BOARD AUDIT COMMITTEE'S ROLE IN ACHIEVING EFFECTIVE ENTERPRISE RISK MANAGEMENT IN THEIR INSTITUTIONS

19 September 2019

Content of Presentation

1) Pre-Amble: Establishing a Case for Enterprise Risk Management in the Public Sector
2) Definition of Risk and Risk Management
3) Pre-Requisites for Implementation of Effective ERM in Institutions.
4) Structured Process of Developing an Institution's ERMF
5) Role of BOD, AC and Management in Achieving Effective ERM in Their Institutions

Pre-Amble

The Public Finance Management Regulations (PFMR) requires the Accounting Officer to ensure that the entity develops:

a. risk management strategies, and

b. a system of risk management and internal control that builds robust business operations

Pre-Amble

***The Mwongozo* Code of Governance for State Corporations** states that:

- The Board has the responsibility of ensuring that the organisation has adequate systems and processes of accountability, risk management and internal controls.

The **Performance Contract** with the Government and performance management requires the institutions to manage risk exposures effectively

WHAT IS RISK?

Risk refers to:

- the **threat** of an event occurring that could undermine or stop your organisation from successfully achieving its objectives.
- **uncertainty** of outcome of actions and events, whether **positive opportunity** or **negative threat**.
- events or conditions that have a negative impact on the achievement of the **organisations' strategic and business objectives**.

WHAT IS RISK?

Organisational Risks will consist of **two** elements:

1. Probability or Likelihood
2. Consequence or Impact

Risk involves the likelihood of undesired event /outcome will occur.

Risk considers the severity of consequence of the event

Risk

WHAT IS RISK MANAGEMENT?

Risk management is not **about avoidance.**

- ✓ It is about maximising the risk/return relationship.
- ✓ It is about taking risks knowingly not unwittingly.

Risk Management is the maintenance of an appropriate balance between **risk** and **control**.

RISK **CONTROL**

WHAT IS RISK MANAGEMENT?

Risk Management

- *A process to identify, assess, manage, and control potential events or situations*
- *to provide reasonable assurance regarding the achievement of the* ***organization's objectives***

(IIA Standards)

WHAT IS RISK MANAGEMENT?

Risk Management

- Is a logical and systematic process
- Considers all the organisation's activities, functions or processes
- Enables an organisation to **minimize losses and maximize opportunities**

WHY IMPLEMENT ORGANISATIONAL ERM?

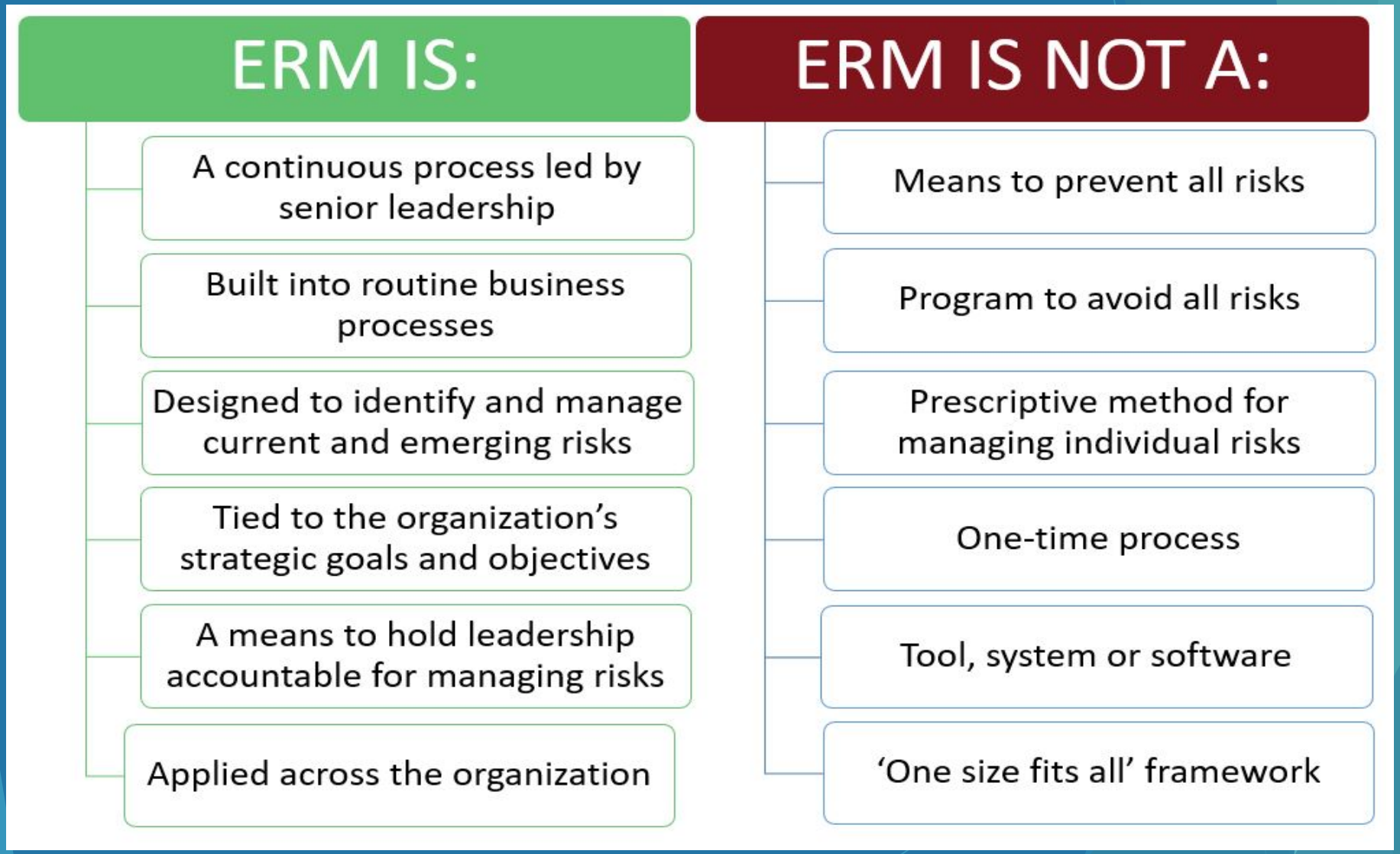
Effective enterprise risk management structures support:

1. Achievement of **strategic**, and **operating objectives**, hence value creation.
2. **Compliance** with laws, regulations and contractual obligations.
3. **Alignment of institution's objectives** with those of its **key stakeholders**.

BENEFITS OF ENTERPRISE RISK MANAGEMENT

- Greater likelihood of achieving objectives
- Serves as an early warning system for potential problems
- Leads to more efficient resource allocation (e.g. capital and cash)
- Provides better information on potential consequences, both positive and negative.
  - Hence helps identify positive opportunities and avoid threats
- Reduces the risk of loss, builds credibility and creates new opportunities for growth

WHAT IS ENTERPRISE RISK MANAGEMENT?



ORGANISATIONAL OBJECTIVES AND RISKS

Organisational objectives, including setting thereof, underlie all effective risk management processes and programmes.

The **objectives** will be in the nature of:

- **Strategic** Objectives;
- **Compliance** Objectives;
- **Operating** Objectives;
- **Sustainability** Objectives;
- **Stakeholder Engagement** Objectives

PRE-REQUISITES FOR EFFECTIVE IMPLEMENTATION OF ERM

1) Risk Management Policy

- Strategy for identifying, measuring, and responding to its internal and external risks;
- Roles of the organization's oversight and stewardship organs in risk management;

PRE-REQUISITES FOR EFFECTIVE IMPLEMENTATION OF ERM

Risk Management Policy should contain:

- Organisational Mandate, Objectives and Functions;
- Purpose, Rationale and Objectives of ERM;
- ERM Process for Risk Identification; Assessment & Ranking; Mitigation;
- Roles & Responsibilities for ERM: Board; Audit Committee; Management; RM Committee or Function; Internal Audit

PRE-REQUISITES FOR EFFECTIVE IMPLEMENTATION OF ERM

2) **Risk Management Framework** that documents:

- Organisation's **risks** and the **causes** of such events /outcomes (**risk universe**)
- **Assessment and categorisation** of the identified risks
- Risk **Mitigation Strategies** and **Controls**
- **Assignment of Responsibility** for management of the risks
- **Implementation** Timelines
- Monitoring and Review Timelines

PRE-REQUISITES FOR EFFECTIVE IMPLEMENTATION OF ERM

3) Monitoring and reporting system

Effective implementation of ERM requires collaborative engagement between:

Governance Organ

- Board and Audit & Risk Committee

Functions that own and manage risks

- Executive and Operating Management

Functions that oversee risks

- Risk Management and Compliance Sections

Functions that provide independent assurance

- Internal Auditors

DEVELOPING THE INSTITUTIONAL RMF

Process of developing and implementing Institutional Risk Management Framework:

1) **Establishing & Identifying** the **Risk Universe**
   - Potential sources of risks from the Internal & External Environment;
   - The specific **risks** facing the institution (**risk events**), and their causes (**risk drivers**).
2) **Assessing / Categorising** the identified risks:
   - ✓ **Analysing** the risks – likelihood / consequence.
   - ✓ **Evaluating** the **Risk Level** (likelihood x impact).

DEVELOPING THE INSTITUTIONAL RMF

Process of developing and implementing the **IRMF**:

3. Risk Treatment

- Strategies may include: **A**voidance; **T**ransfer / Sharing; **A**cceptance; **C**ontrol (**ATAC**)
- Developing and implementing the requisite policies, procedures and internal controls to mitigate the identified risks

DEVELOPING THE INSTITUTIONAL RMF

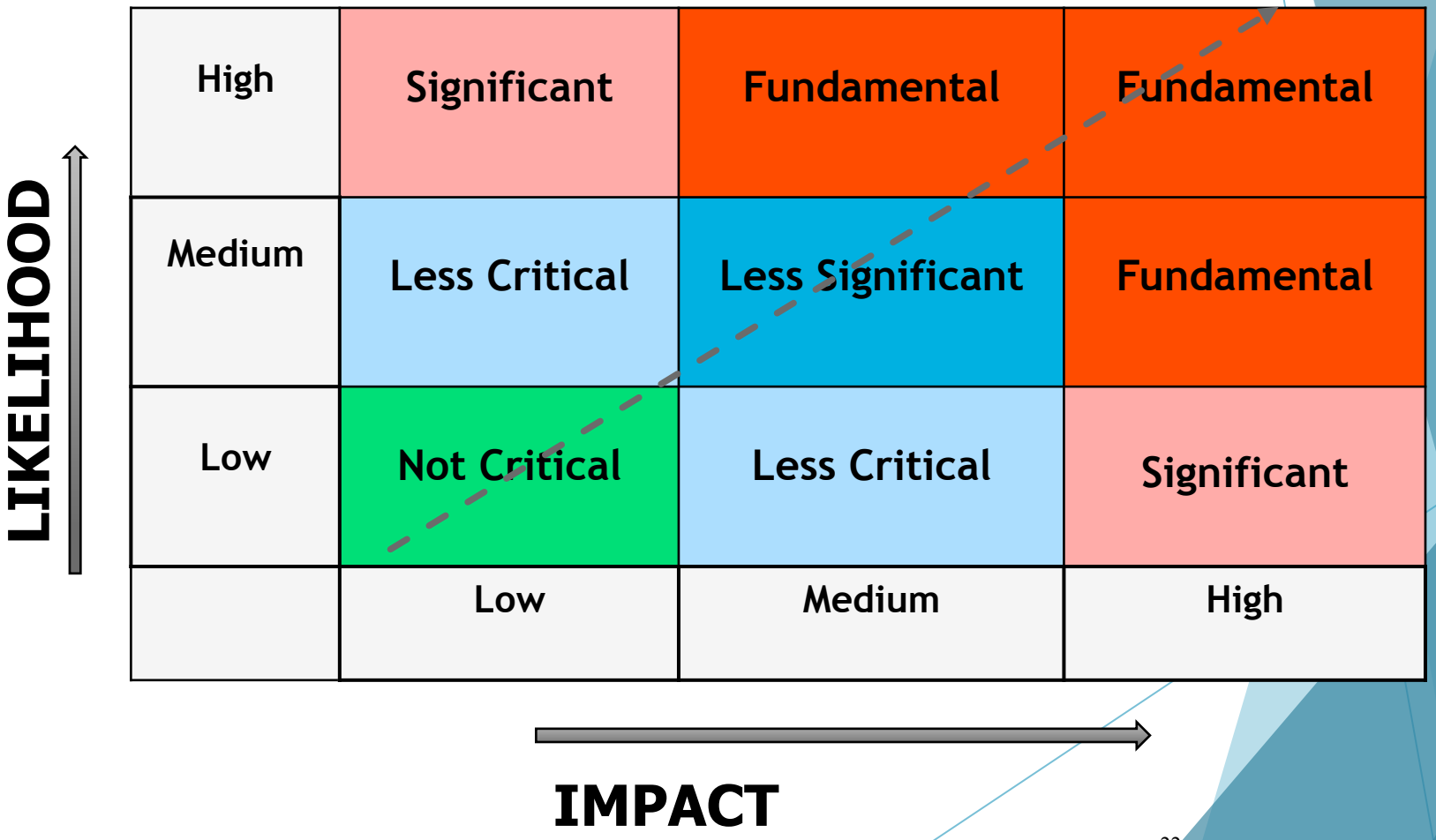
Process of developing and implementing the **IRMF**:

4. **Assigning Responsibility** for requisite control activities
5. **Monitoring** operation and effectiveness of controls.
6. **Feedback** and **Reporting** Mechanism

Audit Committee's Role in Achieving Effective ERM

RISK LEVEL & ASSIGNMENT OF RESPONSIBILITY

The Risk Level can also be depicted graphically by plotting the **Likelihood** against the **Impact**



AC'S ROLE IN ACHIEVING EFFECTIVE ERM

Public Entities should adhere to requirements of the ***Mwongozo Code of Governance*** and other Guidelines on ERM and Internal Control

The Board should support implementation of appropriate structures and systems in respect of:

- Governance;
- Risk Management; and,
- Control

THE BOARD'S ROLE IN RISK MANAGEMENT

The Audit, Risk & Governance Committee, should:

1. Ensure that significant strategic, operational, compliance and financial risks have been identified, prioritised and managed.
2. Support the BOD to determine the level of risks acceptable to the organisation
3. Confirm that strategies are in place to manage risks.
4. Hold management accountable for identifying emerging risks.

INTERNAL CONTROLS

Internal Control **Objectives:**

- **Preventive;**
- **Detective;**
- **Corrective**

Nature of Internal Control:

- **Formal controls** include controls such as physical and authorisation controls, segregation of duties, policies and procedures, etc.
- **Informal controls** include the institutional **ethics**, **culture**, **commitment**, **communication** and teamwork.

FORMAL & INFORMAL CONTROLS

Most frauds, corruption and corporate failures are not due to lack of formal controls.

They arise due to inappropriate application of the **informal controls,** i.e. unethical climate, abuse of power, impunity, and deliberate override of controls by Directors and Senior Management.

The effectiveness of internal control **cannot rise above the ethical values of the people** who create, administer and monitor them, i.e. Directors and Senior Management.

Questions and Open Forum

Thank you

Michael Itote

Management Audit Consulting Ltd
Davard House, 5 Cedar Road, Off Rhapta Road, Westlands
Tel: (+254) 715 096 708 or 736 952 271
E-mail: info@managementaudit.co.ke
www.managementaudit.co.ke