IPPF – Practice Guide

ASSESSING THE ADEQUACY OF RISK MANAGEMENT

USING ISO 31000

DECEMBER 2010

The Institute of Internal Auditors

Table of Contents

Executive Summary

Many organizations are moving to adopt consistent and holistic approaches to risk management and recognize that risk management is a management process that should be fully integrated with the management of the organization. It applies at all levels of the organization — enterprise level, function level, and business-unit level.

The risk management framework must be designed to suit the organization: its internal and external environment. For risk management to be effective, the framework in any organization, regardless of size or purpose, should contain certain essential elements. This guide details three approaches to assurance of the risk management process: a Process Elements approach; an approach based on Principles of Risk Management; and a Maturity Model approach. The assurance process that is used should be tailored to the organization's needs.

Internal auditors should have a means of measuring the effectiveness of risk management in an organization. This can be achieved by the examination of criteria that reflect aspects of the risk management process. The criteria used must be relevant, reliable, understandable, and complete. The aggregate of the observations should allow the auditor to form a conclusion on the organization's level of risk management maturity.

The quality of an organization's risk management process should improve with time. Implementing effective risk management — true ERM — often takes several years. One of the key criteria that internal auditors should consider is whether there is a suitable framework in place to advance a corporate and systematic approach to risk management.

This practice guide uses ISO 31000 as a basis for the risk management framework. Other frameworks may be used to perform the risk assessment. This guidance does not imply implicit or explicit endorsement of this or any other framework.

Introduction

Over the last few years, the importance of managing risk as part of strong corporate governance has been increasingly acknowledged. Organizations are under pressure to identify the significant business risks they face — social, ethical, and environmental as well as strategic, financial, and operational — and to explain how they manage them. The use of enterprise-wide risk management frameworks has expanded as organizations recognize the advantages of coordinated approaches to risk management.

Risk management is defined in the Glossary of the International Standards for the Professional Practice of Internal Auditing (Standards) 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."[1] A comprehensive risk management framework provides an end-to-end link between objectives, strategy, execution of strategy, risks, controls, and assurance across all levels in the organization.

Enterprise risk management (ERM) — or more properly enterprise-wide risk management — is a term in common use. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) 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."

ISO 31000 (Section 4.1) states that the success of risk management "will depend on the effectiveness of the

[1] This is consistent with the International Organization for Standardization's (ISO's) definition of risk management, which is "coordinated activities to direct and control an organization with regard to risk." (ISO Guide 73:2009 Definition 2.1)

management framework providing the foundations and arrangements that will embed it throughout the organization at all levels."[2] A risk management framework refers to the components and organization of risk management within an entity.

Standard 2120 states "the internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes." It continues with the following interpretation.

"Interpretation: Determining whether risk management processes are effective is a judgment resulting from the internal auditor's assessment that:

- *Organizational objectives support and align with the organization's mission;*
- *Significant risks are identified and assessed;*
- *Appropriate risk responses are selected that align risks with the organization's risk appetite; and*
- *Relevant risk information is captured and communicated in a timely manner across the organization, enabling staff, management, and the board to carry out their responsibilities.*

The internal audit activity may gather the information to support this assessment during multiple engagements. The results of these engagements, when viewed together, provide an understanding of the organization's risk management processes and their effectiveness.

Risk management processes are monitored through ongoing management activities, separate evaluations, or both."

The starting point for improving an organization's approach to risk management should be a gap analysis that takes stock and evaluates what processes and systems are present now. If any of the essential parts are missing, it is highly unlikely that risk management will become effective. Internal auditors have an important role to play in assessing and improving risk management in their organizations, and assessing the organization's risk management activities is a critical component in that effort.

This practice guide uses the structure and some of the terminology of ISO 31000. While ISO 31000 is not designed as a basis for certification, its concepts and structures form a basis for assessing any risk management process. The ISO 31000 framework is not the only risk management framework in common use, and this guidance does not imply any endorsement of this particular framework.

Risk Management in the Organization

Governance

The ISO 31000 Risk Management Standard provides guidance for the framework of risk management applicable for organizations of any size. ISO 31000 defines a risk management framework as a "set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organization."[3] The risk management framework, regardless of the level of formality, is inherently embedded in an organization's overall strategic and operational policies and practices. Organizational arrangements include plans, relationships, accountabilities, resources, processes, and activities. The diagram on page 3 (Figure 1) shows a conceptual model that can be used for analysis of these arrangements.

The internal auditor should assess whether the framework takes into consideration and defines risk management responsibilities and the risk management strategy, and whether the elements of the framework allow for the building of a risk-smart workforce and environment while still allowing for responsible risk-taking and innovation.

[2]

[3] Ibid.

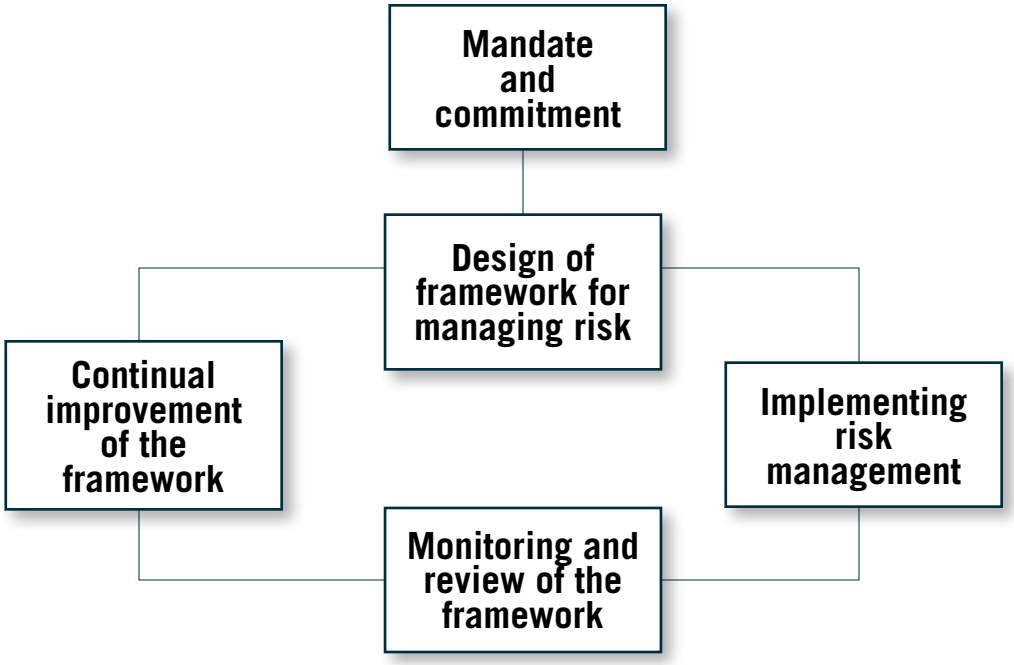

Figure 1 Framework for Managing Risk (ISO 31000)

Responsibilities for Risk Management

The International Organization for Standardization (ISO) defines risk attitude as an "organization's approach to assess and eventually pursue, retain, take or turn away from risk."[4] Management is responsible for setting the organizational attitude regarding risk and the board is responsible for determining whether the risk attitude is aligned with the best interests of shareholders.

Boards provide governance oversight of ERM and should understand key elements of ERM, ask management about risks, and concur on certain management decisions. Stakeholders should be given sufficient information to understand the risk attitude of management and the board, in order to invest in accordance with their tolerances for potential variation in performance. Organizations communicate levels of risk through quarterly and annual reports, press releases, investor calls, etc.

The board has overall responsibility for ensuring that risks are managed and that there is an adequate risk management system in place. In practice, the board will delegate the operation of the risk management framework to the management team. There may be a separate function with specialized skills and knowledge that coordinates and project-manages these activities, but everyone in the organization plays a role in ensuring successful enterprise-wide risk management, and the primary responsibility for identifying and managing risks lies with management.

Monitoring and Assurance

The application of ERM changes over time. The risk attitude can change due to internal or external factors, once-effective risk responses may become irrelevant, and control activities may become less effective or no longer be performed. Changes can be brought about by the arrival of new personnel, changes in entity structure, or

[4]

introduction of new processes. Furthermore, entity objectives, as well the nature of potential events or conditions that may affect the achievement of those objectives, will change. Accordingly, management needs to determine whether the ERM components continue to be relevant and able to address new risks.

A critical element of a sound risk management system is monitoring to ensure it is performing as intended. Monitoring can be done in two ways: through ongoing activities or separate evaluations. This combination of ongoing monitoring and separate evaluations will ensure that ERM maintains its effectiveness over time.

ERM processes incorporate periodic evaluation of risks and risk ratings. The greater the degree and effectiveness of ongoing monitoring, the less the need there may be for separate evaluations. The frequency of separate evaluations necessary for management to have reasonable assurance about the effectiveness of ERM is a matter of management's judgment. In making that determination, consideration is given to the nature and degree of changes, the competence and experience of the people implementing risk responses and related controls, the nature and significance to the business of the risks that are being managed and the results of the ongoing monitoring.

Ongoing monitoring is built into the normal, recurring operating activities of an entity. It can be more effective than separate evaluations, because it is performed on a real-time basis, reacting dynamically to changing conditions, and is ingrained in the entity. Problems will often be identified most quickly by ongoing monitoring processes since separate evaluations take place after the fact. Some entities with sound ongoing monitoring activities will nonetheless conduct a separate evaluation of ERM, or portions thereof. The perceived level of objectivity is greater for separate evaluations than for self-monitoring.

An entity that perceives a need for frequent separate evaluations should focus on ways to enhance its ongoing monitoring activities and, thereby, to emphasize "building in" rather than "adding on" monitoring activities.

The need for assurance arises from the governance processes of an organization. Its origin is in the stewardship relationship between the board of an organization and its stakeholders. This stewardship relationship positions boards to 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 allow the board to monitor the exercise of that power.

The internal audit activity will normally provide assurance over the entire risk management process, including risk management activities (both their design and operating effectiveness), management of those risks classified as "key" (including the effectiveness of the controls and other responses to them), verification of the rigor and reliability of risk assessments, and reporting of the risk and control status.

With responsibility for monitoring and assurance activities traditionally being shared among various parties, including line management, internal auditing, risk management specialists, and the compliance function, it is important that assurance activities be coordinated to ensure resources are used in the most efficient and effective way. It is common for organizations to have a number of separate groups performing different risk management advisory, 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.

The chief audit executive (CAE) is directed by Standard 2050 to coordinate activity with other assurance providers. The use of an assurance map can help achieve this, offering an effective tool to manage and communicate this coordination. Practice Advisory 2050-2 provides more information regarding Assurance Maps.

Internal Auditing and Risk Management

Standard 2100 states that "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.

In support of the risk management process, internal auditing and other independent assurance providers would assess whether:

- The risk management process has been applied appropriately and all elements of the process are suitable and sufficient.
- The risk management process is in keeping with the strategic needs and intent of the organization.
- All significant risks have been identified and are being treated.
- Controls are being correctly designed in keeping with the objectives of the risk management process.
- Critical controls are adequate and effective.
- Review by line management and other nonaudit 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 will:

- Establish an organization-specific, documented risk management framework.
- Provide a structured analysis of the risks of the organization recording:
  - The organizational objective(s) and their associated risks.
  - Potential exposures and assessments of current risk.
  - The organizational position responsible for managing each risk.
  - The key control systems established to manage each risk.

It is not uncommon for the internal audit activity of an organization to work in close cooperation with the risk management function. Some organizations do not have a formal risk management function and, in this case, internal auditing often provides more extensive risk management consulting services to the organization. Internal auditing may provide risk management consulting, provided certain conditions apply:

- It should be clear that management remains responsible for risk management. Whenever internal auditing consults with the management team to set up or improve risk management processes, its plan of work should include a clear strategy and timeline for migrating the responsibility for these activities to members of management.
- Internal auditing cannot give objective assurance on any part of the risk management framework for which it is responsible. Such assurance should be provided by other suitably qualified parties.
- The nature of such services provided to the organization should be documented in the internal audit charter and be consistent with other internal audit responsibilities.

- Any consulting advice or challenge to (or support of) management's decision-making does not involve internal auditing making risk management decisions themselves.

The IIA Position Paper "The Role of Internal Auditing in Enterprise-wide Risk Management" includes the following diagram that illustrates a range of ERM activities and indicates which roles an effective professional internal audit function should and should not undertake.

Internal Audit Review of Risk Management

For higher risk areas where management has acknowledged the need to improve controls, there may be an opportunity for internal auditing to add value to the organization through consulting activities. The middle third of audit activities in Figure 2 above represent advisory and consulting activities, delivered at the entity or business unit/departmental level, in a manner that should maintain internal auditing's independence and objectivity.

Although such advisory and consulting activities can be a valuable part of an audit plan, the scope of this Practice Guide focuses on the assurance activities described on the left side of the fan. Such activities can be categorized in three primary types:

- Assurance on the risk management process itself.
- Assurance on significant risks and management assertions.
- Follow-up of risk treatment plan status.

Assurance on the Risk Management Process

Assurance on the risk management process itself can be performed to provide reasonable assurance to senior management and the board that an organization's risk management program is effectively designed, documented, and operating to achieve its objectives. Potential questions that such assurance should be designed to answer could include:

- Does the risk management program have adequate commitment from organization management, including adequate stature and resources in relation to

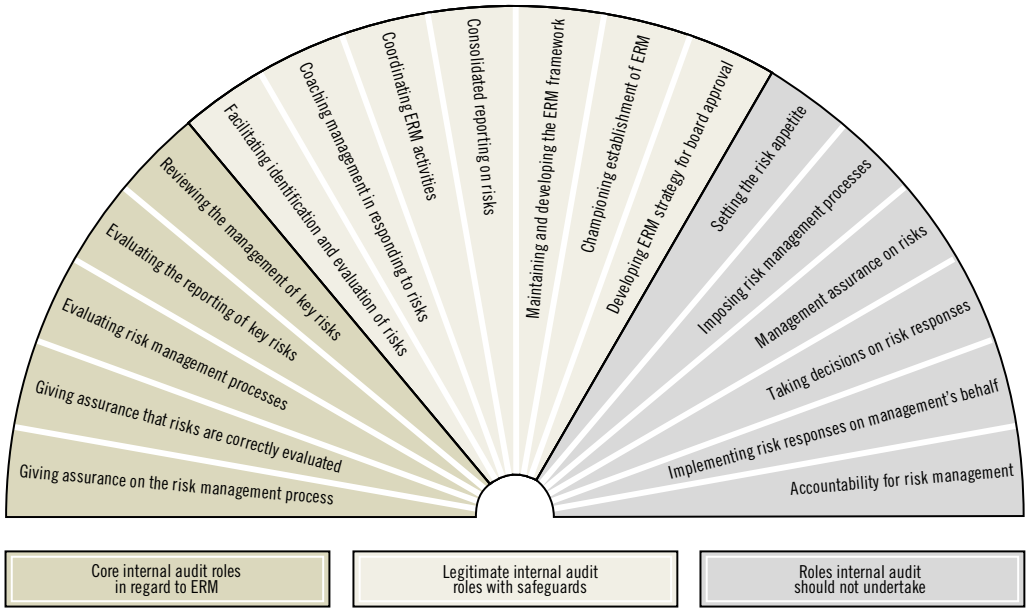

Figure 2 – Internal Audit Role in ERM

risks, and is it an appropriate part of organizational processes and decision-making?

- Are the risk management framework design and risk evaluation criteria appropriate for the internal and external context (environment) of the organization?
- Is there adequate definition and communication of requirements, risk evaluation criteria, and accountability for the development, implementation, and maintenance of the risk management framework and specific risk area evaluations?
- Is the risk attitude established at the proper level in the governance structure of the organization?
- Are internal communication and reporting mechanisms adequate to ensure that key outcomes of the risk management activities are communicated appropriately within the organization (balancing transparency with sensitivity)?
- Do reports to stakeholders adequately reflect the organization's attitude to and treatment of risks?
- Are external communication and reporting mechanisms adequate to comply with relevant legal, regulatory, corporate governance, and disclosure requirements?
- Do adequate performance measures and reporting exist to monitor the design and effectiveness of the risk management framework?
- Are risk evaluation criteria, appetites, responses, and escalation/reporting requirements consistently applied in practice across the organization? Are people with the appropriate knowledge responsible for risk identification? Is the current state of risk identification adequate?
- Are the risk framework and related processes and controls modified as business conditions and organizational needs change?
- Are people with the appropriate knowledge responsible for risk analysis, evaluation, and treatment/response? Are these activities adequately reviewed and approved?
- Are risk treatment plans and status monitored and adequately communicated with appropriate levels of management and the board?

Assurance on Significant Risks and Management Assertions

During all other assurance work where the scope relates to higher potential exposures identified in an organization's risk management process, 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 in a risk-based audit plan will provide assurance not only over those specific risk areas, but serve as assurance of the effectiveness of the overall risk management process.

Follow-up of Risk Treatment Plan Status

For risk treatment or control remediation plans relating to higher potential exposures, especially where plans are relatively longer in duration, it may be appropriate to monitor performance against the plan. At a minimum, such monitoring should be designed to provide management with an assessment of progress against milestones and validate risk treatment plan status reports to the board.

In addition, such monitoring can assess the plan structure, resources, accountabilities, project management, etc. and provide recommendations and considerations to enhance the likelihood of plan success.

Obtaining Audit Evidence

In audits of the risk management process of an organization, Practice Advisory 2120-1, Assessing the Adequacy of Risk Management Processes, paragraph 8, states:

"Internal auditors need to obtain sufficient and appropriate evidence to determine that the key objectives of the risk management processes are being met to form an opinion on the adequacy of risk management processes. In gathering such evidence, the internal auditor might consider the following audit procedures:

- 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 and board minutes to determine the organization's business strategies, risk management philosophy and methodology, appetite for risk, and acceptance of risks.
- Review previous risk evaluation reports issued by management, internal auditors, external auditors, and any other sources.
- Conduct interviews with line and senior 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 and actions taken to remedy issues raised by risk management processes.
- Determine the effectiveness of 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.
- Review risk-related issues that may indicate weakness in risk management practices and, as appropriate, discuss with senior management and the board. If the auditor believes that management has accepted a level of risk that is inconsistent with the organization's risk management strategy and policies, or that is deemed unacceptable to the organization, refer to Standard 2600 and related guidance for additional direction."

Different techniques can be used to obtain audit evidence, including:

- Observations — for example, by being present when risk management is carried out at the different levels of the organization from the board and all the way down to individual departments, programs, projects, and the employees.
- Interviews.
- Document reviews — for example, agendas, supporting documents and minutes from board, executive, or other senior management committees, strategic plans, and supporting documents for resourcing decisions.
- Results from previous audits.
- Reliance on the work of others.
- Analytical techniques — for example, root cause analysis of detected faults.
- Process mapping.
- Statistical analysis — for example, analysis of the types of incident or "near misses."
- Risk model review and assessment.

- Surveys.
- Analysis of control self-assessment.

Often, a combination of different audit techniques will be used to gather sufficient information and evidence to reach a conclusion. The auditor selects the most appropriate procedure for the audit objective of the assignment. The auditor also assesses whether sufficient resources and skills are available to perform all the work required to provide sufficient support for an opinion. The auditor considers whether it might be prudent to decline to express the opinion or to qualify the opinion by excluding certain areas or risks from the scope of the opinion if sufficient resources or skills are not available.

The requirement for evidence will vary depending on the kind of opinion the auditor wishes to render. Positive assurance provides the highest level of assurance and normally also requires the most evidence to support the opinion. Such an opinion implies not only, for example, whether controls/risk mitigation processes are adequate and effective, but also that sufficient evidence was gathered to be reasonably certain that evidence to the contrary, if it exists, would have been identified.

Negative assurance does not provide as much assurance and therefore normally does not require as much audit evidence. When rendering negative assurance, the auditor, for example, states that based on the work done, nothing came to the auditor's attention. By rendering such an opinion, the auditor takes no responsibility for the sufficiency of the audit scope and procedures to find all significant concerns or issues. Such an opinion is generally considered less valuable than positive assurance.

More extensive guidance on opinions can be found in the Practice Guide "Formulating and Expressing Internal Audit Opinions."

Audit conclusions should be factual, objective, and backed by sufficient audit evidence. Sufficiency implies the audit evidence is factual, adequate, and convincing so that a prudent, informed person would reach the same conclusions as the auditor. Audit evidence must be appropriately documented and organized.

The audit activity must not unknowingly provide any level of false assurance (reference PA 2120-2: Managing the Risk of the Internal Audit Activity, paragraph 8). "False assurance" is a level of confidence or assurance based on perceptions or assumptions rather than fact. In many cases, the mere fact that the internal audit activity is involved in a matter may create some level of false assurance. The scope of internal audit activity involvement may be misunderstood and, consequently, false assurance may result.

Assurance of the Risk Management Process

A governing body should be able to determine the extent to which the risk management process in its organization meets the needs of the organization and has adopted generally accepted good practice. Risk management is a critical component of the system of internal control, so deficient risk management processes are an indicator that the organization's system of internal control may be deficient.

It is important that an organization obtains assurance on its risk management process. This assurance must accommodate the possibility that the internal auditor might not be functionally independent of the risk management function. In this case, assurance may be sought from an external party.

Three forms of assurance process that may be used in assessing a risk management process are outlined below:[5]

[5] These approaches are quoted from HB158:2010 Delivering assurance based on ISO 31000:2009 Risk management — Principles and guidelines, A joint publication of Standards Australia, IIA-Australia, and the IIA Research Foundation. HB158 provides a more extensive discussion of these and other issues.

- Process elements approach
- Key principles approach
- Maturity model approach

While each form is self-contained, they each offer a different perspective on the effectiveness of a risk management process in an organization. Often, the adoption of more than one approach can yield the most informative and useful results. The risk management process should be appropriately tailored to the organization, its size, culture objectives, and risk profile. Therefore, the assurance process also needs to be tailored to the organization's needs.

The results of any desk-based review must be validated by examining whether the risk management framework is operating effectively in practice. This means that this type of assurance activity should not be conducted in isolation and should always accompany or involve normal control-based assurance that determines whether:

- Risks are being effectively identified and appropriately analyzed.
- There is adequate and appropriate risk treatment and control.
- There is effective monitoring and review by management to detect changes in risks and controls.

Process Element Approach

This approach checks whether each element of the risk management process is in place. It is essential to validate management's expressions of intent through sufficient audit evidence to substantiate that the element is being satisfied in practice. Management representation alone would rarely be sufficient. ISO 31000 identifies seven components of the risk management process:

- Element 1 – Communication: Sound risk management requires structured and ongoing communication and consultation with those who are affected by the operations of the organization or activity.
- Element 2 – Setting the Context: The external environment (political, social, etc.) and internal environment (objectives, strategies, structures, ethics, discipline, etc.) of the organization or activity must be understood before the full range of risks can be identified.
- Element 3 – Risk Identification: Identifying the risks should be a formal, structured process that considers sources of risk, areas of impact, and potential events and their causes and consequences.
- Element 4 – Risk Analysis: The organization should use a formal technique to consider the consequence and likelihood of each risk.
- Element 5 – Risk Evaluation: The organization should have a mechanism to rank the relative importance of each risk so that a treatment priority can be established.
- Element 6 – Risk Treatment: Sound risk management requires rational decisions about risk treatment. Classically, such treatment is to avoid the activity from which the risk arises, share the risk, manage the risk by the application of controls, or accept the risk and take no further action.
- Element 7 – Monitor and Review: Monitoring includes checking the progress of treatment plans, monitoring controls and their effectiveness, ensuring that proscribed activities are avoided, and checking that the environment has not changed in a way that affects the risks.

Key Principles Approach

This approach is based on the concept that to be fully effective, any risk management process must satisfy a minimum set of principles or characteristics. ISO 31000

[6]

[7] Ibid.

includes a section (Clause 4) on these principles. An audit based on these principles would assess to what extent they are true for the risk management process in an organization:

- **Risk management creates and protects value.**[6] This implies the application of the most rigorous risk management when the value at stake is highest. It also suggests that a range of techniques applicable at various levels of exposure should be available in the organization.
- **Risk management is an integral part of organizational processes.**[7] Risk management should not be seen as an add-on task.
- **Risk management is part of decision-making.**[8] The more important the decision, the more explicit this association should be.
- **Risk management explicitly addresses uncertainty.**[9] Risk assessments would be expected to document areas of uncertainty and consider how best to address the uncertainty identified.
- **Risk management is systematic, structured, and timely.**[10]
- **Risk management is based on the best available information.**[11] Obtaining information can be expensive and the process should provide guidance on what constitutes sufficient information.
- **Risk management is tailored.**[12] It is not an out-of-the-box process and must match the operations of the organization.
- **Risk management takes human and cultural factors into account.**[13] The processes must be appropriate to the competence and culture of those who must use them.
- **Risk management is transparent and inclusive.**[14] There should be appropriate and timely involvement of stakeholders.
- **Risk management is dynamic, iterative, and responsive to change.**[15] The process should be regularly reviewed and respond to changes in the organization and its environment so that it remains relevant.
- **Risk management facilitates continual improvement and enhancement of the organization.**[16] Risk management should mature along with other organizational processes.

Maturity Model Approach

The maturity model approach builds on the assertion that the quality of an organization's risk management process should improve with time. Immature systems of risk management yield very little return for the investment that has been made and often operate as a compliance overhead or an imposition, more concerned with the reporting of risks than with their effective treatment. Effective risk management processes are developed over time, with additional value being provided at each step in the maturation process. This approach provides an assessment of where the organization's risk management process lies on the maturity curve, so that the board and management can assess whether it meets the current needs of the organization and is maturing as expected.

A key aspect of the Maturity Model approach is the linking of risk management performance and progress in the

[8] © ISO. This material is reproduced from either ISO 31000:2009 or ISO Guide 73:2009 with permission of the American National Standards Institute (ANSI) on behalf of the International Organization for Standardization (ISO). No part of this ISO material may be copied or reproduced in any form, electronic retrieval system or otherwise made available on the Internet, a public network, by satellite or otherwise without the prior written consent of ANSI. Copies of this standard may be purchased from ANSI, 25 West 43rd Street, New York, NY 10036, (212) 642-4900, http://webstore.ansi.org.

[9] Ibid.

[10] Ibid.

[11] Ibid.

[12] Ibid.

[13] Ibid.

[14] Ibid.

[15] Ibid.

[16] Ibid.

execution of a risk management plan to a performance measurement and management system. The outputs from such a system can be presented to senior management and the board as evidence of improvement in risk management. The components for such a system normally consist of:

- A protocol of performance standards, considering current approaches to risk management and anticipating future strategic needs. Performance standards are normally supported by a list of more detailed performance requirements that enable measurement of any improvement in performance.
- A guide to how the standards and sub-requirements can be satisfied in practice.
- A means of measuring actual performance against each standard and sub-requirement.
- A means of recording and reporting performance and improvements in performance.
- The periodic independent verification of management's assessment.

Clause 4 of ISO 31000 contains a list of practical and important "principles" that should be the starting point for any maturity evaluation. These principles address not only *"does the process element or system exist"* but also *"is it effective and relevant for your organisation"* and *"does it add value."* In fact, the first principle is that risk management must add value.

Actual performance against each performance standard is assessed using some system of maturity measurement that gives credit for intent, but full scores can only be obtained by the complete implementation and practical application of the standard. A possible system for measuring maturity (based on the original idea of Capability Maturity Models developed by the *Carnegie Mellon University*) is shown below.

MEASURE	NONE	VERY LITTLE	SOME	GOOD	COMPLETE
Meaning	Very little or no compliance with the requirement in any way.	Only limited compliance with the requirement. Management supports the intent, but compliance in practice is poor.	Limited compliance with element statement. Certainly agree with the intent, but limited compliance in practice.	Management completely subscribes to the intent, but there is partially complete compliance in practice.	Absolute compliance with the element statement — in intent and in practice — at all times and in all places.

Figure 3 - Maturity Model – source HB158

Assessing the Quality of Risk Management Documentation

The extent of documentation of an entity's ERM will vary with the entity's size and complexity. Larger organizations usually have written policy manuals, formal organization charts, written job descriptions, operating instructions, information system flowcharts, and so forth. Smaller, less complex organizations typically have considerably less documentation.

Many aspects of ERM may be informal and undocumented and yet can be regularly performed and highly effective. These activities may be tested in the same ways as documented activities. The fact that elements of ERM are not documented does not necessarily mean that it is not effective or cannot be evaluated. An appropriate level of documentation, however, usually makes monitoring more efficient. It is helpful in other respects too. It facilitates employees' understanding of how the process works and their particular roles, and makes it easier to make modifications when necessary.

In deciding to document the evaluation process itself, the internal auditor will usually draw on existing documentation of the entity's ERM processes. Existing documentation will typically be supplemented with additional documents prepared by the auditor, including evidence of the tests and analyses performed in the assessment process. The nature and extent of documentation normally is more substantive when statements about ERM are made to other parties.

When management intends to make a statement to external parties regarding ERM effectiveness, it should consider developing and retaining documentation to support the statement. The internal auditor should consider whether:

- A strategy for managing risk information from all sources is in place.
- Necessary infrastructure for communicating risk information is in place.
- There are common definitions.
- There are guidelines for the creation, deletion, and sharing of risk information.
- There are adequate resources assigned.
- Technology is cost efficient and used where appropriate.
- A proactive approach is taken for monitoring.
- Risk information is part of the planning process.
- Risk information is integrated with performance information.

These considerations and any decisions made to implement activities/processes should be documented. Such documentation may be useful if the statement is subsequently challenged.

Authors

Andrew MacLeod, CIA

Patricia A. MacDonald

Benito Ybarra, CIA

Trygve Sorlie, CIA, CCSA

Brian Foster, CIA

Teis Stokka, CIA

Reviewers and Contributors

Douglas J. Anderson, CIA

Steven E. Jameson, CIA, CCSA, CFSA

James A. Rose, III, CIA

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 International Professional Practices Framework. 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 www.theiia.org/guidance.

Disclaimer

Copyright

The Institute of Internal Auditors

GLOBAL HEADQUARTERS
247 Maitland Ave.
Altamonte Springs, FL 32701 USA

T: +1-407-937-1111
F: +1-407-937-1101
W: www.theiia.org