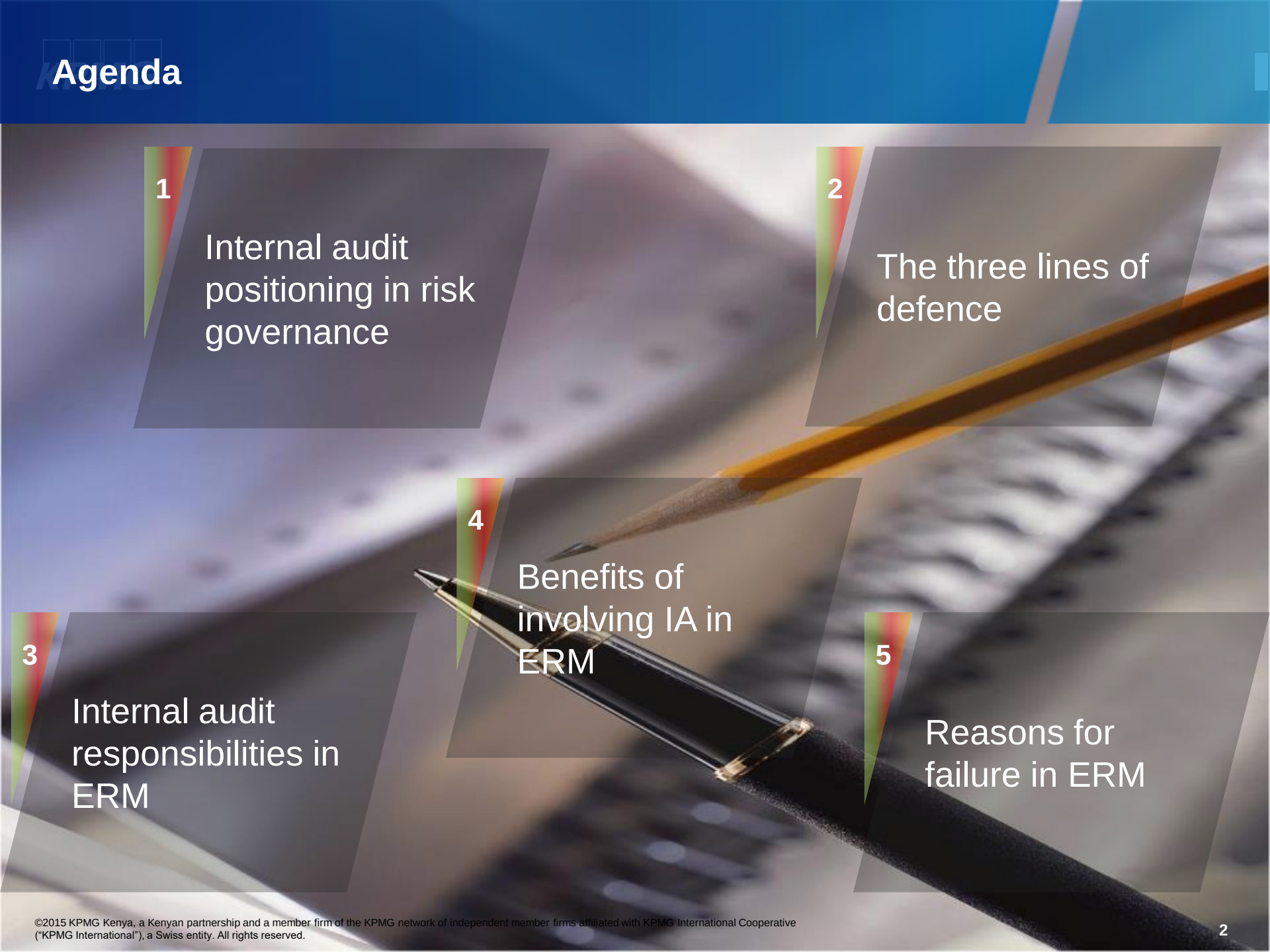
ICPAK Conference| August 2015

Risk Management – Role of Internal Auditor

KPMG

cutting through complexity

Agenda



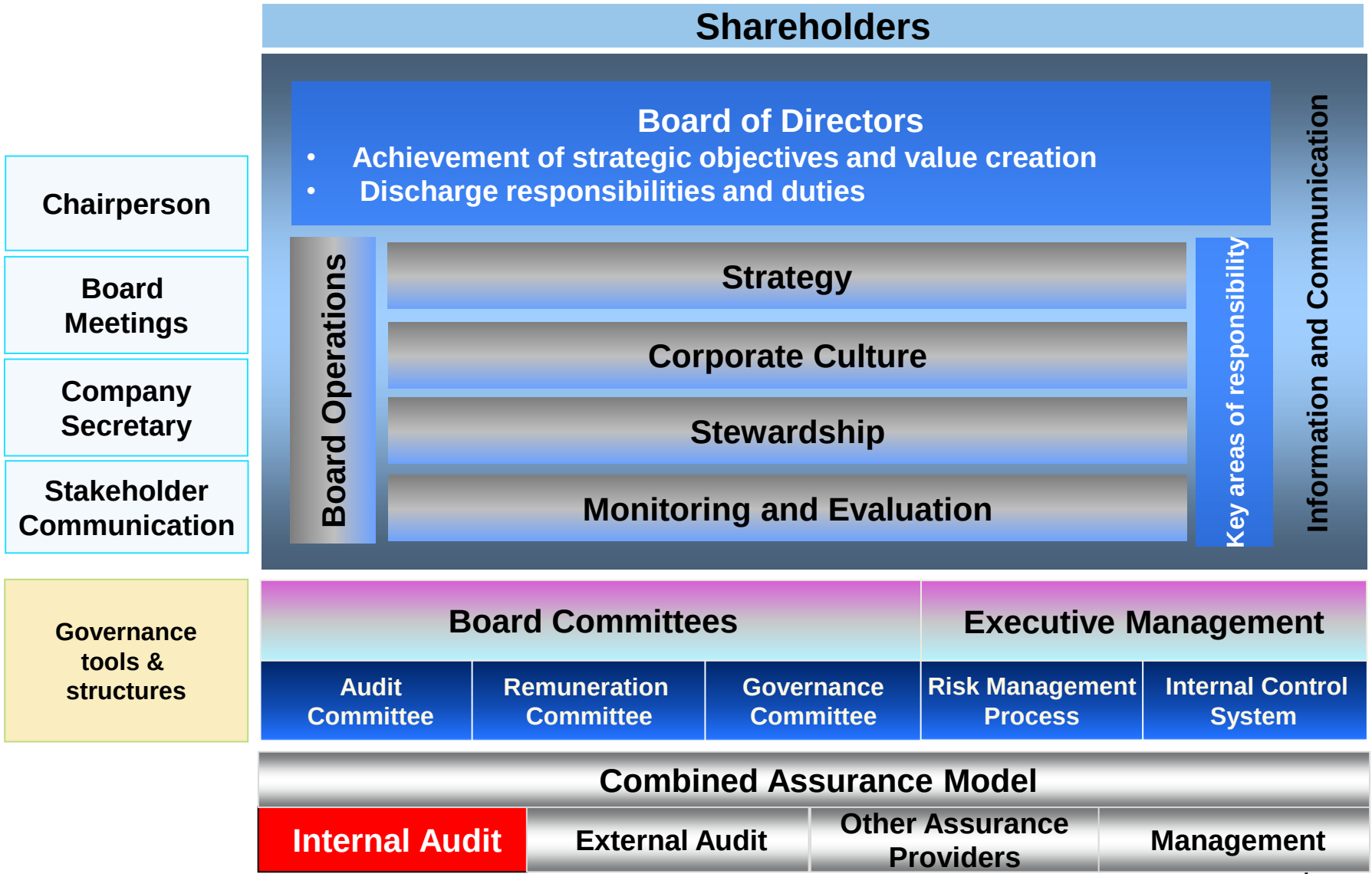
1. Internal audit positioning in risk governance
2. The three lines of defence
3. Internal audit responsibilities in ERM
4. Benefits of involving IA in ERM
5. Reasons for failure in ERM

Internal Audit Positioning in Risk Governance

KPMG

cutting through complexity

Governance Structure



The three lines of defence

KPMG
cutting through complexity

The three lines of defense

First line:

- The first level of control is the **user departments** which are served by procurement

Second line:

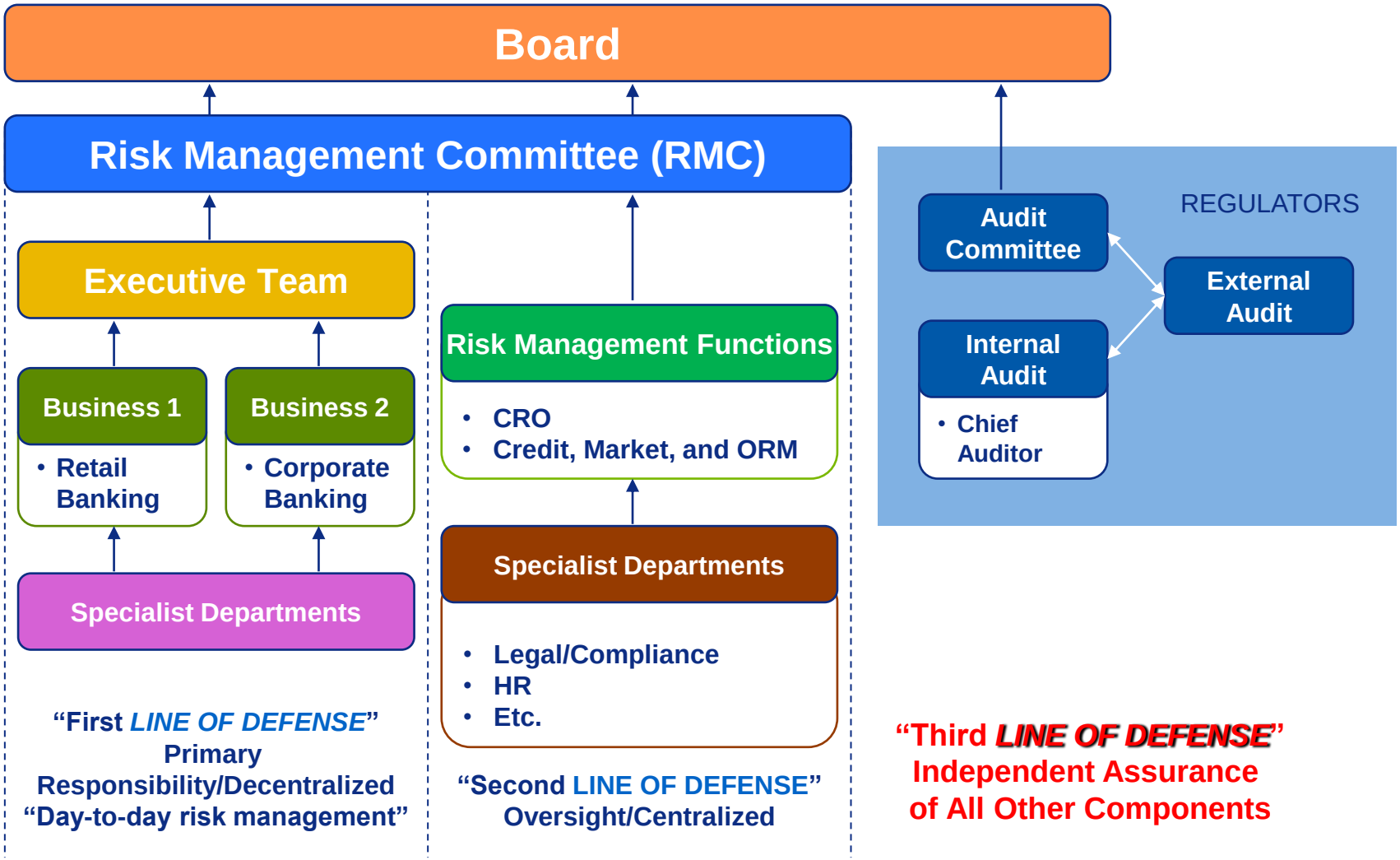
- **Oversight functions** such as finance, HR and risk management set directions, define policy and provide assurance to the board and EXCO

Third line:

- Internal audit and external audit offer **independent challenge** to the assurance provided by operations and oversight functions

Management Responsibilities: Lines of Defense (Bank Model)

MODEL FOR RISK ROLES AND RESPONSIBILITIES



Internal audit responsibilities in ERM

KPMG
cutting through complexity

Responsibility for ERM

- The board has overall responsibility for ensuring that risks are managed.
- In practice, the board will delegate the operation of the risk management framework to the management team.
- There may be a separate function that co-ordinates and manages these activities and brings to bear specialist skills and knowledge.

Everyone in the organization plays a role in ensuring successful enterprise-wide risk management but the primary responsibility for identifying risks and managing them lies with management.

The internal auditor's role in risk management

Internal auditing is an independent, objective assurance and consulting activity. Its core role with regard to ERM is to **provide objective assurance to the board** on the **effectiveness of risk management.**

Research has shown that board of directors and internal auditors agree that the two most important ways that internal auditing provides value to the organization are in **providing objective assurance** that the **major business risks** are being managed appropriately and providing assurance that the risk management and **internal**

Core Internal Audit roles in ERM

- Giving assurance on 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.

Legitimate internal auditing roles with safeguards

- Facilitating identification and evaluation of risks.
- Coaching management in responding to risks.
- Coordinating ERM activities.
- Consolidating the reporting on risks.
- Maintaining and developing the ERM framework.
- Championing establishment of ERM.
- Developing risk management strategy for board approval.

Roles internal auditing should NOT undertake

- Setting the risk appetite.
- Imposing risk management processes on management.
- Providing assurance to management on ERM.
- Taking decisions on risk responses.
- Implementing risk responses on management's behalf.
- Accountability for risk management.

Safeguards

- Management remains responsible for risk management.
- An internal audit charter documenting IA's responsibilities
- Internal audit **should not** manage any of the risks on behalf of management.
- Internal audit should provide advice, challenge and support to management's decision making.
- Internal audit **cannot** give objective assurance on any part of the ERM framework for which it is responsible
- Any work beyond the assurance activities should be recognized as a consulting engagement

Benefits of involving IA in ERM

KPMG
cutting through complexity

Risk 1.0: Prevents risk management from being a defense game

Risk 1.0 means managing risk with mitigation:

- **HEDGING**
- **INSURANCE**
- **AUDITS**
- **OVERSIGHTS**

The traditional approach of Risk Management 1.0 is about preserving value rather than *adding* value.

Identifies business vulnerabilities

Businesses can be vulnerable to:

- Supply chain disruptions
- Workforce actions
- Geopolitical instabilities
- Reputational harm
- Legal challenges
- Hacking
- Fraud and misconduct
- Technological advancements
- New emerging business models

Identifies the opportunity in risk

- Many organizations lack a system to identify signals of change.
- Traditionally the CRO is responsible for covering the downside of risk.
- But who is responsible for the upside of risk?

Helps answer key questions in strategy

What are our signals of change?

What are our headaches?

Do we have the right appetite for risk?

How do we convert insights into action?

How do we de-risk the downside?

Reasons for Failure in ERM

KPMG
cutting through complexity

Reasons for ERM failure

- Lack of buy-in from the board
- Poor risk culture
- Over-quantification
- Lack of defined risk governance structures
- Failure to define risk appetite
- Failure to embed ERM in operations (SOPs)

KPMG

cutting through complexity

Thank You

Daniel Karuga

Senior Manager

Internal Audit, Risk and Compliance Services

dkaruga@kpmg.co.ke