POSITIONING INTERNAL AUDIT IN RISK GOVERNANCE

Presentation by:

CPA John Wachiuri, MBA, CISA,CIA
Head, Internal Audit, Family Bank Limited
Thursday, 15th, August, 2019

Uphold public interest

Presentation agenda

Outline

- Key ERM Concepts
- Snapshot of ERM Process
- Corporate Governance vs Risk Governance
- Objectives of ERM
- Concept of 3 lines of Defense

Outline

Outline

- IA Role in Governance
- IA role in Risk Management
- Communicating acceptance of risks
- Corporate Scandals
- Path to Quality
- Conclusion

- We advice our clients not to hire the most brilliant managers.

- Risk in inversely proportional to knowledge.

- Otherwise there would be too many wealthy University Professors.

KEY CONCEPTS FROM IPPF

- **RISK** The possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of impact and likelihood.
- **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
- ERM: **a structured**, consistent, and continuous process across the entire organization for **identifying**, **assessing**, deciding on **responses** to risks and **reporting** opportunities and threats that affect achievements of objectives: IIA definition.
- **Governance:** The combination of processes and structures implemented by the board to inform, direct, manage, and monitor the activities of the organization toward the achievement of its objectives.

RISK MANAGEMENT PROCESS

SNAP SHOT OF THE RISK MANAGEMENT PROCESS

Risk identification	• **Retrospective risks**: Historical, Those that have happened • **Prospective:** Futuristic
Risk Analysis	• Risk= **Impact * Likelihood**
Risk Evaluation	• Is risk **acceptable** or **unacceptable,** • **Rank the risks**
Risk Treatment	• **Eliminate** or **contain** • Accept, Avoid, Retain
Monitor & Review	• **Effectiveness** of the ERM, Internal Audit reviews

What is Risk Governance

Corporate Governance

- The system by which companies are **directed** and **controlled**.
- The system of rules, practices, and processes by which a firm is directed and controlled.

Risk Governance

- The **architecture** within which risk management operates in an organization.
- Reflects, & seek to sustain and evolve, the organization's **risk culture**.
- A fundamental part of corporate governance.

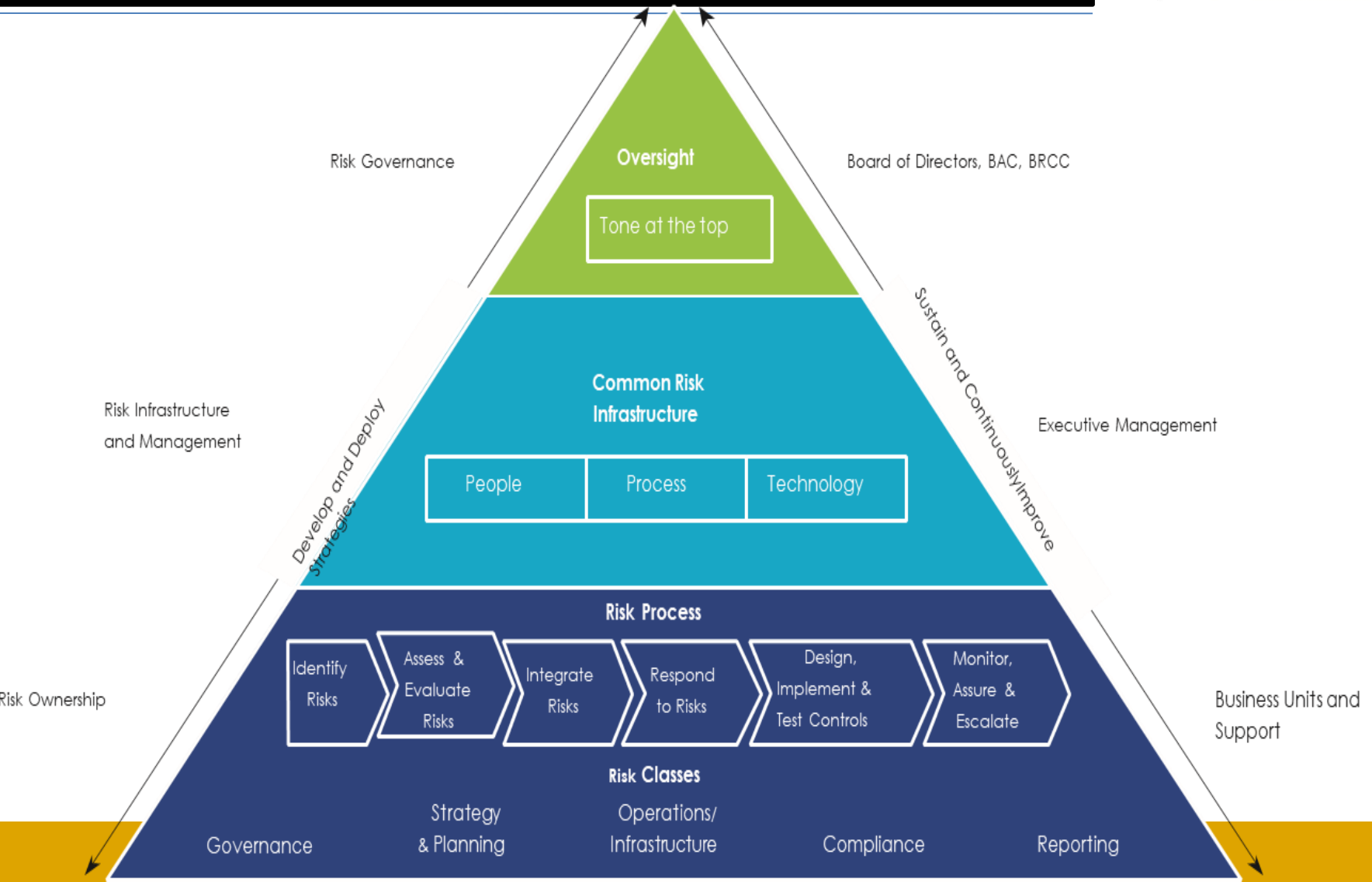
Risk Governance Continued

- **The British Standard BS13500** defines governance as: 'system by which the whole organization is directed, controlled and held accountable to achieve its core purpose over the long term'.
- **The UK Corporate Governance Code** states that 'good governance should facilitate efficient, effective and entrepreneurial management that can deliver the long-term success of the company'.
- Good risk governance should result in risk being accepted and managed within known and agreed risk appetites.

Risk Governance.....

- Risk governance should put in place a **structure of risk responsibility** throughout the organization.
- Everybody in the organization will be **aware of their own risk responsibilities and accountabilities** and those of others with whom they work.
- Governance delivers effective accountability, including the accountability of the governing body to its owners.
- **Risk governance** is an **integral part of the day to day running of the business** and is not about just complying with a set of rules.

Risk Governance



Snap shot of objectives of risk management

Minimize threats and enhance opportunities.

Identify, evaluate, mitigate and control risks

Determine key risk indicators (KRI) and key performance indicators (KPI) to align effort to meet organizational strategic goals.

SWOT analysis: Establish Strengths and weaknesses

Business continuity- Sustainability

Align resources to reduce Threats and impact

Concept of 3 lines of defence

1st Line: Business Units	• Involved in **day to day risk management. Own and manage risks**. • Directly implement policies, processes and procedures. • 100% adherence to processes and procedures. • Include staff in first line of business
2nd Line: Risk, Compliance, Support functions e.g. IT,	• **Oversee implementation of risk management**. • Provide guidance and direction • Develop risk management framework • Include Risk and Compliance and other support functions e.g. Finance, HR, • Prevent risks from crystalizing
3rd Line: Oversight, Internal Audit, External Audit, CBK Inspection	• Review 1st and 2nd lines of defence. • **Provide independent , perspective and challenge** the process. • Review ERM, internal controls and Governance processes. • Include Internal Audit, External Auditors, Regulators etc.

Internal Audit Role in Governance- IPPF 2110

Internal audit activity must assess and make appropriate recommendations to improve the organization's governance processes for:

- Making **strategic** and **operational decisions**.
- **Overseeing risk management** and control.
- Promoting appropriate **ethics and values** within the organization.
- Ensuring **effective organizational performance** management and accountability.
- **Communicating risk** and **control information** to appropriate areas of the organization.
- Coordinating the activities of, and communicating information among, the **board, external and internal auditors, other assurance providers, and management**

Review of Strategic and Operational Decisions

Board Minutes

Past audit reports

Governance documents e.g. Board Charter

Interviews with departmental heads

Check for consistent decision-making processes

Review the processes that lead to operational and strategic decision making

Overseeing risk management and control- Internal Audit to review:

- Process for conducting the **annual risk assessment**
- **Minutes from meetings** wherein risk management strategy was discussed
- **Previously** conducted risk assessments
- **Interview key risk management personnel** such as compliance, risk, and finance officers.
- **Benchmarking** and Industry trends

Internal Audit Role in Governance- IPPF 2110....

Area of Review by Internal Auditor	Work to be done by internal auditor
Promoting appropriate ethics and values	❑ Mission and value statements, Code of conduct ❑ Hiring and training processes ❑ An anti-fraud and whistleblowing policy & Investigation process. ❑ Surveys and interviews may be used to gauge whether the organization's efforts result in sufficient awareness of its ethical standards and values.
Effective organizational performance management and accountability	❑ Process for staff compensation, objective setting, and performance evaluation. ❑ Measurements such as key performance indicators ❑ Incentive plans (e.g., bonuses) ❑ Check whether they are appropriately designed and executed to ❑ prevent or detect unacceptable behavior or excessive risk-taking and to support actions aligned with the organization's strategic objectives.

Internal Audit Role in Governance- IPPF 2110....

Area of Review by Internal Auditor	Work to be done by internal auditor
Communicating risk and control information to appropriate areas of the organization	❑ Access **internal reports**, newsletters, relevant memos and emails, & ❑ Staff **meeting minutes** to determine whether risk information and controls are complete, accurate, and distributed timely. ❑ **Surveys and interviews** to gauge employees' understanding of their responsibilities over risk and control processes and the impact to the organization if those responsibilities are not fulfilled. ❑ Evaluate how the area under review **communicates** risk and control information.
Coordinating the activities, communicating information among, the board, external and internal auditors, other assurance providers, and management	❑ Review the **meetings for board**, audit committee, and finance committee and determine how frequently they occur. ❑ Attend the meetings as participants or **observers.** ❑ Review the **meeting minutes**, work plans, and **reports** distributed among the groups to learn how these parties coordinate activities and communicate with each other.

IPPF 2120- Risk Management

Requirements of IPPF 2120 on Risk Management:

The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes by assessing whether:

- ***Organizational objectives*** *support and align with the organization's mission.*
- ***Significant risks*** *are identified and assessed.*
- ***Appropriate risk responses*** *are selected that align risks with the organization's risk appetite.*
- *Relevant* ***risk information is captured and communicated*** *in a timely manner across the organization, enabling staff, management, and the board to carry out their responsibilities.*

IIA Position Paper on role of internal audit in risk management

Cores Roles- Assurance Activities

Legitimate Internal Audit Roles and Safeguards

Roles Internal Audit **should not undertake**

IIA Position Paper on role of internal audit in risk management

Core Roles- Assurance	Consulting Activities	Should not undertake
❑ Adequacy of the risk management process ❑ That risks are correctly evaluated. ❑ Assurance on overall risk management process. ❑ Evaluating reporting of key risks ❑ Reviewing management of key risks	❑ Facilitate identification and **evaluation** of risks ❑ Coaching management in responding to risks ❑ Coordinating ERM activities ❑ Coordinating reporting of risks ❑ Maintaining and developing ERM framework ❑ Champion establishment of ERM ❑ Develop ERM strategy for Board approval ❑ Facilitating workshops on risk management ❑ ***Key to note: IA should not assume any risk management role.***	❑ Setting risk appetite ❑ Imposing risk management processes ❑ Taking **decisions** on risk responses ❑ Implementing risk response on managements behalf ❑ Accountability for risk management ❑ Directing staff on risk management actions

IIA Position Paper on role of internal audit in risk management

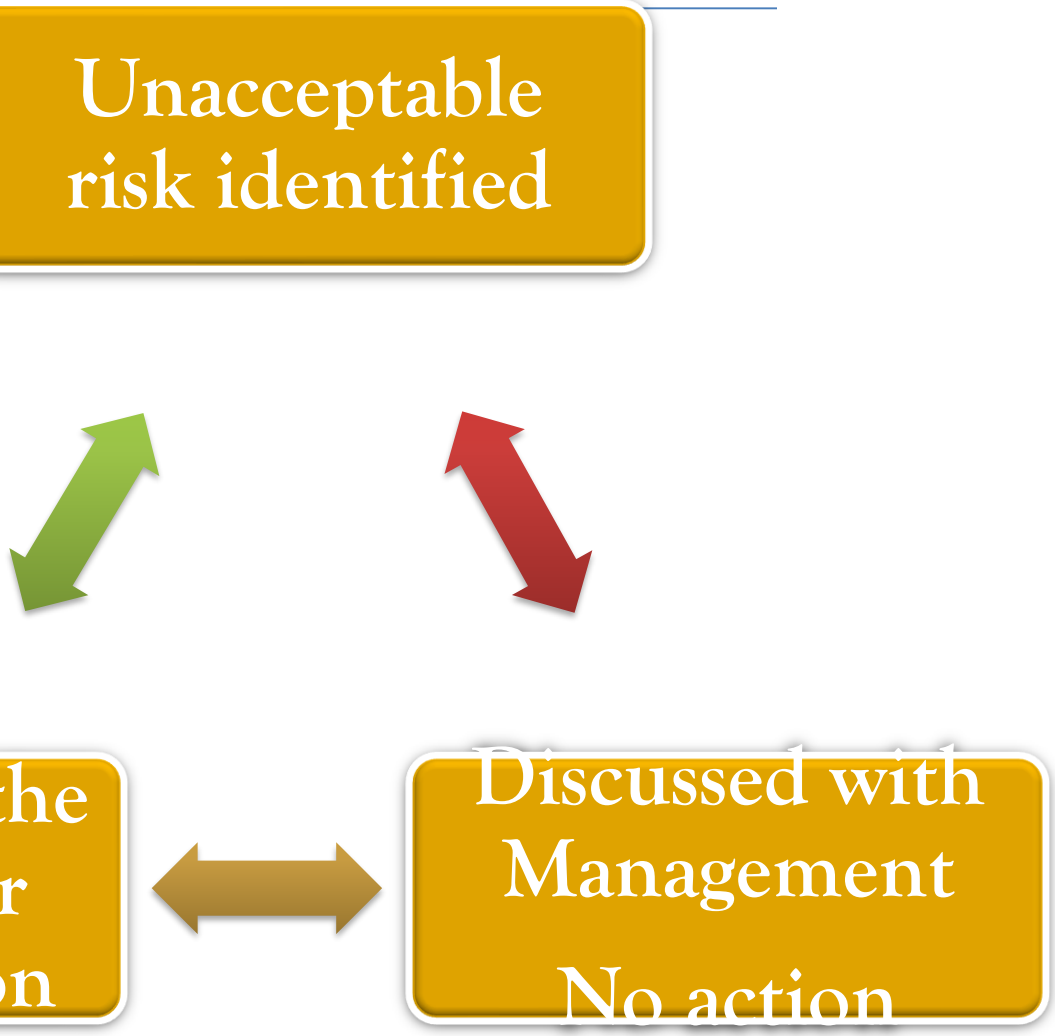
Consulting: Safeguard to IA independence:

- Clear that **management** remains **responsible** for risk management
- IA role clearly **documented** in the **internal audit charter** approved by Board Audit Committee
- IA should **not manage risks** on behalf of management.
- IA should **not take risk management decisions;** only challenge, advice, support.
- If IA is responsible for some risk management functions then **don't give assurance** on such area. Appoint another independent 3rd party to give assurance: **Self Review Risk**
- Any work by IA in risk management beyond assurance should be recognized as **consulting.**

Broad areas that Internal Audit provides assurance

- **Risk management processes**, both their design and how well they are working;
- **Management** of those risks classified as **'key'**, including the effectiveness of the controls and other responses to them; &
- Reliable and **appropriate assessment** of risks and **reporting** of risk and control status.

IPPF 2600- Communicating acceptance of risks



IPPF 2600- Communicating acceptance of risks

- If Head of Audit concludes that management has accepted a level of risk that may be unacceptable to the organization, the HOIA must **discuss the matter with senior management**.
- If the HOIA determines that the matter has not been resolved, then he/she must communicate the **matter to the board.**
- The identification of risk accepted by management may be observed through an assurance or consulting engagement, monitoring progress on actions taken by management as a result of prior engagements, or other means.
- It is not the responsibility of the chief audit executive to resolve the risk.

IPPF 2600- Communicating acceptance of risks- Risk beyond tolerable level

- Those that harm organization's **reputation**
- Those that **harm people**
- Result in significant regulatory **fines**, limitations to business, **penalties**
- **Fraud** or other illegal acts
- Significant **impediments** to achieving strategic objectives

ENRON SCANDAL

Nature of Scandal	❑ Reported in October 2001, led to the **bankruptcy** of the Enron Corporation, an American energy company and the **dissolution** of **Arthur Andersen**, one of the five largest audit and accountancy partnerships in the world. ❑ Enron colluded with its Auditor Anderson to inflate profits, Creative Accounting. ❑ The largest bankruptcy reorganization in American history at that time. ❑ Enron was cited as the biggest audit failure.
Repercussions	❑ Share price fell from **US$90.75 per share** in mid-2000, to **less than $1 by** the end of November 2001. ❑ Enron filed for bankruptcy under Chapter 11 of the United States Bankruptcy Code. **Enron's $63.4 billion in assets** made it the largest corporate bankruptcy in U.S. history until WorldCom's bankruptcy the next year.

ENRON SCANDAL

Then what happened

- Enron's shareholders lost $74 billion in the four years before the company's bankruptcy
- Many executives at Enron were indicted for a variety of charges and some were later sentenced to prison.
- Enron's auditor, Arthur Andersen, found guilty in a US District Court of illegally destroying documents relevant to the SEC investigation which voided its license to audit public companies, effectively closing the business.

CORPORATE SCANDAL ENRON AND ANDERSO

- Sentenced to jail:

(i) Andrew Fastow (Chief Finance Officer) .

(ii)Jeffrey Skilling, the C.E.O


WHY THERE WAS NO WARNING OF ENRON'S COLLAPSE
REGULATORS
POLITICIANS
STOCK
AWALYSTS

World Com Scandal

- USA second largest long distance telephone company

- Booked operating expenses as capital expenditures on the balance sheet instead of income statement
- Inflating revenues with bogus accounting entries from "orate unallocated revenue accounts".

- Internal auditors revealed $3.8 billion worth of fraud.
- Total assets had been inflated by about $11 billion
- Top executives dismissed.

CORPORATE SCANDALS- BARRING BANK

- **Barings Bank** was founded in 1762 as the **John and Francis Baring Company** by Francis Baring,

- Barings was brought down in 1995 due to unauthorized trading by its head derivatives trader in Singapore, **Nick Leeson.**

- Leeson was supposed to be arbitraging, seeking to profit from differences in the prices of Nikkei 225 **futures contracts** listed on the Osaka Securities Exchange in Japan and the Singapore International Monetary Exchange.

- Instead of buying on one market and immediately selling on another market for a small profit, the strategy approved by his superiors, **Leeson bought on one market then held on to the contract, gambling on the future direction of the Japanese markets.**

CORPORATE SCANDALS- BARRINGS BANK

- Leeson was the only floor manager for Barings' trading on the Singapore International Monetary Exchange and also the unit's head of settlement operations.

- In the latter role, Leeson was charged with ensuring accurate accounting for the unit.

- No segregation of duties.

CORPORATE SCANDALS- BARRINGS BANK

- By allowing Leeson, as trading floor manager, to settle his own trades, Barings short-circuited normal accounting and internal control/audit safeguards.

- Leeson operated **with no supervision** from London—an arrangement that made it easier for him to hide his losses.After the collapse, several observers, including Leeson himself, placed much of the blame on the bank's own deficient internal control and risk management practices. A number of people had raised concerns over Leeson's activities but were ignored.

- By December 1994, Leeson had cost Barings £200 million. If the company had uncovered his true financial dealings then, collapse might have been avoided as Barings still had £350 million of capital.

Other Corporate Failures

- **HSBC Holdings Plc** agreed to pay a record **$1.92 billion in fines** to U.S. authorities for allowing itself to be used to launder a river of drug money flowing out of Mexico and other banking lapses.

- **Standard Chartered Singapore** was on Dec 2, 2016 fined **$5.2 million** and **S$2.4 million** respectively by the Monetary Authority of Singapore (MAS) for breaches of anti-money laundering (AML) requirements

Local cases of Corporate Failures

❑Dubai Bank	Under liquidation.
❑Local Bank	Placed under Receivership then acquired by a foreign bank.
❑Imperial Bank	Under receivership, being bought by KCB
❑Kenya Finance Bank	Liquidated together with other Banks.
❑Local Supermarkets	Under Statutory Management

Lessons learnt from scandals/failures

- There is a **direct correlation** between governance, risk management, controls and financial performance as well as future sustainability of the organization.

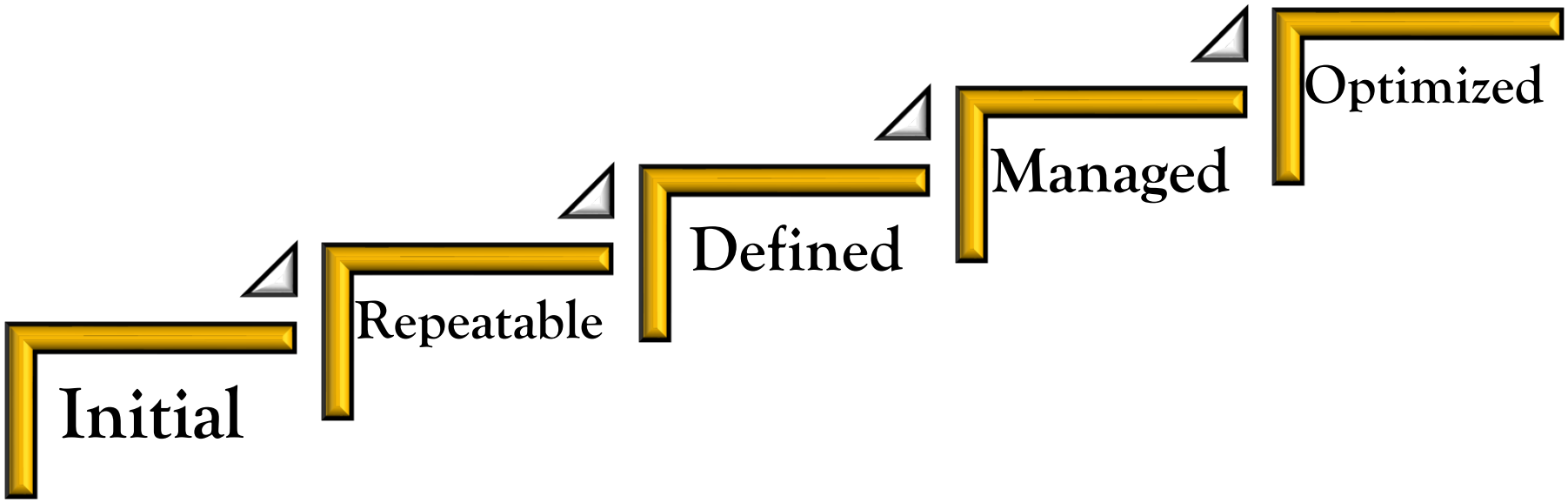
- The organizations that **outperform the market** have very strong risk management, internal control and governance frameworks.

- **Weaknesses** in **ERM** lead to **revenue leakages**, **losses** through **frauds**, high costs eventual **collapse of organizations.** We cannot allow this to happen in our organizations.

Benefits of a Robust ERM

- Greater likelihood of **achieving** strategic objectives;
- Consolidated **reporting** of disparate risks at board level;
- Improved **understanding** of the key risks and their wider implications;
- Identification and **sharing** of cross business risks;
- Greater management **focus** on the **issues that really matter;**
- ***F*ewer surprises** or crises; **doing the right things**
- Focus on **doing right things in the right way**;

Path to ERM Quality



Risk Maturity Model

Stage	Culture	Governance	Process
1: Initial	Risk belongs to internal audit	HOIA, Audit Committee Chair	Risk- Based Auditing
2: Repeatable	Risk considered on a need basis	Business Managers	As- needed risk & control self- assessment process
3: Defined	Risk info shared among internal audit and control functions	C- Suite/ Board Members	Common risk language, risk assessment process used by IA & control functions
4: Managed	Risk integrated in strategic planning, risk appetite stated & communicated	All levels of management and Board	Common risk language, consistent risk assessment process in place
5: Optimized	Risk integrated in all decision making, compensation, goals	Total participation	Common risk language, aggregated risk reporting established in org

Key to ERM Success- Internal Auditor to assess whether

Culture:

1. Is culture conducive to open discussions on risk?
2. If no policies existed, how would management operate?
3. Does culture overshadow intent Policies and procedures?
4. Is culture conducive to risk man
5. Is management focus on risk a t box exercise?

Governance:

1. Is there support from the top in ERM?
2. Is risk info used in decision making, strategy setting?
3. Is ERM driven from Board, Senior Management

2018 Corruption Percepti Index

Best	Worst
1. Denmark	1. Libya
2. New Zealand	2. Afghanistan.
3. Finalnd	3. Equatorial Guinea
4. Singapore	4. Guinea Bissau
5. Sweden	5. Sudan
6. Switzerland	6. North Korea
7. Norway	7. Yemen
8. Netherlands	8. South Sudan
9. Canada	9. Syria
10 Germany	10 Somalia

Conclusion

- Risk management is a **fundamental element of corporate governance**. **Management is responsible** for establishing and operating the risk management framework on behalf of the board.
- **Internal auditor's core role** in relation to ERM: To **provide assurance** to management and to the board on the effectiveness of risk management.
- ERM brings many benefits as a result of its **structured, consistent and coordinated approach**.
- When internal auditing extends its activities beyond assurance role, it should apply certain safeguards, including treating the engagements as consulting services in **order to protect its independence and the objectivity of its assurance services.**
- ERM can help raise the profile **and** **increase effectiveness of internal audit**

References

- IIA Postion Paper on Role of Internal Auditing in Enterprise Wide Risk Management: January 2009
- IIA Implementation Guide to IPPF No 2120 on Risk Management
- IIA Implementation Guide No 2600 on Communicating Aceptance of Risks:
- IPPF Practice Guide by IIA on Assessing Adequacy of Risk Management using ISO 31,000: December 2010
- IIA Position Paper on The 3 Lines of Defence in Effecive Risk Management: Jan 2013

Warren Buffet Quotes

- Risk comes from not knowing what you are doing
- Risk can be greatly reduced by concentrating on only on a few things.
- Investment decisions should be made on the basis of the most probable compounding of after- tax net worth with minimum risk
- Its madness to risk losing what you need in pursuing what you simply desire
- If you buy things you don't need today, you will sell things you need tomorrow.

Warren Buffet Quotes

- Rule no 1: Never Lose Money, Rule No 2, never forget rule No 1.
- Should you find yourself in a chronically leaking boat, energy devoted to changing vessels is likely to be more productive than energy devoted to patching leaks.
- When looking for people to hire I look for 3 things, Integrity, Competence and skills. If you don't have integrity, the other 2 will kill you.
- Honesty is a very expensive gift, don't expect it from cheap people

Interactive Session

Thank You

Contacts

Mobile: +254721404014

Email:
jwachiuri@familybank.co.ke

or

jmwachiuri@gmail.com