INTERNAL AUDIT CONFERENCE

Presentation by:

Nasumba Kizito Kwatukha

CPA,CIA, CISA,CFE,CISSP,CRMA,CISM

29TH March 2017

Uphold public interest

Agenda

Risk Management, Compliance and Internal Audit:

Opportunities and challenges in Convergence

- *Emergence of GRC concept*
- *Internal Audit and role in Governance Risk and Compliance*
- *Risk Management and role in GRC*
- *Opportunities and Challenges in Convergence*

Audit and Investigation are different…draft/ final report

GRC at a glance

Coordinated strategy for managing the broad issues of governance, enterprise risk management (ERM) and compliance

Why G.R.C

- *Achieve objectives while optimizing risk profile and protecting value*
- *Operate within legal, contractual, internal, social, and ethical boundaries*
- *Provide relevant, reliable, and timely information to appropriate stakeholders*
- *Enable the measurement of the performance and effectiveness of the system."*

Link with COSO and ISO 31000

COSO *framework defines internal control as a process, effected by an entity's board of directors, management. Designed to provide "reasonable assurance" regarding the achievement of key objectives-*
Framework is silent on assignment of duties

Eight framework components of Effective and Adequate Internal-
COSO *and* MWONGOZO *guideline:*
Control Environment-Sets the Risk Appetite
Risk Identification , assessment and response
Monitoring Activities
Information flow and Communication

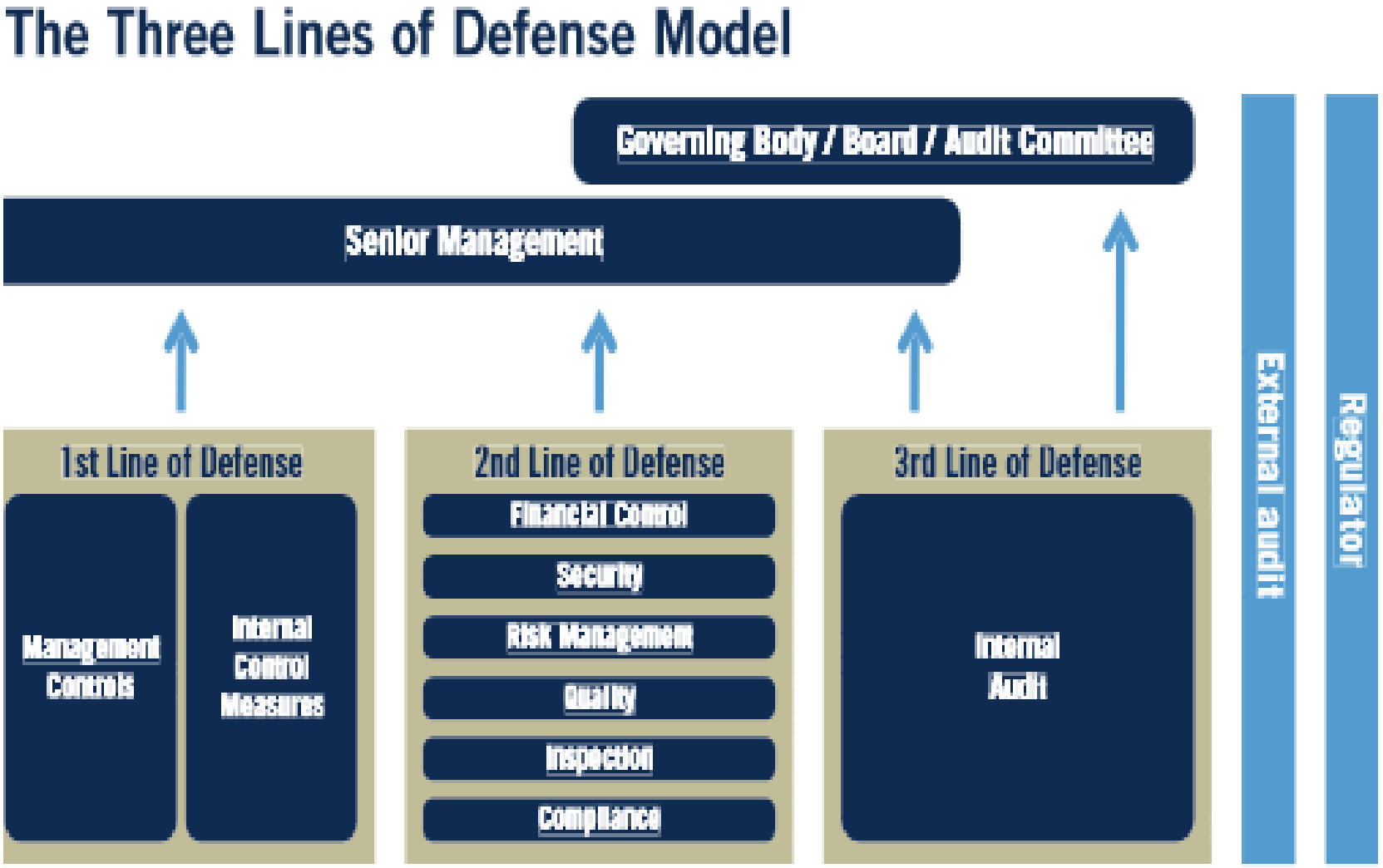
Definition of Audit:

Internal audit helps organizations achieve their objectives through evaluating and improving the effectiveness of risk management, control and governance processes in an organization

Role of Internal Audit in Strategy-COSO UPDATE"

Redefine the Internal Audit Charter to move from operations to Strategy through performance and Linking Risk Universe to Organization objectives.

3 lines of Defense



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

3 Lines of defense Cont'd

*Every organization has objectives it strives to achieve. In pursuit of these objectives, the organization will encounter events and circumstances which may threaten the achievement of these objectives-**risks***

The Three Lines of Defense (the Model) addresses how specific duties related to risk and control could be assigned

Directors and management should understand the critical differences in roles and responsibilities of these duties and how they should be optimally assigned.

Internal Audit Cont'd

COSO Framework is used to manage risk and control to accomplish objectives.

The organization structure is well defined by the 3 layer defense with each layer playing a distinct role in the Internal Control

The functions at each of the lines of defense will usually vary: some functions may be combined or split across the lines of defense.

E.g., in some organizations, parts of a compliance function in the second line may be involved in designing controls for the first line, while other parts of the second line focus primarily on monitoring

Defense Lines

Functions that own and manage risks-1st Line

Functions that oversee risks-2nd Line

Functions that provide independent assurance-3rd

Operational managers develop and implement the organization's control and risk management processes and must be adequately skilled to perform these tasks within their area of operations

1st Line of Defense- Key

Figure 4. COSO and the 1st Line of Defense

2nd Line of Defense

Includes risk management and compliance functions put in place by management.

Help ensure controls and risk management processes implemented by the first line of defense are operating

They often work closely with operating management to help define implementation strategy, provide expertise in risk, implement policies and procedures, and collect information to create an enterprise-wide view of risk and control-data analytics, monitor KRISs and Escalation of Incidence

2nd Line of Defense Cont'd

This will vary significantly depending on the organization's size and industry.

In large, publicly traded, complex, and/or highly regulated organizations, these functions may all be separate and distinct unlike smaller, privately owned, second-line functions may be combined or nonexistent.

E.g. Combine the legal and compliance functions into a single department; combine a health and safety department with an environmental function or human resources

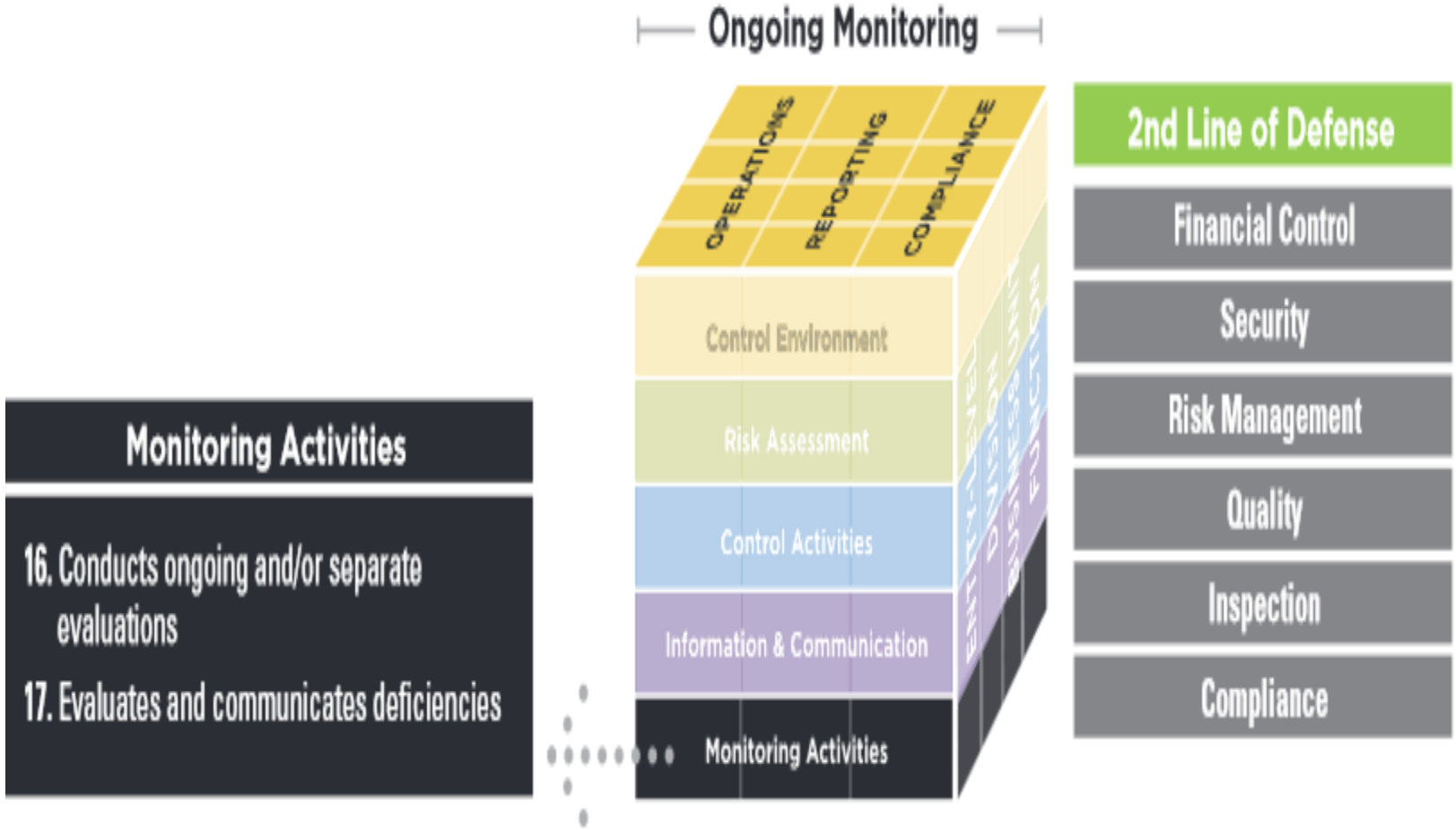
2nd Line of Defense Cont'd

Some or all of the duties of the second line may also be retained by managers within the first line of defense

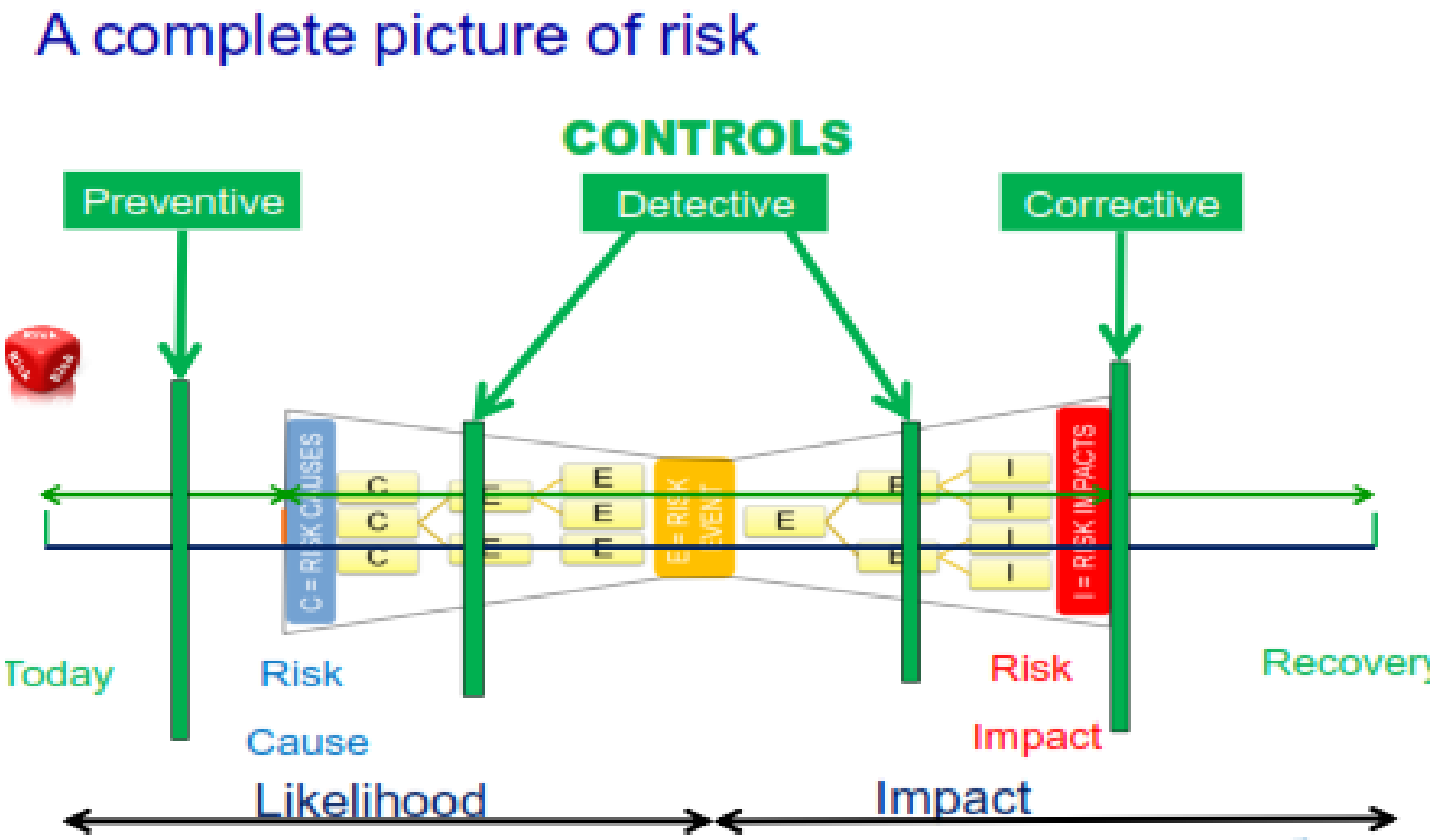
Create a department within ICT to handle Information Security

Typical second-line functions include specialty expertise groups such as Risk Management; Financial Control, Physical Security, Quality, Health and Safety, Inspection

2nd Line of Defense Cont'd



2nd Line of Defense Cont'd



3rd Layer of Defense

Risk is the uncertainty on objectives as the business pursues its objectives.

The process of risk assessment; risk mapping and data intelligence is purely a management function

What Internal Audit does is to evaluate and improve the effectiveness of risk management, control, and governance processes

3rd Layer of Defense

Internal Audit is:

- *Highly independent and objectivity with reporting lines*

- *Internal auditors do not design or implement controls as part of their normal responsibilities and are not responsible for the organization's operations.*

- *Assurance is regarding governance, risk, and control.*

3rd Layer of Defense

Control Environment

1. Demonstrates commitment to integrity and ethical values
2. Exercise oversight responsibility
3. Establishes structure, authority and responsibility
4. Demonstrates commitment to competence
5. Enforces accountability

Risk Assessment

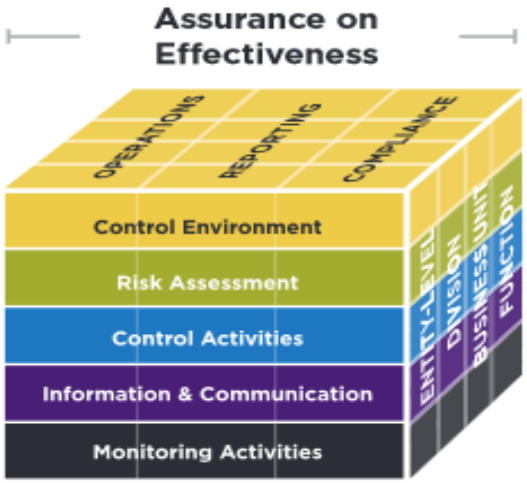
6. Specifies suitable objectives
7. Identifies and analyzes risk
8. Assesses fraud risk
9. Identifies and analyzes significant change

Control Activities

10. Selects and develops control activities
11. Selects and develops general controls over IT
12. Deploys through policies and procedures

Information & Communication

13. Uses relevant information
14. Communicates internally
15. Communicates externally



3rd Line of Defense

Internal Audit

Convergence ....

Convergence is (GRC) the integration and of siloed management assurance information into a unified framework. It produces:

- *A single seamless shared assurance universe for planning and reporting*
- *A common language of risk and control*
- *Common methodologies-Ranking and Prioritization*

Convergence ....

- *The three lines each have the same ultimate objective: Internal audit can take up some duties of risk management*

- *The two Lines of defense should feed into the Internal Auditors Work plan*

- *The Risk Universe should rotate around organization objective which the internal Auditor will provide assurance on*

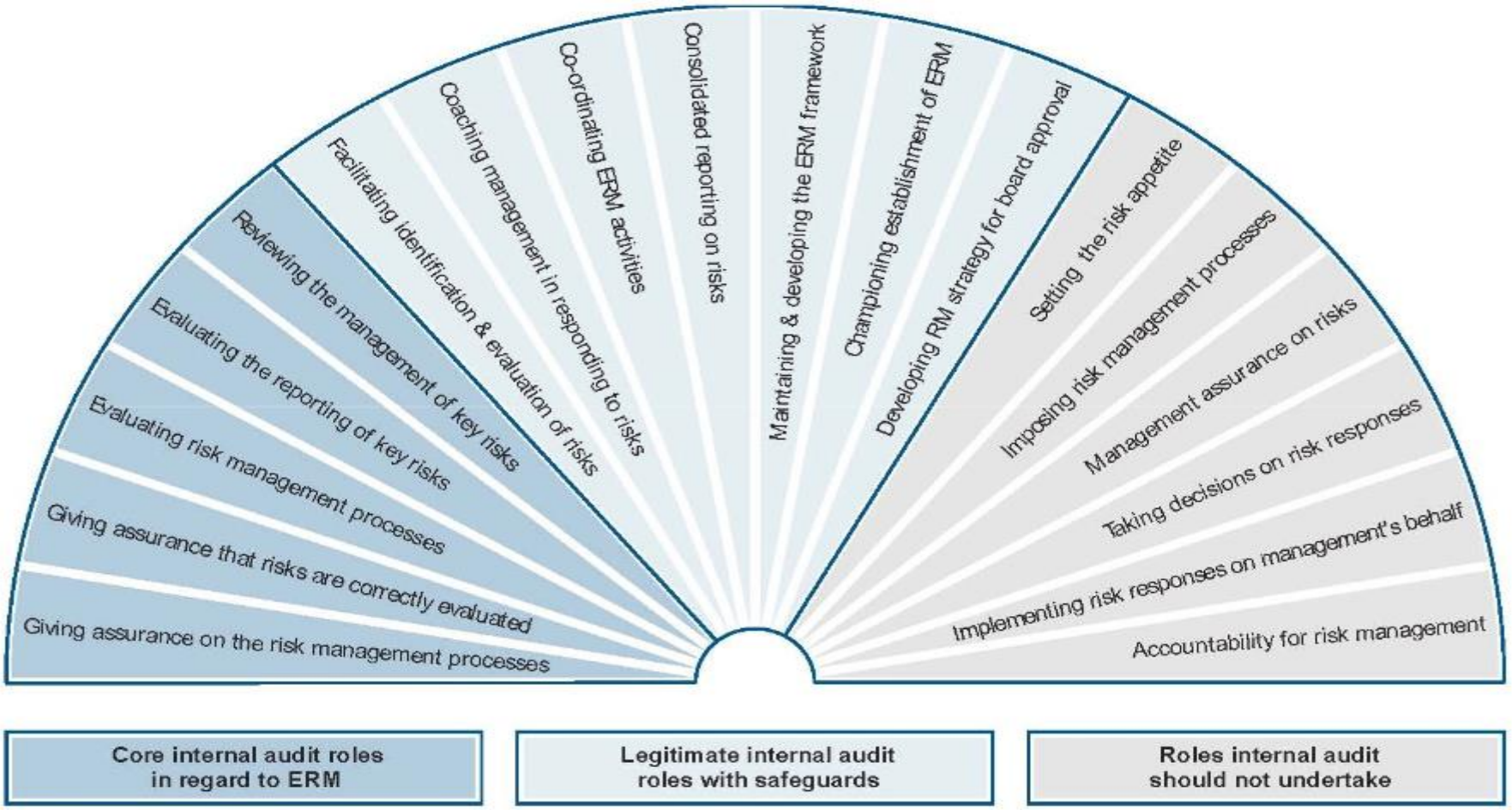
Convergence ....

- *Internal Audit Role at the Second Line of Defense should be limited and short term and is better placed to introduce risk management in an organization*

- *If long term then the Board should recognize the inability of the Internal Audit function to remain objective.*

- *Combining this roles saves on costs but it impairs objectivity*

Convergence ....



Convergence ....

- *Internal Audit can be used to champion establishment of Proper Governance framework but they should never own the risk management process*

Interactive Session

Interactive Session

NASUMBA KIZITO KWATUKHA

CPA, CIA,CFE,CISM,CISA,CISSP,CRMA

nasumbak@yahoo.com

0728-771-497