# GOVERNANCE, RISK MANAGEMENT AND COMPLIANCE TRENDS BY FCPAK ERIC KIMANI

# CONTENTS

- Overview
- Conceptual Definition
- Implementation of Strategic Risk Governance
- Success Factors
- Changing Internal Audit Roles in GRC
- Contemporary Internal Audit Report
- Conclusion

# OVERVIEW

- **Historical Perceptive to Strategy Governance of Risk**
  - **2007/2008 Economic Crunch/Global Melt down**
  - **WHY?**

- Risk management not linked to strategy
- Weak Board of Directors oversight on Risk Management Activities due to Knowledge Gap
- Lack of a clearly defined risk appetite.
- Inadequate and often fragmented technological infrastructures that hindered effective risk identification and measurement; and
- Silo approach to risk management
- Weak Control & Compliance Framework

# STRATEGIC GOVERNANCE OF RISK

**Conceptual definition**

- Strategic Governance of Risk is also referred to as
- Governance, Risk Management & Compliance (GRC) and this entail
- Integration of governance, risk assessment and mitigation, and compliance and control activities to operate in synergy and balance.
  - **Internal Audit** –provide assurance to the Board on effectiveness on institution's GRC
- **GRC Approach:**focuses on maintaining the right balance between risk and reward
- **Objective**: An effective risk management program focuses simultaneously on value protection and value creation.

# STRATEGIC GOVERNANCE OF RISK

- **Board of Directors** set a broad vision and objectives of GRC Framework
- **Governance Processes** define the governance structure, processes and responsibilities
- **Enterprise Risk Management** Framework addresses contemporary, emerging and dynamic business risks
- **Regulatory and Compliances** are managed through an effective framework and compliance management process
- **Internal Audit** is an integral part of the GRC framework which assesses the effectiveness of other GRC elements

# STRATEGIC GOVERNANCE OF RISK

Strategic Risk Governance also known as GRC is a *continuous process* that is embedded into the culture of an organization and governs how management

- identifies and protects against material and relevant risks,
- monitors and evaluates the effectiveness of internal controls, and;
- responds and improves operations based on learned insights from internal audit findings on the assurance of GRC Framework
- Governance Processes define the governance structure, processes and responsibilities.

# IMPLEMENTION OF STRATEGIC RISK GOVERNANCE

- Risk Governance is basically the responsibilities of BOD;
  - Approve Enterprise Risk Management Framework that aligns with Strategy
  - Common Risk definition
  - Transparency and full disclosure to governing bodies
  - Internal Audit Assurance to the BOD on the effectiveness of GRC
- Risk Infrastructure and Management
  - Institute uniform and Common Risk Infrastructure that is independent and report to Board Risk Committee comprising
    - Risk Management Process
    - Adequately skilled Risk Management Team led by CRO
    - Risk Automation to drive risk analysis, measurement and monitoring
  - **Executive Management is responsible for daily implementation of Enterprise Risk Management Framework**
  - **Risk Management assurance and monitoring reports**
- Risk Ownership & Accountability
  - Business Unit Responsibilities
  - Support Function
- **Compliance**: institutionalize a compliance culture of zero penalties

# GOVERNANCE RISK & COMPLIANCE FRAMEWORK

- Corporate Governance Management
  - Annual Evaluation of institution's corporate governance
  - Remediation Strategies
  - Corporate Governance Performance Monitoring
  - Internal Audit Assurance
- Risk Management
  - Strategic & entity level risk assessment
  - Alignment of strategic & entity level risks with operational controls
  - Development of Risk Mitigation
  - Risk Monitoring
- Compliance Management
  - Internal Control & Matrix development
  - Internal Control Evaluation
  - Internal Monitoring
  - Regulatory & Legislation Compliance Matrix development
  - Regulatory & Legislation Compliance Observance
  - Regulatory & Legislation Compliance Monitoring

# SUCCESS FACTORS

1. Addresses business needs and strategically align to the organization's overall objective.
2. An integrated approach of risk and control with accurate and timely communication of risk information to the decision making
3. Strong collaboration and teamwork.
4. A risk aware culture.
5. Demonstrated return on investment on GRC implementation.
6. Risk awareness and training for risk owners

# WHY GRC FAILS

1. Lack of shared vision for risk management and compliance
2. Ineffective stakeholder engagement
3. Ineffective change management.
4. Project implementation delay

# CHANGING INTERNAL AUDIT ROLE UNDER GRC

- Board Audit Committee reviews the GRC initiatives, priorities, process, framework and implementation plans of GRC model
- Internal Audit is an integral part of the GRC framework which assesses the effectiveness GRC elements (Governance, Risk & Compliance) and provide assurance to the Board of Directors.
- Anti-fraud Governance Structure defines the framework for fraud avoidance and detection through the use of process and technology

# CHANGING INTERNAL AUDIT ROLE UNDER GRC

| S/N | TRADITIONAL APPROACH | PROCESS VALUE ADDED/DEVELOPMENTAL | STRATEGIC VALUE ADDED/FORWARD LOOKING |
|---|---|---|---|
| 1 | Policing | Collaboration with stakeholders | Business Partners to risk owners |
| 2 | **Transactions Based**-Accounts & Verification, detection, fraud & investigation | **Risk based** (focus on activities that matter to the organization). | **Solution provider** to Business growth and sustenance, |
| 3 | Inspection | Adequacy of Controls | Adviser and Mentor |
| 4 | Lower level of accountability | Robust accountability | |
| 5 | Compliance Based | System Based (Horizontal/Vertical) | |
| 6 | Joining up signoffs and year end confirmations for accepting and following policy | Policy related proactive awareness creation and implementation | |
| 7 | Key Focus- Detailed Financial Review | All function-Financial and Non-Financial | Key issues for the business |

# PROGRESSION OF INTERNAL AUDIT FUNCTION

- Risk & Control Effectiveness
  - Risk Based Internal Audit
  - Risk Control Self Assessment
- Operational Efficiency
  - Operational Framework
  - System integrity with business operations and business need
- Governance Process
  - Risk Management Committee
  - Audit Committee effectiveness
- Cost Efficiency
  - Cost Optimization and Rationalization plans
- Performance Efficiency
  - Key Performance Indicators and Key Results Areas
  - Balanced Scorecards
- Business Strategy & Plan
- Review of Business Strategies and plans
  - Review of Annual Business Plans
  - Budgets & Budgetary Controls

| S/N | RISK MANAGEMENT | INTERNAL AUDIT |
|---|---|---|
| 1 | Develop Enterprise Risk Management Framework | Audit the adequacy and effectiveness of the risk management framework |
| 2 | Implement Enterprise Risk Management Framework | Audit implementation of the risk management framework |
| 3 | Advise Management on integration of risk management into business operations and their roles in making it work | Audit management's commitment to risk management and the take up of their roles |
| 4 | Advise on the allocation of accountability for risks, controls and tasks | Audit whether accountable managers fulfill those roles and are capable |
| 5 | Advise Management and Board on the interpretation of risk management information | Provide independent assurance of the risk management information submitted to the Board |
| 6 | Provide appropriate risk management status and performance information to the Board Audit and Risk Committees | Provide independent view on the credibility and reliability of the risk management of the risk management information submitted to the Board Audit and Risk Committee. |
| 7 | Acts as an advisor and mentor to management on risk management matters | Act as independent reviewer to provide assurance on management's capability and performance in risk management |
| 8 | Review Governance, institute global best practice Enterprise Risk Management and Compliance | Internal Audit provides assurance on Governance, risk and compliance |

# CONTEMPORARY AUDIT FINDINGS

**Rating High, Medium Low on risk profiling**

**High**

Substantial financial loss, possibly in conjunction with other weaknesses in the control framework or the organizational entity or process being audited

Serious violation of corporate strategies, policies, or values

Significant adverse regulatory impact, such as loss of operating licenses or material fines

**Medium**

Timely management attention is warranted. This is an internal control or risk management issue that could lead to financial loss, reputation damage, adverse regulatory impact

**Low**

As this is a low priority issue, routine management attention is warranted

# CONCLUSION

Strategic Governance requires that the Internal Audit be more proactive in their audit approach using collaborative and consultative approach to create and protect shareholders value. The following are the benefits of GRC for Internal Audit

- Quick identification of potential issues due to rapid authorization flow, giving greater visibility within the organization
- Reducing runtimes audit plans through self-managed reports and evidence centralized online
- Improved coordination and utilization of resources area
- Timely and accurate business operations (continuous monitoring)
- Improved process of remediation and risk management

# Parting Shot

THANK YOU!

# Interactive Session