Dovetailing & Augmenting Enterprise Risk Management, Compliance, Controls Environment and Audit

Presentation by:

Sospeter Thiga
Group Head of Risk, Compliance & Performance Monitoring, CPF FS Ltd
Thursday, 20th September 2018

Uphold public interest

Agenda

- S1 Definition of Terms
- S3 Emerging Risk Areas
- S2 Drivers of Internal Controls Environment
- S3 Dovetailing and Augmenting ERM
- S4 Case Study: MTN Nigeria
- S5 Teaser: Dynamic Risk Assessment

Key Discussion Areas

Definition of Terms

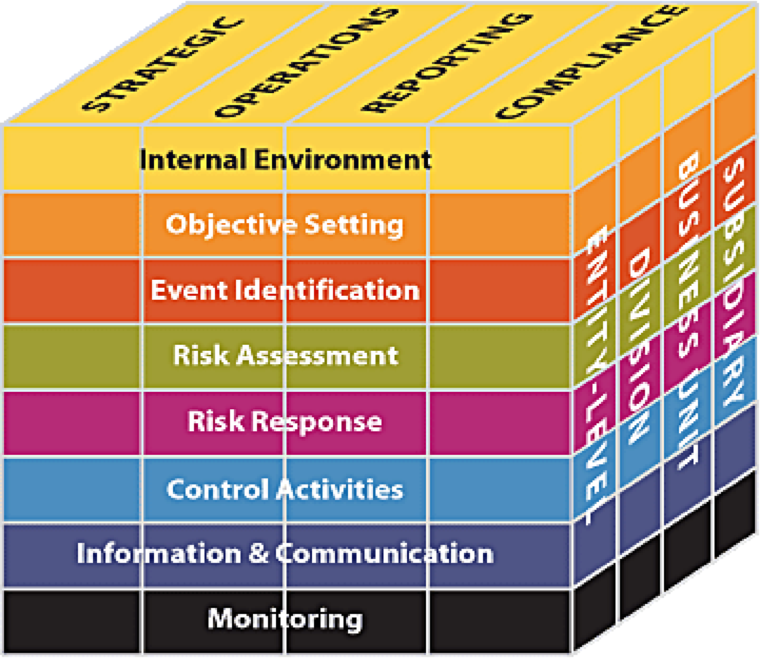
Enterprise Risk Management (ERM) is defined by (COSO) as "a process, effected by an entity's board of directors, management and other personnel, applied in strategy-setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.“

Source: coso

Definition of Terms

This enterprise risk management framework includes four categories:

1. Strategic: high-level goals, aligned with and supporting its mission
2. Operations: effective and efficient use of its resources
3. Reporting: reliability of reporting
4. Compliance: compliance with applicable laws and regulations



Source: coso

Definition of Terms

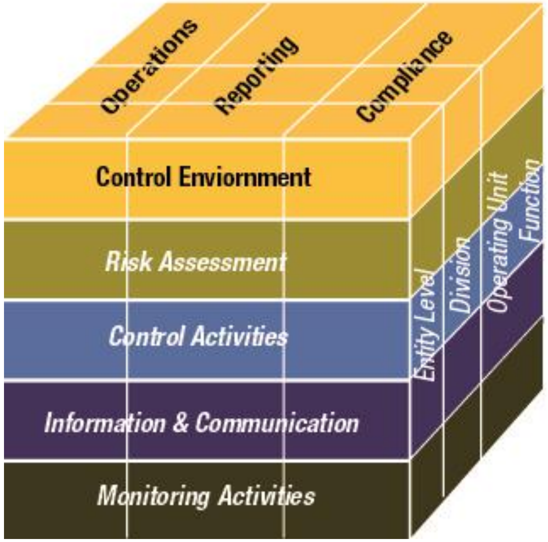
The COSO framework defines internal control as a process, effected by an entity's board of directors, management and other personnel, designed to provide "reasonable assurance" regarding the achievement of objectives in the following categories:

1. Effectiveness and efficiency of operations
2. Reliability of financial reporting
3. Compliance with applicable laws and regulations.

Definition of Terms

The COSO Internal Control framework has five components namely:

1. Control Environment
2. Risk Assessment
3. Control Activities
4. Information and Communication
5. Monitoring



Definition of Terms

We generally talk of control activities interchangeably with internal controls.

COSO defines control activities as the policies and procedures that help ensure management directives are carried out. They help ensure that necessary actions are taken to address the risks that may hinder the achievement of the entity's objectives.

Definition of Terms

Control activities occur throughout the organization, at all levels and in all functions. They include a range of activities as diverse as approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets and segregation of duties.

Definition of Terms

Control environment: COSO explain that the control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. Control environment factors include the integrity, ethical values, management's operating style, delegation of authority systems, as well as the processes for managing and developing people in the organization.

Definition of Terms

- Compliance involves conformity with laid down procedure, laws, regulations, directives.
- It's the prerogative of management to ensure compliance across the organization.
- As such compliance is part of the internal control environment of an organization.

Definition of Terms

1. Financial auditing is the process of examining an organization's financial records to determine if they are accurate and in accordance with any applicable rules (including accepted accounting standards), regulations, and laws.
2. External auditors come in from outside the organization to examine accounting and financial records and provide an independent opinion on these records.

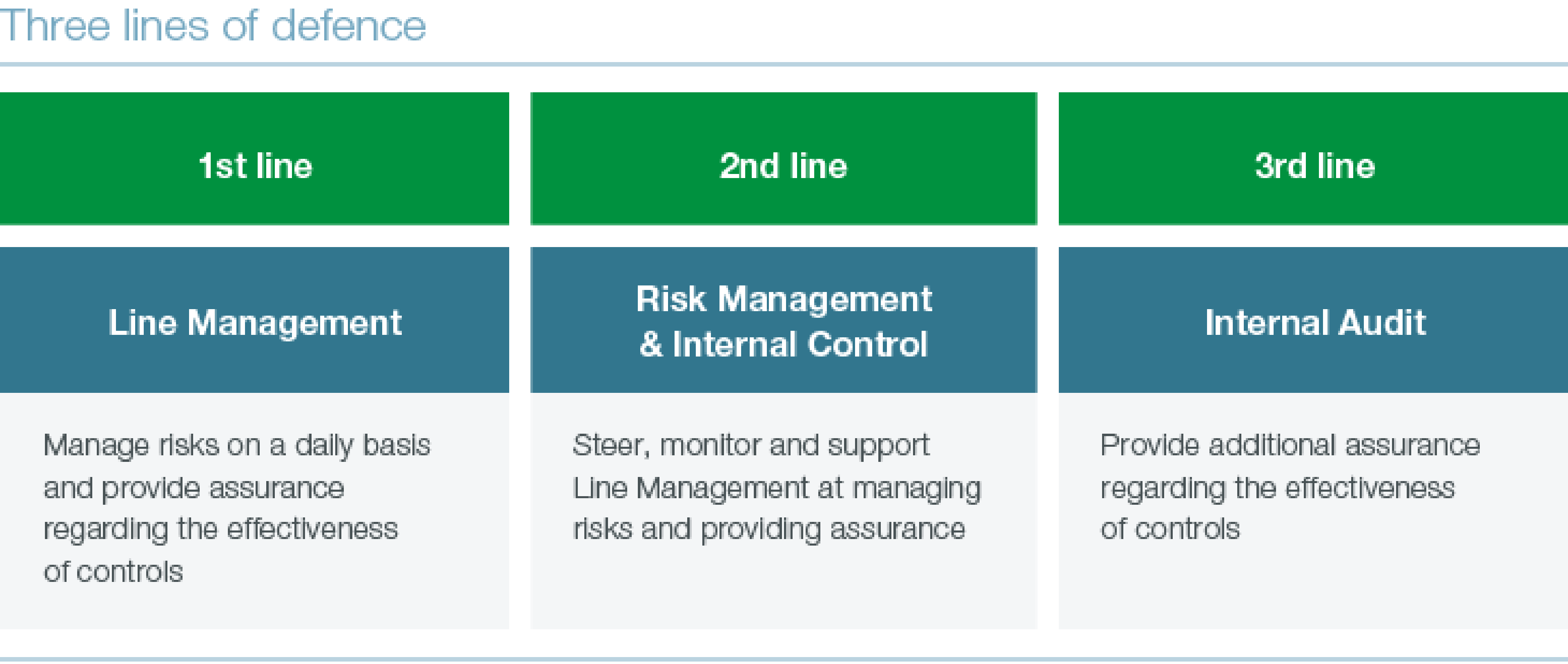
Source: accountingedu.org

Definition of Terms

3. Internal auditors work for the organization as internal employees to examine records and help improve internal processes such as operations, internal controls, risk management, and governance.

Source: accountingedu.org

Definition of Terms

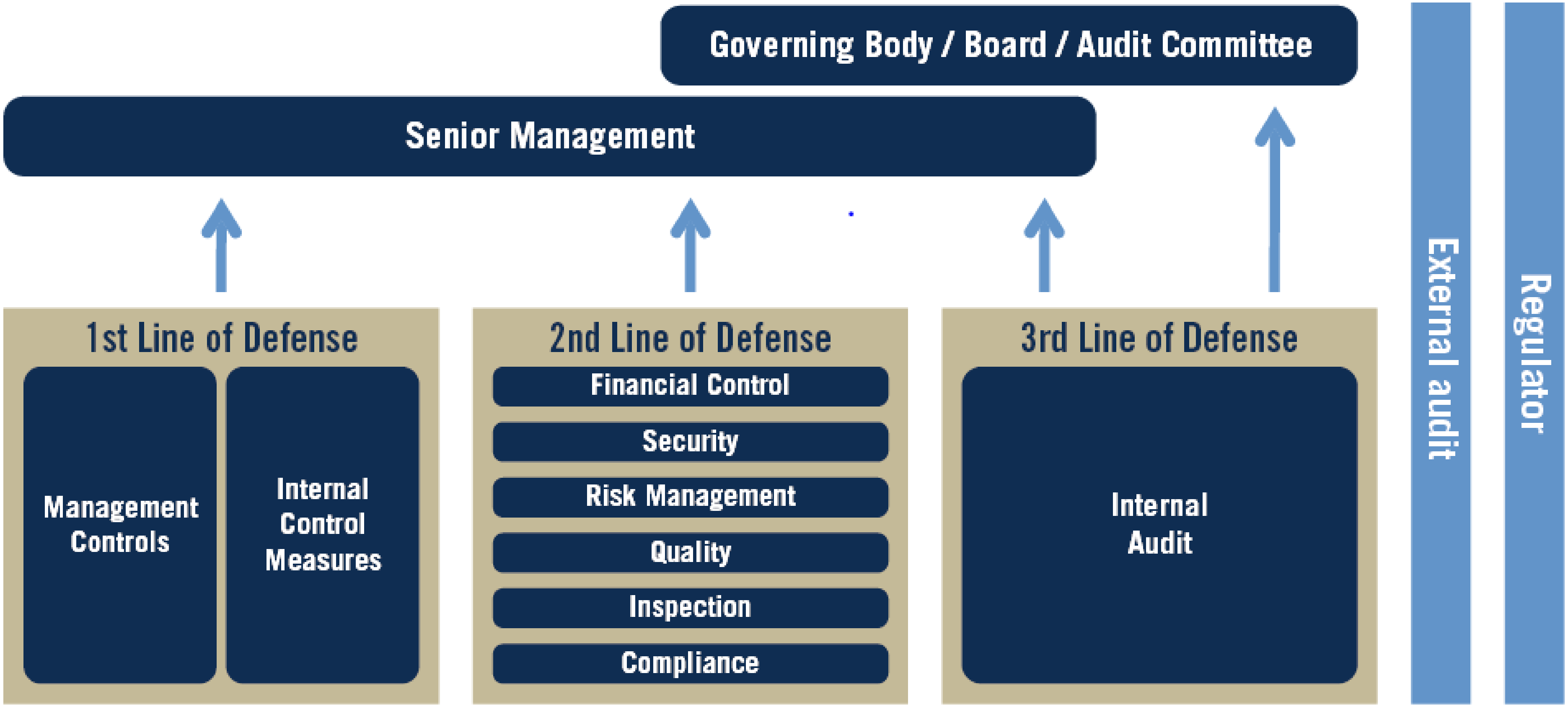


Three lines of defence

1st line	2nd line	3rd line
Line Management	**Risk Management & Internal Control**	**Internal Audit**
Manage risks on a daily basis and provide assurance regarding the effectiveness of controls	Steer, monitor and support Line Management at managing risks and providing assurance	Provide additional assurance regarding the effectiveness of controls

Definition of Terms

The Three Lines of Defense Model



Governing Body / Board / Audit Committee

Senior Management

1st Line of Defense

Management Controls

Internal Control Measures

2nd Line of Defense

Financial Control

Security

Risk Management

Quality

Inspection

Compliance

3rd Line of Defense

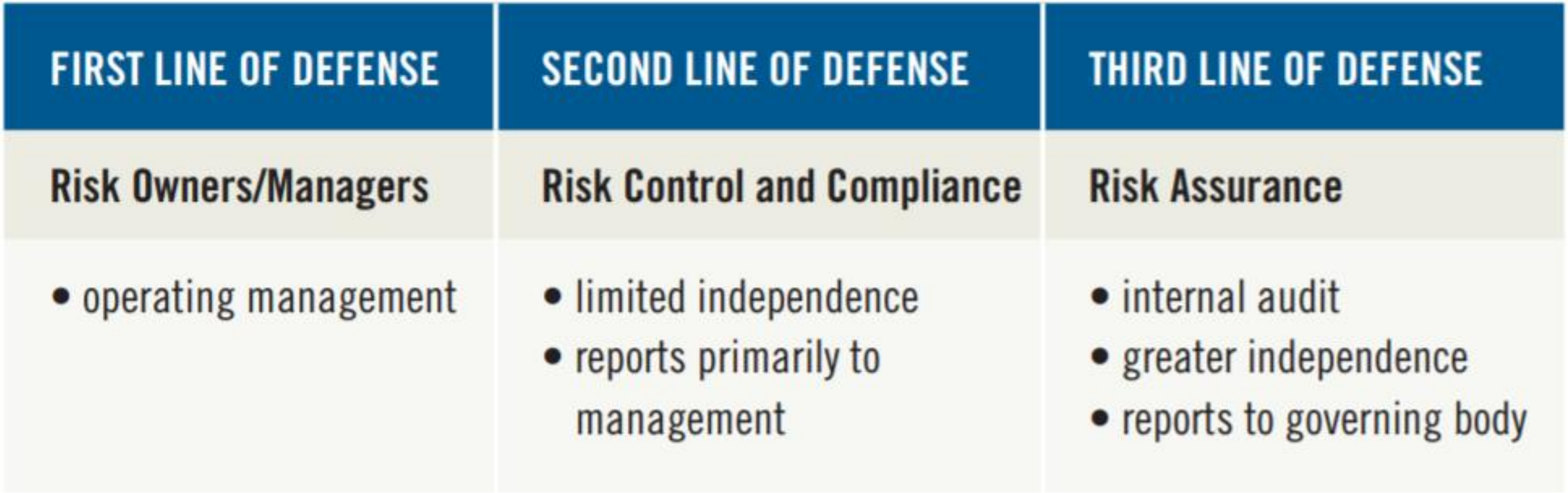
Internal Audit

External audit

Regulator

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

Definition of Terms



FIRST LINE OF DEFENSE	SECOND LINE OF DEFENSE	THIRD LINE OF DEFENSE
Risk Owners/Managers	Risk Control and Compliance	Risk Assurance
• operating management	• limited independence • reports primarily to management	• internal audit • greater independence • reports to governing body

Source: theiia

Augmenting and Dovetailing

- Dovetailing: fit or cause to fit together easily and conveniently synonyms: fit in, go together, be consistent, agree, accord, concur, coincide, match, fit, be in agreement, conform, equate, harmonize, fall in, be in tune, correlate, correspond, tally;
- Augmenting: make (something) greater by adding to it; increase. synonyms: increase, make larger, make bigger, make greater, add to, supplement, top up, build up, enlarge, expand, extend, raise, multiply, elevate, swell, inflate;

Augmenting and Dovetailing

Why dovetail and augment?

- Remove duplication of roles;
- Eliminate internal control gaps;
- Resolve conflicts and stalemates over incidences;
- Drive the accomplishment of Organizational goals.
  - Whose role is it to drive fraud prevention and detection mechanisms?

Augmenting Risk Management….

Video: Mike Nolan on augmenting risk

Emerging Risk Areas

1. Organization culture has been said to be the biggest risk to corporate performance. Staff commitment and behavior. Governance perspective as well – do we take a short cut? Close to the edge but not over it yet. Volkswagen emission scandal.
2. Cyber security cannot be said to be overrated.
3. Disruptive technology. We are all turning out to be IT companies, think of Fintech – Agency banking models, Uber, Amazon/Alibaba, Samantha

Emerging Risk Areas

4. Growing concerns over sustainability worldwide. Shall we still have a world to live in in future? Are you concerned about the impact of your organization's decisions and activities to the society and environment? Chana, Brazil – dust masks norm.
5. Political risk – getting entangled with China, are we losing our hard fought independence? Are we selling our birth right?

Drivers of a Strong Internal Control Environment

Drivers of strong internal control environment:

a) An independent, efficient and knowledgeable Board.

b) An independent and competent Internal Audit Function.

c) A Functional Risk Management & Internal Controls Framework.

d) The right Tone at the Top: water cannot rise above its level.

Drivers of a Strong Internal Control Environment

Drivers of strong internal control environment:

e) Strong ethical culture: preach water and drink water.

f) Competent senior management.

g) Continual improvement – Kaizen – change is the constant.

Drivers of a Strong Internal Control Environment

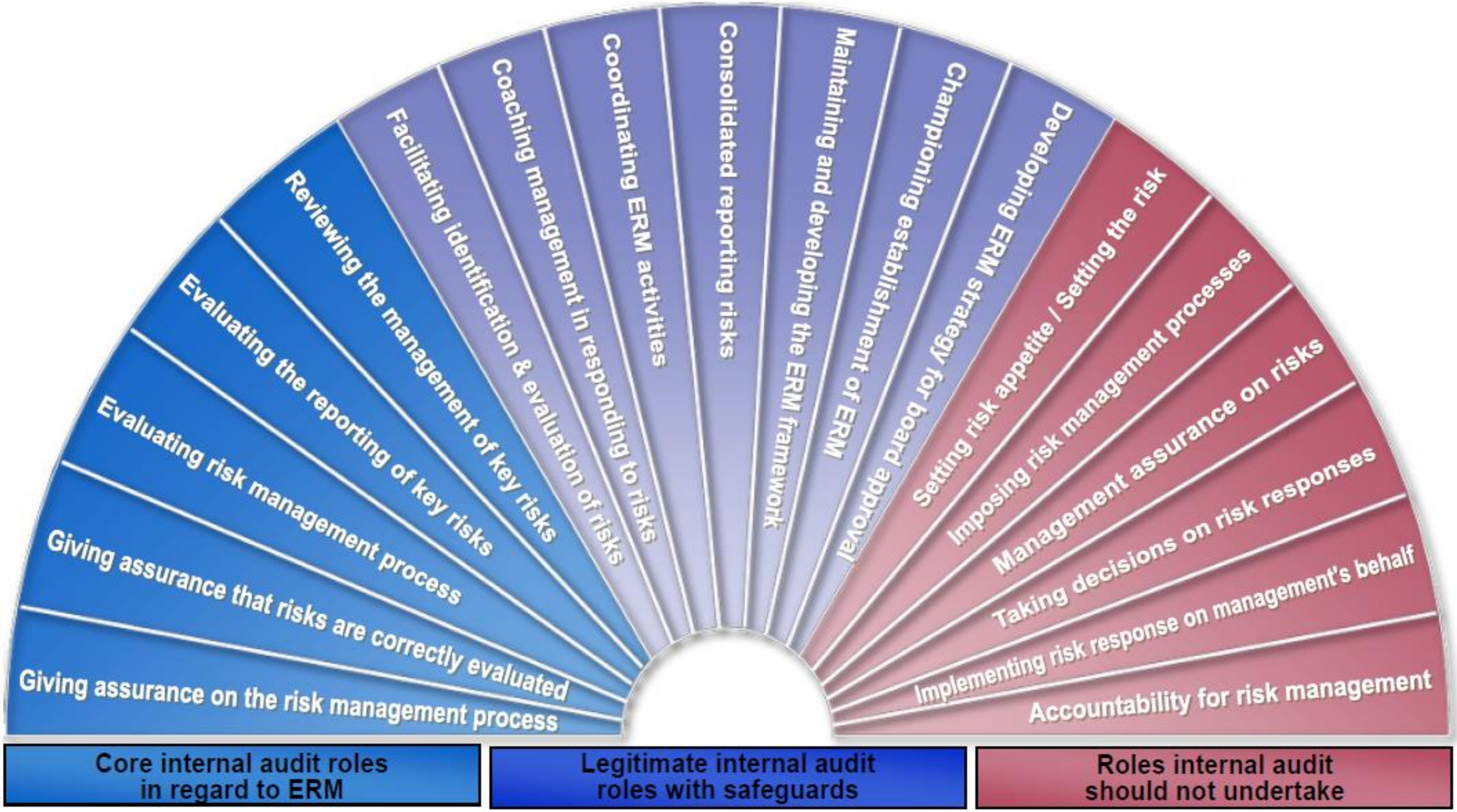
Questions for you…

How do you ensure a strong internal controls environment…?

Augmenting Risk Management….

1. Regular cross function interactions to break down the silos and Chinese walls.
2. Training and awareness of the teams, senior management and the Board to get the right perspective.
3. Relying on the work of the other team. e.g. Risk based Audit approach & assurance services.

Augmenting Risk Management….


Giving assurance on the risk management process
Giving assurance that risks are correctly evaluated
Evaluating risk management process
Evaluating the reporting of key risks
Reviewing the management of key risks
Facilitating identification & evaluation of risks
Coaching management in responding to risks
Coordinating ERM activities
Consolidated reporting risks
Maintaining and developing the ERM framework
Championing establishment of ERM
Developing ERM strategy for board approval
Setting risk appetite / Setting the risk
Imposing risk management processes
Management assurance on risks
Taking decisions on risk responses
Implementing risk response 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

Augmenting Risk Management….

4. Integration and alignment of some roles. Such as …risk assessments. Identify overlaps and duplications, align them.
5. Policy change, updates and benchmarking. Policy drives implementation.
6. Driving culture change that supports a strong internal control environment and risk management. Remember culture eats strategy for breakfast. How do you do this?

Augmenting Risk Management....

7. Entrenching risk to management decision making and management style.
8. Offering continuous risk/audit/compliance advisories. Being proactive.
9. Becoming a reliable partner to management for strengthening internal control environment - WITFM.
10. Setting/influencing the right tone at the top. Presenting a united front.

4th Line of Defense

The 4th Line of Defense

- Regulators and External auditors can be considered to be an additional line of defense.
- This happens only when effectively coordinated.
- They can provide assurance to stakeholders, the Board and senior management.
- It is in our best interest to ensure that regulators and external auditors perform their role effectively.

Augmenting Risk Management….

Questions for you…

1. Which of these ideas mean most to you?
2. Which new idea will you choose to implement back at your organization?
3. What additional idea would you want to share with the group that has worked very well for you?

Case Study: MTN Nigeria

From an IIA Perspective

- ✓ Risk and control processes should be structured in accordance with the Three Lines of Defense model.
- ✓ Each line of defense should be supported by appropriate policies and role definitions.
- ✓ There should be proper coordination among the separate lines of defense to foster efficiency and effectiveness.

From an IIA Perspective

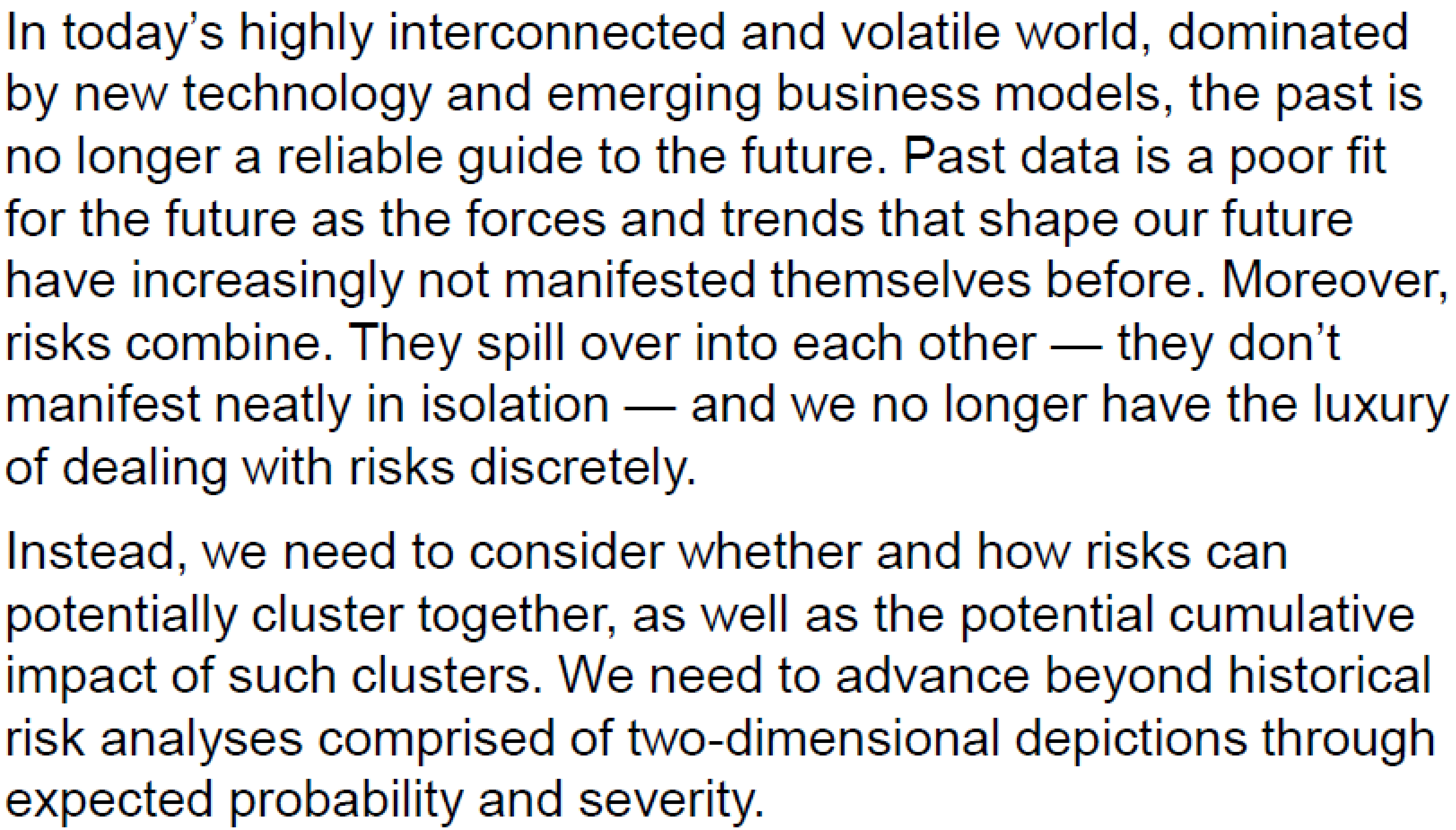
- ✓ Risk and control functions operating at the different lines should appropriately share knowledge and information to assist all functions in better accomplishing their roles in an efficient manner.
- ✓ Lines of defense should not be combined or coordinated in a manner that compromises their effectiveness.

From an IIA Perspective

- ✓ In situations where functions at different lines are combined, the governing body should be advised of the structure and its impact. For organizations that have not established an internal audit activity, management and/or the governing body should be required to explain and disclose to their stakeholders that they have considered how adequate assurance on the effectiveness of the organization's governance, risk management, and control structure will be obtained.

Source: https://na.theiia.org/

Teaser… Dynamic Risk Assessment



In today's highly interconnected and volatile world, dominated by new technology and emerging business models, the past is no longer a reliable guide to the future. Past data is a poor fit for the future as the forces and trends that shape our future have increasingly not manifested themselves before. Moreover, risks combine. They spill over into each other — they don't manifest neatly in isolation — and we no longer have the luxury of dealing with risks discretely.

Instead, we need to consider whether and how risks can potentially cluster together, as well as the potential cumulative impact of such clusters. We need to advance beyond historical risk analyses comprised of two-dimensional depictions through expected probability and severity.

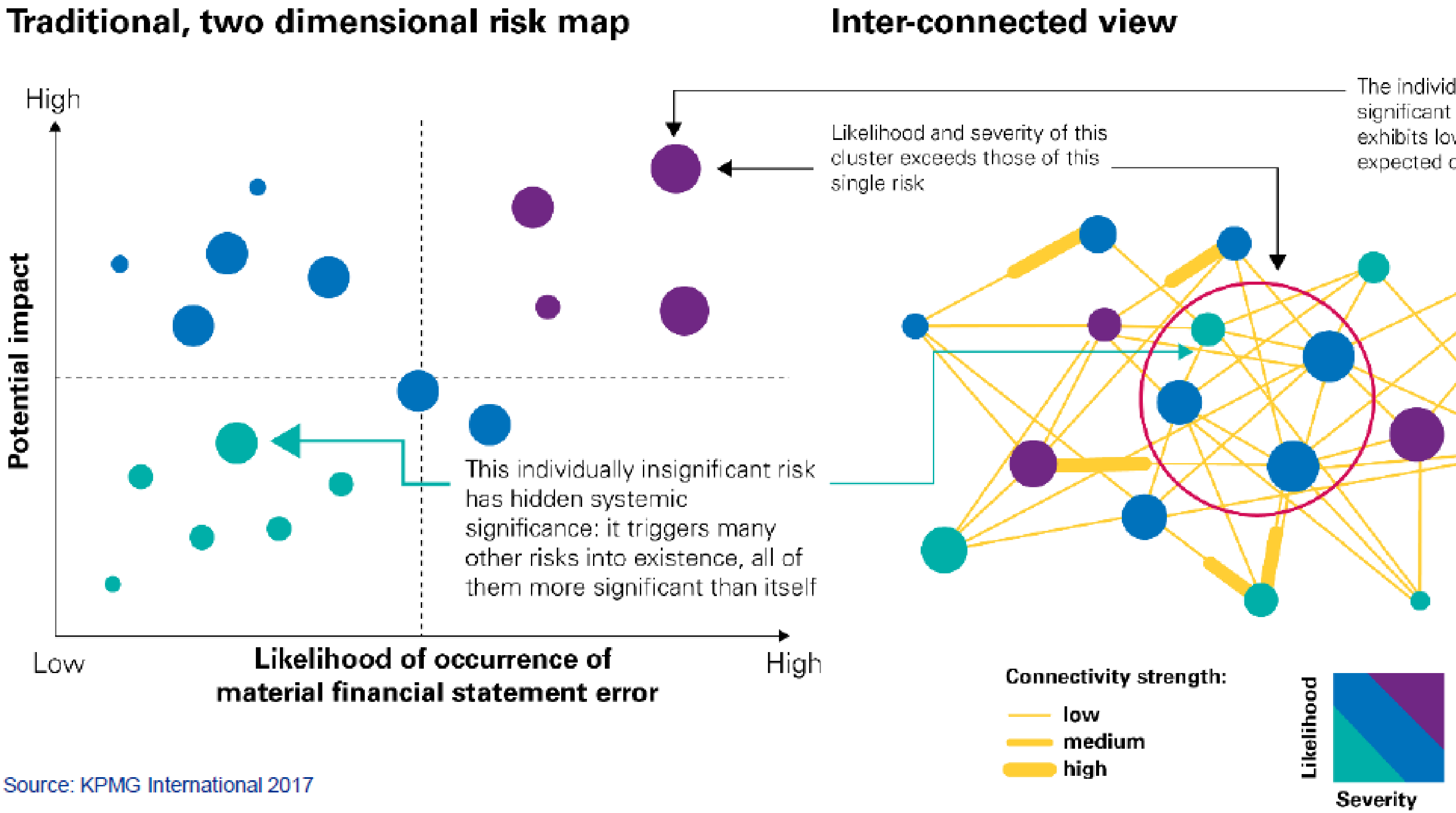
Source: KPMG

Teaser… Dynamic Risk Assessment

"While the traditional assessment of risk focuses on single risk events with high likelihood and severity, DRA rebalances our assessment of risk by analyzing business risks' velocity and their potential interconnectedness(contagion)."

Source: KPMG

Teaser… Dynamic Risk Assessment



Traditional, two dimensional risk map

Inter-connected view

This individually insignificant risk has hidden systemic significance: it triggers many other risks into existence, all of them more significant than itself

Likelihood and severity of this cluster exceeds those of this single risk

The individually most significant risk exhibits low levels of expected contagion

Source: KPMG International 2017

Teaser… Dynamic Risk Assessment

Video: KPMG’s Dynamic Risk Assessment

Networking....

ICPAK
Uphold Public Interest

WhatsApp

A whatsapp group for all Heads of Audit and Risk that enables networking and mentorship opportunities. - 0722676484

Q
&
A