropriate level of independent assurance provided on the whole process of risk identification, evaluation and control?
- Is the methodology for gaining independent assurance defined with particular reference to the role of internal audit and to the role of any other review bodies working within the [Center]?

Adapted from UK Treasury guidance material

REPORTING ON RISK MANAGEMENT

Good practice

Prepare periodic, summary management reports on the results of Center-wide risk management activities

In order for risk assessment activities to be effective as high level management tools, Centers should prepare annual or semi-annual reports (the timing and frequency of which should be agreed with the Boards) which summarize the results of the implementation of the Center's risk management and internal control policy and the assessments of major risks carried out in the period. Such reports should cover such things as:

- Status of any aspects of the risk management policy where implementation has only begun or is pending
- Extent of involvement of Center staff, including those based outside headquarters
- Summary ratings of the most significant Center-level risks, e.g. those with high impact and high or medium likelihood, including trend information
- Details of mitigation action plans for these risks

Suggested formats for such reports will be the subject of a future discussion note.



Good practice

Prepare Board statements on risk assessment and internal control that are supported by the Center's internal risk management system

One key CGIAR donor has, since 2004, conditioned its (increased) unrestricted funding to the CGIAR Centers on the Boards of the Centers preparing statements on risk assessment and internal control, including alignment with CGIAR principles and guidelines. This also has potential value in giving other donors assurance and thus encouraging them to provide more unrestricted funding. But it also provides a focus for Boards to obtain assurance from Center management on the status of risk management in their Centers, and to be systematically informed of action plans in this regard.

The Code of Corporate Practice and Conduct published by South Africa's King Commission promotes public statements on risk management by corporate boards, based on a systematic documented assessment of the processes and outcomes surrounding key risks. The Code provides that the board "should, at a minimum disclose:

- That it is accountable for the process of risk management and the system of internal control, which is regularly reviewed for effectiveness and for establishing appropriate risk and control policies and communicating these throughout the company;
- That there is an ongoing process for identifying, evaluating and managing the significant risks faced by the company, that has been in place for the year under review and up to the date of approval of the annual report and financial statements;
- That there is an adequate system of internal control in place to mitigate the significant risks faced by the company to an acceptable level. Such a system is designed to manage, rather than eliminate the risk of failure or maximize opportunities to achieve business objectives. This can only provide reasonable, but not absolute, assurance;
- That there is a documented and tested process in place that will allow the company to continue its critical business processes in the event of a disastrous incident impacting on its activities;
- Where material joint ventures and associates have not been dealt with as part of the group for the purposes of applying these recommendations. Alternative sources of risk management and internal control assurance applied to these activities should be disclosed, where they exist;
- That any additional information in the annual report to assist understanding of the company's risk management processes and system of internal control should be provided as appropriate; and
- Where the board cannot make any of the disclosures set out above, it should state this fact and provide a suitable explanation."

Such a statement would be supported by the periodic management reporting recommended above. A suggested form of Board statement, and the underlying research to prepare it – undertaken by the



CGIAR Internal Auditing Unit and drawing on practice in donor agencies, other scientific research institutes and private sector organizations – has been documented in a separate Discussion Note.

Appropriate forms of communication of Board statements to donors and other stakeholders, such as in Center annual reports or similar publications, is an important consideration.

Good practice

Implement, preferably through existing internal management reporting processes, reporting by unit/activity managers on the status of risk management at their level, including changes in previously reported risk analysis and actions proposed

Boards and top management of organization who prepare enterprise-wide reports on risk management often require unit / activity managers to submit a unit / activity level statement. This provides assurance in respect of the unit / activity on the management of risk and compliance with management and control systems. It reinforces accountability for (risk) management throughout the organization, focuses attention on risk and control issues that should be communicated within the organization, and forms part of the documentation process that supports the organization's overall report.

The status reports should at least contain an evaluation of any changes in the previously reported risk analysis and the actions to manage the changes. They should also be a basis of action – where risks are deemed to be insufficiently controls, proposed mitigating measures and targets dates for implementation should be communicated in the reports.

The World Bank and DFID are two examples of CGIAR donors who implement this process on an annual basis, in conjunction with their organization's annual external reporting process. In the case of the DFID, the reports include key performance data, an outline of action planned to remedy shortfalls in expected performance and an assessment of high-level risks to achievement of their objectives.

This type of reporting can be quite complex – and uncomfortable for some – to introduce, with its explicit attention to accountability. Implementation should be accompanied by strong efforts related to communication and orientation of managers. The process also needs to be coordinated centrally, as part of the annual reporting cycle.

LIMITATIONS OF RISK MANAGEMENT

The COSO ERM Framework notes that enterprise risk management, no matter how well designed and operated, does not ensure an entity's success. The achievement of objectives is affected by limitations inherent in all management processes. Shifts in donor policy or programs, partner actions or economic conditions can be beyond management's control. Human decision-making can be faulty, and breakdowns can occur because of such human failures as simple error or mistake. Enterprise risk



management cannot change an inherently poor manager into a good one. Additionally, controls can be circumvented by the collusion of two or more people, and management has the ability to override the enterprise risk management process, including risk responses and controls. Thus, while enterprise risk management can help management to achieve its objectives, it is not a panacea.

The design of enterprise risk management must also reflect the reality of resource constraints, and the risk management benefits must be considered relative to their costs. In addition, there is always a need to balance efforts to control and manage risk with the need to maintain an environment in which opportunities (which comes attached with risks) can be grasped. Imbalance can lead, as South Africa's 2003 King Report put it vividly, to "the loss of flair when enterprise gives way to administration".

Exposure Draft: October 2003

First Update: January 2004

Second Update: July 2004

Third Update: February 2005

Fourth Update: June 2006

Author: John Fitzsimon