KPMG

cutting through complexity™

# Internal Auditors and Enterprise Risk Management (ERM)

# ICPAK Presentation

April 2014

# Disclaimer

This presentation is made by KPMG Kenya, a member firm of the KPMG network of independent firms affiliated with KPMG International, a Swiss cooperative. KPMG International provides no client services. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm.

This presentation has been prepared solely and exclusively for the benefit, information and use by the participants of the Enterprise Risk Management training and for the sole and exclusive purposes of communicating material related to the training. These slides cannot be used by the participants of the training for any purposes other than as expressly stated herein; neither can these slides be disclosed to, referred to, or used by, any other third party. KPMG accepts no liability or responsibility whatsoever, resulting directly or indirectly from the disclosure of the presentation contents to any third party and/or the reliance of any third party on the contents of the presentation, either in whole or in part, and the participants of the training agrees to indemnify KPMG in this respect.

# Agenda:
# Internal Auditors and Enterprise Risk Management (ERM)

1. What is ERM
2. Drivers of ERM
3. What is Internal Auditing
4. The evolution of Internal Audit and ERM
5. Levels of Risk Within the Enterprise
6. Role of Internal Audit in ERM

# What is Enterprise Risk Management (ERM)?

COSO defines ERM as:

"ERM is a process effected by an entities 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 help manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievements of entity objectives."

# What is Enterprise Risk Management (ERM)?

The ERM definition broken down

- Is a process
- Is effected by people
- Is applied in strategy setting
- Is applied across the enterprise
- Is designed to identify events potentially affecting the entity and manage risk with its risk appetite
- Provides reasonable assurance
- Is geared to the achievement of objectives

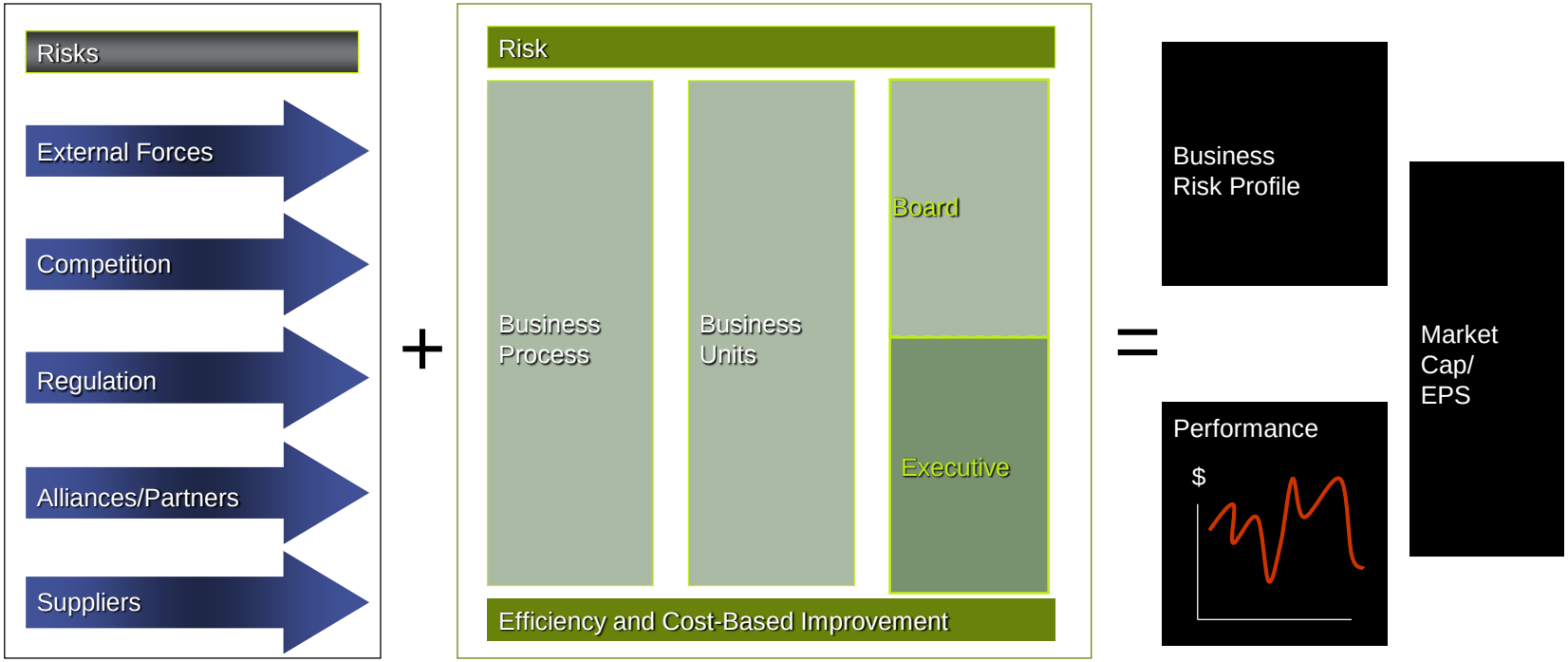
# Enterprise-wide Risk Management (ERM)

ERM is about integrating risk management into business critical systems and processes – and in doing that in a consistent way across the organisation

The consistency aspect is very important: to enable communications across and up and down the company, to prevent wasted resources from ‘reinventing the wheel’ and – most importantly – like with Accounting Standards, to enable consistent and coherent decision making and reporting

# Why is risk a key business issue?

Risk is now seen as an issue that affects all parts of the business and influences business success and failure . . .

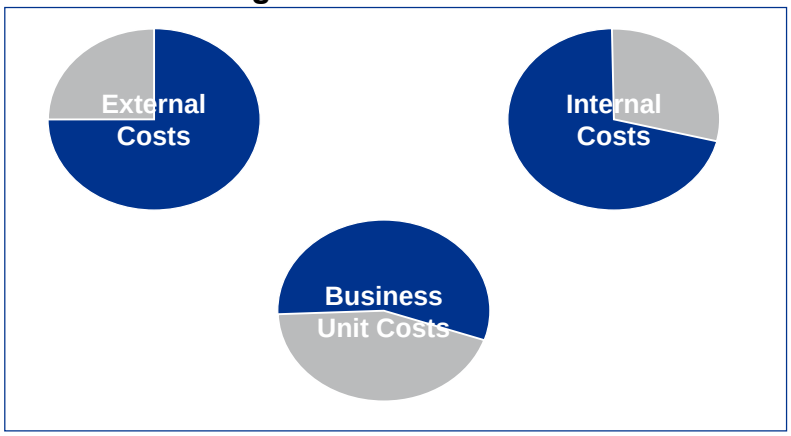



. . . consequently, risk management is increasingly the focus of the Board and executive management, and is proactive versus reactive

# ERM Drivers
# What does the picture look like in organizations today?

**Organizations have historically invested heavily in risk management and internal control but without a clear view of what potential benefit this delivers for the organization.**

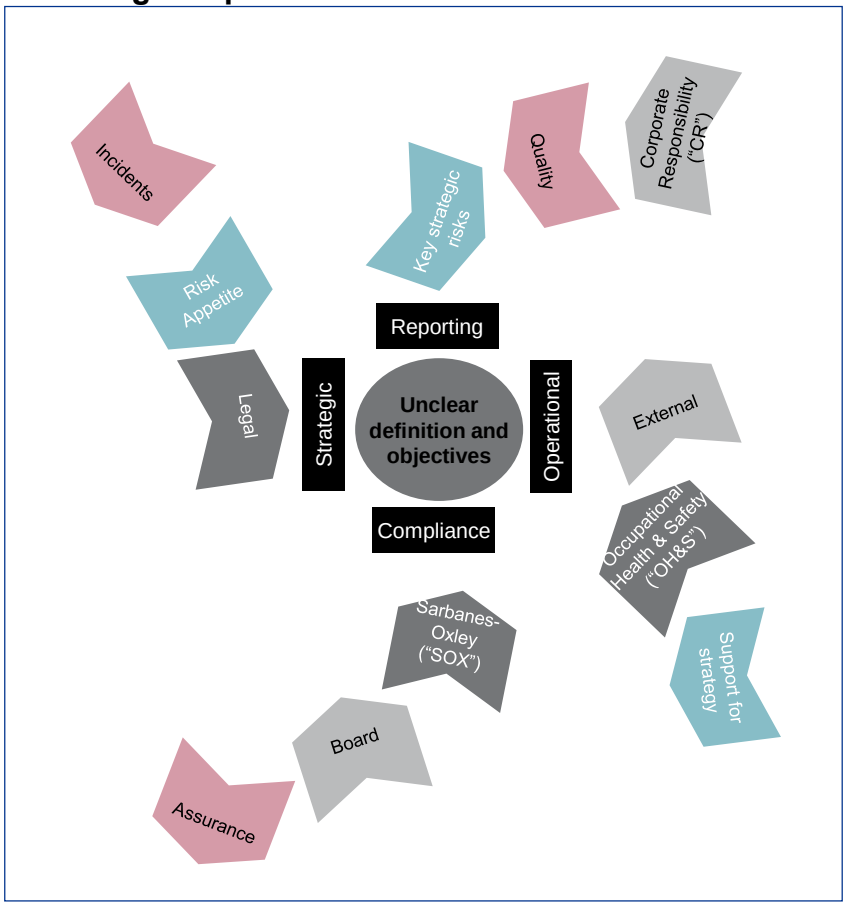
**The costs are significant…**



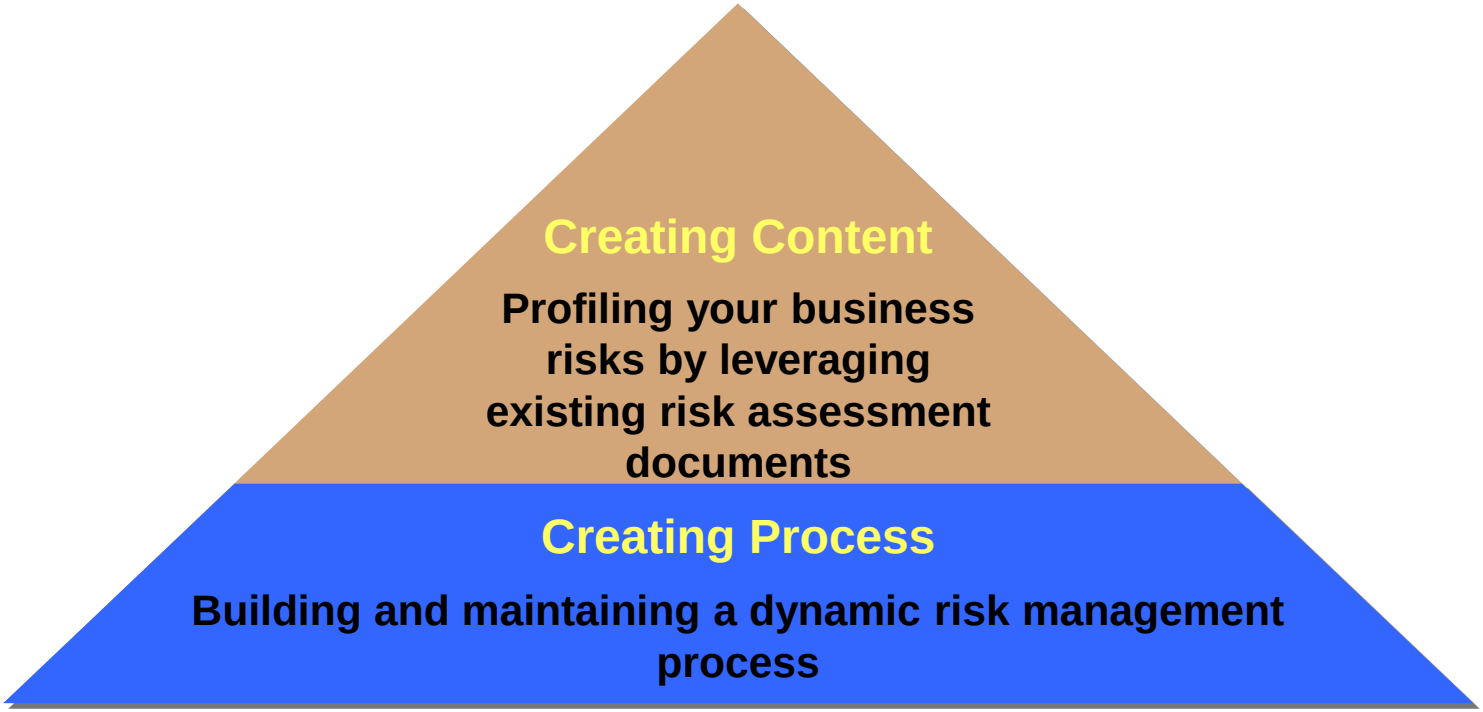

**…and the entire organization is being engaged**

| | | |
|---|---|---|
| | Board | |
| | Executive management | Audit Committee |
| Research and Development "R&D" | Committees of the Board | Internal Audit |
| Production | Group Functions (insurance, OH&S) | External audit |
| Sales | Risk and Governance | |

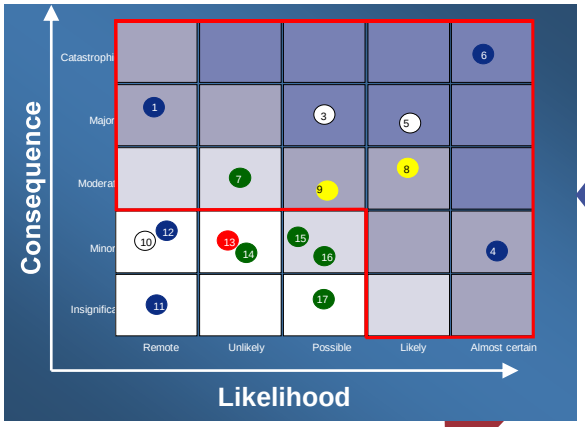
**Resulting in a picture like this…**



# Effective Enterprise Risk Management Is Essentially Doing Two Things Well



# ERM Content and Process




**Top Risks (those that threaten)**

1. Strategic Priorities
2. Business Model
3. Corporate Existence

**KPMG ERM Framework**

| Framework Element |
|---|
| 1. Risk Governance |
| 2. Risk Assessment |
| 3. Risk Quantification & Aggregation |
| 4. Risk Monitoring and Reporting |
| 5. Risk & Control Optimization |

**Create Content**

**Creating Content**

Identifying, evaluating and prioritizing enterprise risks

**Creating Process**

Building and maintaining a dynamic risk management framework and process to achieve sustainability

**Create Process**

# What is Internal Auditing?

The Institute of Internal Auditors defines Internal auditing as:

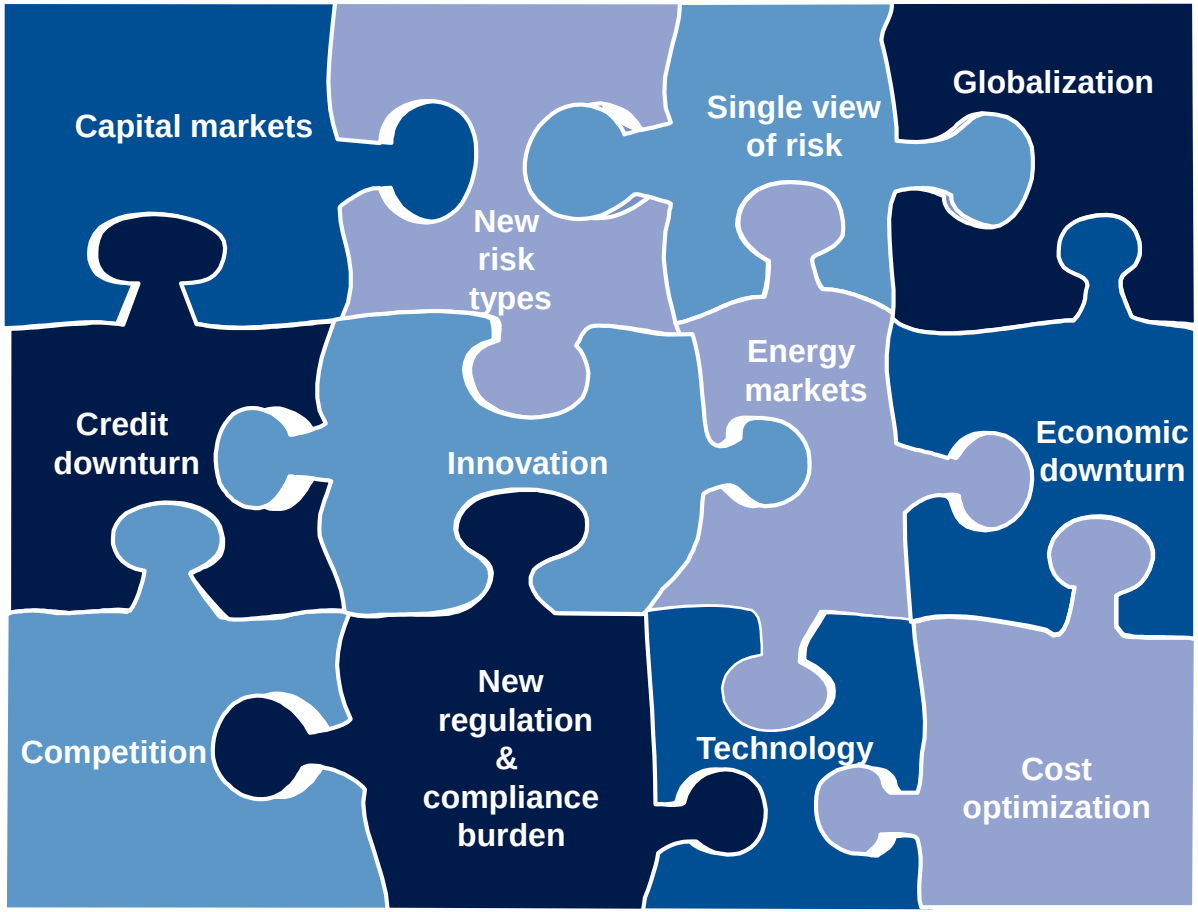
"Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, 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.

# Setting the Scene – A Compelling Case for Change

The risk landscape is changing rapidly….




…and Internal Audit departments must be structured to change with it.

# The Evolution of Internal Audit
## *Adding Value to the Business in New Ways*

- New demands from the board, senior organizational leaders, and regulators are requiring Internal Audit functions to refocus their efforts beyond regulatory compliance issues.

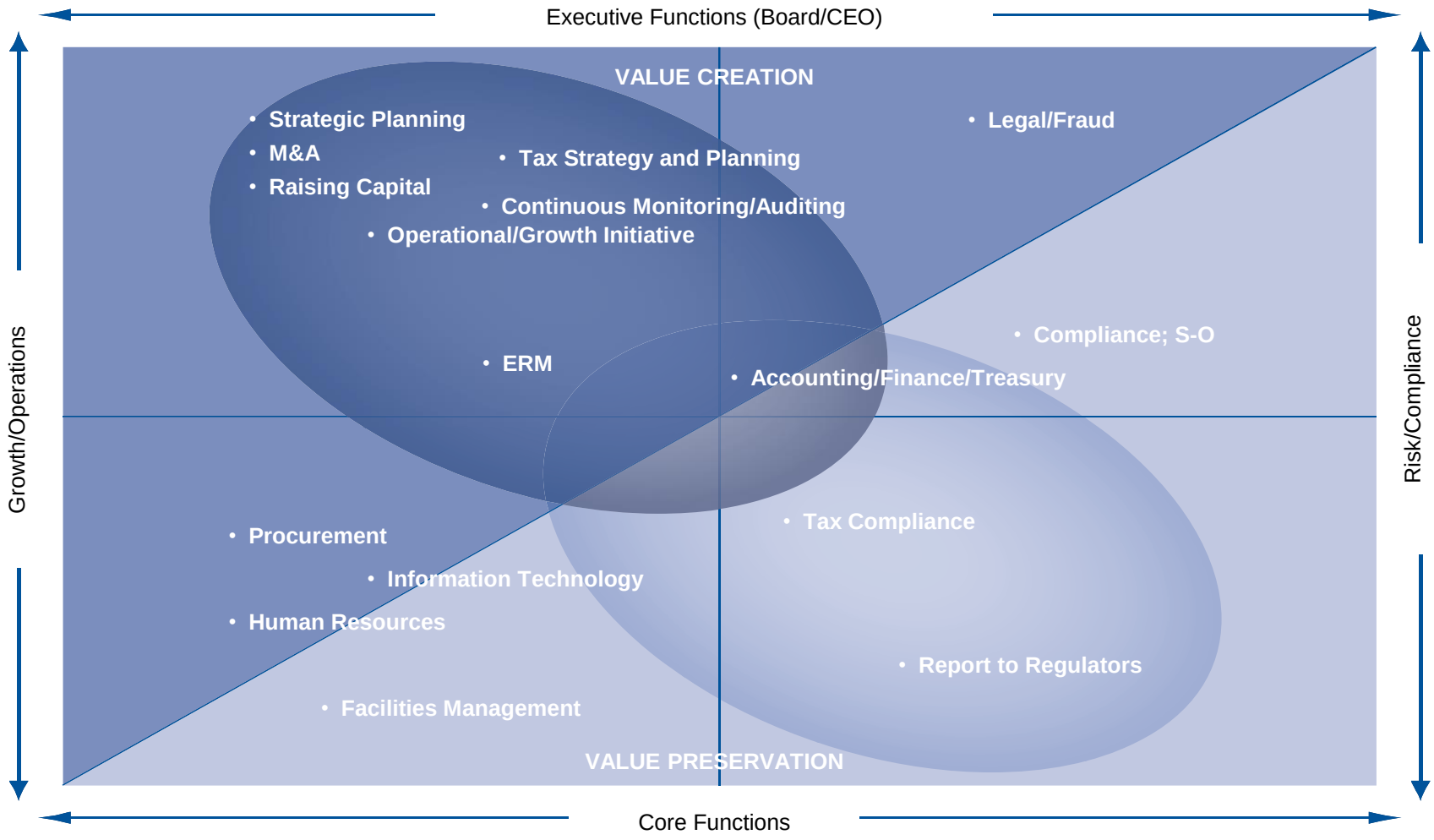
- Many leaders have recognized the need for Internal Audit to play an expanded role – one that builds on its historic focus on value preservation (a control focus) to encompass activities related to value creation (a performance focus).

- Such a shift should enable Internal Audit –with the objectivity of its perspective and the rigor of its processes – to add value to the business in new ways.

- Achieving leading Internal Audit capabilities, however, requires a significant investment in skilled resources, methods, training, career paths and technical infrastructure.

- Maintaining those capabilities requires a sustained level of investment.

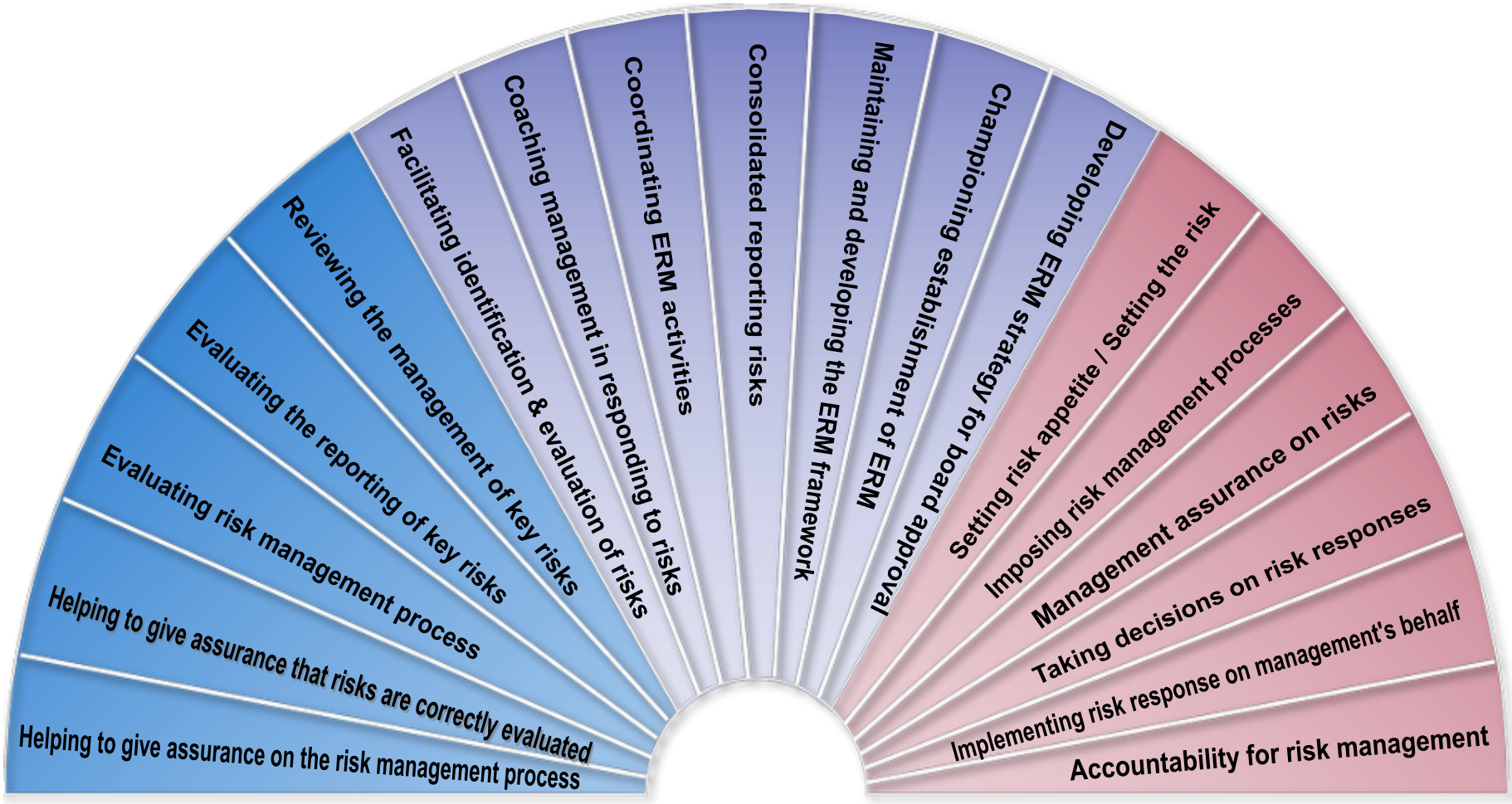
# The Evolution of Internal Audit
## *Adding Value to the Business in New Ways*



# The Evolution of Risk Management

## *The old ways of managing risk no longer work*

# Enterprise Risk Management
## *Creating Process – Role of Internal Audit*



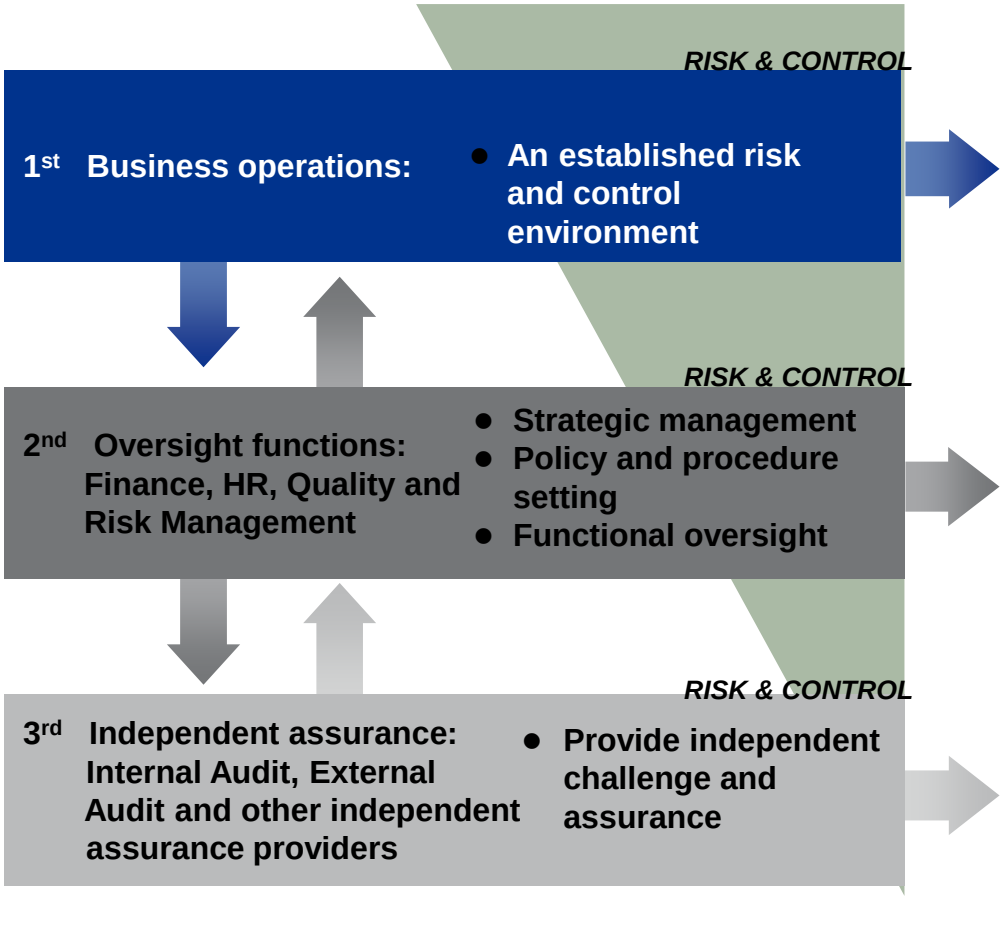

***Source: IIA UK and Ireland***

# Role of Internal Audit in ERM

| | |
|---|---|
| **Primary functions** | ▪ Assess sufficiency of ERM program and processes.<br>▪ Provide liaison between risk owners/senior management and the Board.<br>▪ Assess adequacy of risk evaluation and quantification.<br>▪ Provide special investigations as requested.<br>▪ Test organizational compliance with risk management processes & functions.<br>▪ Evaluate risk reporting processes and templates.<br>▪ Review and assess risk management of identified risks, including key risks. |
| **Secondary functions** | ▪ Provide risk consulting services, including facilitating risk awareness workshops.<br>▪ Assist risk management and the Board with improving risk reporting.<br>▪ Leverage Internal Audit's control and organizational experience during risk assessments.<br>▪ Help champion ERM within the organization while performing its Internal Audit functions. |
| **Inappropriate functions** | ▪ Assume management responsibilities within ERM processes.<br>▪ Set or approve the risk appetite.<br>▪ Approve risk management policies, procedures and/or framework.<br>▪ Implement any risk mitigation or risk response measure.<br>▪ Assume accountability for risk management. |

# Roles and Responsibilities
# Lines of defence

**You need a simple philosophy to be clear on accountabilities as outlined by the "Three Lines of Defense" model below.**




### First line

- The first level of the control environment is the **business operations** which perform day to day risk management activity

### Second line

- **Oversight functions** in the company, such as Finance, HR and Risk Management set direction, define policy and provide assurance

### Third line

- Internal and external audit are the third line of defense, offering **independent** challenge to the levels of **assurance** provided by business operations and oversight functions

# Roles and Responsibilities
## Lines of Defense against Risk

### Executive Management's Role

- Accountable to the board and shareholders for ensuring that the organization is:
  - Compliant with laws and regulations
  - Reporting complete and accurate financial and operational information
- Establishes the strategic and operational objectives that direct the organization's tolerance for risk
- Sponsors the Enterprise Risk Management (ERM) program and Internal Audit reviews

# Roles and Responsibilities
## Lines of Defense against Risk

### Process Owner's Role

- Key responsibility includes identification and management of risks. Monitors organizational processes during the normal course of business to ensure that:
  - New risks are identified and reported to Risk Management
  - Risk events and triggers are monitored
  - Internal controls are appropriately designed and operating effectively

# Roles and Responsibilities
## Lines of Defense against Risk


### Risk Management's Role

- Establish policy and process for risk management including guidance and coordination between constituencies
- Defines risk events based on executive management's strategic and operational objectives and liaison with Senior management and Board
- Identify enterprise trends, synergies, and opportunities for change
- Develops an ERM program to manage that risk:
  - Define the organization's tolerance and appetite for risk
  - Catalogs and quantifies risk events and triggers
  - Coordinates the development of mitigation strategies
  - Monitors progress and reports

# Roles and Responsibilities
## Lines of Defense against Risk


### Internal Audit's Role

- Conducts objective reviews to provide assurance that the internal controls are appropriately designed and operating effectively and mitigate the appropriate risks.
- Advocates and provides recommendations for continuous improvement to organizational processes
- Provide assurance that risk-management processes are adequate and appropriate.

# Questions

# Thank you

## Presenter's contact details

**Daniel Karuga**
**Senior Manager**
**Risk Consulting**
**KPMG Kenya**
**+254 709 576 262**

**dkaruga@kpmg.co.ke**

KPMG

cutting through complexity™