PUBLIC SECTOR KNOWLEDGE BRIEF

Internal audit’s role in enterprise risk management

Achieving strategic risk alignment without impairing independence

The Institute of
Internal Auditors

Contents

Introduction

ERM and internal audit provide assurances

Due to the global nature of today's business environment, there are many business opportunities, and just as many risks — both of which churn and change constantly. Because of this, organizations need to manage and monitor both the opportunities and the risks, and an enterprise risk management (ERM) framework is an important tool that can be used to provide assurance when facing those risks.

ERM is used throughout organizations for identifying strategic risks and for developing business practices to avoid surprises from those same that can lead to project failure, scandals, or significant damage to the organization. One of the most widely used ERM frameworks was developed by The Committee of Sponsoring Organizations of the Treadway Commission (COSO) in 2004 and updated in 2017. The COSO ERM Framework addresses the evolution of ERM and the need for organizations to improve their approach to managing risk to meet the demands of an evolving business environment.

ERM is a structured, consistent process that benefits the entire organization by identifying, assessing, deciding on responses to, and reporting on opportunities and threats that affect an organization's objectives. Now more than ever, organizations, including governments across the country, face unique risks. For the past decade or so, organizations have been working to establish their own comprehensive ERM programs, often with internal audit leading the process.

This knowledge brief, which includes information from a March 2018 IIA webinar by Crowe, will:

- **Explain ERM and its approach for establishing and maintaining an ERM program.**
- **Examine the roles of management and internal audit in the ERM process.**
- **Consider how management and internal audit can collaborate and remain distinct and independent throughout the ERM process.**
- **Discuss the evolving role of internal audit in ERM.**

A renewed focus on ERM components

Establish oversight and continuous improvement

Broaden the focus of risk management

As operating environments become increasingly complex, risks become more diverse and challenging to manage. Under traditional risk management approaches, the process can become somewhat fragmented; risk is viewed as something to be avoided; reactive and ad hoc behavior is accepted; and risk management activity is transaction-oriented (cost-based), narrowly focused, and functionally-driven (Guide to Enterprise Risk Management).

Under the ERM framework, the process is integrated; risk is viewed more positively (organizations take on the risks to seize opportunities); proactive behavior is expected; and the risk management activity is strategic, value-based, broadly focused, and process-driven (Guide to Enterprise Risk Management). ERM encourages a mindset that challenges the status quo.

More organizations have been looking to ERM to launch new programs or as a stimulus for existing programs. The goal is to establish the oversight to drive continuous improvement of risk management practices and the ever-changing operating environment. A broad process that is sometimes hard to focus on and fully understand, ERM covers the different risk components of government organizations, but due to the political workings inherent to government organizations, unique risks exist. The table on the next page identifies some of those risks.

Uncertainty — in and of itself — creates risk, and ERM broadens the focus of risk management to all significant resources of enterprise value. By understanding the key external and internal variables contributing to uncertainty, over time, management can more effectively run the organization and realize   the organization’s potential. ERM will help government organizations meet challenges by establishing oversight, control, and discipline to drive continuous improvement of risk management.

ERM Components and Risks

Component	Risk
Economies	Economies consistently send the message to government entities to do more with less. This message, delivered by budget cuts and constrained resources, can result in greater risks. As such, it has become challenging to segregate duties in order to provide for proper internal controls, and, with less resources, some required activities may be overlooked or even neglected entirely.
Regulators	New and existing regulatory requirements require a great deal of attention. Often complex, the requirements are heavily scrutinized, and noncompliance in some cases can have significant repercussions with regulatory agencies and through public perception.
Employees	The key risk here is trying to determine whether or not the employees are receiving what they need to perform their duties. Are they receiving adequate training and development related to their job responsibilities? Do they understand the new and evolving requirements related to their duties? Do responsibilities appropriately align with their development? Are they being provided with too much opportunity that may cause potential issues for the government?
Media and Public	Governments historically have relied heavily on the media and regulators for accountability, but currently the public sector is experiencing uncertainty in this area. Media management (e.g., social media) is receiving a great deal of focus as some of the risks that organizations face related to social media have played out in recent months.
Data Transparency	As technology advances, an increasing amount of data is available to entities. As that data's use is determined, the data may also be made available to the public — creating an additional risk.
Constituents	The focus in this area is to make sure that constituents remain well-informed, feel heard and supported, and have trust in the government.
Technology	Technology is a hot topic of discussion, particularly the subject of cyber security risk. Cyberattacks have led to loss of government data, theft of assets, reputational damage, and, in some cases, poor service delivery.

Source: Internal Audit's Role in ERM: Achieving Strategic Risk Alignment Without Impairing Independence, IIA webinar presented by Crowe, March 8, 2018.

Implementing an ERM framework

Manage uncertainties with a well thought-out plan

Redefine how business is conducted

The future is inherently unknown. Like all endeavors in today's dynamic business environment, government programs operate in a world of increasing risks, and they do not know what mandates or challenges they will face from day to day. In recent years, many government entities have been on the receiving end of new legislation and regulations that require them to better manage risk and improve controls in discrete areas. Generally, to comply with the requirements of each of these new mandates, agencies have put into place costly compliance programs that do not always optimize value (Managing Risk in Government: An Introduction to Enterprise Risk Management).

As government agencies search for more effective ways to face daily challenges, a promising approach is implementing an ERM framework. ERM redefines the value proposition of risk management by providing an organization with the processes and tools needed to become more anticipatory and effective at evaluating, embracing, and managing the uncertainties it faces, and elevates risk management to a strategic level (Guide to Enterprise Risk Management). An ERM framework:

- **Identifies potential risks that may hinder objectives.**
- **Empowers every member to participate in risk management.**
- **Reduces surprises and unexpected losses to the organization.**
- **Moves the focus to the big issues rather than the nebulous issues.**
- **Improves resource deployment based on risk.**
- **Provides tools and capabilities to identify, adapt, and respond to change.**

Occasionally, certain organizations find themselves starting down the path of developing and implementing an ERM program, including convening workgroups, obtaining support, developing a risk appetite, and preparing risk statements and draft responses, but then after the initial activities are performed, a variety of competing priorities may result. In order to protect the work and move forward, it is important to stay the course. The ERM framework can be successfully applied to all organizations, large and small, public and private, to create a risk-intelligent enterprise as long as it is embedded in the culture as a day-to-day consideration and everyone involved in its implementation is of the same mind.

For ERM to work effectively, there must be a full understanding of the organization's risk profile, its culture, and its resource capacity to implement and sustain the initiative. For some agencies, it will take a holistic approach to realize the full impact of risk management. For others, having some variation of ERM, no matter the scale or scope, will be enough to point the agency in the right direction toward better performance, management, and results. In either case, the aim is to redefine how business is conducted (Managing Risk in Government: An Introduction to Enterprise Risk Management).

Internal audit's evolving role

Opportunities to serve

Guidance to provide

Internal auditing is an independent, objective assurance and consulting activity Its core role with regard to ERM is to provide objective assurance on the effectiveness of risk management. Two of the most important ways that internal auditors add value are by 1) providing objective assurance that the major business risks are being managed appropriately and 2) providing assurance that the risk management and the internal control framework is operating effectively (The Role of Internal Auditing in Enterprise-wide Risk Management).

In the past, internal audit plans focused primarily on performing audits within the core financial functions of an organization, including accounts payable, payroll, and petty cash. Today, the scope of internal audit's work has expanded greatly and will more than likely continue to change. Internal audit has been asked to play a more dynamic role across all aspects of an organization and is expected to be more aligned with the overall strategic direction and risks.

Organizations are looking to internal audit to help refine risk management processes and leverage information about organizational risks. This includes providing ERM guidance. Collaboration between the disciplines of internal audit and risk management can lead to stronger risk practices in meeting stakeholder expectations.

However, it is important to note that each organization is unique. Each organization needs a tailored approach, and ERM is not a compliance exercise but a *mindset* that facilitates information-sharing across the organization, making management better equipped to make important and timely decisions.

The scope of internal audit's function and area of service is too wide for just one skillset. The emerging internal audit role now includes asset management, business models, change management, general management, environmental impact, products/services, finance, operations, compliance, and technology. Internal audit can play a critical role in the initial ERM setup and in its ongoing success by providing guidance in:

- **Risk management education and training.**
- **Risk management consulting engagements.**
- **Evaluations of strategic risks.**
- **Assessment of the ERM framework:**
    - **Components and principles are functioning as expected.**
    - **Components are operating in an integrated manner (no silos).**
    - **Established controls are adequate to execute the relevant principles**

Source: Internal Audit's Role in ERM: Achieving Strategic Risk Alignment Without Impairing Independence

Benefits to gain

There are several benefits to internal audit's being involved in the ERM program. One of the biggest benefits is that it adds to the value proposition of the internal audit department within the organization and with the key stakeholders. Value is added by seeking and exploiting opportunities, improving business performance, and preventing avoidable loss events. Internal audit's involvement changes the relationship with management into one that is cohesive and communicative vs. a relationship that is strained.

Benefits to the internal audit function:

- **Broader impact — not limited to compliance and financial statements.**
- **More robust and relevant internal audit plan.**
- **Increased knowledge and expertise in internal audit. Various growth and training opportunities for the internal audit staff.**

Benefits to the organization:

- **Improves management and leadership decision-making.**
- **Improves strategic planning efforts.**
- **Fosters a risk-based organizational culture (tone from the top).**
- **Establishes a foundation of knowledge to build a tailored ERM program.**
- **Links audit efforts and results to top-of-mind critical risks and initiatives as viewed by management.**
- **Enables the organization to plan and respond better to changes.**
- **Allows more effective management of the downside of risk while leveraging the upside of risk.**
- **Increases the probability of achieving the organization's goals and objectives.**

84%

of participants in an IIA webinar said they are willing to accept the role of ERM champion, but only in a supporting/ advisory capacity, with all decision-making authority and accountability residing with management.

7%

said they would not be willing to accept the role, as it would result in an impairment to auditor independence.

Source: Webinar polling questions from Internal Audit's Role in ERM: Achieving Strategic Risk Alignment Without Impairing Independence

Source: https://www.theiia.org/sites/auditchannel/Pages/video.aspx?v=AzdzRyZTE69KtDHsQ01KjSG2X4DVxJxo

However, it is important to note that in spite of all the benefits to gain, there are still a number of barriers preventing some government organizations from investing in ERM. Some of the challenges that are faced when designing an effective ERM program include: competing priorities, organizational culture, insufficient resources, lack of perceived value, perception that ERM adds bureaucracy, or lack of senior-level ERM leadership. In light of the perceived barriers, organizations need to have a viable risk management platform that addresses existing and potential risks and provides feedback to relevant people to evaluate and resolve.

Boundaries to draw and respect

Standard 1100: Independence and Objectivity requires the internal audit activity to remain independent. To implement this standard, CAEs and auditors need to understand policies and activities that could enhance or hinder such a mindset. Therefore, there are clear boundaries that must be drawn and respected when implementing an ERM framework. Those boundaries can be clarified using a simple litmus test:

Is it a management function (e.g., a decision-making role)?

✓ **If yes, this could impair independence.**

Is it an assurance function?

✓ **If yes, it may be an acceptable internal audit role.**

✓ **If lines are blurred, it may need additional safeguards to protect independence.**

There is of course a muddled middle ground to consider, where lines may be blurred. In these circumstances, the function is open to be performed by internal audit, provided safeguards are in place, such as taking steps to formally identify management as the decision-maker and communicating that understanding to management and other key stakeholders. Some examples include:

✓ **Facilitating risk assessment workshops.**

✓ **Coaching/educating management.**

✓ **Coordinating ERM activities.**

✓ **Maintaining the ERM framework.**

✓ **Serving as ERM champion.**

✓ **Developing the ERM strategy for leadership.**

Internal audit may provide consulting services that improve an organization's governance, risk management, and control processes.

Audit Focus

IIA Standard 1100: Independence and Objectivity

The internal audit activity must be independent, and internal auditors must be objective in performing their work.

IIA Standard 1110: Organizational Independence

The chief audit executive must report to a level within the organization that allows the internal audit activity to fulfill its responsibilities. The chief audit executive must confirm to the board, at least annually, the organizational independence of the internal audit activity.

> **1110.A1** – The internal audit activity must be free from interference in determining the scope of internal auditing, performing work, and communicating results. The chief audit executive must disclose such interference to the board and discuss the implications.

What's more, because internal audit offers expertise in considering risks, understanding the connections between risks and governance, and in facilitation, it is well qualified to act as champion for ERM, especially in the early stages of its introduction (IIA Position Paper: The Role of Internal Auditing in Enterprise-wide Risk Management).

When internal auditors have a detailed understanding of their duties, it allows them to provide the appropriate level of assessment work for the given situation.

Expanding internal audit’s position

Work closely with management

Creating a dynamic team

Internal audit should be a part of every ERM undertaking, as its principal role is to analyze the existing reporting tools and risk management practices, and seek out anything that could possibly impact the internal control systems.

That being said, when an organization desires to move to an ERM environment, internal auditors should collaborate with senior management to identify and review the risks that the organization is facing. Then internal audit can determine whether those risks have been identified and assessed properly. Doing so mitigates the possibility of overlooking gaps in policies and defines new risk tolerances.

As risks grow and become more complex, internal audit’s role is likely to expand in areas such as risk governance, culture and behavior, sustainability, and other non-financial measures.

Source: Internal Audit’s Role in Corporate Governance

To be effective, ERM requires a setting that is open and encourages communication about risks. Therefore, in addition to its principal role, internal audit can add value by being a proponent of solid communication within the organization, particularly between management and the stakeholders. Additionally, regular interaction with all factions, including employees, managers, and the risk management team will make a difference in the organization’s risk culture and in how well communication flows — eliminating barriers. The ERM framework, if executed properly, provides a valuable opportunity to create a dynamic team, wherein all are of the same mind when it comes to mitigating risks.

Identifying emerging risks

As organizations grow, adapt, and expand operations, the related risks may do the same. While some risks are easier to identify and measure than others, some are not as apparent. Here again is an opportunity for internal audit to add value by helping organizations discover any new risks created from expansion. Focusing on a number of areas internal audit has not traditionally covered can help auditors augment the organization’s value-creating efforts. There are many areas to consider in the context of a risk-based internal audit plan:

- Data analytics and continuous auditing.
- Strategic initiatives and planning.
- Tone at the top/corporate culture.
- New business lines and geographic regions.
- Tax strategy and planning.

In addition to identifying emerging risks, internal audit may extend its involvement in ERM, provided certain conditions apply, by coordinating certain reporting activities. The IIA maintains that the board and management are responsible for actual risk management (IIA Position Paper: The Role of Internal Auditing in Enterprise- wide Risk Management); however, internal audit can customize reporting to meet the organization's needs by issuing consultative types of reports for organizations that are in the initial stages of ERM, or by performing audits and issuing assurance reports for organizations that are more mature in ERM.

Staying in the proper lane

The interpretation of Standard 1100: Independence and Objectivity, affirms that "there should be no threat to internal audit's ability to carry out its responsibilities in an unbiased manner." So yes, certain conditions do apply to internal audit's role in ERM. In other words, while internal audit should update its role to support effective risk management, when it comes to management's responsibility of implementing risk mitigation processes and procedures, internal auditors and management alike need to understand fully that internal audit's advice is exactly that, advice. Anything more than that threatens internal audit's independence as an assurance provider and the objectivity of the internal auditors.

There are a range of ERM activities that will likely improve an organization's risk management control and governance processes, and there are roles that an effective internal audit activity should and should not undertake (see IIA Position Paper: The Role of Internal Auditing in Enterprise-wide Risk Management):

Internal Audit's Core Assurance Roles

- **Provide assurance on the risk management process.**
- **Provide assurance that risks are correctly evaluated.**
- **Evaluate the reporting of key risks.**
- **Review the management of key risks (including testing controls).**

Internal audit's roles with safeguards

- Facilitate identification and evaluation of risks.
- Coach management in responding to risks.
- Coordinate ERM activities.
- Consolidate reporting on risk.
- Champion establishment of ERM.

Roles internal audit should not undertake

- Setting risk appetite.
- Imposing risk management processes.
- Providing management assurances on risk.
- Making decisions on risk responses.
- Implementing risk responses on management's behalf.
- Assuming accountability for risk management.

Conclusion

Improve the way risks are managed

Management is aggressively pushing for internal audit to play a more prominent role in risk management, and with an ERM focus, internal audit can move beyond its monitoring role to help influence and improve how risks are managed before they become challenges. By facilitating the management on risk assessment and evaluating ERM, internal audit can add more value to the organization.

Internal audit's core role in relation to ERM is to provide management with assurance about the effectiveness of all risk management endeavors. When internal audit extends its activities beyond this core role, it must apply safeguards, including treating the engagements as consulting services, and therefore applying all relevant Standards. In this way, internal audit will continue to protect its independence.

Internal Audit's Role

- **Greater assurance that internal controls and risk management procedures are in place and aligned with objectives.**
- **Forward-looking efforts combined with the traditional point-in-time and past-focused reviews.**
- **Increased attention and commitment to focus on strategic and emerging risks.**

Sources

Enterprise Risk Management—Integrating Strategy and Performance (Committee of Sponsoring Organizations of the Treadway Commission (COSO), 2017). For more information, visit https://www.coso.org/Pages/erm.aspx.

Guide to Enterprise Risk Management: Frequently Asked Questions (Protiviti, 2006).

Internal Auditing's Role in Corporate Governance (IIA Position Paper, May 2018).

Internal Audit's Role in ERM: Achieving Strategic Risk Alignment Without Impairing Independence (Crowe, webinar presented for The IIA's American Center for Government Auditing, March 8, 2018).

Managing Risk in Government: An Introduction to Enterprise Risk Management, 2nd edition (IBM Center for The Business of Government, 2010). Written by Dr. Karen Hardy.

The Role of Internal Auditing in Enterprise-wide Risk Management (IIA Position Paper, January 2009).

About The IIA

The IIA is the internal audit profession's most widely recognized advocate, educator, and provider of standards, guidance, and certifications. Established in 1941, The IIA today serves more than 200,000 members from more than 170 countries and territories. The IIA's global headquarters are in Lake Mary, Fla. For more information, visit www.theiia.org.

Disclaimer

The IIA publishes this document for informational and educational purposes. This 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 material.

Copyright

The Institute of
Internal Auditors

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101