



SECTION H.2 - INTERNAL AUDIT SUPPORT TO ENTERPRISE RISK MANAGEMENT

Introduction

Risk management is a key responsibility of management. To achieve its business objectives, management should ensure that sound risk management processes are in place and functioning. Boards and Board committees, including Audit Committees, have an oversight role to determine that appropriate risk management processes are in place and that these processes are adequate and effective.

CGIAR Centers have been requested by at least one key donor, for the Board to produce an annual statement commenting on risk management. The CGIAR IAU has produced a Good Practice Note on Enterprise Risk Management (ERM), and a Discussion Note on Board Statements on Risk Management and Internal Control, to assist Centers implement systems to support such Board Statements, in a way that conforms with widely recognized standards and guidelines issued by various CGIAR member countries including the US COSO Risk Management Framework and the Australia/New Zealand Standard on Risk Management which will form the basis of a future ISO Standard. The Note sets out a methodology which is consistent with these standards and guidelines.

At present each Center adopts its own policies on ERM and internal control. The CGIAR IAU Good Practice Note promotes that these policies be adopted by the Center Boards, and many Centers have done this, using the Good Practice Note as input to their policy document. The Note is periodically updated from experience in the application of the policies in the Center, and may be used for a possible future overall CGIAR guideline on this topic.

Internal auditors are encouraged to assist both Center management and the Board by examining, evaluating, reporting, and recommending improvements on the adequacy and effectiveness of management's risk processes.

Internal auditors acting in a consulting role can assist the Center in identifying, evaluating, and implementing risk management methodologies and controls to address those risks and in coordinating assessments and reporting within the Centers.



Ref.	Policy and Practice Requirements	IIA Standards and Other References
H.2-1	<p>Policy: Internal Audit shall promote the Center’s adoption and maintenance of a comprehensive enterprise risk management system for which responsibilities of the Board and management are clearly established.</p> <p>Discussion:</p> <ul style="list-style-type: none"> ▪ An effective ERM system should include policies which promote the definition and implementation of clear responsibilities of the Board and managers (including risk management committees and coordinators) in relation to Center risk management. They should also include a process of reporting that ensures the Board and senior management discuss the most significant risks on a regular basis. ▪ An effective ERM system should comprise periodic assessments at both operational and strategic (enterprise-wide) levels ▪ This requires both bottom-up and top-down risk assessments, which should be taken into account in overall Center-wide assessment summaries. ▪ An effective risk management system should also promote initiatives to identify and act on opportunities. Risk management is not intended to induce aversion to change or action. When considering new opportunities, Centers should make appropriate formal assessments of potential risks as an integral part of the analysis. 	<p>Standard 2120 – Risk Management - The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes</p> <p>Practice Advisory 2120-1 Assessing the Adequacy of Risk Management Processes</p>



<p>H.2-1:1</p>	<p>Practice Requirement:</p> <p>Internal Audit shall promote the self-assessment by Center management and Board of significant exposures to risk and provide inputs from Internal Audit’s own assessments and audit results to assist the Center in this process. The end result should be an assessment that can be both fully owned by Center management and consistent with Internal Audit’s own understanding of the most significant risks.</p>	
<p>H.2-1:2</p>	<p>Practice Requirement:</p> <p>Internal Audit shall promote Center risk assessments that evaluate the exposures and mitigation activities relating to the organization's governance, operations, and information systems regarding the</p> <ul style="list-style-type: none"> ▪ Reliability and integrity of financial and operational information. ▪ Effectiveness and efficiency of operations. ▪ Safeguarding of assets. ▪ Compliance with laws, regulations, and contracts. 	<p>Standard 2120.A1 Risk Management - The internal audit activity must evaluate risk exposures relating to the organization’s governance, operations, and information systems</p>
<p>H.2-1:3</p>	<p>Practice Requirement:</p> <p>Internal Audit shall promote Center risk assessments that evaluate exposures and mitigation activities relating to both financial and scientific fraud.</p> <p>Discussion:</p> <p>See also Section H.3 on Internal Audit Support to Financial Fraud Prevention and Detection</p>	<p>Standard 2120.A2 Risk Management - The internal audit activity must evaluate the potential for the occurrence of fraud and how the organization manages fraud risk</p>
<p>H.2-1:4</p>	<p>Practice Requirement:</p> <p>Internal Audit shall promote a process whereby the Center’s Board and senior management receive periodic reports of the results of the risk</p>	<p>Practice Advisory 2120-1 Assessing the Adequacy of Risk Management Processes</p>



	<p>management processes, as a basis for an annual Board Statement on Risk Management and Internal Control which can then be made available to all stakeholders.</p>	
<p>H.2-1:5</p>	<p>Practice Requirement:</p> <p>Internal Audit shall promote clear identification within the Center for responsibilities relating to risk management, including its own. In relation to its own responsibilities, these can encompass research on policies and methodologies for Centers to use, training Center staff, facilitation of risk assessments by Center Boards, management and staff, and coordination of risk assessments and reporting. However Internal Audit shall not be responsible for managing risks (except those relating to its own operations).</p> <p>Discussion:</p> <ul style="list-style-type: none"> ▪ The Center’s policy setting out its risk management framework should identify the responsibilities relating to risk management ▪ Responsibilities and activities should be coordinated between all groups and individuals with a role in the Center’s risk management process. In general: <ul style="list-style-type: none"> ○ The Board should be responsible for establishing the overall risk management framework and for monitoring its implementation ○ Determining the risk appetite of the Center, including acceptance of residual risks identified in risk assessments, should be the responsibility of management, with inputs in key/strategic areas from the Board ○ Ownership of risks identified in risk 	<p>Practice Advisory 2120-1 Assessing the Adequacy of Risk Management Processes</p> <p>Standard 2120.C3 Risk Assessment – When assisting management in establishing or improving risk management processes, internal auditors must refrain from assuming any management responsibility by actually managing risks.</p>



	<p>assessments should be assigned to Center senior managers with related responsibilities</p> <ul style="list-style-type: none">○ Identifying, assessing, mitigating, and monitoring activities on a continuous basis may be assigned at the operating level; and○ Periodic overall assessment of the implementation of the risk management framework should reside with Internal Audit activity, with validation of controls identified as in place shared between Internal Audit, External Audit and other Center commissioned external reviewers (e.g. Biosafety reviews, OH&S reviews, CCERs, ISO external audits). <ul style="list-style-type: none">▪ Depending on the maturity of the Center’s risk management system, Internal Audit’s role in the risk management process may change over time and may be found at some point along a continuum that ranges from:<ul style="list-style-type: none">○ Auditing the risk management process as part of the internal audit plan○ Active, continuous support and involvement in the risk management process such as participation on oversight committees, monitoring activities, and status reporting○ Managing and coordinating the risk management process.▪ Risk management coordination functions may be undertaken by Internal Audit at the Board’s and management’s request to help get the process going. However, there should be agreement and arrangements made so that, in the medium to longer term, these roles are transferred to management.	
--	---	--



<p>H.2-2</p>	<p>Policy: The internal audit activity shall assist the Center by monitoring and evaluating the effectiveness of the organization's risk management system, including the effectiveness of controls and other activities to mitigate any identified risks.</p>	<p>Standard 2120 – Risk Management - The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes</p> <p>Standard 2130 – Control: The internal audit activity must assist the organization in maintaining effective controls by evaluating their effectiveness and efficiency and by promoting continuous improvement.</p>
<p>H.2-2:1</p>	<p>Practice Requirement:</p> <p>The individual assurance and consulting assignments in the annual internal audit work plans should include, as objectives, an evaluation of the risks and mitigating actions relevant to the scope of those assignments. The results should be considered in the overall evaluation of the enterprise risk assessment.</p>	<p>Practice Advisory 2120-1 Assessing the Adequacy of Risk Management Processes</p> <p>Standard 2120.C1 - During consulting engagements, internal auditors must address risk consistent with the engagement's objectives and be alert to the existence of other significant risks.</p>
<p>H.2-2:2</p>	<p>Practice Requirement:</p> <p>The annual Internal Audit work plan for each Center shall include time for assessing and reporting on the Center's risk management processes. The assessment should incorporate</p>	<p>Practice Advisory 2120-1 Assessing the Adequacy of Risk Management Processes</p> <p>Standard 2120.C2 –</p>



	<p>the results of other recently completed internal audit assurance and consulting assignments, as well as external audits and other independent reviews.</p> <p>Discussion:</p> <ul style="list-style-type: none"> ▪ The Head of Internal Audit should obtain an understanding of management’s and Board’s expectations of the internal audit activity in the Center’s risk management process. ▪ The Center Internal Audit charter should make reference to risk management responsibilities. ▪ Internal auditors should be alert to newly emerging risks and risk exposures. The CGIAR IAU shall play a facilitating role in sharing learning about risks across the Centers. ▪ Internal auditors are expected to identify and evaluate significant risk exposures in the normal course of their duties, whether through: <ul style="list-style-type: none"> ○ Specially programmed reviews of the overall ERM process ○ Assurance audit assignments ○ Consulting/advisory assignments ○ Informal reviews and assessments and discussions with Center staff 	<p>Internal auditors must incorporate knowledge of risks gained from consulting engagements into their evaluation of the organization’s risk management processes.</p>
<p>H.2-2:3</p>	<p>Practice Requirement:</p> <p>The annual and medium term internal audit plans shall indicate what part of the Center’s risk spectrum will be covered by the assurance audits being proposed.</p> <p>Discussion:</p> <ul style="list-style-type: none"> ▪ Senior management and the Board normally expect that Internal Audit will perform sufficient audit work and gather 	



	<p>other available information during each year so as to form a judgment about the adequacy and effectiveness of at least a subset of the Center’s risk management and control processes.</p> <ul style="list-style-type: none"> ▪ The rationale for prioritizing the internal audit coverage of risks should be explained, including how other risks not covered in the plan may be covered through other independent review activities in that period. 	
<p>H.2-2:4</p>	<p>Practice Requirement:</p> <p>The internal audit plans shall include audit assignments to review the design and effectiveness of internal controls in place to manage particular risks within the organization’s governance, operations, and information systems regarding the:</p> <ul style="list-style-type: none"> ⊙ Reliability and integrity of financial and operational information; ⊙ Effectiveness and efficiency of operations; ⊙ Safeguarding of assets; and ⊙ Compliance with laws, regulations, and contracts. <p>Discussion:</p> <ul style="list-style-type: none"> ▪ To the extent that the Head of Internal Audit expresses an overall opinion on internal control within the organization, this should be based on sufficient audit evidence obtained through the completion of audits of internal controls and, where appropriate, reliance on the work of other assurance providers. The type of overall opinion on controls influences the scope of the medium term and annual internal audit plans (see Section G.1) ▪ During consulting engagements, internal 	<p>Standard 2130 – Control:</p> <p>The internal audit activity must assist the organization in maintaining effective controls by evaluating their effectiveness and efficiency and by promoting continuous improvement.</p> <p>Standard 2130.A1 Control</p> <p>- The internal audit activity must evaluate the adequacy and effectiveness of controls in responding to risks within the organization’s governance, operations, and information systems</p> <p>Practice Advisory 2130-1</p> <p>Assessing the Adequacy of Control Processes</p>



	<p>auditors should address controls consistent with the engagement’s objectives and be alert to the existence of any significant control weaknesses.</p>	
H.2-2:5	<p>Practice Requirement:</p> <p>With regard to reliability and integrity of information, internal auditors should consider the risks and controls relating to validity, accuracy, completeness, and security.</p> <p>Discussion:</p> <ul style="list-style-type: none"> • Where the information is produced by automated systems these elements must be tested in the audit of the systems. Consideration should be given to use of computer assisted audit tools and techniques (see Section I.3C) • The general IT controls over the environment that hosts the automated system should also be assessed in the areas of: <ul style="list-style-type: none"> ○ Organization and planning ○ Solution delivery ○ Change management ○ IT services delivery ○ Information security management 	<p>Practice Advisory 2130.A1-1 Information Reliability and Integrity</p>
H.2-2:6	<p>Practice Requirement:</p> <p>With regard to reliability and integrity of information, internal auditors should consider the risks and controls relating to privacy of information stored in the Center.</p> <p>Discussion:</p> <ul style="list-style-type: none"> • The main private information concerning individuals stored in Center manual and 	<p>Practice Advisory 2130.A1-2 Evaluating an Organization’s Privacy Framework</p>



	<p>automated systems are (a) internal information:</p> <ul style="list-style-type: none">○ Salary and benefit information of staff○ Personal information of staff○ Medical information of staff and their dependents, in relation to health and life insurance programs and OH&S programs <p>and (b) research information:</p> <ul style="list-style-type: none">○ Household data collected as part of research projects○ Results of human subject testing carried out as part of research projects <ul style="list-style-type: none">● In general, the privacy frameworks governing internal and research related information will be different and subject to separate evaluations● In conducting such an evaluation of the management of the organization's privacy framework, the internal auditor:<ul style="list-style-type: none">○ Considers the laws, regulations, and policies relating to privacy in the jurisdictions where the organization operates;○ Liaises with the Center's legal counsel as necessary to determine the exact nature of laws, regulations, and other standards and practices applicable to the organization and the country/countries in which it operates;○ Liaises with information technology specialists to determine that information security and data protection controls are in place and regularly reviewed and assessed for appropriateness;○ Considers the level or maturity of the	
--	---	--



	organization's privacy practices	
H.2-2:7	<p>Practice Requirement:</p> <p>Internal Auditors shall address internal controls over areas subject to consulting engagements, during the course of the engagements, and shall incorporate information on the design and effectiveness of internal controls gained from these engagements as well as assurance engagements, when assessing overall controls and the effectiveness of risk management systems.</p>	<p>Standard 2130.C1 – During consulting engagements, internal auditors must address controls consistent with the engagement's objectives and be alert significant control issues</p> <p>Standard 2130.C2 – Internal auditors must incorporate knowledge of controls gained from consulting engagements into evaluation of the organization's control processes.</p>
H.2-2:8	<p>Practice Requirement:</p> <p>In their evaluations of internal controls, internal auditors shall ascertain the extent to which management has established adequate criteria to determine whether control objectives and goals have been accomplished. If adequate, internal auditors shall use such criteria in their evaluation. If inadequate, internal auditors shall work with management to develop appropriate evaluation criteria.</p> <p>Discussion:</p> <ul style="list-style-type: none"> ▪ For some topics, the CGIAR IAU's Good Practice Notes contain criteria against which control objectives can be measured. These are prepared with input from relevant communities of practice within the CGIAR System. 	<p>Standard 2210.A3 Control – Adequate criteria are needed to evaluate controls. Internal auditors must ascertain the extent to which management has established adequate criteria to determine whether objectives and goals have been accomplished. If adequate, internal auditors must use such criteria in their evaluation. If inadequate, internal auditors must work with management to develop appropriate evaluation criteria.</p>



<p>H.2-2:9</p>	<p>Practice Requirement:</p> <p>Internal audit assignments should, as part of their scope, consider the extent to which operating and program goals and objectives have been established and conform to those of the Center overall, and the extent to which results are consistent with these established goals and objectives and any associated risks.</p>	<p>Standard 2130.A2 Control - Internal auditors should ascertain the extent to which operating and program goals and objectives have been established and conform to those of the organization.</p> <p>Standard 2130.A3 Control - Internal auditors should review operations and programs to ascertain the extent to which results are consistent with established goals and objectives to determine whether operations and programs are being implemented or performed as intended.</p>
<p>H.2-2:10</p>	<p>Practice Requirement:</p> <p>Internal Audit shall obtain sufficient evidence to satisfy itself on the adequacy of the Center’s risk management processes.</p> <p>Discussion:</p> <ul style="list-style-type: none"> ▪ In gathering such evidence, the internal auditor should consider the following types of audit procedures: <ul style="list-style-type: none"> ○ Research and review reference materials and background information on risk management methodologies as a basis to assess whether or not the process used by the organization for the particular risk areas is appropriate and represents best practices for the industry. 	<p>Practice Advisory 2120-1 - Assessing the Adequacy of Risk Management Processes</p>



	<ul style="list-style-type: none">○ Research and review current developments, trends, industry information related to the business conducted by the organization, and other appropriate sources of information to determine risks and exposures that may affect the organization and related control procedures used to address, monitor, and reassess those risks.○ Review corporate policies, Board, and Audit Committee minutes to familiarize with the evolution of the Center’s business strategies, risk management philosophy and methodology, appetite for risk, and acceptance of risks.○ Review previous risk evaluation reports by management, internal auditors, external auditors, and any other sources that may have issued such reports.○ Conduct interviews with line and executive management to determine business unit objectives, related risks, and management’s risk mitigation and control monitoring activities.○ Assimilate information to independently evaluate the effectiveness of risk mitigation, monitoring, and communication of risks and associated control activities.○ Assess the appropriateness of reporting lines for risk monitoring activities.○ Review the adequacy and timeliness of reporting on risk management results.○ Review the completeness of management’s risk analysis, actions taken to remedy issues raised by risk management processes, and suggest improvements.○ Determine the effectiveness of	
--	---	--



	<p>management’s self-assessment processes through observations, direct tests of control and monitoring procedures, testing the accuracy of information used in monitoring activities, and other appropriate techniques.</p> <ul style="list-style-type: none"> ○ Review risk-related issues that may indicate weakness in risk management practices and, as appropriate, discuss with management, the audit committee, and the board of directors. Internal Audit should report to management where it believes that management has accepted a level of risk that is inconsistent with the Center’s risk management strategy and policies ▪ The challenge for Internal Audit is to evaluate the effectiveness of the Center’s system of risk management and controls based on the aggregation of many individual assessments. Those assessments are largely gained from internal audit engagements, management’s self-assessments, the external auditor’s work and work by other external reviewers. 	
<p>H.2-2:11</p>	<p>Practice Requirement:</p> <p>Internal Audit shall provide an opinion on the effectiveness of the overall risk management process, and on the effectiveness of risk management in particular areas where sufficient evidence has been gathered to support such an opinion</p> <p>Discussion:</p> <ul style="list-style-type: none"> ▪ As Internal Audit resources are limited and Centers face a broad array of risks, it is not feasible to expect Internal Audit to provide a comprehensive opinion on an annual basis covering the Center’s management of 	<p>Practice Advisory 2120-1 - Assessing the Adequacy of Risk Management Processes</p> <p>Practice Advisory 2130-1 Assessing the Adequacy of Control Processes</p>



	<p>all risks.</p> <ul style="list-style-type: none">▪ The opinion section of the report should be normally expressed in terms of negative assurance; that is, the audit work performed for the period and other information gathered did not disclose any significant weaknesses in the risk management and control processes that have a pervasive effect. If the risk management and control deficiencies or weaknesses identified are significant and pervasive, the assurance section of the report may be a qualified or adverse opinion, depending on the projected increase in the level of residual risk and its impact on the Center’s objectives.▪ An expectation gap may exist surrounding Internal Audit’s work in evaluating and providing assurance about the state of risk management and control processes. Management and the Board may have high expectations about the internal audit coverage (and may blame internal audit for not anticipating exposures which later result in losses to the Center). On the other hand, internal auditor’s may have more modest expectations that derive from knowledge of practical limitations on audit coverage and from self-doubt about generating sufficient evidence to support an informed and objective judgment. The Head of Internal Audit should be mindful of the possible gap between what a reader of an internal audit report on risk management presumes and what actually happened during the year. He or she should use the report as another way to address different mental models and to suggest improving the capacity of the function or reducing the constraints to access and audit effectiveness.	
--	--	--



	<ul style="list-style-type: none"> ▪ If Internal Audit is called upon by the Board and management to manage and coordinate risk management process to help get the process going, the internal audit assurance during such period would be accordingly limited. 	
<p>H.2-2:12</p>	<p>Practice Requirement:</p> <p>When the Head of Internal Audit believes that senior management has accepted a level of residual risk that <i>may be</i> unacceptable to the Center, s/he shall discuss the matter with senior management. If the decision regarding residual risk is not resolved, the Head of Internal Audit and senior management shall report the matter to the board for resolution.</p>	<p>Standard 2600 – Resolution of Senior Management’s Acceptance of Risks -</p> <p>When the chief audit executive believes that senior management has accepted a level of residual risk that may be unacceptable to the organization, the chief audit executive must discuss the matter with senior management. If the decision regarding residual risk is not resolved, the chief audit executive must report the matter to the board for resolution</p>