Perspectives on Enterprise Risk Management

The Institute of Internal Auditors

The Audit Committee: A Holistic View of Risk

Keeping Priorities in Order

Certainly, it is an understatement to say that today's audit committee members have a lot on their plates. A quick glance at an audit committee meeting agenda will reveal far more issues than can be adequately addressed during the few short hours reserved for an audit committee session. It is likely that audit committee members sometimes leave their meetings feeling less than perfectly satisfied with the comprehensiveness of the information they have received, or the thoroughness of their discussions.

Given their broad range of oversight responsibilities, what can audit committee members do to determine their agendas and priorities are appropriate? How can they ensure that the most critical issues rise to the top and subsequently get the attention they deserve?

From a big-picture perspective, there is nothing more important to an organization's success — or to its very survival — than its ability to manage risks.

It has been said that every risk ultimately results in a financial risk. Surely, that has proven true in many business failures over the years. Failure to pay attention to day-to-day activities, changes in the economy, and the demands of consumers and regulators have resulted in immeasurable financial losses. And unheeded risks to an organization's reputation have brought many a company to its knees.

In a KPMG/National Association of Corporate Directors survey of public company audit committees, 80 percent felt that failure, resulting from poor risk management, couldn't happen to them. However, 50 percent thought it could happen to other companies. Could these statistics point to a blind spot?

Are you fully aware of your organization's overall risk strategy? Has it clearly been articulated and have the risks been made fully transparent to you? Can you affirm that the risk process is robust, independent, and fully aligned with your organization's overall strategy? Is a risk management culture instilled throughout the entire enterprise?

Clearly, knowing about and understanding both internal and external risks that can potentially impact the organization, and ensuring that these risks are managed to an optimal level, should be top priorities for board and audit committee members. This, in short, is enterprise risk management, or ERM.

Why ERM is Important

Every entity, whether for profit or not, exists to realize value for its stakeholders.

Value is created by informed and inspired management decisions in all aspects of an entity's activities, from strategy setting to operations. Entities that fail to recognize the risks from both external and internal sources, and fail to manage those risks effectively can destroy value — in absolute or relative terms — for shareholders and other stakeholders, including the community and society at large.

Among the many outcomes of organizations' inability to effectively manage risks are bankruptcies, frauds, restatements of earnings, plummeting stock values, and loss of customers, careers, business partners, and overall credibility. Of course, managing risks optimally implies a balance between risk and reward — and clarification of acceptable risk thresholds.

ERM supports value creation by enabling management to:

- Deal effectively with potential future events that create uncertainty.
- Respond in a manner that reduces the likelihood of downside outcomes and increases the upside.

Effective ERM:

- Is an ongoing, entity-wide process to identify, evaluate, analyze, respond to, monitor, and communicate on risks.
- Is effected by people at all levels.
- Occurs in strategy setting.
- Applies to every unit.
- Provides reasonable assurance.
- Enables continuous improvement in decision-making.
- Helps achieve objectives.

Trends Toward Integration

The Conference Board — the global research organization best known for its Consumer Confidence Index and Leading Economic Indicators — identified and documented, among others, the following trends. These trends support shifting a board's focus toward ERM and its integration within the strategic oversight responsibilities of the board:

- Evolving legal developments, such as listing standards and regulations, make it prudent for directors to ensure they have a robust ERM oversight process in place.
- An increasing number of directors acknowledge they must oversee business risk as part of their strategy-setting role.
- Directors today believe strategic risk, rather than financial risk, is their key concern.
- Making ERM oversight improvements is critical to effective governance. Less than half of directors surveyed have access to robust techniques for risk oversight, and the majority do not use a ranking system as part of their risk assessment process.

ERM helps ensure effective reporting and compliance with laws and regulations and helps prevent losses — whether in the form of revenues or reputation. An ERM approach to risk is applicable to any organization, regardless of its industry or sector.

Inherent in the ongoing ERM process are a variety of activities that help an organization achieve its performance and profitability targets. These include aligning risk appetite and strategy, enhancing risk response decisions, reducing operational surprises and losses, identifying and managing multiple and cross-enterprise risks, seizing opportunities, and improving deployment of capital.

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) states that ERM is 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.

COSO's *Enterprise Risk Management — Integrated Framework* defines essential components, suggests a common language, and provides clear direction and guidance for ERM. Enterprise risk management requires an entity to take a "portfolio" view of risk, which examines the entire organization, from the enterprise level to a division or subsidiary, to the level of a single business unit's processes.

COSO

COSO is a voluntary private sector organization dedicated to improving the quality of financial reporting through business ethics, effective internal controls, and corporate governance. COSO comprises five major professional associations: The Institute of Internal Auditors (IIA), the American Accounting Association (AAA), the American Institute of Certified Public Accountants (AICPA), Financial Executives International (FEI), and the Institute of Management Accountants (IMA).

COSO's Framework

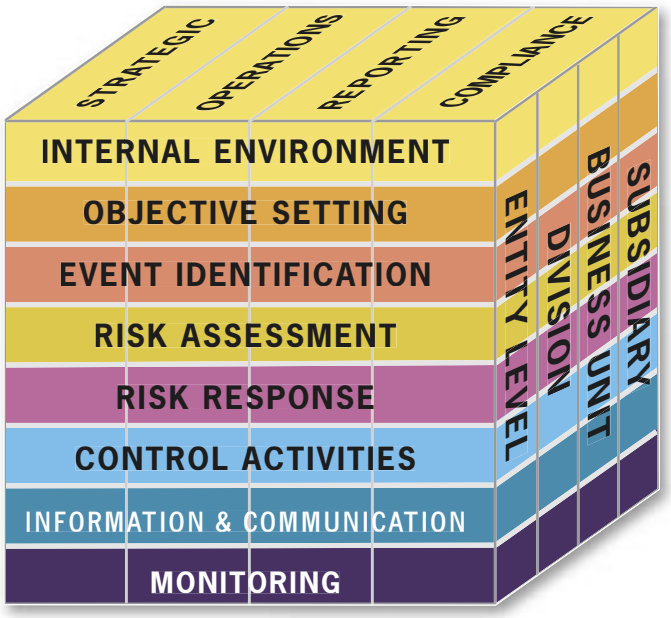
Within the context of an entity's mission or vision, management establishes strategic objectives, selects strategy, and sets aligned objectives cascading through the enterprise in four categories:

- Strategic – high-level goals, aligned with and supporting its mission.
- Operations – effective and efficient use of its resources.
- Reporting – reliability of reporting.
- Compliance – compliance with applicable laws and regulations.

This categorization of entity objectives allows a focus on separate aspects of ERM while taking a holistic approach to risk, and enabling management to consider how individual risks interrelate. The distinct but overlapping categories, as well as safeguarding of resources, address different entity needs and may be the direct responsibility of different executives.

ERM must be integrated with management processes. It examines eight interrelated components:

1. Internal Environment – management sets a risk philosophy and establishes the entity's risk culture and risk appetite.
2. Objective Setting – management considers its risk appetite in the setting of objectives.
3. Event Identification – management identifies the events, both internal and external, that present risk or opportunity to the organization. Opportunities are channeled back to strategy and objective-setting processes.
4. Risk Assessment – the likelihood and impact of risks are assessed to clarify the extent to which they might impact objectives. This employs a combination of qualitative and quantitative methodologies and forms a basis for the management of those risks.
5. Risk Response – management makes the decision as to whether the risk should be avoided, accepted, reduced, or shared; and then develops a set of actions to align the risks with the organization's risk tolerance.
6. Control Activities – policies are established to ensure management's risk responses are carried out effectively.
7. Information and Communication – thorough and timely communication takes place to ensure roles and responsibilities can be performed effectively in the process of identifying, assessing, and responding to risk.
8. Monitoring – ongoing ERM monitoring occurs, and modifications are made as warranted.



Risk Inventory

How does an organization begin to get a handle on risk and its effective management? According to The Conference Board, it is critical to take an inventory of risk factors pertaining to each driver of success.

The risk inventory should comprise financial (including market, credit, and liquidity risks and fraud), operational (including product risks, distribution channels, information security, and business continuity), business (including technological disruption, disintermediation, and competition changes), governance (CEO succession and compliance with laws and regulations), and human resource (employee relations and business conduct and ethics) risks.

Risk Management around the World

COSO's ERM Framework was designed for global application, and many organizations in countries around the world have embraced it and use it as a basis for their risk management efforts.

Other ERM resources and frameworks include:

- Federation of European Risk Management Associations: www.ferma.eu
- Foreign and Commonwealth Office: www.fco.gov.uk
- Australian Standard 4360 Risk Management Portal: www.riskmanagement.com.au
- IIA-UK and Ireland Risk and Control Knowledge Centre: www.iia.org.uk
- Risk Management Reports: www.riskreports.com
- Treasury Board of Canada's Integrated Risk Management Framework: www.tbs-sct.gc.ca *(search using keywords "Integrated Risk Management")*

Who's Responsible

Virtually no one within an organization is exempt from contributing to the effectiveness of ERM. Certainly, there's no substitution for establishing and maintaining high organizational standards in regard to ethical values and integrity of those who are hired. With this as a baseline, management and the board should ensure that risk management is embedded in everyday business decisions throughout the company on an enterprise-wide basis and that each aspect of the organization understands and owns its role in the ERM process.

While the board of directors provides monitoring, guidance, and direction, it is the CEO who has ultimate ownership for the organization's ERM. The CEO works closely with senior managers to set the tone at the top, which shapes the organization's values, principles, and policies that influence all aspects of the ERM process. A cascading responsibility exists, and each level of management in the organization should stay informed on and take ownership of the risks at that level.

A risk management team may be led by the chief financial officer or some other designee of executive management and the board. In some organizations, a chief risk officer serves as part of the management team and is assigned a role in the ERM process as a key job responsibility. This role, however, should be as facilitator or challenger. It is important for the organization to clarify roles so that all members of the management team understand their direct risk responsibilities.

Many corporate boards recognize a need for the organizations they serve to improve ERM capabilities. Based on extensive work in governance and risk, The Conference Board, together with McKinsey & Company and KPMG's Audit Committee Institute, makes six key recommendations for the effective oversight of ERM.

1. To begin with, whether assigned to the audit committee, a risk committee, or the full board, the responsibility for risk management oversight should be clarified, structured, and reflected in the charters.
2. The board should be well prepared to assume its oversight role by undergoing risk management training, participating in relevant discussions, and providing analysis of the organization's risk profile.
3. The organization's risk management process should include appropriate oversight of management's assessment of enterprise-wide risk, the controls in place to mitigate the risks, and the monitoring of risk.
4. An integrated reporting framework should consist of business unit reports aggregated to a company-level risk report, in conjunction with board reports.
5. A process should be in place to assess and monitor risk management performance, including addressing such issues as the effectiveness of committee structures and charters, the level of the board's understanding of risk policies, and the level of productivity of management and board communications.
6. There should be direct board interaction with the managers most acquainted with the organization's key risks.

Internal Auditing and the Audit Committee

The audit committee of the board of directors and the internal auditors are interdependent and should be mutually accessible, with the internal auditors providing objective opinions, information, support, and education to the audit committee; and the audit committee providing validation and oversight to the internal auditors.

A direct channel of communication between the chief audit executive (CAE) and the audit committee is essential.

The internal auditors regularly should report to the audit committee significant risk exposures and control issues, corporate governance issues, and other requested information.

The CAE and the audit committee also should meet at regular frequencies without management and the external auditors present. Clearly, the audit committee and internal auditors have interlocking goals, and should maintain a strong working relationship, mutual trust, and robust dialogue.

Audit Committee Checklist for Risk Management Oversight

- Know the extent to which management has established effective ERM.
- Be aware of and concur with the organization's risk appetite.
- Learn who is responsible for risk identification, assessment, and management throughout the organization; and meet periodically with those individuals.
- Discuss with management how risks, including fraud risks, are identified and how those risks are assessed in regard to likelihood and impact.
- Understand internal auditing's role and planned coverage, and meet periodically with the CAE to discuss ERM.
- Review financial reporting risks, weigh them against the organization's risk appetite, and discuss with management how effective the controls in place are to mitigate those risks.
- Ensure all audit committee members are receiving the information needed in the appropriate format, so that effective evaluation of the risk management process can be made.

SOURCE: The IIA Research Foundation handbook, *Audit Committee Effectiveness-What Works Best, 3rd Edition*

The *International Standards for the Professional Practice of Internal Auditing (Standards)* include safeguards for the internal auditors to apply so that independence and objectivity are maintained when providing assurance and consulting services.

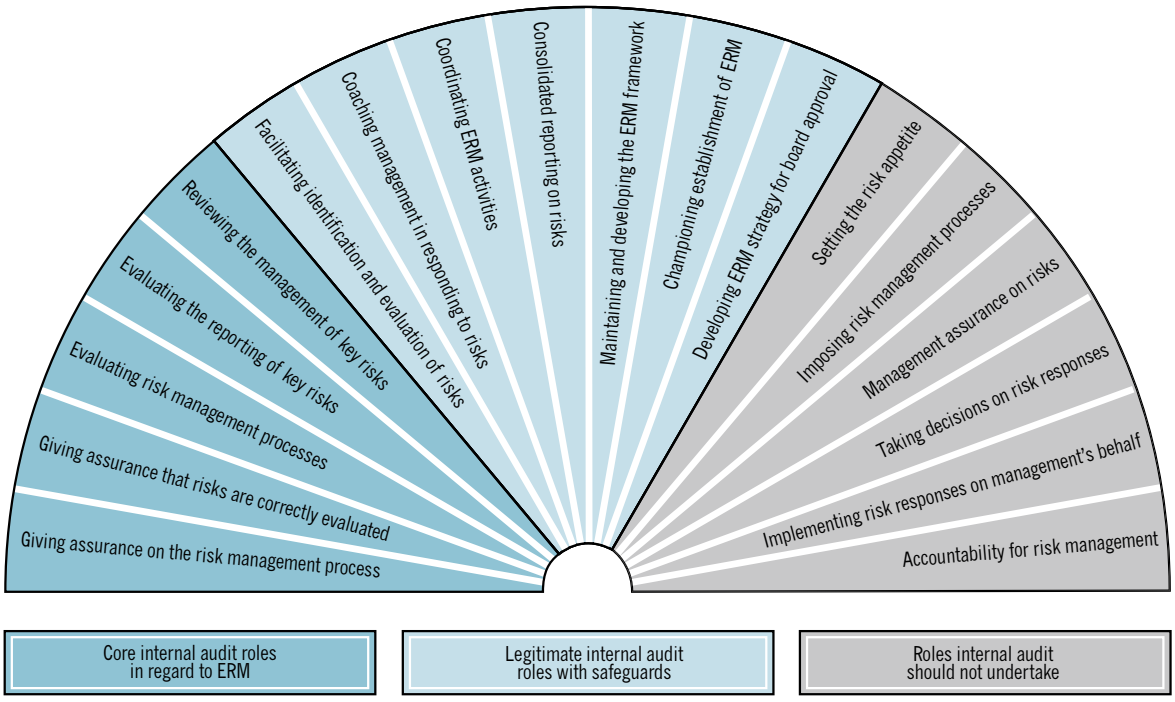
Internal Auditing's Value to the ERM Process

The Role of Internal Auditing in Enterprise-wide Risk Management, a position paper released by The Institute of Internal Auditors (IIA), discusses how the internal auditors add value. It identifies the two main factors a CAE should take into account when determining internal auditing's role in ERM. Does the activity raise any threats to internal audit independence and objectivity? Is it likely to improve the organization's risk management, control, and governance processes?

Although the internal auditors do not have primary responsibility for ERM implementation or maintenance, they play an important role in monitoring, examining, evaluating, and reporting on ERM. They also assist management and the board or audit committee by recommending improvements to ERM processes.

Internal audit activities may include:

- Reviewing the adequacy and effectiveness of the entity-wide ERM processes (including the processes to identify, analyze, manage, and report on risks) and providing recommendations for improvement.
- Reviewing critical control systems and risk management processes and responses for adequacy and effectiveness.
- Providing advice in the design and improvement of control systems and risk-mitigation strategies.
- Implementing a risk-based approach to planning and executing the internal audit process.
- Ensuring that internal audit resources are directed at those areas most important to the organization.
- Challenging the basis of management's risk assessments and evaluating the adequacy and effectiveness of risk-treatment strategies and the reliability of management's assurances.
- Providing assurances on the completeness, accuracy, and appropriateness of management's classification and reporting of risks.
- Facilitating ERM workshops.



Graphic designed by The IIA-UK and Ireland.

A Final Word

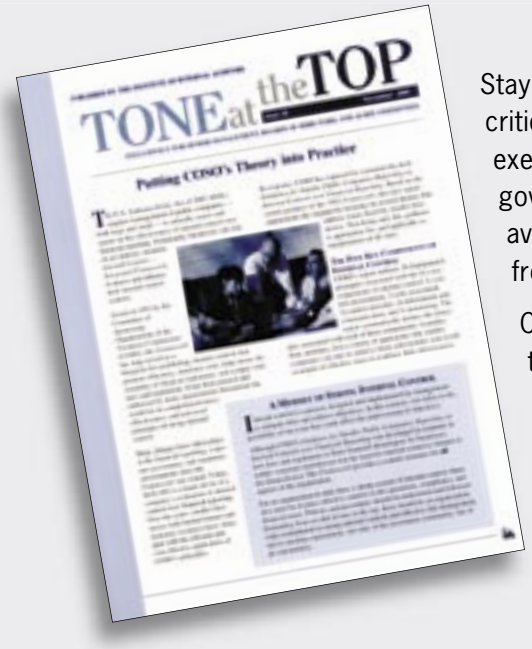
It is important to reiterate that enterprise risk management is not about eliminating risk. Without risk, there could be no change. And without change, growth could not occur.

ERM, however, takes a holistic view of organizational risks. This perspective enables management and the board to assess their "risk appetite," and to, based on intelligent examination, determine the level of risk throughout the organization they are willing to accept in pursuit of their mission or vision.

To fly, we have to have resistance.

– Mya Lin

FREE SUBSCRIPTION



Stay in the know about ERM and other issues critical to audit committees, boards, and executive management. The IIA's corporate governance newsletter – *Tone at the Top* – is available both electronically and in hard copy, free of charge.

Contact pr@theiia.org to ensure you receive this timely resource in the format of your choice. Please designate "Code E" when you make your request.

The IIA's guidance staff is available to respond to your questions about ERM and other governance issues. For more information, contact guidance@theiia.org at The IIA's global headquarters. Also visit the professional guidance section of The IIA's Web site at www.theiia.org for additional resources on risk, internal control, and governance.

THE INSTITUTE OF INTERNAL AUDITORS (IIA) is the acknowledged leader, recognized authority and chief educator for the profession worldwide. Established in 1941, The IIA has 246 affiliates around the world and serves more than 130,000 members in internal auditing, risk management, governance, internal control, IT auditing, education, and security in 160 countries.

The world's leader in certification, education, research, and technical guidance for the profession, The Institute sets the *International Standards for the Professional Practice of Internal Auditing* and provides leading-edge guidance. Serving as internal auditing's global professional association, The IIA certifies professionals through the stringent Certified Internal Auditor® (CIA®) program and specialty certification programs, such as the Certification in Control Self-Assessment (CCSA®), Certified Government Auditing Professional (CGAP®), and Certified Financial Services Auditor (CFSA®).

The IIA presents leading-edge conferences and seminars for professional development; promotes quality assurance and improvement; provides benchmarking; and creates growth and networking opportunities for specialty groups.

The IIA Research Foundation produces forward-thinking educational products and works in partnership with experts from around the globe conducting valuable research projects on the top issues affecting the business world today. The IIA also brings great value to its members through *Internal Auditor*, the award-winning professional magazine, and other outstanding periodicals that address the profession's most pressing issues and challenges and present viable solutions and exemplary practices.

As the global voice of the profession, The IIA promotes quality, professionalism, effective governance, ethical business practices, and world-class internal auditing. Dedicated to providing extensive support and services to help internal auditors add value across the board, The Institute delivers best-practice guidance and information to internal audit practitioners, executive management, boards of directors, and audit committees all around the world.

The Institute of Internal Auditors

247 Maitland Avenue
Altamonte Springs, FL 32701-4201 USA
Fax: +1-407-937-1101
Tel: +1-407-937-1100
Web: www.theiia.org

06544 – MF/GD