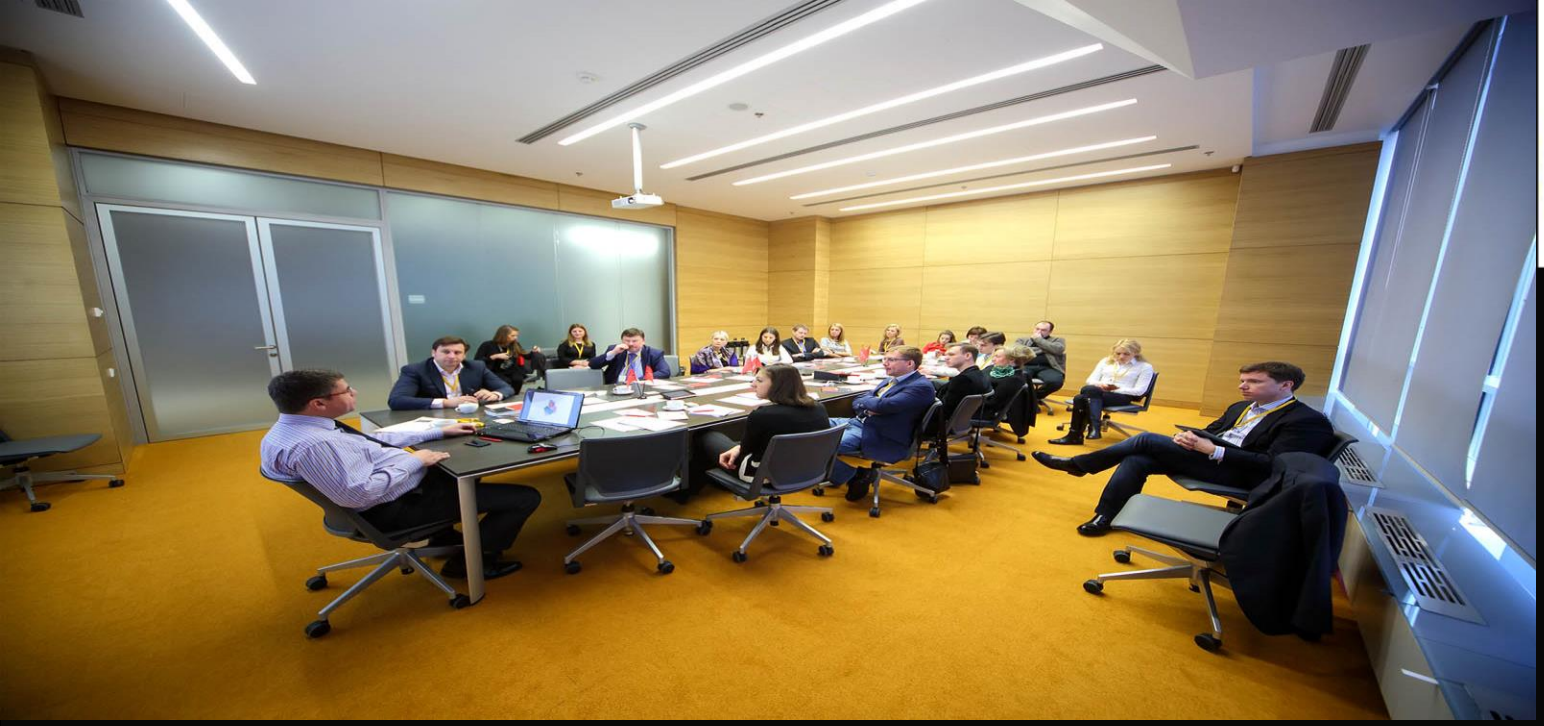


# Role of Board of Directors in Risk Management

Presentation by:

CPA Erick Audi

Thursday, 15th November 2018

# Presentation Agenda

- Introduction & Definitions
- Legal Provisions/Guidelines on Role of the Board in Risk Management
- Functions of the Board of Directors
- Role of the Board in Risk Management & Corporate Strategy
- BOD Tools and Techniques for Risk Management
- Best Practices on Risk Management for Boards
- Questions Boards should ask about Risk Management
- Conclusions
- Questions and Answers

# Introduction

The Board is ultimately responsible for an organization's risk management framework. Management are responsible for designing and implementing the RM framework.

The Board's role is to ensure the framework is sound and to oversee the effective operation of the framework. Since the global financial crisis, there is a greater focus by boards, their auditors and regulators on risk management

# Introduction

# Introduction

A transformation is under way at boards with respect to their role in enterprise risk management (ERM). In the wake of the global financial crisis, boards are taking a much more active role in risk oversight. They are reexamining governance structure and roles, risk policies and limits, and assurance and reporting processes.

This change is very significant and positive. Of the key groups that provide independent risk monitoring—boards, auditors, regulators, rating agencies, and institutional investors—the board of directors is the only group with both the direct responsibility and the greatest leverage in ensuring that sound risk management is in place.

# Risk Appetite (Definition):

- The amount of risk that an organization is willing to seek or accept in the pursuit of its long term objectives.

- In contrast to **Risk Tolerance (see below),** Risk Appetite is about what the organization does want to do and how it goes about it. So, it is the board's responsibility to define risk appetite.

- Risk appetite statements are used to articulate what risks the organization will take in pursuit of its objectives; the extent to which such risks will be retained; and the risks that will be avoided. It is clearly one of the prerequisite if the organization is to effectively identify and manage risks within an acceptance level.

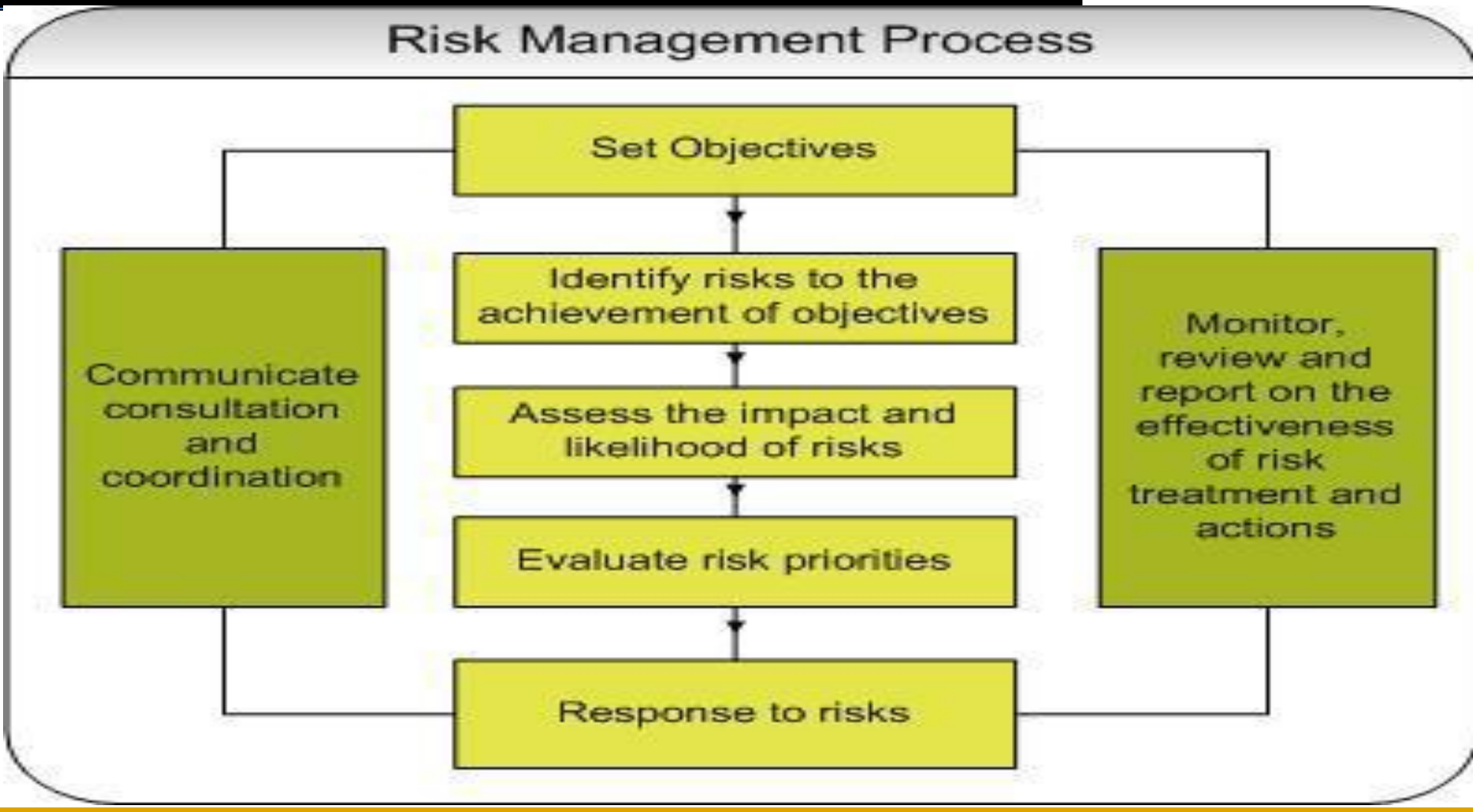
# Definitions.....

**Risk Tolerance (Definition):**

- The boundaries of risk taking outside of which the organisation is not prepared to venture in the pursuit of its long term objectives.

- Risk tolerance can be expressed in terms of absolutes, e.g., “we cannot expose more than x% of our capital to losses in a certain line of business” or “we will not deal with certain types of customers“

# Risk Management Overview



# What are the Harms that Come from Not Managing Risks

- Decline in credibility
- Inability to influence others
- Reputational loss
- Missed opportunity
- Failure to meet objectives

***The only alternative to risk management is crisis management --- and crisis management is much more expensive, time consuming and embarrassing.***

***JAMES LAM, Enterprise Risk Management, Wiley Finance © 2003***

# Crisis Management Versus Risk Management

- Crisis management is concerned with responding to, managing and recovering from an unforeseen event.

- Risk management is concerned with identifying, assessing and mitigating any activity or event that could cause harm to the business. Risks can be strategic or operational in nature.

- *An example of a strategic risk is not preparing adequately for new trends and shifts in the marketplace, while an example of an operational risk is the cost overrun on an infrastructure project.*

# CMA Code of Corporate Governance

- The Board shall have an effective risk management framework for the company in place.
- The Board shall determine the company's level of risk tolerance and actively identify, assess and monitor key business risks to safeguard shareholders' investments and the company's.
- The Board shall confirm the effectiveness of the company's risk management and internal control practices on a regular basis.

# CMA Code of Corporate Governance

- The Board shall, at least annually, ensure that a review of the effectiveness of the company's risk management practices and internal control systems is conducted and report to shareholders that they have done so. The review shall cover all material controls including financial, strategic, operational and compliance.

# PFMA, Regulations, 2015

**Section 165. (1)** The Accounting Officer shall ensure that National Government entity develops;

- Risk management strategies, which include fraud prevention mechanism; and
- A system of risk management and internal control that builds robust business operations.

# Treasury Circular No 3 of 2009, 23rd February 2009

- National Treasury had directed that all Public Sector Institutions set up an integrated Risk Management Framework.
- AC to oversight the risk management framework.
- Accounting officers to assume ownership of the RM framework.
- Fraud and Corruption risk management to form part of the RMF.

# Treasury Gazette Notice – Audit Committee Guidelines in National Government.

- The Audit Committee should review the entity's internal financial controls (*that is, the systems established to identify, assess, manage and monitor financial risks*).

- The entity's management is responsible for the identification, assessment, and management and monitoring of risk, for developing, operating and monitoring the system of internal control and for providing assurance to the Board and Executive Management that it has done so.

# Treasury Gazette Notice – Audit Committee Guidelines in National Government.

- Where the board or a risk committee is expressly responsible for reviewing the effectiveness of the internal control and risk management systems, the audit committee should receive reports from management on the effectiveness of the systems they have established and the conclusions of any testing carried out by internal and external auditors.

# Mwongozo Code of Governance

The Board shall:

- Ensure the development of a policy on risk management, which should take into account sustainability, ethics and compliance risks.
- Set out its responsibility for risk management in the Board Charter.
- Approve the risk management policy and the risk management framework.
- Delegate to management the responsibility to implement the risk management plan.
- Monitor that risks taken are within the **set tolerance and appetite levels.**
- Review the implementation of the risk management framework on a quarterly basis.

# Mwongozo Code of Governance

- Appoint a Committee responsible for risk management in the organization and ensure that the Committee obtains relevant technical advice where necessary.
- Evaluate the performance of the Committee once a year.
- Establish a risk management function within the organization.
- Ensure that risk assessment is carried out on a continuous basis.
- Receive from the Internal Audit function, a written assessment of the effectiveness of the system of internal controls and risk management.
- Receive assurance from Management that the risk management framework is integrated in the daily activities of the organization.

# Functions of the Board of Directors

- Define the company's mission, vision, its strategy, goals, risk policy plans and objectives, including approval of its annual budgets;
- Oversee the corporate management & operations, management accounts, major capital expenditures and review corporate performance and strategies at least on a quarterly basis;
- Identify the corporate business opportunities as well as principal risks in its operating environment, including the implementation of appropriate measures to manage such risks or anticipated changes impacting on the corporate business;
- Develop appropriate staffing & remuneration policy including the appointment of the CEO and the senior staff, particularly the finance director, operations director and the company secretary as may be applicable;

# Functions of the Board of Directors

- Review on a regular basis, the adequacy and integrity of the company's internal control, acquisition and divestitures and management information systems, including compliance with applicable laws, regulations, rules and guidelines;
- Establish and implement a system that provides necessary information to the shareholders, including shareholder communication policy for the company;
- Monitor the effectiveness of the corporate governance practices under which the company operates and propose revisions as may be required from time to time; and
- Take into consideration, the interests of the company's shareholders in its decision- making process.

# Role of the Board in Risk Management

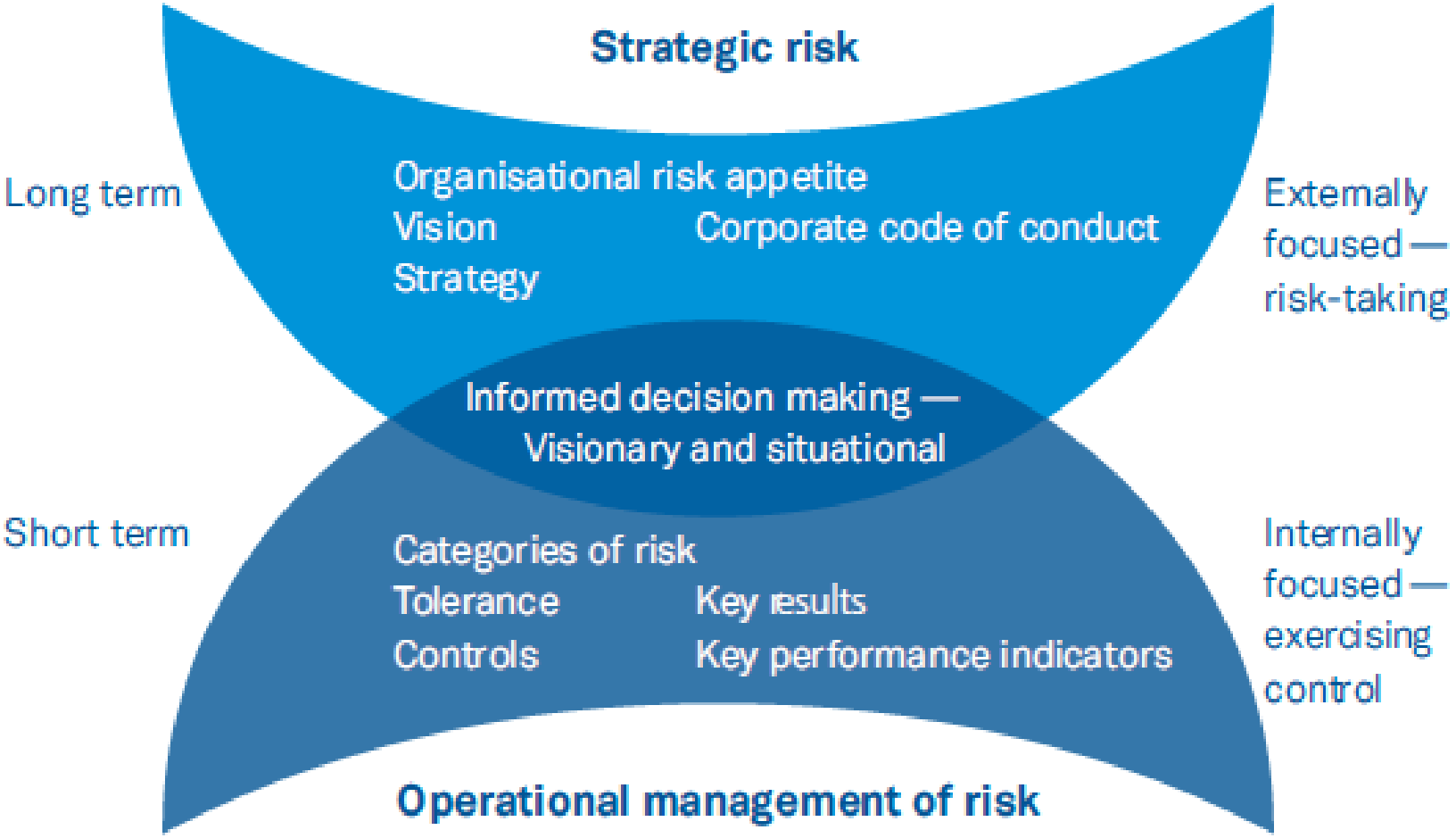
**The Board should know about and evaluate the:**

- ✓ Most significant risks facing the company
- ✓ Possible effects on shareholders
- ✓ Company's management of a crisis
- ✓ Importance of stakeholder confidence in the organization
- ✓ Communications with the investment community

**The Board should ensure that:**

- ✓ Sufficient time is devoted to discuss risk strategy
- ✓ Appropriate levels of awareness exist throughout the company
- ✓ Risk-management processes work effectively
- ✓ A clear risk-management policy is published

# Summary of the Board's Role in oversight of Risk Management



# Not an Easy Task-Identified Risks

## Not an easy task - Identified Risks

- Strategic
  - Unfocused strategy
  - Strategy not aligned with capabilities
  - Complacency arising from past success
  - Unsuccessful acquisition/abortive bid
  - Failure to manage major changes
  - Reputational risk
  - Loss of investors' confidence
  - Political/general economic risk
- People
  - Management leadership weak
  - Inadequate succession planning
  - Loss of key executives
  - Poor employee motivation
  - Internal communication weaknesses
- Marketplace
  - Failure to respond to market trends
  - Missed opportunities – new tech., global markets
  - Weak or obselete brands
  - Over-reliance on a few customers
  - Poor customer satisfaction – quality/timeliness
- Ethical
  - Failure to enact high standards of ethics
  - Obtaining contracts unethically
  - Stakeholder concerns on products/business probity – poor community relations
- Suppliers/Outsourcers
  - Over-dependence on suppliers/outsourcers
  - Failure to manage cost/quality of outsourced service
  - Supply chain problems
  - Joint ventures, strategic alliances not working
- Financial
  - Cash flow/going concern problems
  - Treasury operations risk
  - Susceptibility to fraud/accounting irregularities
- Legal/Compliance
  - Failure to protect intellectual property
  - Health, safety, environmental issues
  - Litigation risk
  - Breach of competition, corporate, employee, tax laws

# Key ERM Levers for the Board

- In academia, the acronym GPA means "grade point average." In the context of board risk oversight, the same acronym can be used to remember these key levers: **governance, policy, and assurance**. In brief, all boards must adopt these levers in their **ERM oversight.**

- **Governance**. Establish an effective governance structure to oversee risk. How should the board be organized to oversee ERM? What is the linkage between strategy and risk management? How can the independence of the risk management function be strengthened?

# Key ERM Levers.....

**Policy.** Approve and monitor an ERM policy that provides explicit risk-tolerance levels for key risks.

- Do risk management policies and risk-tolerance levels effectively capture the board's overall risk appetite and ERM expectations?

- What is the linkage between risk policies and compensation policies?

# Key ERM Levers.....

**Assurance**. Establish assurance processes to ensure that an effective ERM program is in place.

What are the performance metrics and feedback loops for ERM? How to improve the structure and content of board reports?

How should that assurance be disclosed to investors, rating agencies, and regulators?

# Key ERM Levers

- These key levers enable boards to play a constructive and effective role in ERM.
- Board members are not involved in day-to-day operations, and they have limited time to review materials and have discussions with management.
- But by using these levers, they can effectively oversee ERM and the key risks facing the organization.

# What are some choices for dealing with risk?

Determining the most appropriate method to deal with the risks facing an organization will depend on the nature of those risks. In general terms, an organization will have a choice between:

- **Avoiding the risk** by dis-continuing the activity that generates it;
- **Preventative control** that reduces the likelihood of the risk occurring (for example, only allowing new business initiatives to proceed if they have been assessed and approved from a business risk perspective);

# What are some choices for dealing with risk?

- **Corrective controls** that reduce the consequences of the risk if it occurs (for example, contingency planning, back-up systems, business continuity plans);
- **Transferring the risk** to another party (for example, by contract, insurance, outsourcing, joint ventures or partnerships);
- **Accepting the risk** and having plans in place in case the risk eventuates.

# Tools and Techniques used by Boards to oversight Risk Management Function

- Board Charter
- Board Work Plan
- ERM Policy Framework Policy and Plan
- Strategic Risk Register
- Audit & Risk Management Committee of the Board
- ERM Steering Committee
- Establishing the Risk Management Function separate from IA
- Training and Awareness

# Best Practices on Risk Management

- Senior ownership and sponsorship of RM
- Senior Management Remuneration incentives
- Risk Authority & Responsibility
- Identification and reporting of key material risks
- Risk Appetite and limits
- Staff expertise and skills
- Risk Capital Planning
- Stress testing as part of RM process
- Risk assessment for new products and ventures

# Other important considerations

- Establishing an internal audit function is another important consideration in designing an effective risk management framework. An internal audit function can assist the board in overseeing the effective implementation and operation of the organization's risk management framework.

- In particular, an internal audit function can provide the board with valuable assurance that key risk mitigating strategies including internal controls are operating effectively.

- A pro-active internal audit function can also provide valuable benchmarks and insights into how to improve the effectiveness of the organization's risk management framework.

# Key design elements of an effective risk management framework?

The Board establishes the organization's risk appetite. The board should establish a risk management framework that provides mechanisms for:

- identifying risks including any emerging risks;
- the regular review of the risks facing the organization and the updating of the organisation's risk registers;
- determining the materiality of those risks and the development of a plan to minimize the impact of such risk on the organisation;
- formulation and updating of the organisation's risk management processes and procedures to address the significant risks;

# Key design elements of an effective risk management framework?

- monitoring that the risk culture of the organisation is consistent with the board's risk appetite and risk priorities;
- monitoring the extent to which the organisation's risk management processes and procedures have been implemented and operating effectively; and
- monitoring and evaluation of the personnel within the organization responsible for risk management.

# Questions the Board should ask about Risk Management

- What are the company's top strategic risks, how severe is their impact and how likely are they to occur? – Managing enterprise risk at a strategic level requires focus, meaning generally emphasizing no more than five to 10 risks.
- How often does the company refresh its assessment of the top risks? – The enterprise wide risk assessment process should be responsive to change in the business environment. A robust process for identifying and prioritizing the critical enterprise risks, including emerging risks, is vital to an evergreen view of the top risks.
- Who owns the top risks and is accountable for results, and to whom do they report? – Once the key risks are targeted, someone or some group, function or unit must own them. Gaps and overlaps in risk ownership should be minimized, if not eliminated.

# Questions the Board should ask about Risk Management

- How effective is the company in managing its top risks? – A robust process for managing and monitoring each of the critical enterprise risks is essential to successful risk management, and risk management capabilities must be improved continuously as the speed and complexity of business change.
- Are there any organizational "blind spots" warranting attention? – Cultural issues and dysfunctional behavior can undermine the effectiveness of risk management and lead to inappropriate risk taking or the undermining of established policies and processes. For example, lack of transparency, conflicts of interest, a shoot-the-messenger environment and/or unbalanced compensation structures may encourage undesirable behavior and compromise the effectiveness of risk management.

# Questions the Board should ask about Risk Management

- Does the company understand the key assumptions underlying its strategy and align its competitive intelligence process to monitor external factors for changes that could alter those assumptions? – A company can fall so in love with its business model and strategy that it fails to recognize changing paradigms until it is too late.

- While no one knows for sure what will happen that could invalidate the company's strategic assumptions in the future, monitoring the validity of key assumptions over time as the business environment changes is a smart thing to do.

# Questions the Board should ask about Risk Management

- Does the company articulate its risk appetite and define risk tolerances for use in managing the business?

- The risk appetite dialogue helps to bring balance to the conversation around which risks the enterprise should take, which risks it should avoid and the parameters within which it should operate going forward.

# Questions the Board should ask about Risk Management

- Does the company's risk reporting provide management and the board information they need about the top risks and how they are managed? Risk reporting starts with relevant information about the critical enterprise risks and how those risks are managed.

- Are there opportunities to enhance the risk reporting process to make it more effective and efficient? Is there a process for monitoring and reporting critical enterprise risks and emerging risks to executive management and the board?

# Questions the Board should ask about Risk Management

- Is the company prepared to respond to extreme events? – Does the company have response plans for unlikely extreme events? Has it prioritized its high-impact, low-likelihood risks in terms of their reputational effect, velocity to impact and persistence of impact, as well as the enterprise's response readiness?

- Does the board have the requisite skill sets to provide effective risk oversight? – To provide input to executive management regarding critical risk issues on a timely basis, directors must understand the business and industry, as well as how the changing environment impacts the business model.

# Preparing for the Unexpected

Boards are responsible for ensuring management has developed and implemented appropriate crisis management plans and monitoring such plans over time.

**Questions for Boards**

- Does the organisation have a Crisis Management plan?
- Does this include a robust communications plan with staff and key stakeholders?

# Preparing for the Unexpected

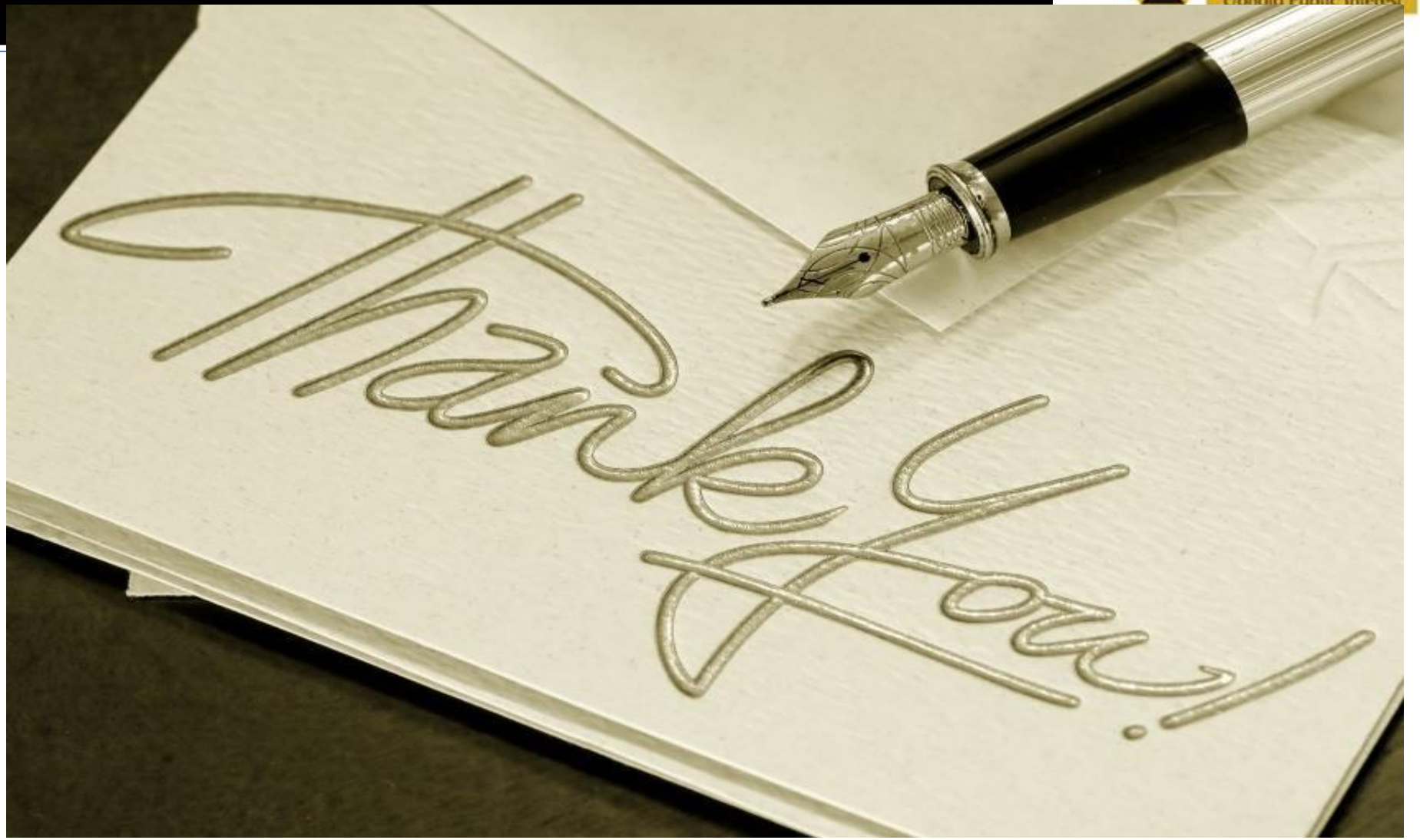
Does this ensure access to critical resources (operational, financial, human and technological resources)?

- Does this deal with the organization's key risks and vulnerabilities?
- Does this address health and safety, e.g. of staff working remotely?
- What are the roles and responsibilities of the board/directors in crises?
- Is the board/executive team ready/capable to deal with a crisis?
- Is an independent review of the crisis plan needed?

# Conclusion

- Board members are not involved in day-to-day business activities, but they have the ultimate responsibility to ensure that an effective ERM program is in place.
- What can they do to effectively oversee ERM and the key risks facing the organization? They have three key levers. First, a well-thought out governance structure should be put in place to organize risk management and oversight activities.
- Second, risk policies and risk-tolerance levels should be established to articulate the board's expectations and risk appetite.
- Finally, boards should establish assurance processes and feedback loops to gauge the effectiveness of the ERM program. In short, boards must increase their risk GPA.

# Questions & Answers



*Contacts: CPA Erick Audi*

*Email: eaudi@Kengen.co.ke or*

*audi.otieno@gmail.com*

*Mobile Nos: 0702-949 960 or*

*0721-693 705*