
KUWAIT ENTERPRISE RISK MANAGEMENT CONFERENCE
4th Edition | 2017

ADNAN ZAKARIYA

Managing Director, Protiviti

Towards that Best Governance through a Collaborative approach to Risk

Session Overview

"The Corporate world is becoming increasingly complex with fresh risks and mitigating methodologies emerging every day. While businesses are putting a lot more emphasis on risk management, very little has been done on implementing an effective, disciplined and collaborative risk management program. This while creating the complexity for risk accountability and governance also creates an awesome opportunity for the internal auditors in pursuing newer audit activities through better collaboration with risk management and working towards a common goal in addressing the strategic risks to help organizations face the future with Confidence".

.

Key challenges associated with the above are:

- What is the role of Internal Audit and ERM with respect to Strategic risks?
- How does Internal Audit and ERM help Board and Audit Committee to discharge its oversight responsibilities, such as maintaining oversight of risk and the appropriateness of the system of executive compensation?
- Is Internal Audit really an enabler for establishing and regaining enterprise risk management momentum?
- What are the Core Internal Audit roles in regards to ERM?
- Where can Internal Audit play a legitimate role with safeguards?
- What are the grey areas in Risk governance which Internal Auditing should not undertake?

Our session on the "Journey Towards Best Governance" will address the above challenges along with the opportunities associated with improving and shaping to the new Challenges in Risk Governance

Risk Mitigating Methodologies

Internal auditing today – a reminder of the basic concept

Internal audit is not just about checking transactions and ensuring the records reflect the operational actions of the staff.

It is important to understand what internal audit is about and seeking to achieve and is defined as:

- Internal audit is an *independent(1), objective assurance(2)* and *consulting activity(3)* designed to *add value (4)* and *improve an organisations operations(5)*.

- It helps an organisation accomplish its objectives by bringing a *systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and processes(6)*.

Risk Overview

What is Risk?

Risk is defined as any event, action, or inaction that hinders an organization's achievement of its business objectives

Exposure to the consequences of uncertainty constitutes a risk

- Risk = "What Can Go Wrong?"
- Risk continues to exist, even with a control
- Risk has two attributes: Cause and Effect

There are many forms of risk in an organisation, eg reputational risk, strategic risk, compliance risk, operational risk, network security risk, legal risk.

To address risks more effectively, organisations may use a risk management approach that identifies, assesses, manages, and controls potential events or situations.

Risk may be viewed as:

- An influence on the achievement of a business objective.
- A possibility that the outcome of an action or event could bring adverse impacts resulting in direct losses of earning / capital or imposition of constraints on the organisation's ability to meet its business objectives.
- The probability that the actual return on an investment will differ from its expected return.
- The potential that a chosen action or activity (including the choice of inaction) will lead to a loss (an undesirable outcome).

Post Crisis Perspective – What Failed Us?

Remuneration Practices

- Bonus driven remuneration structures encouraged reckless/excessive risk taking
- Remuneration not linked to long term interests of the company and shareholders
- Remuneration problems at sales and trading function level
- Weak link between remuneration and performance (long-term strategy)
- Financial targets against which compensation was assessed not measured on a risk adjusted basis

Risk Management

- Failure to use ERM for informed management's decision making
- Stress testing and scenario analysis revealed several deficiencies in financial service providers
- Unclear transmission of risk information through effective channels (corporate governance issue)
- Mismanagement of Credit Risk
- Warning signs for Liquidity Risk ignored

Board Practices

- Structural Weakness: Absence of guidance for appropriate boardroom behavior
- Inadequate independent oversight of the executive management by Non-Executive Directors
- Lack of Quality Board Members
- Insufficient disclosure of material information on foreseeable
- Lop sided composition of Risk and Audit Committees

Shareholder (In)activism

- Disconnect between size of shareholding and voting behavior
- Lack of involvement and action by institutional shareholders reduced accountability of both boards and management

Risk Management : Missing Element

Some common risk management problems in Codes

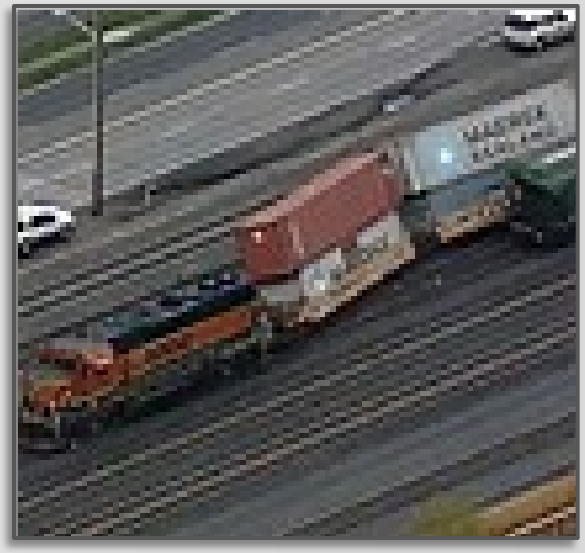
Key Findings

- Most Codes focused only on **Risk disclosures** by the company
- The Audit Committee requirements in the codes were in respect of "financial risk exposures".
- No explicit requirement for the whole board to consider the risk management processes and framework as a whole.
- Most Codes / guidelines in the world did not provide comprehensive guidance in developing a risk management and assurance framework.
- Risk management standards had lagged throughout the world

Source: Corporate Governance and the Financial Crisis : Key Findings and Main Messages, OECD, June 2009

Five Strategic Risks That Could Derail IIA's Progress

- Failure to concentrate on high-risk areas: "Where was internal audit?"
- The emergence of competitive risk, controls and governance functions that "outperform" us. (including IT systems performing audit functions)
- Failure to align with expectations of key internal audit stakeholders.
- High-profile failures of internal auditor integrity.
- Failure to embrace professional standards.



Internal Audit – The Journey so far

Providing Assurance on ERM

One of the key requirements of the board or its equivalent is to gain assurance that risk management processes are working effectively and that key risks are being managed to an acceptable level. It is likely that assurance will come from different sources. Of these, assurance from management is fundamental. This should be complemented by the provision of objective assurance, for which the internal audit activity is a key source. Other sources include external auditors and independent specialist reviews.

Internal auditors will normally provide assurances on three areas:

Internal Auditing's Role with Strategic Risks:

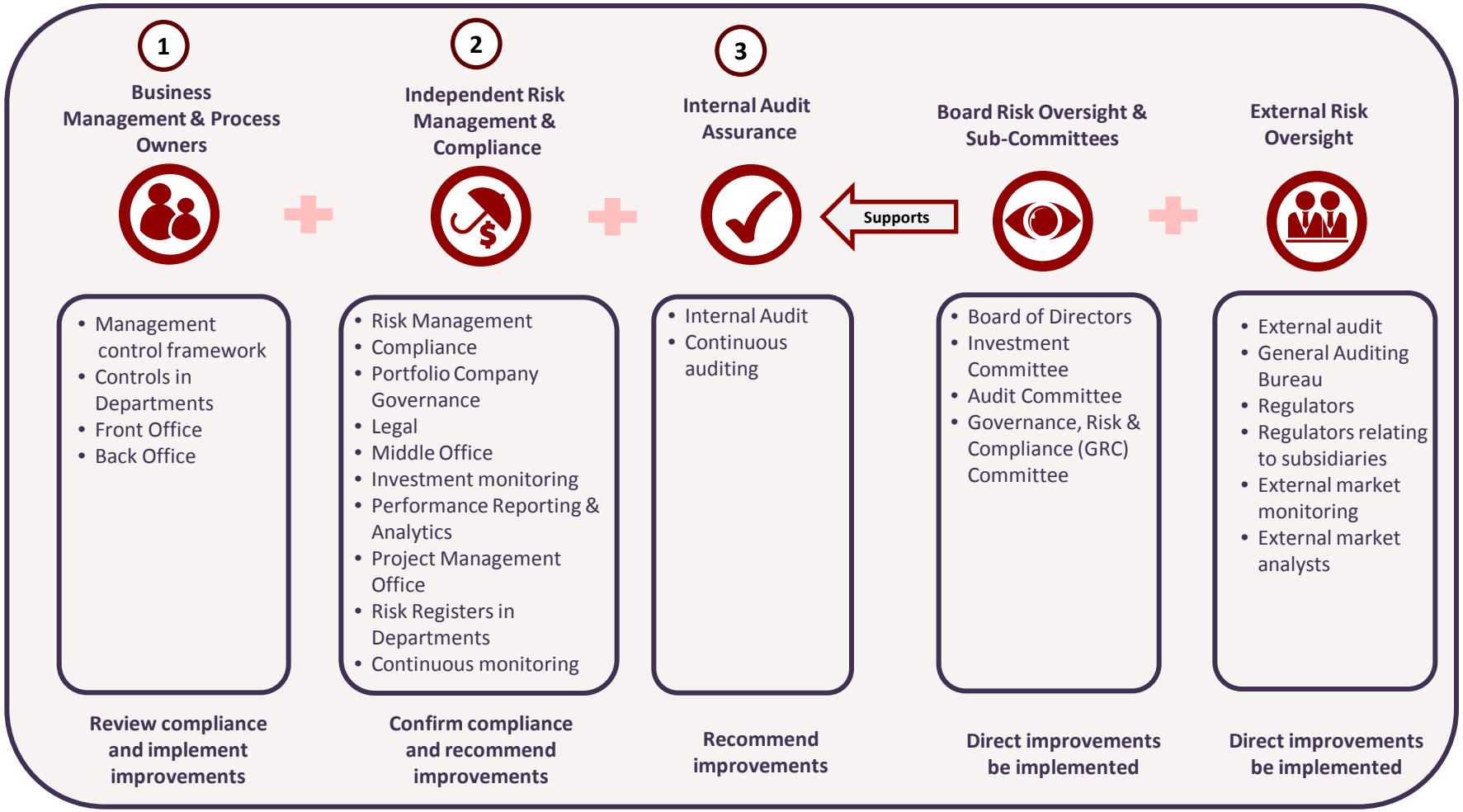
Strategic risks tend to be more difficult to identify, assess, and audit. As such, many internal audit activities spend little or no time on strategic risks.

- Ensure that the organization's audit committee, board of directors as a whole, or other board committee is giving appropriate attention to the organization's catastrophic and strategic risks and related risk management activities.
- Expand the internal audit risk assessment process to include an evaluation of the risks embedded in the organization's core business strategies or the strategies of the organization's primary lines of business.
- Consider how best to cover exposure to various elements of the organization's audit universe that are geographically dispersed and appear to have limited financial exposure or complexity.

Internal Audit – The Journey so far

	Checking Up to 1960s	Compliance 1960s – 1980s	System-based 1980s – 1990s	Risk-based 1990s – 2010s	Partnership 2010s –	Value-based Emerging
Independence	Independent of activities audited	Independent of activities audited	Independent of activities audited	Independent of activities audited	Independent of activities audited	Independent of activities audited
Serving	Finance	Finance	Finance / organization departments	Organisation departments	Organisation	Organisation
Reporting to	Generally CFO	Generally CFO	Generally CFO	Emerged to CEO and then Audit Committee reporting	Audit Committee for operations; CEO for administration	Audit Committee for operations; CEO for administration
Objective	Assurance	Assurance	Assurance	Assurance	Assurance & advisory; value-adding	Assurance and advisory; value-adding; proactive; key agent of change
Focus	Historical	Historical	Historical	Historical	Forward-looking	Forward-looking; insights
Coverage	**Controls**	**Controls**	**Controls**	**Controls**	**Governance, risk management, controls**	**Governance, risk management, controls**
Outcome	Detect mistakes	Detect mistakes	Improve controls	Improve organization department controls	Improve organization departments	Improve organization; actively seek innovation
Fraud focus	Detect fraud	Detect fraud	Detect fraud	Detect fraud	Prevent fraud	Prevent fraud
Reports go to	Management	Management	Management	Management; emerged to Audit Committee	Management and Audit Committee	Management and Audit Committee
Standards	No	Standards in 1978	Internal Audit Standards	Internal Audit Standards	Internal Audit Standards	Internal Audit Standards
Resourcing	In-house	In-house	In-house	In-house; emerged to co-sourced	Co-sourced; subject matter experts, guest auditors	Co-sourced; subject matter experts; guest auditors
Staff qualifications	Financial	Financial	Financial	Financial	Some non-financial disciplines	Many disciplines
Planning	Cyclical annual plan	Cyclical annual plan	Cyclical 5-year plan	Risk-based 3-year plan	Risk-based 3-year or annual plan	Risk-based rolling plan
Audit types	Compliance	Compliance	System	Operational	Integrated	Service catalogue
Management requested services	No	No	No	Some	Yes	Yes; many

Three Lines of Defense Model – Collaboration?

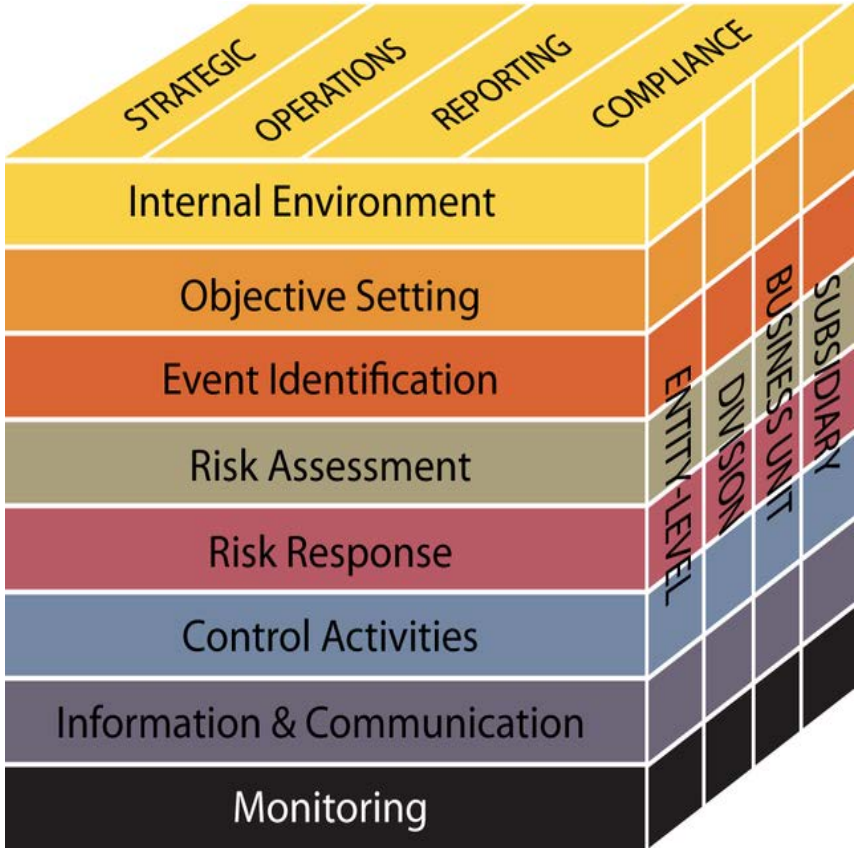


Linkage of risk appetite and strategy – Collaboration?

The key components of risk appetite, when integrated, present crucial links between risk, corporate and finance strategy.

- A well integrated risk appetite helps **direct corporate strategy** towards risk-adjusted growth options and optimize returns for shareholders while limiting the downside
- The risk appetite framework also forms the basis for **allocation of capital** within the organization crucial to the firm's finance strategy
- A well developed risk appetite framework also **enables the board and senior management to take important decisions** on extent of leverage to be undertaken and the allocative basis for a stable growth process. This has implications on corporate and finance strategy

COSO ERM vs. internal control framework – Overlaps?



What is an Internal Control Framework?

Core COSO Principles	Key Elements
▪ Principle 1: Integrity & Ethical Values ▪ Principle 2: Independence and oversight ▪ Principle 3: Structures, authorities and reporting lines ▪ Principle 4: Competent personnel ▪ Principle 5: Accountability	▪ Demonstrate commitment to integrity and ethical values ▪ Exercise oversight responsibility ▪ Establish structure, authority and responsibility ▪ Demonstrate commitment to competence ▪ Enforce accountability
▪ Principle 6: Specification of Objectives ▪ Principle 7: Identification of risks to objectives ▪ Principle 8: Fraud Risk Assessment ▪ Principle 9: Assessment of changes	▪ Specify suitable objectives ▪ Identify and analyze risk ▪ Assess fraud risk ▪ Identify and analyze significant change
▪ Principle 10: Development of control activities ▪ Principle 11: Technology based controls ▪ Principle 12: Policies based controls	▪ Select and develop control activities ▪ Select and develop general controls over technology ▪ Deploy policies and procedures
▪ Principle 13: Quality of Information ▪ Principle 14: Internal Communication ▪ Principle 15: External Communication	▪ Use relevant information ▪ Communicate internally ▪ Communicate externally
▪ Principle 16: On-going Monitoring / Separate Evaluations ▪ Principle 17: Internal Control deficiencies	▪ Conduct ongoing and/or separate evaluations ▪ Evaluate and communicate deficiencies

Moving Towards Best Governance

Governance Related to Risk Management

Robust governance arrangements, which includes a clear organizational structure with well defined, transparent and consistent lines of responsibility, effective processes to identify, measure, monitor and report the risks it is or might be exposed to, and adequate internal control mechanisms, including sound administrative & accounting procedures

Core Components of Corporate Governance Framework

Board & Management Structure	Management & Accountability	Transparency and Disclosures	Remuneration Practices

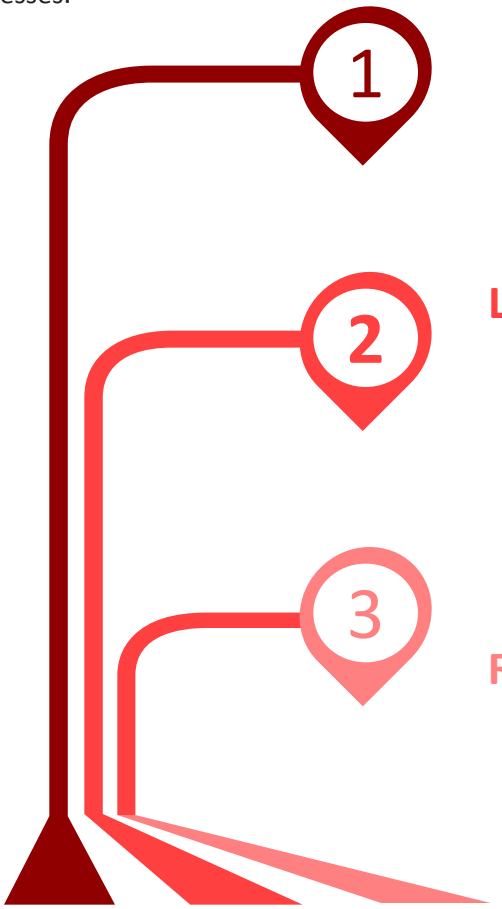
The core Corporate Governance components effectively translate into the following Risk Management Framework Components

Risk Management Framework

- **Risk Appetite and Strategy** → Define the levels of acceptable risks
- **Risk Tolerances and Limits** → Set tolerances and limits across geographies, business units, products
- **Risk Governance Framework** → Develop a sound governance structure for BoD, Committees, and functions with no conflicts of interest
- **Risk Mgmt Framework** → Develop a robust risk identification, assessment, measurement, control, monitoring and reporting framework
- **Risk Systems** → Implement risk systems based on the principle of proportionality
- **Risk Control and Oversight** → Develop effective risk control mechanisms and checks
- **Internal Audit** → Establish an independent audit function and promote its efficiency

Role of Internal Audit in ERM

Listed below are a range of ERM activities and indicates which roles an effective professional internal audit activity should and, equally importantly, should not undertake. The key factors to take into account when determining internal auditing's role are whether the activity raises any threats to the internal audit activity's independence and objectivity and whether it is likely to improve the organization's risk management, control and governance processes.



Core Internal Audit Roles

- Giving assurance that the control systems are effective
- Giving assurance on risk management processes
- Giving assurance that risks are correctly evaluated
- Evaluating Risk Management process
- Evaluating reporting of material risks
- Reviewing the management of material risks

Legitimate Internal Audit roles with safeguards

- Giving advice on identifying and evaluating risks
- Championing establishment of ERM
- Facilitating risks workshop
- Facilitating Management's response to risks
- Central coordinating point for ERM
- Monitoring risks across the business
- Holistic reporting on risks
- Operating the ERM Framework
- Developing RM strategy for board approval

Roles Internal Audit should not undertake

- Setting the risk appetite
- Imposing risk management processes
- Assurance by management on control and risk
- Taking decision on risk responses
- Managing risks on management's behalf
- Accountability for risks and controls

Legitimate Internal Audit Roles with Safeguards

Safeguards:

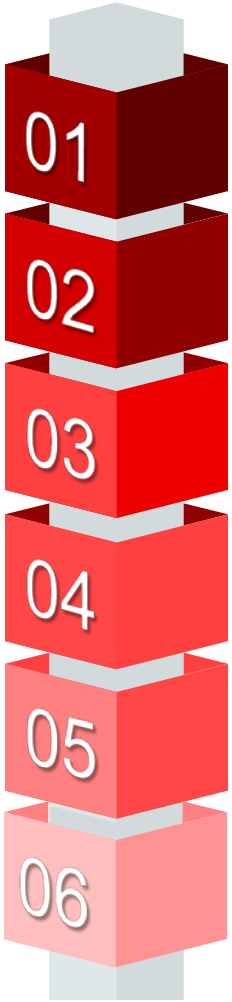
Internal auditing may extend its involvement in ERM, as shown in the aforementioned diagram, provided certain conditions apply. The conditions are:

- It should be clear that management remains responsible for risk management.
- The nature of internal auditor's responsibilities should be documented in the internal audit charter and approved by the audit committee.
- Internal auditing should not manage any of the risks on behalf of management.
- Internal auditing should provide advice, challenge and support to management's decision making, as opposed to taking risk management decisions themselves.
- Internal auditing cannot also give objective assurance on any part of the ERM framework for which it is responsible. Such assurance should be provided by other suitably qualified parties.
- Any work beyond the assurance activities should be recognized as a consulting engagement and the implementation standards related to such engagements should be followed.

Areas of overlapping Interest

Sr. No.	Risk management	Internal audit
1	Develop the risk management framework	Audit the adequacy and effectiveness of the risk management framework
2	Implement the risk management framework	Audit implementation of the risk management framework
3	Advise management on integration of risk management into business operations and their roles in making it work	Audit management's commitment to risk management and the take up of their roles
4	Advise on the allocation of accountability for risks, controls and tasks	Audit whether accountable managers fulfill those roles and are capable
5	Advise management and the Board on the interpretation of risk management information	Provide independent assurance of the risk management information submitted to the Board
6	Provide appropriate risk management status and performance information to the Board Audit and Risk Committee	Provide an independent view on the credibility and reliability of the risk management information submitted to the Board Audit and Risk Committee
7	Act as an advisor and mentor to management on risk management matters	Act as an independent reviewer to provide assurance on management's capability and performance in risk management

Key opportunities for internal audit in risk governance



01 Internal audit functions should take the initiative to educate and train the board and executive management on risk management concepts and principles.

02 Internal audit functions should focus more on consulting activities or even extend implementation support to promote risk management processes, while ensuring sufficient safeguards to avoid any impairment to independence and objectivity.

03 In organizations without formal risk management and dedicated risk function, internal audit functions should take the lead role in risk management processes. This does not mean that internal audit will be managing risk.

04 Provide assurance on the overall risk management framework and process as required by the IIA Standard 2120 – risk management and communicate results to the board and executive management

05 Additionally, internal audit can provide assurance on how organizations are responding to emerging concepts such as auditing risk culture, the adequacy of risk appetite statements, and the integration of risk management efforts across the business.

06 Internal audit functions should ensure their activities are coordinated and aligned with other risk functions and assurance providers thereby ensuring a common understanding of risks across the organization.

Addressing Strategic Risks

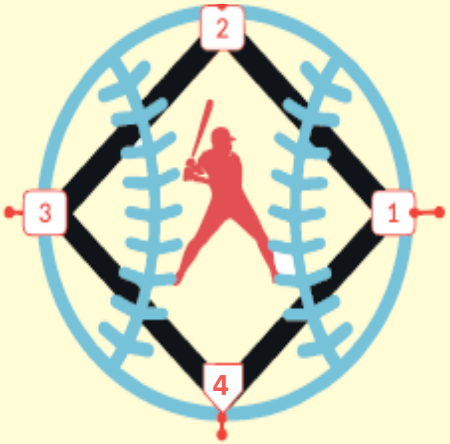
. . . Let's Play Ball

Apply scenario analysis

In business environments exposed to disruptive change, adaptive processes are needed to rapidly alter underlying assumptions to reflect newly changed circumstances

EVALUATE Competitive Intelligence

Remember disruptive change is a double-edge sword. Align key drivers and scenarios with the greatest impact



Understand critical assumptions

Preparation is the key of staying in front of the risks
Understand the contrarian point of view

Distill and demystify timely information for decision - makers

What separates the winners from the losers is the ability to recognize vital signs of change and act decisively

To recap

So what is the Emerging role?

- Preparing and IA strategy linked to organization strategy and goals. This would focus on the four pillars viz. People, Process, Systems and Governance
- Appropriate positioning of IA function in the organization
- IA function structured based on the organization strategy
- CAE skills more focused on leadership and management
- Rotation program
- IA involved in induction of managers and above levels
- Cohesive working with CEO/Senior Management and partnering with them on improving governance across the organization
- Conducting workshops and awareness programs for management and BAC
- Develop a working integration between ERM, Compliance and Internal audit
- Continuous auditing in critical areas
- Moving towards short spanned and focused audits instead of long duration and large scoped audits
- Focus towards integrated audits (Process and Technology)

So what is the Emerging role (contd.)

- IA function structured as a Value Assurance activity. In addition to executing audits as per IA plan, IA also gets involved in advising on the following:
  - New investments (feasibility, risks, benefits etc.),
  - Emerging risks,
  - Projects
- Process and Risk based IA plan instead of department / function based
- Periodic review of emerging risks
- Risk and Control maturity reporting by IA
- Dedicated team focusing on fraud parameters
- Dedicated team on QA
- Working meetings with AC
- Quarterly / half-yearly rolling 3 year IA plan

Key Imperatives For the Remainder of the Decade

- Enhancing and leveraging a continuous focus on risks
- Solidifying IA's expertise to address key risks
- Providing assurance on risk management effectiveness
- Enhancing IA's proficiency with data mining and analytics
- Securing a "seat at the table" for operational and strategic discussions
- Management periodically evaluates changes in the business environment to identify risks inherent in the corporate strategy
- There is a process to identify emerging risks. Scenario analysis is applied to understand the potential impact of risks emerging from changes in the external environment.
- Management apprises the board in a timely manner of significant risks or significant changes in the organization's risk profile .
- Board is aware of the critical risks facing the organization. There is an enterprise-wide process in place where the board members can advise on the mitigating factors of those risks and perform adequate risk oversight.
- There is a periodic board-level dialogue regarding management's appetite for risk and the entity's risk profile is consistent with the risk appetite.

Our thoughts

- Chief Risk Officer should constantly collate Chief Audit Executive's comments on identification of key risks impacting the organization, development of ERM framework, monitoring of risk responses, etc.
- On the other hand, when internal auditing extends its activities beyond this core role, it should apply certain safeguards, including treating the engagements as consulting services and, therefore, applying all relevant Standards.
- Internal auditor's core role in relation to ERM should be to provide assurance to management and to the board on the effectiveness of risk management.
- In this way, internal auditing will protect its independence and the objectivity of its assurance services. Within these constraints, ERM can help raise the profile and increase the effectiveness of internal auditing.

Face the Future with Confidence

protiviti®