COORDINATING RISK MANAGEMENT AND ASSURANCE

MARCH 2012

The Institute of Internal Auditors | *Global*

Table of Contents

Executive Summary

Risk management is fundamental to organizational control and a critical part of providing sound corporate governance. It touches all of the organization's activities. The establishment of an effective enterprise-wide risk management system is a key responsibility of management and the board, which are responsible for adopting a holistic approach to the identification of organizational risks, creating controls to mitigate those risks, and monitoring and reviewing the identified risks and controls. They should ensure that risk management is integrated into the organization, both at the strategic and operational levels.

With responsibility for assurance activities traditionally being shared among management, internal audit, risk management, and compliance, it is important that assurance activities be coordinated to ensure resources are used in an efficient and effective way. Many organizations operate with traditional (and separate) internal audit, risk, and compliance activities. It is common for organizations to have a number of separate groups performing different risk management, compliance, and assurance functions independently of one another. Without effective coordination and reporting, work can be duplicated or key risks may be missed or misjudged.

Many internal audit functions work in close cooperation with risk management. Some organizations do not have a formal risk management function and in this case the internal audit activity often provides risk management consulting services to the organization. Internal audit should not give independent assurance on any part of the risk management framework for which it is responsible. Other suitably qualified parties should provide such assurance.

Introduction

Standard 2050: Coordination states, "The chief audit executive [CAE] should share information and coordinate activities with other internal and external providers of assurance and consulting services to ensure proper coverage and minimize duplication of efforts." This responsibility requires the CAE's inclusion and participation in the organization's assurance provider framework. This framework can consist of internal audit, external audit, governance, risk management, or other business control functions/disclosures performed by the organization's management team. Inclusion and participation in this framework helps ensure that the CAE is aware of the organization's risks and controls in relation to organizational goals and objectives.

Boards will use various sources to gain reliable assurance, including management, internal audit, and third parties. As discussed in Practice Advisory 2050-2: Assurance Maps, an assurance map is a valuable tool for coordinating risk management and assurance activities to increase the efficiency and effectiveness of risk management assurance investments made by an organization.

Risk Management and Assurance (Assurance Services)

The *International Standards for the Professional Practice of Internal Auditing* (**Standards**) Glossary defines risk management as "a process to identify, assess, manage, and control potential events or situations to provide reasonable assurance regarding the achievement of the organization's objectives." This is consistent with the International Standards Organization's definition of risk management, which is "coordinated activities to direct and control an organization with regard to risk."

Enterprise risk management (ERM) — also known as enterprise-wide risk management — is a commonly used term. The Committee of Sponsoring Organizations of the Treadway Commission defines it 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 risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."

Assurance services should be objective and professional, and can be obtained from a range of assurance providers. Such providers can be internal — such as internal audit, workplace health and safety, compliance, and security — as well as external, such as statutory audit.

The Glossary of the Standards defines assurance services as "an objective examination of evidence for the purpose of providing an independent assessment on governance, risk management, and control processes of the organization."

There are generally three parties involved in assurance services:

- The person or group directly involved with the entity, operation, function, process, system, or other subject matter, and oversight functions such as risk management, compliance, and finance.
- The person or group making the assessment (the assurance provider).
- The user of the assessment, such as executive management and the board.

Assurance Framework

The need for assurance arises from an organization's governance processes. Its origin is in the stewardship relationship between the board of an organization and its shareholders. This stewardship relationship demands that boards establish processes to both delegate and limit power to pursue the organization's strategy and direction in a way that enhances the prospects for the organization's long-term success. Assurance processes are needed to allow the board to monitor the exercise of that power.

Risk management is a management process that promotes the efficient and effective achievement of organizational objectives. Assurance and risk management are complementary processes. In support of the risk management process, the major role of internal audit and other independent assurance providers is to provide assurance that:

- The risk management process has been applied appropriately and that elements of the process are suitable and sufficient.
- The risk management process is keeping with the strategic needs and intent of the organization.
- Processes and systems are in place to ensure that all material risks have been identified and are being treated.
- All prioritized intolerable risks have cost-effective treatment plans in place.
- Controls are being correctly designed in keeping with the outputs of the risk management process.
- Key controls are adequate and effective.
- Risks are not over-controlled or inefficiently controlled.
- Line management review and other non-audit assurance activities are effective at maintaining and improving controls.
- Risk treatment plans are being executed.

- There is appropriate and as-reported progress in the risk management plan.

In support of the assurance process, the risk management process should:

- Establish an organization-specific, documented risk management policy and framework.
- Assign responsibility for effective identification and management of significant risks.
- Provide a structured analysis of the risks of the organization recording:
  – Risks, their associated exposures, and current risk ratings.
  – The organizational objective(s) to which the risk applies.
  – The organizational position responsible for identifying and managing each risk.
  – Key control systems established to identify and manage each risk.

The assurance strategy is closely aligned with the corporate or other strategic plans of the organization. The legal, legislative, cultural, and economic environment in which the organization is operating, as well as the nature of the organization's activities and its long-term plans drives assurance needs.

It is an important first step to identify who will be the users of organizational assurance. Clearly, the board and management are the primary users. Other users may include the owners, regulators, government, or customers for whom the organization is a critical supply component. In today's highly interconnected economy, external entities may require assurance of the organization as part of their own risk management process.

The required assurance may range from providing comfort to the board when they need to approve the formal financial statements or the contents of the annual report to the

provision of a formal statement of compliance or comfort to an external body.

The assurance objectives will dictate the assurance strategy and level of rigor employed, but the basic requirements include assurance that:

- All material risks have been identified.
- Risks have been accurately analyzed and evaluated.
- Key controls are both adequate and effective.
- Management is appropriately addressing intolerable risks.

There are three fundamental classes of assurance providers, differentiated by the stakeholders they serve, their level of independence from the activities over which they provide assurance, and the robustness of that assurance. They are:

- Those who report to management or are part of management (management assurance), including individuals who perform control self-assessments, quality auditors, environmental auditors, and other management (designated assurance personnel).
- Those who report to the board, including internal audit.
- Those who report to external stakeholders (financial statement assurance), a role traditionally fulfilled by the independent/statutory auditor.

The level of assurance desired will vary depending on the risk and other factors such as regulations. Who should provide that assurance will vary based on the ability of the assurance provider to deliver the necessary level of independence and objectivity, as well as the historical organizational design of the entity and skill sets available within the assurance group.

The Respective Roles of Risk Management, Internal Audit, Compliance,and Other Assurance Providers

Assurance providers for an organization may include:

- Line management and employees (management provides assurance as a first line of defense over the risks and controls for which they are responsible).

- Senior management.

- Internal and external auditors.

- Compliance.

- Quality assurance.

- Risk management.

- Environmental auditors.

- Workplace health and safety auditors.

- Government performance auditors.

- Financial reporting review teams.

- Subcommittees of the board (such as audit, actuarial, credit, governance).

- External assurance providers, including surveys, specialist reviews (health and safety), etc.

Refer to The IIA's Practice Guide, Reliance on Internal Audit by Other Assurance Providers (December 2011), for more information on the range of internal and external assurance providers. Also, refer to The IIA's Position Paper, The Role of Internal Auditing in Enterprise-wide Risk Management, (January 2009) regarding what roles are appropriate for internal audit in regard to risk management.

The internal audit activity will normally provide assurance coverage over parts of the organization approved in the internal audit charter or terms of engagement letter. This coverage should include risk management processes (both their design and operating effectiveness), management of those risks classified as high risk (including the effectiveness of the controls and other responses to them), verification of the reliability and appropriateness of the risk assessment, and reporting of the risk and control status.

With responsibility for assurance activities traditionally being shared among management, internal audit, risk management, and compliance, it is important that assurance activities are coordinated to ensure resources are used in the most efficient and effective way. Many organizations operate with traditional (and separate) internal audit, risk, and compliance activities. Compliance is defined in the the Glossary of the *Standards* as "adhering to the requirements of laws, industry, and organizational standards and codes, principles of good governance and accepted community and ethical standards." A compliance program is a series of activities that when combined are intended to achieve compliance. Without effective coordination and reporting, work can be duplicated or key risks may be missed or misjudged.

Risk management is fundamental to organizational control and a critical part of providing sound corporate governance. It touches all of the organization's activities. For this reason many organizations have moved to adopt a more formalized ERM process.

Coordination Role of the CAE

IIA Standard 2050: Coordination states that the CAE should share information and coordinate activities with other internal and external providers of assurance and consulting services to ensure appropriate coverage and minimize duplication of efforts. This responsibility requires the CAE's inclusion and participation in the organization's assurance provider framework. This framework can consist of internal audit, external audit, governance, risk management, and other business control functions/disclosures performed by the organization's management team. Inclusion and participation in this framework helps

ensure that the CAE is aware of the organization's risks and controls in relation to goals and objectives.

Most internal audit functions perform annual and engagement-based risk assessment activities to help prioritize risks according to their potential impacts on the organization's achievement of goals and objectives. At the macro-level, these activities assist the internal audit activity to develop a proposed audit plan to submit to the board. At the micro-level, these activities help prioritize the scope of audit work and assurance being provided by internal audit engagements.

It is important that the work performed by assurance providers is understood and assessed by the CAE on an ongoing basis. This helps ensure that appropriate due professional care is exercised in the performance of internal audit work, including risk assessment activities performed to derive proposed audit plans submitted to the board. This also helps the board understand the coverage provided by the organization's assurance providers to better assess appropriate assignment of resources and potential exposures due to non-coverage.

Coordination between assurance providers includes regular sharing of reports and outcomes of assurance activities. This formal coordination should occur on a regular basis and include time for discussion and review of techniques and methods used to reach conclusions. This includes management's responses and an understanding of activities performed to mitigate any risks or control deficiencies identified.

The CAE may develop an annual report to be shared with the organization's board and executive management team. This report should outline the organization's assurance provider framework, the coverage of the assurance being provided, areas of high risk, and residual/un-mitigated risk areas within the organization. Another alternative would be for the CAE to coordinate the development and distribution of this report through the organization's gover-

nance or risk management function. Regardless of the origin of the report, it is important that the CAE can rely on the techniques and methods performed by the assurance providers.

A thorough, documented and continuous risk management process is part of good governance and an important management tool to provide assurance that appropriate controls are in place to achieve the objectives of an organization.

The establishment of an effective enterprise-wide risk management system is a key responsibility of management. Boards and management are responsible for adopting a holistic approach to the identification of organizational risks, creating controls to mitigate those risks, monitoring and reviewing the identified risks and controls, and ensuring that risk management is integrated into the organization — both at the strategic and operational levels. Some organizations have delegated independent risk management functions, but others do not have an independent risk management function and require internal audit to provide consulting services in this area. Internal audit can assist in identifying, evaluating, and facilitating risk management methodologies. Internal audit also is responsible for evaluating the effectiveness and contributing to the improvement of the risk management process.

Identifying risks in a systematic way supports sound decision making. It is about performing a thorough analysis of the organization on various levels, describing events that might occur, deciding on the importance of those risks, and developing adequate measures to deal with them.

Using the Risk Management Process in Internal Audit Planning

The documentation of risk management in an organization can be at various levels below the strategic risk management process. Many organizations have developed risk registers that document risks below the strategic level, providing documentation of significant risks in an area and related inherent and residual risk ratings, key controls, and mitigating factors. An alignment exercise can then be undertaken to identify links between the items included in the audit universe documented by the internal audit activity and risk categories and aspects described in the risk registers.

Some organizations may identify several high (or higher) inherent risk (potential exposure) areas. While these risks may warrant internal audit attention, it is not always possible to review all of them. Where the risk register shows a high, or higher, ranking for inherent risk (or major potential exposure) in a particular area, and the current risk remains similarly high with no action by management or internal audit planned, the CAE should report those areas to the board with details of the risk analysis and reasons for the lack of, or ineffectiveness of, internal controls.

In addition to evaluating the effectiveness of the organization's risk management process and contributing to its improvement, internal audit also uses the results of the risk management process to develop annual audit plans and individual audit engagements.

Internal audit is often asked to deliver better results with strained resources. This can be achieved by strategically placing internal audit work where it can be most effective in delivering the best results and having the highest effect on the outcome of the strategic and operational goals of the business entity. One of the tools of achieving this is

to base internal audit plans and individual audit engagements on the main identified internal risks and controls.

Internal audit should prepare short- and long-term audit plans to ensure that their activities are covering the main risk areas and internal controls of the organization. As business circumstances can change substantially, continuous monitoring and periodic revision of annual plans — with at least yearly reviews of longer term plans — are needed to ensure that audit plans are flexible, based on up-to-date information and cover changing priorities and risk areas.

Standard 2010: Planning states that "the [CAE] must establish risk-based plans to determine the priorities of the internal audit activity, consistent with the organization's goals." Also, Standard 2010.A1 states "the internal audit activity's plan of engagements must be based on a documented risk assessment, undertaken at least annually. The input of senior management and the board must be considered in this process."

Standard 2120: Risk Management states, "the internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes."

The following are steps to consider in the preparation of internal audit plans to determine risks and exposures that may affect the achievement of the organization's goals and objectives:

- Research and review corporate documents such as enterprise business plans, strategic plans, enterprise risk assessments, yearly reports, minutes of board meetings, minutes of management meetings, outside reports, external audit reports and other appropriate sources.

- Review previous internal audit plans, progress reports, and works in progress.

- Consult senior management of the organization and

solicit information regarding concerns or risks areas.

- Conduct a risk assessment of the issues and determine priorities for the annual audit plan.

- Prepare a draft audit plan.

- Communicate the proposed audit plan to stakeholders.

- Seek feedback and validation of the major risk areas to review.

- Finalize the audit plans.

- Present to management and the board for approval.

- Regularly monitor, review, and re-evaluate the plans in light of changing circumstances.

While the broader rationale and objective of an internal audit are developed in the annual planning phase, detailed research and work are needed at the onset of the audit to define the detailed objective and scope and develop criteria and methodology.

Standard 2201: Planning Considerations states that "In planning engagements, internal auditors must consider:

- The significant risks to the activity, its objectives, resources, and operations and the means by which the potential impact of risk is kept to an acceptable level.

- The adequacy and effectiveness of the activity's risk management and control systems compared to a relevant control framework or model.

- The opportunities for making significant improvements to the activity's risk management and control processes."

Also, **Standard 2210: Engagement Objectives** states, "Internal auditors must conduct a preliminary assessment of risks relevant to the activity under review. Engagement objectives must reflect the results of this assessment." With regard to consulting engagements, Standard 2120. C1 states, "During consulting engagements, internal au-

ditors must address risk consistent with the engagement's objectives and be alert to the existence of other significant risks."

Thorough planning of an internal audit is crucial to its success. It provides an opportunity to become familiar with the entity being audited; to gather relevant issues, concerns, and risks; to complete a risk assessment, and determine the objectives and scope of the audit.

In developing an audit engagement plan, the internal audit team should conduct a formal, comprehensive and documented risk assessment to identify audit issues and risk events. This involves significant research, consulting with management of the entity or area under review, and becoming familiar with the entity or area.

Risk assessment methods can vary; however, all risk assessments should cover the following points:

- Description of the risk event (negative occurrence, undesirable event).

- Likelihood of the event happening (strong, moderate, weak).

- The impact of negative occurrence on the achievement of goals and objectives (high, moderate, low).

- Current controls (systems, policies, procedures, etc.) in place and their effectiveness (effective/not effective).

- Ranking of the risk events.

Every potential audit highlights a wide range of issues for examination. However, it is not necessary, reasonable, or cost effective to look at them all. The audit team has to be cognizant of, and concentrate its efforts on, the most important and high-risk issues.

By ranking the possible risk events, this process will identify the issues with the most significance and highest ranking. At this point, a decision can be made

regarding which issues are material and will be audited in light of the audit's objective, and take into consideration other factors such as auditability, resources, and time lines. The results of the risk assessment should be presented and discussed with management of the entity under review to ensure their concurrence and validation.

Preparation of Assurance Maps

Boards will use various sources to gain reliable assurance, including management, internal audit, and third parties. Many organizations operate with separate internal audit, risk, and compliance functions, and it is not uncommon for organizations to have a number of separate groups performing different risk management functions independently of one another. As discussed in Practice Advisory 2050-2, an assurance map is a valuable tool for coordinating these risk management and assurance activities to increase the efficiency and effectiveness of assurance investments made by an organization. Assurance maps can help:

- Identify duplication and overlap in assurance coverage, allowing the board and senior management to decide if the overlap is necessary, intentional, or should be eliminated.

- Define scope boundaries and roles and responsibilities for various assurance providers to ensure the right resources are focused on the right risks. This can enhance the effectiveness of assurance providers by ensuring they are focused on the areas that need their attention, and by clearly articulating the expectations of the board and senior management.

- Assist in identifying any gaps in assurance coverage that need to be addressed.

It is the responsibility of the CAE to understand the assurance requirements of the board and the organization, clarify the role the internal audit activity fills, and the level of assurance it provides. However, given their unique vantage point to assurance activities in the organization, the

CAE can take this one step further and help in the creation of an assurance map for the organization. This will not only assist the board in providing governance oversight, but also will assist the CAE in ensuring the audit activity is optimizing its resources for maximum assurance value, and creating a more connected assurance community through effective coordination.

Feedback on Significant Risk Areas in Internal Audit Reports

During all assurance work, particularly where the scope relates to significant potential exposures identified in an organization's risk management process, audit approach, audit procedures, and communications should be designed to evaluate management's assertions on the effectiveness of controls in bringing risk within an organization's risk tolerance threshold.

Reports to management and the board can describe the potential exposure and management's assessment of current risks (with the implied value of the controls in place) together with the audit evaluation of the risk ratings. Any differences should be fed into management's risk management process for consideration.

The cumulative effect over time of such assurance activities over specific risk areas using a risk-based audit plan will provide assurance not only over those areas, but also on the effectiveness of the overall risk management process.

Assessment by Internal Audit of the Adequacy of Risk Management

Internal audit should provide assurance as required by Standards 2100: Nature of Work, 2120: Risk Management and 2400: Communicating Results to senior management,

and ultimately the board, that the organization is managing its risks effectively. Insofar as internal audit will need to include the adequacy of risk management within this scope there are two dimensions to consider:

1. Whether the risk management function includes all appropriate risk areas within its remit.

2. Whether the risk management function is operating effectively.

The main elements of the assessment that internal audit will need to encompass are covered to a large extent by Practice Advisory 2120-1: Assessing the Adequacy of Risk Management Processes. The main features are:

- Boards of management, as part of their oversight role, may direct internal audit to assist by reviewing and reporting on the adequacy of risk management.

- Management and the board are responsible for risk management; however, internal auditors acting in a consulting role can assist management in this responsibility.

- Where the organization does not have a formal risk management process, the CAE should formally discuss the situation with management and the board.

The CAE should establish that:

- There is a culture of effective risk management.

- There is a clear understanding at all levels of the potential exposures or inherent risks facing the organization (e.g., a risk register).

- There is a clear understanding of the current level of risk within the organization.

- The amount of risk taken at every level of the organization is clearly defined and understood.

- Adequate and effective controls exist to mitigate risks.

- There is an appropriate method of communicating

the effectiveness of the status of the risk management system to senior management and the board.

The CAE has three important functions in the review of risk management, and as in any other audit assignment:

- Test the controls.

- Report any missing or ineffective controls.

- Recommend improvements.

The Promotion of Risk Management by Internal Audit

Standard 2100 states, "The internal audit activity must evaluate and contribute to the improvement of governance, risk management, and control processes using a systematic and disciplined approach." The internal audit activity often has a role providing independent and objective assurance to the organization's board regarding the effectiveness of an organization's ERM activities. This helps ensure key business risks are being managed appropriately and the organization's system of internal controls is operating effectively and efficiently.

Risk management is a management process that promotes the cost-effective achievement of organizational objectives. Assurance provides reliable information about the achievements of risk management activity. Assurance and risk management are complementary processes.

Often the internal audit activity of an organization will work in close cooperation with the risk management function. By independently reviewing the risk management process of an organization, internal audit can promote risk management throughout the organization and the audit process can be aligned with risk management frameworks. Consistent risk language used throughout the organization can be adopted by internal audit.

Internal audit's review of risk identification, risk evaluation, control identification and evaluation, and appropriate risk treatments challenges and enhances risk registers and the risk management framework.

Where Internal Audit Facilitates Risk Management

Some organizations do not have a formal risk management function, and in this case the internal audit activity may provide risk management consulting services to the organization. Internal audit may provide risk management consulting provided certain conditions apply:

- It should be clear that management remains responsible for risk management even in those organizations where internal audit has been asked to facilitate the risk management program. Internal audit should not manage any risks on behalf of management, nor make final decisions regarding the enterprise's risk appetite or level of resource allocation to control or mitigate risk. Whenever internal audit acts to help the management team to set up or to improve risk management processes, the audit committee should approve its plan of work.

- The nature of internal audit's responsibilities should be documented in the internal audit charter and approved by the board. Any work beyond the assurance activities should be recognized as a consulting engagement and the implementation standards related to such engagements should be followed.

- Internal audit should provide advice, challenge, and act as a support to management's decision making, as opposed to making risk management decisions. Internal audit cannot give objective assurance on any part of the risk management framework for which it is responsible. Other suitably qualified parties should provide such assurance.

The IIA's Position Paper, The Role of Internal Auditing

in Enterprise-wide Risk Management (January 2009), describes roles that are appropriate for internal audit in regard to risk management.

Impact on Internal Audit Where a Formal Risk Management Function Does Not Exist

When an organization does not have a risk management function, it typically requires increased effort from the CAE to communicate risk management and assurance activities to the board. Increased importance is placed on the quality of the internal audit risk assessment as the sole view of risk the board may be exposed to.

The CAE should promote the risk management function as an important activity that assists the organization in achieving its objectives, and provides recommendations for establishing such a process. If requested, the CAE can play a proactive consultative role in assisting with the initial establishment of a risk management process for the organization. However, while the internal audit function can facilitate or enable the creation of risk management processes, they should not be responsible for the processes or management of the identified risks. Initially, the internal audit function can facilitate management's risk assessment processes; however, it is advisable to have such facilitation activities separated from assurance activities in the CAE's organization.

If internal audit's role exceeds normal assurance and consulting activities such that independence could be impaired, the CAE should conform to the disclosure requirements of the *Standards*.

Authors:

Andrew MacLeod, CIA, CMIIA

Brian Foster, CIA

Patricia Macdonald

Andy Robertson

Teis Stokka, CIA

Benito Ybarra, CIA

Reviewers:

Doug Anderson, CIA, CRMA

Andy Dahle, CIA

Steve Jameson, CISA, CCSA, CFSA, CRMA

David Zechnich, CIA, CPA

About the Institute

Established in 1941, The Institute of Internal Auditors (IIA) is an international professional association with global headquarters in Altamonte Springs, Fla., USA. The IIA is the internal audit profession's global voice, recognized authority, acknowledged leader, chief advocate, and principal educator.

About Practice Guides

Practice Guides provide detailed guidance for conducting internal audit activities. They include detailed processes and procedures, such as tools and techniques, programs, and step-by-step approaches, as well as examples of deliverables. Practice Guides are part of The IIA's IPPF. As part of the Strongly Recommended category of guidance, compliance is not mandatory, but it is strongly recommended, and the guidance is endorsed by The IIA through formal review and approval processes. For other authoritative guidance materials provided by The IIA, please visit our website at https://globaliia.org/standards-guidance.

Disclaimer

The IIA publishes this document for informational and educational purposes. This guidance material is not intended to provide definitive answers to specific individual circumstances and as such is only intended to be used as a guide. The IIA recommends that you always seek independent expert advice relating directly to any specific situation. The IIA accepts no responsibility for anyone placing sole reliance on this guidance.

Copyright

120362