Role of Internal Audit in Enterprise Risk Management

Presentation by:

CPA Erick Audi

Thursday, 15th November 2018

Presentation Agenda

- Introduction & Definitions
- Role of IA in Risk Management
- Three lines of Defense Model
- IPPF Standards
- How Internal Audit Helps ERM
- How ERM Helps Internal Audit
- Developing Relationship between ERM and IA
- Collaborating the efforts of IA and RM
- Conclusions
- Questions and Answers

Introduction

The Institute of Internal Auditors defines Internal auditing as:

An ***independent, objective assurance and consulting activity designed to add value and improve an organization's operations***. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.

What do internal auditors do?

- Systematically analyzing business processes.
- Objectively assessing the effectiveness of processes.
- Independently reporting on their findings and making recommendations to improve the effectiveness of the processes.
- Using their knowledge to help spread good practices throughout the organization.

Definitions.....

- **Assurance–a positive declaration intended to give confidence**
- **Assurance Services:** An objective examination of evidence for the purpose of providing an independent assessment on governance, risk management, and control processes for the organization.
- **Consulting–giving professional advice**
- **Consulting Services:** Advisory and related client service activities, the nature and scope of which are agreed with the client, are intended to add value and improve an organization's governance, risk management, and control processes without the internal auditor assuming management responsibility.

Risk Management

- Risk Management is a structured, consistent and continuous process for identifying, assessing, deciding on responses to and reporting on opportunities and threats that affect the achievement of an entity's objectives.
- Risk is measured in terms of impact and likelihood.
- Risk management is a fundamental element of corporate governance
- Clearly, responsibility for Risk Management rests with the Board and Executive Management!

COSO Definition

ERM is a process……

- effected by an entity's board of directors and other personnel
- applied in strategy-setting and across the enterprise
- designed to identify potential events that may affect the entity
- manage risk to be within its risk appetite
- provide reasonable assurance regarding the achievement of entity objectives.

Risk Management Overview

IPPF Standards.....

Standard 2120

- The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes.
- **The IA needs to ascertain whether:**
- Organizational objectives support and align with the organization's mission;

IPPF Standards.....

- 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.

Role of IA in Risk Management

- The IIA issued a position paper on the role of internal auditing/assurance services with regards to risk management and consulting role they may undertake depending on the risk maturity of the organization.

- It is expected that as the **organization's risk maturity increases** and risk management becomes more embedded that **internal audit's role in championing risk management is reduced.**

Role of IA in Risk Management

The IIA Position Paper, The Three Lines of Defense in Effective risk management and Control, clearly outlines the operational line management as first level of defense; various risk and compliance functions as second line of defense and the internal audit as third line of defense.

In other words: those who manage risks, those who oversee risks, and those who provide independent assurance on risks.

"*A risk management function (and/or committee) facilitates and monitors the implementation of effective risk management practices by operational management and assists risk owners in defining the target risk exposure and reporting adequate risk-related information throughout the organization.*"

Role of IA in Risk Management

WHAT SHOULD IA DO –RISK MGT

- Internal auditing can provide consulting services (e.g. tools to used, co-ordinate) so long as they have no role in actually managing risks -that is management responsibility.
- **Tools** –can provide tools like risk register templates for a standardized approach
- **Co-ordinate** –IAs understand risks & controls so can champion and assist management, however senior management must actively be involved, endorse & support ERM

Role of IA in Risk Management

- Internal Audit is not responsible for the organization's risk management.
- The internal auditor should ***never assume any management responsibility for risk and should avoid being involved in any risk management activities that might compromise their independence or objectivity.***
- Prohibiting internal audit from having operational responsibility or authority over areas audited.

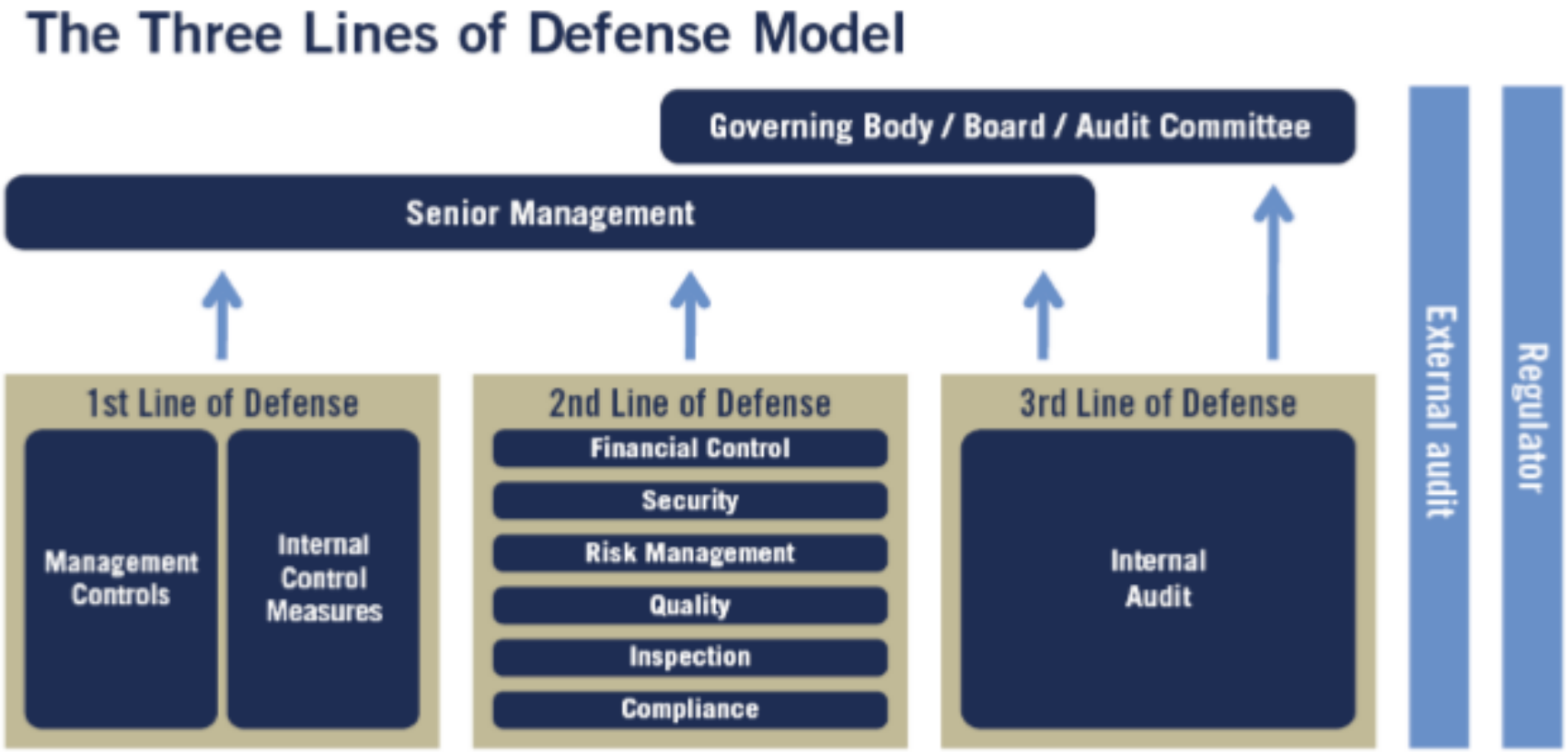
Role of IA in Risk Management

Where are you in your organization with regards RM and your roles as IA?

- *"The functional head for enterprise risk management (ERM) depends on maturity of the organization. In a smaller organization, CAE's can start and lead ERM as a functional head of governance, risk and compliance. Initially, the internal audit team can take it forward and after a period of time, internal audit has to decide on the best approach to hand over the risk management responsibilities."*

- *"If there is no risk management program in the company, then the CAE should take on and lead the risk function to begin with".*

The Three lines of Defense Model



Adapted from ECIIA/FERMA *Guidance on the 8th EU Company Law Directive, article 41*

First Line Defense

- Front-line employees must understand their roles and responsibilities about processing transactions.
- Employees must follow a systematic risk process and apply internal controls and other risk responses to treat the risks associated with those transactions.

- *Risk efforts are led by the chief financial officer or other officers in some of the companies. However, it is important to recognize the three lines of defense model here and the potential conflicts of combining a function that own and manages risks and a function that is primarily responsible for over-seeing risks.*

Second Line of Defense

- The enterprise's compliance and risk functions that provide independent oversight of the risk management activities of the first line of defense.
- Company may have their own management and governance committees as part of ERM structure, or have direct reporting lines into the ERM structures.
- Responsibilities include participating in the business unit's risk committees, reviewing risk reports and validating compliance to the risk management framework requirements

Third Line of Defense

- Internal and external auditors who report independently to the Board charged with the role of representing the enterprise's stakeholders relative to risk issues.
- The auditors review the first & second line of defense activities and results to ensure the ERM arrangements and structures are appropriate and are discharging their roles and responsibilities completely and accurately.
- *"Enterprise Risk Management as a second line of defense should have a degree of independence from the business managers although not necessarily as high as the Internal Auditing function."*

Role of IA in Risk Management

Assurance is obtained from:

- Management of the entity –periodic reports (effectiveness of the RM process, emerging risks, failures of control measures, etc.)
- Internal Auditors –who should provide independent & objective assurance on the effectiveness of the RM process
- Others –external auditors, etc.

Role of IA in Risk Management

- The risk lead role should report to an appropriate level of authority that provides adequate independence to facilitate transparent communication on risks. Ideally the lead role for risk efforts should have a functional reporting line to risk oversight authority where board or board subcommittee acts as the risk oversight authority.

- "*Where the lead role for the risk program is the chief risk officer, he or she should also have access to audit committee or other board level committee to have the required authority and autonomy.*"

Advantages of Internal Audit Involvement in ERM

- Gain insight into the organization strategy
- Understand what Executive Management is most worried about.
- Establish ourselves as risk experts in the organization
- Show that we can be part of the solution, not just identifying problems.
- Gain a “seat at the table”

What is Audit Looking at?

Reactive

Proactive

Professional View Point –Role of IA

- Clearly, Risk Management is a second level defense function while internal auditing is the third level of defense responsible for entity wide assurance including the adequacy of risk management processes. As pointed out previously the independence and objectivity of internal audit gives it the unique positioning as overall assurance provider. Internal audit functions are supposed to ensure and maintain its independence and objectivity as per the IIA standards.
- ***IIA position paper on The Three Lines of Defense in Effective Risk Management & Control*** clearly recognizes this difference which says, *"the high level of independence available and expected of internal audit function is not available in the second line of defense".* Hence, it is critical that internal audit maintains its objectivity and independence to discharge its responsibilities adequately.

Business View Point- Role of IA

- The argument in favor of internal audit taking over the risk role is that it is not practical to expect a dedicated risk function and team in organizations of *all size and nature.*
- Smaller organization might be unwilling to invest or may not be able to afford costs in risk management. In such cases, IA may provide support in establishing risk management.
- Another view point is that in organization where risk practices are not matured, assurance requirements may not be relevant or add value and therefore compromise of objectivity may not arise. In such circumstances, IA teams are better positioned to support ERM and to lead the efforts.

IA Assurance Roles.....

Internal auditors will normally provide assurances on three areas:

- Risk management processes, both their design and how well they are working;
- Management of those risks classified as '*key*', including the effectiveness of the controls and other responses to them; and
- Reliable and appropriate assessment of risks and reporting of risk and control status.

Internal Audit Consulting Activities

- Making available to management tools and techniques used by internal auditing to analyze risks and controls
- Being a champion for introducing ERM into the organization, leveraging its expertise in risk management and control and its overall knowledge of the organization
- Providing advice, facilitating workshops, coaching the organization on risk and control and promoting the development of a common language, framework and understanding
- Acting as the central point for coordinating, monitoring and reporting on risks
- Supporting managers as they work to identify the best way to mitigate a risk.

IA Core roles in RM

- Reviewing the management of key risks
- Evaluating the reporting of key risks
- Evaluating and giving assurance on the RM processes
- Giving assurance that risks are correctly evaluated.

IA Roles with safeguards

- Facilitating the identification & evaluation of risks
- Coaching management in responding to risks
- Coordinating ERM activities
- Consolidated reporting on RM
- Drafting RM strategy for board approval
- Championing the establishment of ERM

Roles IA should not perform

- Setting the risk appetite
- Imposing RM processes
- Providing assurance (on behalf of management) on risks
- Taking decisions on risk responses
- Implementing mitigations/controls on behalf of management
- Accountability for RM

IA roles -Conditions and safeguards

The following safeguards should be considered while internal audit takes on risk responsibilities:

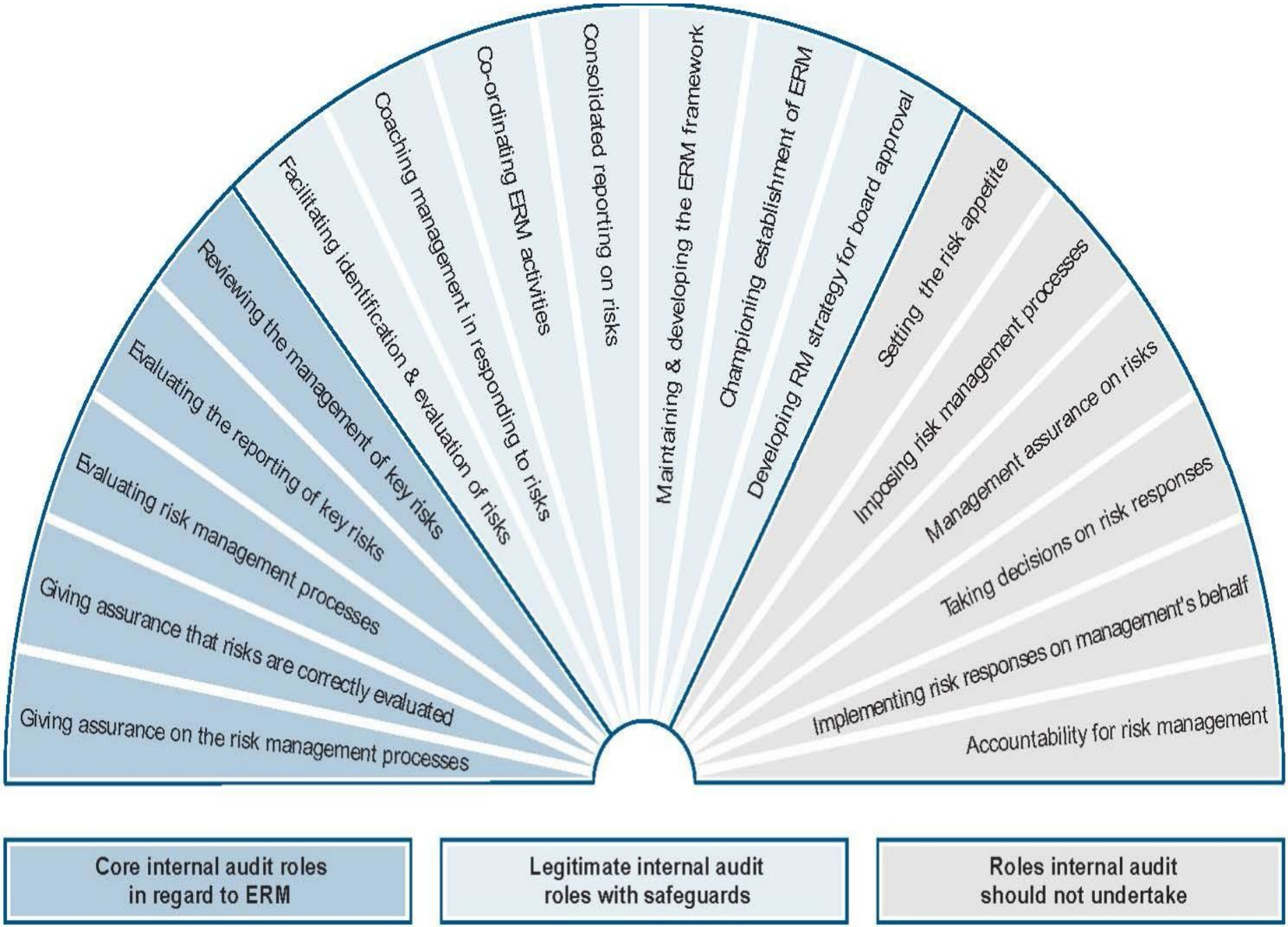
- Internal audit's responsibility of risk should be time bound and should be short term. IA should hand over risk role to the business or separate risk function once reasonable maturity of risk processes is attained. Internal Audit should have a clear road map in this regard.
- While internal audit may play an active role in implementing ERM, it should ensured that internal audit does not own risk.
- Internal audit team should abstain from directly being responsible for decision making on mitigating the risks while it can provide advice and needed support.

IA roles -Conditions and safeguards

- For large organizations, internal audit taking on risk role may not be appropriate unless it is during the initial years of implementing risk management.
- Overall risk to the organization from internal audit taking on risk role should be considered and evaluated.
- The potential compromise of internal audit's independence/objectivity and rationale for internal audit taking on risk responsibility along with evaluation of overall risk to the organization should be reported to the audit committee/board and the risk oversight body if different from board/audit committee.

IA roles -Conditions and safeguards

- Management remains responsible for risk management.
- Nature of IA's responsibilities should be documented in the IA Charter.
- Any work beyond the assurance activities should be recognized as a consulting engagement and the implementation standards related to such engagements should be followed.


Giving assurance on the risk management processes
Giving assurance that risks are correctly evaluated
Evaluating risk management processes
Evaluating the reporting of key risks
Reviewing the management of key risks
Facilitating identification & evaluation of risks
Coaching management in responding to risks
Co-ordinating ERM activities
Consolidated reporting on risks
Maintaining & developing the ERM framework
Championing establishment of ERM
Developing RM strategy for board approval
Setting the risk appetite
Imposing risk management processes
Management assurance on risks
Taking decisions on risk responses
Implementing risk responses on management's behalf
Accountability for risk management
Core internal audit roles in regard to ERM
Legitimate internal audit roles with safeguards
Roles internal audit should not undertake

How Audit Helps ERM

Evaluating Strategic Risks

- Has management identified strategic risks?
- Has management developed sound methodologies to mitigate those risks?
- Has management implemented monitoring to detect strategic risks before a disaster hits?

How Audit Helps ERM

Strategic risks are what sink the ship

- What role can IA play in strategy review?
- Has Risk Management been involved in strategy?

Sharing of Data

- Audit reports and annual risk assessment
- Information obtained from business units

How ERM Helps Audits

Allows Internal Auditors to:

- Better shape the work plan to address areas the organizations sees as high risks
- Advise leadership on overall organizational risk prioritizations
- Gaps in their plan: "What if" scenarios, inter-dependencies / cross organizational risks

Audit needs to assess its own "audit risk" to be included in the overall ERM

- Extensive communication with ERM.
- Risk Mitigation/Quantification.
- Audit Plan update.

What Internal Audit can do?

- **Educator:** CAE can help senior executives understand ERM
- **Facilitator:** risk assessments are needed and IA does that continuously.
- **Coordinator:** ensure there is consistent deployment across the organization.
- **Integrator**: assist with risk data collection and reporting of exposures and audit results
- **Evaluator:** review the effectiveness of ERM, etc.

Develop Relationships between IA & ERM

Talk to:

- People to find out what keeps them up at night
- ✓ *Board and Audit Committee*
- ✓ *Management and the people that do the work*
- Get out of the office and participate in organizational events
- Understand your audience for effective communications
- Relate this in risk terms that the audience understand
- Provide reports and services that add value

Collaborating the efforts of IA and RM

- Where separate risk functions exist, it is important to coordinate the activities of internal audit and risk
- Linking the audit plan and the enterprise risk assessment, and share other work products.
- Sharing available resources wherever and whenever possible.
- Cross-leveraging each function's respective competencies, roles and responsibilities.
- Assessing and monitoring strategic risks.

"The International Standards for the Professional Practice of Internal Auditing requires chief audit executives to "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."

Gaining Stature

- Have an opinion
- Be pro-active
- Be realistic with risk –don't overplay your hand
- When you raise the alarm, they will listen

Spread the Message

- Educate and train Audit Committee and Management on ERM.
- Find ways to provide risk management advisory services –not audits.
- Assess the risks of not having the right people and skills in your organization and mitigate as necessary.
- Seek opportunities to perform more risk management consulting services in support of whoever is managing the risk management program.

Practical Tips For Those with limited ERM Involvement

- Assess the feasibility of tying annual audit planning with the ERM process.
- Compare audit plan against the top risks identified through ERM
- Report on ERM risks through existing audits with an “Other Observations” or “Recommendations” section
- Consider a business continuity audit
- Ask to sit in on ERM committee meetings

Practical Tips For Those with No ERM Involvement

- Start small.
- Consider an audit of the company's overall risk management framework
- Incorporate corporate strategy discussions into annual audit planning
- Build a knowledge base by asking enterprise risk questions on existing audits
- Incorporate enterprise/strategic risk discussions into Audit Committee presentations.

Conclusion

- Internal Audit and ERM can work together to improve the risk profile of the organization.
- Internal Audit delivers significant value to the ERM process through collaboration and education
- Setting expectations with business and Risk Managers is critical to the success of the ERM program
- Auditing ERM is a function of ERM program and overall risk management maturity.
- Communication and reporting is a key feature of any IA and ERM function to improve the risk profile of the company

Conclusion

Internal auditors can assist an organization to achieve its objectives by not only utilizing its "process or control-based" knowledge, but also "risk-based" knowledge.

In addition, by facilitating the management on risk assessment, consolidating key risks faced by the organization, evaluating ERM and enhancing the internal control systems, internal auditing can create value for the organization.

Questions & Answers

Contacts: CPA Erick Audi

Email: eaudi@Kengen.co.ke or

audi.otieno@gmail.com

Mobile Nos: 0702-949 960 or

0721-693 705