



Discussion paper – Center Board Statements on Risk Management

I. SUMMARY

This paper seeks to summarize the results of research, and of discussion to date with a range of financial and internal audit professionals within the CGIAR, on the most appropriate form of public reporting by Center Boards on risk management and internal control. The paper puts forward the following proposal, with a view to stimulating wider discussion among, and getting eventual agreement from, CGIAR Centers on a Board statement:

Once a risk management system is established in a Center along the lines recommended in the CGIAR Internal Auditing Unit's Good Practice Note on Center-wide Risk Management, then a statement should be prepared for and adopted by the Board on an annual basis, for public reporting purposes (included in an appropriate section of the Center's annual report or similar publication), that adopts the most useful aspects of the example statements and provides summary information on the risk management and internal control system in place in the Center.

The statement should also draw attention to:

- the Center's risk management system having been designed so the Center meets the requirements established in the risk management codes and standards promulgated, or published as exposure drafts, in a number of CGIAR member countries; and
- processes in place or proposed by which the Center collaboratively assesses, with other Centers, CGIAR System Office components and special purpose entities such as AIARC, the shared risks arising from joint activities and the activities of common service providers within the System.

A proposed form of wording is presented in the detailed discussion section of this paper.



II. DETAILED DISCUSSION

Introduction

DFID has recently encouraged the Boards of CGIAR Centers to prepare public statements on risk assessment and internal control, including alignment with CGIAR principles and guidelines. This coincides with a move in various countries to apply similar requirements to Boards of private sector companies and public institutions. Center Board statements have potential value in giving donors assurance and thus encouraging donors to provide more unrestricted funding.

The CGIAR Internal Auditing Unit's Good Practice Note on Center-wide Risk Management summarizes the results of research on standards for enterprise risk management. That Note summarizes a set of good practices drawn from a number of standards from various countries, and identifies the preparation of board statements as a good practice. The Note anticipates further research on the form of board statements, and this Discussion Paper reports the results to date of this research.

Guidelines on Board Risk Statements

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 is the most expansive of the guidelines and standards reviewed, with regards to board statements, and provides that the board "should, at at 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 maximise 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.”

Examples of Risk Statements

Practice with regard to the form of board statements was reviewed in a range of public and private sector organizations. Examples shown in Annex I are the most relevant found in terms of addressing aspects of the King Commission Code's guidance. These come from:

- Donors – the United Kingdom Department for International Development (DFID), the World Bank (IBRD), and the International Development Research Center of Canada (IDRC)
- Publicly Funded Scientific Research Organizations – the Commonwealth Scientific and Industrial Research Organization of Australia (CSIRO), the Council for Scientific and Industrial Research of South Africa (CSIR)
- Private Sector Scientific Enterprises – Reed Elsevier plc (United Kingdom), a scientific publishing organization

All examples are taken from publicly available annual reports of these organizations. The coverage of the statements, their level of detail and their location in the reports varies quite considerably. The common feature is a statement on the existence of a risk management and internal control system, overseen by the board, and executed by management. There is also usually some description, even if only in broad terms, of the types of risks that are managed.

A Proposal for CGIAR Center Board Statements

This Discussion paper proposes that, once a risk management system is established in a Center along the lines recommended in the CGIAR Internal Auditing Unit's Good Practice Note on Center-wide Risk Management, then a statement should be prepared for and adopted by the Board on an annual basis, for public reporting purposes (included in an appropriate section of the Center's annual report or similar publication), that adopts the most useful aspects of the example statements and provides summary information on the risk management and internal control system in place in the Center.



The report should also draw attention to:

- the Center’s risk management system having been designed so the Center meets the requirements established in the risk management codes and standards promulgated, or published as exposure drafts, in a number of CGIAR member countries; and
- processes in place or proposed by which the Center collaboratively assesses, with other Centers, CGIAR System Office components and special purpose entities such as AIARC, the shared risks arising from joint activities and the activities of common service providers within the System.

A suggested form of wording is proposed below. Actual terminology will differ to suit particular Centers e.g. Boards may have titles other than “Board of Trustees”; Audit Committees may be substituted with “Finance and Audit Committee” or other titles adopted by Centers; Annual reports may be substituted for some Centers by other publicly distributed documents such as the “Director General’s Report”.



Proposed Board Statement on Risk Management

“The Center’s Board of Trustees has responsibility for ensuring an appropriate risk management system is in place to identify and manage high and significant risks to the achievement of the Center’s business objectives, and to ensure alignment with CGIAR principles and guidelines which have been adopted by all CGIAR Centers. These risks will include financial, operational, and reputational risks that are inherent in the nature, modus operandi and location of the Center’s activities, and are dynamic as the environment in which the Center operates changes. They represent the potential for loss resulting from inadequate or failed internal processes or systems, human factors, or external events. They include low impact (and therefore irrelevance) of scientific activities, misallocation of scientific efforts away from agreed priorities, loss of reputation for scientific excellence and integrity, business disruption and information system failure, liquidity problems, transaction processing failures, loss of assets including information assets [*for some Centers:* and germplasm held in trust], failures to recruit, retain and effectively utilize qualified and experienced staff, failures in staff health and safety systems and failures in the execution of legal, fiduciary and agency responsibilities.

The Board has adopted a risk management policy, communicated to all staff, that includes a framework by which the Center’s management identifies, evaluates and prioritizes risks and opportunities across the organization; develops risk mitigation strategies which balance benefits with costs; monitors the implementation of these strategies; and periodically reports to the Board on results. This process draws upon risk assessments and analysis prepared by the Center’s business unit staff, internal auditors, Center-commissioned external reviewers, and the external auditors. The risk assessments also incorporate the results of collaborative risk assessments with other CGIAR Centers, System Office components and other entities in relation to shared risks arising from jointly managed activities. The risk management framework seeks to draw upon best practice promoted in codes and standards promulgated in a number of CGIAR member countries, and it is subject to ongoing review as part of the Center’s continuous improvement effort.

Risk mitigation strategies include the implementation of systems of internal control which, by their nature, are designed to manage rather than eliminate the risk. The Center endeavors to manage risk by ensuring that the appropriate infrastructure, controls, systems and people are in place throughout the organization. Key practices employed in managing risks and opportunities include business environmental scans, clear policies and accountabilities, transaction approval frameworks, [*for some Centers:* quality management systems subject to external certification,] financial and management reporting and the monitoring of metrics which are designed to highlight positive or negative performance of individuals and business processes across a broad range of key performance areas. The design and effectiveness of the risk management system and internal controls is subject to ongoing review by the Center’s internal audit unit, which is independent of business units and reports on the results of its audits directly to the Director General and the Board through Board’s Audit Committee.

The risk management framework has been in place for the year under review and up to the date of approval of the annual report and financial statements. [*or for the first year:* Implementation of the risk management framework has begun this year. The Board expects to be bale to report on the implementation of this framework from 200X”]



EXAMPLES OF RISK STATEMENTS IN PUBLICLY AVAILABLE ANNUAL REPORTS

Example 1 - UK Department for International Development: - Accounting Officer Statement 2002 – www.dfid.gov.uk

As Accounting Officer, I have responsibility for maintaining a sound system of internal control that supports the achievement of departmental policies, aims and objectives, set by the department's Ministers, whilst safeguarding the public funds and departmental assets for which I am personally responsible, in accordance with the responsibilities assigned to me in Government Accounting.

The system of internal control is designed to manage rather than eliminate the risk of failure to achieve policies, aims and objectives; it can therefore only provide reasonable and not absolute assurance of effectiveness.

The system of internal control is based on an ongoing process designed to identify the principal risks to the achievement of departmental policies, aims and objectives, to evaluate the nature and extent of those risks and to manage them efficiently, effectively and economically. This process has been in place for the year ended 31 March 2002 and up to the date of approval of the annual report and accounts and accords with Treasury guidance.

As Accounting Officer, I also have responsibility for reviewing the effectiveness of the system of internal control. My review of the effectiveness of the system of internal control is informed by the work of the internal auditors and the executive managers within the department who have responsibility for the development and maintenance of the internal control framework, and comments made by the external auditors in their management letter and other reports. Key internal controls in DFID in 2001/2 are as follows:

- A Finance and Audit Committee, reporting to the Management Board and to me, was established in the course of the year in order to enhance senior level scrutiny of finance and audit issues. This Committee has external and non-executive representation and is chaired by a non-executive for audit business.
- The Management Board also established Development, Human Resources, and Knowledge & Communications Committees to oversee work across the Department in these areas.



- All Directors provided me with an annual assurance for their division on the management of risk and compliance with management and control systems. They included 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.
- Country and Institutional Strategy Papers identify policies and priorities for key programmes based on an analysis of key issues, strengths and weaknesses. Annual reviews monitor progress and update these assessments.
- Annual Business Plans set out specific objectives for each department and set out how organisation and management issues will be addressed.
- Clear guidelines were in place for appraisal of programme spending proposals, including assessments of risks and how these would be managed. Delegations of authority to approve proposals were clear and complied with established procedures; sample assessments were made by senior managers of decisions taken under such delegated authority.
- Internal audit work followed a programme approved by the Management Board; an annual review of the work of Internal Audit and follow up to it was considered by the Finance and Audit Committee.
- Performance standards for Accounts, Facilities Management, Human Resources, Information Systems and Procurement are set out in Service Level Agreements. These define expected performance standards and efficiencies and are subject to regular monitoring and review.
- Consistent compliance with prescribed procedures is promoted and supported through Office Instructions and other guidance, training programmes, Help Desks, and central scrutiny and checks.
- The establishment of additional overseas offices, which are required for our effectiveness, gives rise to additional management risks. We have reviewed our arrangements for setting up and subsequently supporting overseas offices in order to ensure that standards of financial and people management are maintained throughout DFID.
- Infrastructure and systems development and procurement comply with standard Government procedures which require full risk assessment and risk management processes; project boards, reporting to senior managers and Management Board committees, oversee new developments.
- We have in place, for our various offices, contingency plans to respond to threats to the security and effectiveness of our staff and key systems and where possible to maintain continuity of operations
- We have strengthened our Finance Department through introducing professionally qualified staff to ensure we are able to meet the



requirements and reap the full benefits of resource accounting and budgeting.

Over the coming year we will be taking further action, notably on management of risk. In particular we plan to strengthen further the identification and monitoring of risk at corporate, divisional and departmental levels, to ensure that clear policies on risk and its management are effectively communicated throughout DFID and to relate risk assessment more explicitly to PSA objectives. Together with existing measures, I am confident that this will enable us to comply fully with standards that will be expected for Statements of Internal Control from the beginning of 2003/4.”



Example 2 - World Bank - IBRD Annual Report 2003 – Financial Statements - Management’s Discussion and Analysis: June 30, 2003 – www.worldbank.org

“The risk management governance structure includes a Risk Management Secretariat supporting the Management Committee in its oversight function. The Risk Management Secretariat was established in FY 2002 to support the Management Committee, particularly in the coordination of different aspects of risk management, and in connection with risks that cut across functional areas. For financial risk management, there is an Asset/Liability Management Committee chaired by the Chief Financial Officer..... Country credit risk, the primary risk faced by IBRD, is identified, measured and monitored by the Country Credit Risk Department, led by the Chief Credit Officer..... Market risks, liquidity risks and counterparty credit risks in IBRD’s financial operations are identified, measured and monitored by the Corporate Finance Department, which is independent from IBRD’s business units.....

Primary responsibility for the management of operational risk resides with each of IBRD’s managers. These individuals are responsible for establishing, maintaining and monitoring appropriate internal control procedures in their respective areas. The processes and procedures by which IBRD manages its risk profile continually evolve as its activities change in response to market, credit, product, and other developments. The Executive Directors, particularly the Audit Committee members, periodically review trends in IBRD’s risk profiles and performance, as well as any significant developments in risk management policies and controls.

Operational risk is the potential for loss resulting from inadequate or failed internal processes or systems, human factors, or external events, and includes business disruption and system failure, transaction processing failures and failures in execution of legal, fiduciary and agency responsibilities. IBRD, like all financial institutions, is exposed to many types of operational risks. IBRD attempts to mitigate operational risk by maintaining a system of internal controls that is designed to keep that risk at appropriate levels in view of the financial strength of IBRD and the characteristics of the activities



and markets in which IBRD operates. Since 1996, IBRD has used a COSO-based integrated internal control framework. IBRD's approach to operational risk management continues to evolve each year as IBRD seeks to adopt best practice. IBRD uses several tools to monitor and control operational risk. These tools include self assessment workshops, business process reviews in the finance, treasury and accounting areas, annual cascading internal representation letters from business unit managers, and compliance reviews. These tools are used to assist business units in identifying key operational risks and assessing the degree to which they mitigate these risks and maintain appropriate controls. Action plans are developed for issues identified. In addition, these action plans and the risks they are intended to address are evaluated on an annual basis by an internal panel. The panel evaluates and categorizes the risks to determine if they pose a threat to management's ability to make a positive assertion on the adequacy of internal controls surrounding IBRD's external financial reporting. The results of the work undertaken to evaluate the effectiveness of internal controls over financial reporting are reported to the Audit Committee through an annual report.

IBRD attempts to mitigate operational risk by maintaining a system of internal controls that is designed to keep that risk at appropriate levels in view of the financial strength of IBRD and the characteristics of the activities and markets in which IBRD operates. Since 1996, IBRD has used a COSO-based integrated internal control framework. IBRD's approach to operational risk management continues to evolve each year as IBRD seeks to adopt best practice. IBRD uses several tools to monitor and control operational risk. These tools include self assessment workshops, business process reviews in the finance, treasury and accounting areas, annual cascading internal representation letters from business unit managers, and compliance reviews. These tools are used to assist business units in identifying key operational risks and assessing the degree to which they mitigate these risks and maintain appropriate controls. Action plans are developed for issues identified. In addition, these action plans and the risks they are intended to address are evaluated on an annual basis by an internal panel. The panel evaluates and categorizes the risks to determine if they pose a threat to management's ability to make a positive assertion on the adequacy of internal controls surrounding IBRD's external financial reporting. The results of the work undertaken to evaluate the effectiveness of internal controls over financial reporting are reported to the Audit Committee through an annual report.

The Audit Committee is appointed by the Board to exercise, on its behalf, oversight and assessment of the effectiveness of financial policies and reporting, fiduciary controls, various aspects of financial, business, operating, and reputational risk, quality of earnings, and internal controls. In the execution of this role, the Committee discusses with management and the external auditors financial issues and policies which have an important bearing on the institution's financial position and risk-bearing capacity. It also reviews the internal audit work program with the Auditor General, and management.”



Example 3 - IDRC Canada – Annual Report 2002-2003 – Sections on Corporate Governance and Assessing and Managing Risk – www.idrc.ca

“Risk management

The Finance and Audit Committee ensures that the principal risks of the Centre's business have been identified, that they are being properly managed, and that assets are well-protected. An annual risk assessment exercise carried out by Audit Services assists them in this task. Plans to address risk management in the context of the next Program of Work and Budget will be presented for Board approval in March 2004. For a more detailed



discussion of the risks involved in IDRC's work, see *Assessing and Managing Risk*, on page 9.

Assessing and Managing Risk

In India, massive communal violence in Gujarat left thousands of Muslims dead or displaced. The violence created dangerous conditions for staff of several projects in the area. A project on women's empowerment has faced some particularly tough challenges. Some staff resigned and others requested transfers. Travel was disrupted, affecting monitoring and other project activities. As a result, one of the research sites had to be relocated. The project has also introduced new elements to the workplan — including initiatives to help staff understand and address issues arising from the violence. These sorts of risks — and developing ways to overcome them — are part of IDRC's "business" of supporting research for development. Almost by definition, embarking on research involves exploring the unknown and testing the uncertain.

It is these variables, especially in the novel areas of IDRC-supported research, that can inspire innovation. Managing the risks associated with the Centre's work while not limiting the flexibility of staff and our research partners to respond to development challenges requires constant effort. The following examples show how the Centre works to strike this balance.

Project and administrative risk

Before a project is supported by IDRC, it must be appraised by a team of program staff. For large proposals, this includes a visit to the site by the responsible program officer. The appraisal includes an assessment of inherent risks that could affect the project's implementation, such as political and economic problems, social unrest, climatic changes, and inadequate sources of information. Before approval, each project budget is reviewed by a grant administration officer, who verifies the legal identity and status of the proposing institution and assesses the administrative risk, in accordance with IDRC's financial control framework. In the case of large projects with new institutions, the risks are assessed on site. The findings help to determine the grant conditions to be applied to the project. Once a project is approved, program officers monitor its progress and help address any unexpected developments. Grant administration officers work with program officers and conduct regular compliance reviews throughout the life of the project. Senior grant administration managers also regularly visit institutions that have high volumes of IDRC funding to review managerial, administrative, and financial capabilities. The findings seek to confirm earlier assessments and help to determine if contract adjustments are necessary.

Reviews

IDRC undertakes special reviews and assessments of countries where difficult conditions have either limited or precluded Centre programming. In the past, such a study has been conducted in Nigeria. In December 2002, senior management requested reviews of Nepal



and Palestine, both of which are experiencing conflict and unrest. These studies help the Centre determine how to support research and researchers in high-risk countries.

Health and security

IDRC's work requires frequent travel to areas that can pose health and personal security risks. Some Centre staff are posted to these same areas. Accordingly, the Centre employs several means to minimize these risks. These include the following:

A Security and Emergency Planning Team (SEPT), composed of senior managers, deals with emergency situations that pose a risk to the safety of Centre staff. For example: SEPT has monitored SARS-related issues on a daily basis, circulated regular advisories on travel to regions affected by SARS, and provided staff with information on the virus and how to prevent its transmission.

Health Services staff provide vaccines, prophylactic medication, and information on other preventive health measures to all staff before any international travel.

Travel bans and advisories from the Department of Foreign Affairs and International Trade are issued to staff on a regular basis. A ban prohibits IDRC staff from traveling to a particular country or area experiencing dangerous conditions. Advisories indicate that travelers should exercise caution. In addition, extensive information on IDRC's internal Web site outlines security precautions for staff while traveling. The Centre also provides all staff with ergonomically sound workstations and furnishings, and offers ergonomics training: 42 staff members were trained in 2002/03. First-aid and CPR courses are also offered: 13 staff members availed themselves of these courses in the past year. Senior management requested reviews of Nepal and Palestine, both of which are experiencing conflict and unrest."



Example 4 - CSIRO Australia – Annual Report 2002-2003 – Chapter on Corporate Governance – www.csiro.au

“Risk management program

The Board has responsibility for ensuring an appropriate risk management framework is in place to identify and manage high and significant risks to the Organisation.

To this extent, CSIRO undertakes a systematic program of organisation-wide and divisional contract and project specific risk assessments. These are designed to identify, evaluate and prioritise risks and develop risk mitigation strategies. The Risk Assessment and Audit Unit facilitates this process utilising a methodology consistent with the Australian Risk Management Standard AS/NZS-4360.



An organisational risk profile is completed semi-annually and reported to the Audit Committee. The Executive Team is responsible for the implementation of mitigation strategies.

The Audit Committee reviews the organisational high and significant risks and management's risk-mitigation strategies through regular reports from the Risk Assessment and Audit Unit.

A risk management policy and associated guidelines were issued in July 1997.

It is the responsibility of the operational management of CSIRO to develop and implement risk-mitigation strategies. In appropriate circumstances, insurance is used as a method to transfer the financial impact of risk.

Internal control

The Board is responsible for ensuring an appropriate internal control framework is in place and operating. Through the Audit Committee it reviews management's policies, procedures framework and internal compliance.”



Example 5 - CSIR South Africa – Annual report 2003 - www.csir.co.za

“Risk management

In the case of risk management, the CSIR Board is accountable for the process of risk management and the system of internal control. These are reviewed regularly for effectiveness. Appropriate risk and control policies are established and communicated throughout the organisation. The CSIR Board retains control through the final review of key risk matters affecting the organisation. Risk management in the CSIR is an ongoing process and is focused on identifying, assessing, managing and monitoring all known forms of significant risk across all business units and group companies. This has been in place for the year under review and up to the date of approval of the annual report and financial statements. CSIR systems have been put in place to review aspects of economy, efficiency and effectiveness. Management is involved in a continuous process of improving procedures to ensure effective mechanisms for identifying and monitoring risks, such as skills, technology, contracting, HIV/AIDS, reputation, Parliamentary Grant, legislation compliance, professional liability and general operating risks. Equal consideration is given to matters of safety, health and the environment as to the more obvious risks, such as financial risks. There is a documented and tested process in place, which will allow the company to continue its critical business process in the event of a disastrous incident impacting on its activities.

Operating risk management

The CSIR endeavours to minimise operating risk by ensuring that the appropriate



infrastructure, controls, systems and people are in place throughout the group. Key practices employed in managing operating risk include segregation of duties, transaction approval frameworks, financial and management reporting and monitoring of metrics, which are designed to highlight positive or negative performance across a broad range of key performance areas.

Financial risk management

Financial risks are managed within predetermined procedures and constraints as identified and detailed in the various policies and the setting of annual goals and objectives. Compliance is measured through regular reporting against the business goals, internal audit checks and external audit verification.”



Example 6 - Reed Elsevier plc - 2003 annual report -
www.investis.com/reedelsevier/csr/risk.shtml

“Reed Elsevier has implemented an ongoing process for identifying, evaluating and managing the significant risks faced by the respective businesses.

We have an established framework of procedures and internal controls, set out in a group Policies and Procedures Manual, with which the management of each business is required to comply. Group businesses are required to maintain systems of internal control, which are appropriate to the nature and scale of their activities and address all significant operational and financial risks that they face. The board of Reed Elsevier Group plc has adopted a schedule of matters that must be brought to them.

Each business group has identified and evaluated its major risks, the controls in place to manage those risks and the level of residual risk accepted. Risk management and control procedures are embedded into the operations of the business and include the monitoring of progress in areas for improvement that come to management and board attention. The major risks identified include business continuity, protection of IT systems and data, challenges to intellectual property rights, management of strategic and operational change, evaluation and integration of acquisitions, the recruitment and retention of personnel, and business reputation. The Strategy Committee considers major strategic risks to the businesses.

The Reed Elsevier Group plc Audit Committee receives regular reports on the management of material risks and reviews these reports with executive management. The Audit Committee also receives regular reports from both internal and external auditors on internal control matters. In addition, each business group is required, at the end of the financial year, to review the effectiveness of its internal controls and report its findings on a detailed basis to the management of Reed Elsevier Group plc. These reports are summarised and submitted to the Audit Committee of Reed Elsevier Group plc as part of the annual review of effectiveness. The Chairman of the Audit Committee reports to the board on any significant internal control matters arising.”