KPMG

# Governance Risk and Compliance

## THE 2ND PUBLIC SECTOR AUDIT CONFERENCE

Institutional Risk Management Policy Framework (IRMPF) and GRC

October 2016

# Disclaimer

This presentation is made by KPMG Advisory Services Ltd, a member firm of the KPMG network of independent firms affiliated with KPMG International, a Swiss cooperative. KPMG International provides no client services. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm.

This presentation has been prepared solely and exclusively for the benefit, information and use by the participants of **THE 2ND PUBLIC SECTOR AUDIT CONFERENCE** and for the sole and exclusive purposes of communicating material related to the conference. These slides cannot be used by the participants of the conference for any purposes other than as expressly stated herein; neither can these slides be disclosed to, referred to, or used by, any other third party. KPMG accepts no liability or responsibility whatsoever, resulting directly or indirectly from the disclosure of the presentation contents to any third party and/or the reliance of any third party on the contents of the presentation, either in whole or in part, and the participants of the workshop agrees to indemnify KPMG in this respect.

# Agenda

- What is GRC – Understanding the need for a coordinated approach
- Key challenges in implementation of the IRMPF and other risk management frameworks
- GRC drivers in the current environment – What does GRC look like in the public sector?
- GRC transformation in the public sector. What we need to look at:
  - Culture and governance
  - Managing change
  - Adoption by users
  - Governance and risk. What questions should board members be asking?
- Key messages

*The goal of GRC convergence is to breakdown traditional silos and replace this fragmented approach with a single view of risk*

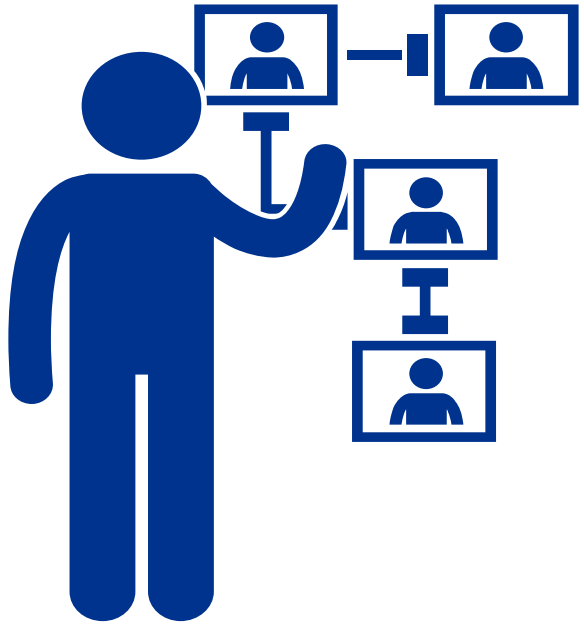
# What is GRC?


- GRC is the integration of all *governance*, *risk assessment* and *mitigation, and compliance and control* activities to operate in synergy and balance.
- GRC is a *continuous process* that is embedded into the culture of an organization and governs how management;
  - identifies and protects against relevant risks,
  - monitors and evaluates the effectiveness of internal controls, and;
  - responds and improves operations based on learned insights.

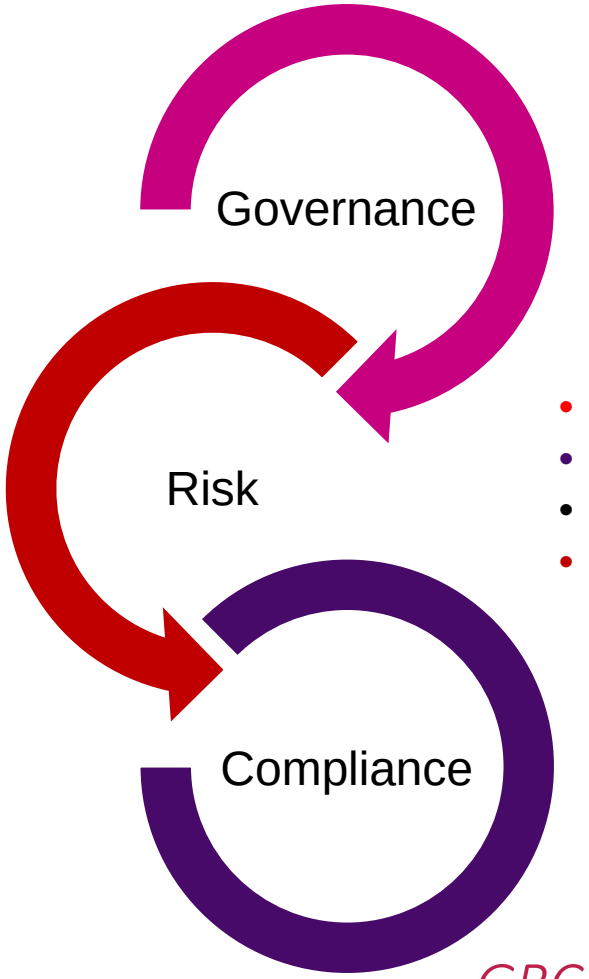
*A GRC strategy can help create business value by reducing costs, identifying operational inefficiencies, rationalizing controls, and enabling identification and management of risks*

# Key challenges in implementation of the IRMPF


- Inadequate tone at the top – Governance role in risk oversight
- Silo approach to risk management
- Risk management not linked to strategy
- Lack of a clearly defined risk appetite
- Three lines of defence not working effectively
- Risk management is not a one size fits all. There is need to define the risk universe prior to implementation



# What does GRC look like in the Public Sector




- Leading practices – The King code of Corporate Governance
- Mwongozo code of corporate governance
- Emerging regulations – The CMA Code of Corporate Governance for issuers of Security to the public 2015.

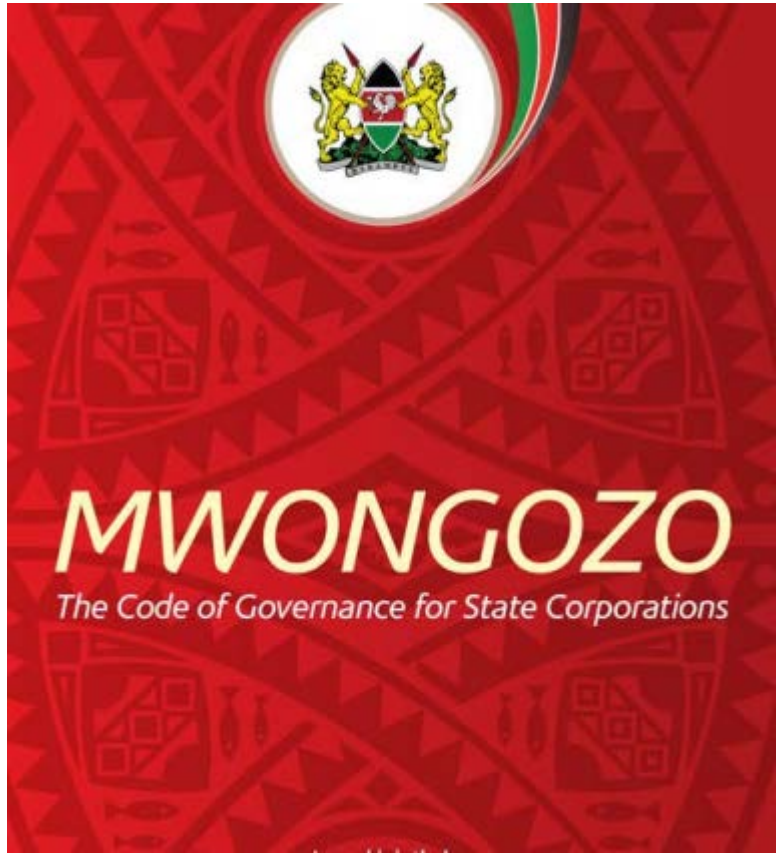
- **Institutional Risk Management Policy Framework (IRMPF)**
- Business Continuity Management
- Business sustainability
- Emerging threat of Cybersecurity

- Laws and regulations
- Standards e.g. ISO 9001
- Policies and procedures

*GRC convergence ensures a coordinated and value adding approach to management of governance, risk and compliance issues*

# Governance and risk. The Mwongozo code of corporate governance. What is it about?

- Transparency and Disclosure
- Accountability, Risk Management and Internal Control
- Ethical Leadership and Corporate Citizenship
- Shareholder Rights and Obligations
- Stakeholder Relationships
- Sustainability and Performance Management
- Compliance with Laws and Regulations.




***Successful integration of GRC will help state corporations comply with the Mwongozo Code of Corporate Governance and ensure board accountability of risk?***

***"Good governance must be well coordinated and orchestrated"***

# GRC Drivers in the Current Business Environment

**Governance**

- Meet stakeholder expectations on effective board oversight and demonstrate commitment to Corporate Governance
- Strategy, Value Creation and Innovation – the board's role in strategy formulation and monitoring implementation
- Keep up with leading practices in corporate governance such as the King Code and locally, the Mwongozo code of governance.
- Controls risk and compliance – How effective are the board audit and risk committees in managing risk
- New regulations which may require significant changes to business models and introduce new risks (e.g. in the banking sector)
- Recent and existing global anti-bribery & corruption regulations and increased enforcement activities are posing new challenges

# GRC Drivers in the Current Business Environment

## Strategy

- Beyond regulation:  provides a competitive advantage versus industry peers
- Link to risk: develop strategy through linkage and understanding of enterprise risks

## Performance

- Increasing expectations of greater transparency,  accountability and management of costs due to shrinking resources.
- Better leverage of supporting systems and tools (i.e., GRC tools) to help align risk and control functions
- Reduce costs through risk consolidation and cross-functional efficiencies
- Pro-active and separate (three) lines of defense balanced with integration and collaboration between converging disciplines

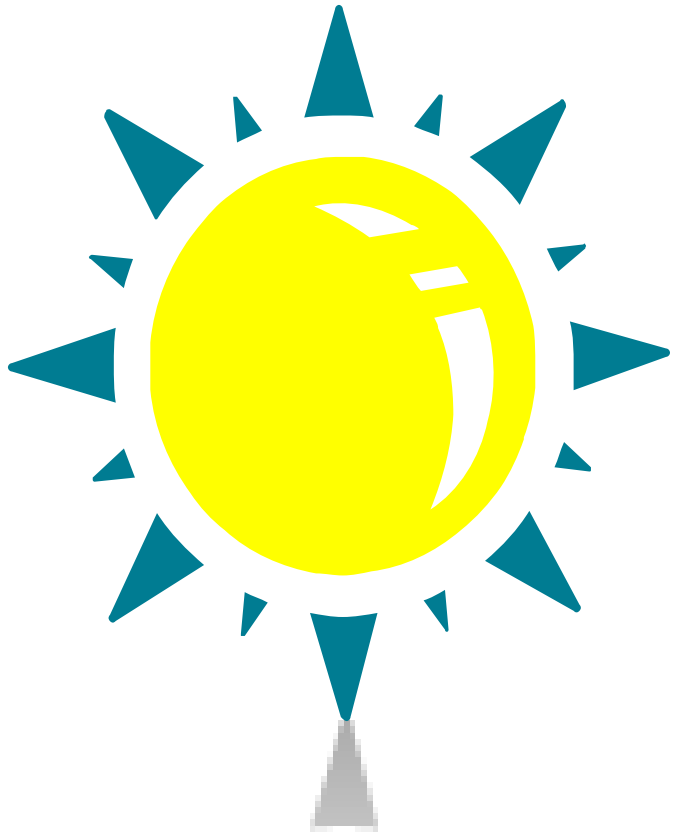
# GRC: Fail and Success Factors - Failure of some banks can be attributed to lack of an effective GRC system!!!!

| Why GRC Fails | Critical Success Factors |
|---|---|
| 1. Lack of a shared vision for risk management and compliance. | 1. Addresses business needs and strategically align to the organization's overall objectives; |
| 2. Ineffective stakeholder engagement | 2. An integrated approach of risk and control with accurate and timely communication of risk information to the decision makers |
| 3. Ineffective change management | 3. Strong collaboration and teamwork |
| 4. Project implementation delays | 4. End user awareness and training |
| | 5. A risk aware culture |
| | 6. Demonstrated return on investment on GRC implementation |

# How can we ensure effective GRC Implementation

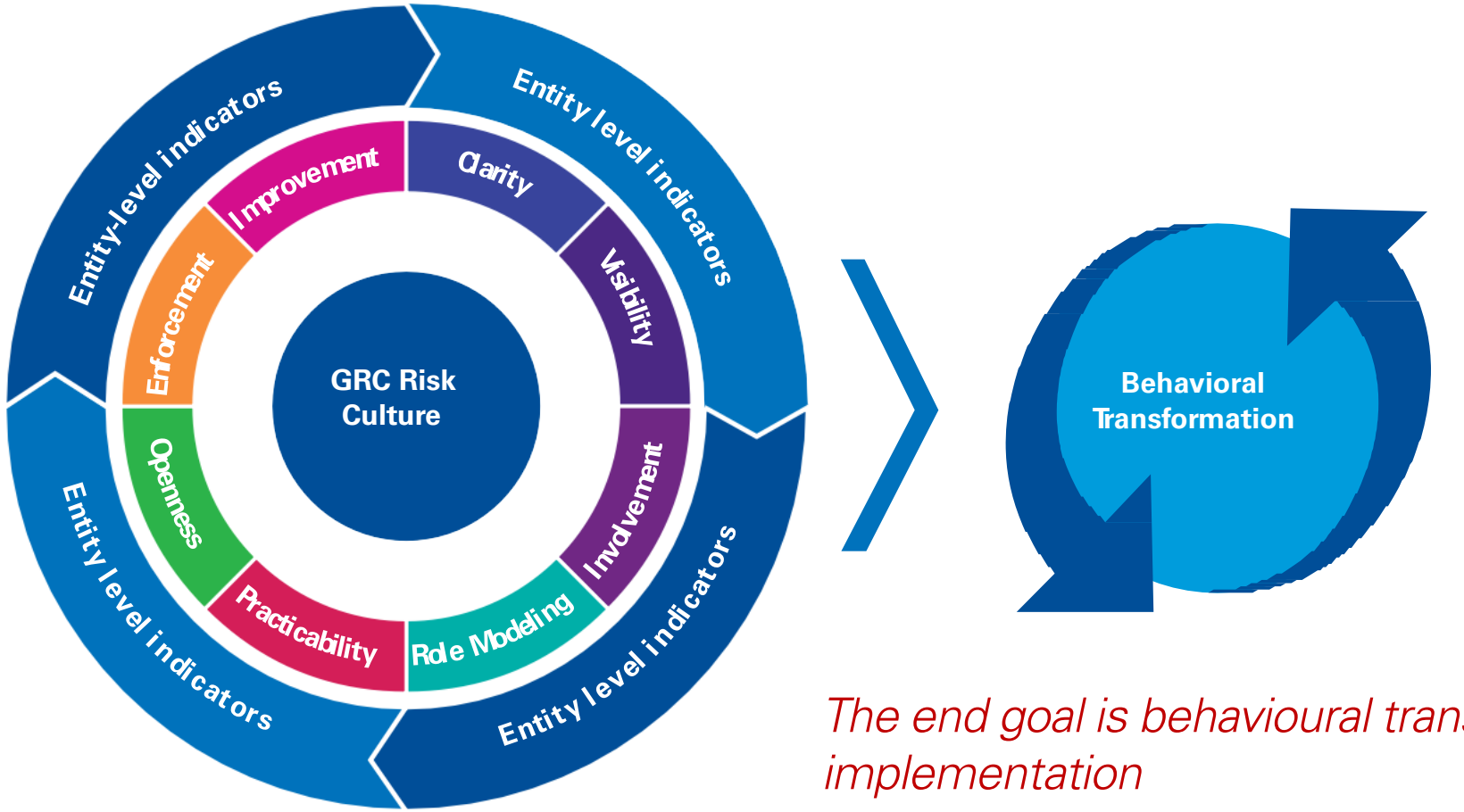
- Organizations can better implement GRC and ensure the intended benefits are realized by focusing on the following "***hot spots***"

1. **Organizational culture and governance**
2. **Effective change management**
3. **End user awareness**
4. **Board accountability for risk**



# Culture and governance

Laying the foundation of trust is an integral part of GRC organizational transformation. An effective GRC Risk Culture understands the goal: **Transform efficiently to meet business and regulatory demands**.







1. Improvement
2. Clarity
3. Visibility
4. Involvement
5. Role modelling
6. Predictability
7. Openness
8. Enforcement
9. Improvement

*The end goal is behavioural transformation for effective GRC implementation*

# How can sustainable change lead to an effective GRC journey?

| Essential change management practices | Benefits |
|---|---|
| Leadership alignment | Consistent messaging and tone from leaders |
| Clear platform and vision for change | Clarity on project rationale, anticipated benefits and objectives; greater project momentum |
| Active leadership involvement | Senior-level role models who support the project |
| Leader and stakeholder commitment | Project seen as high priority; project stays on schedule |
| Effective communication | Clear project awareness and understanding; alignment of individual efforts to organizational expectations |
| Active stakeholder engagement | Broader buy-in and greater realization of GRC benefits |
| Aligned performance measurements | Motivate desired behaviors to sustain change |
| Timely training and preparation | Stakeholders prepared; more seamless implementation |

***Affected stakeholders will need to collaborate on the rationale behind the program and in defining the goals to be achieved.***

# Adoption by Users

**Adoption depends on widespread acceptance of the system**

**Reduce uncertainty and anxiety**

**Appoint a trusted GRC champion to lead transformation**

**Provide open communication**

**Include end user-adoption training and piloting**

**Identify the benefits for users and provide information that helps**

# Governance and risk. What questions should board members be asking?

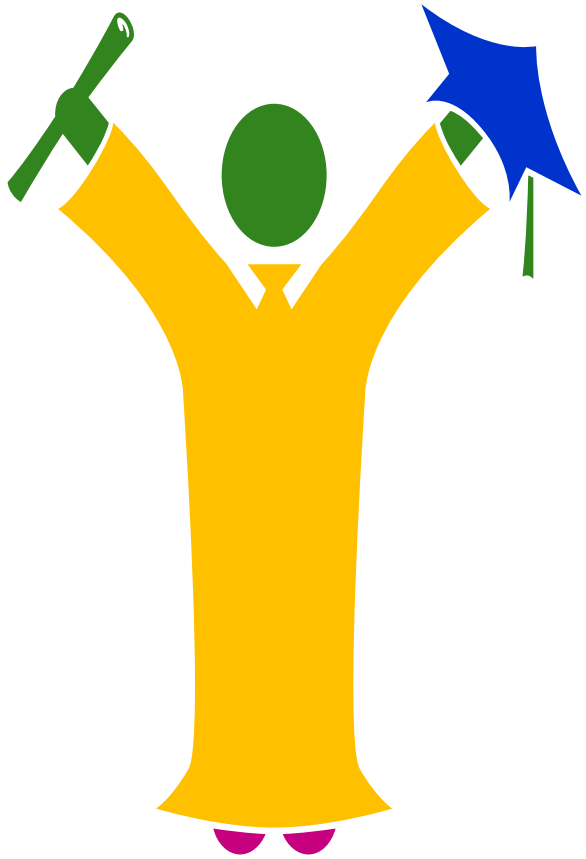
- How do we integrate risk management with the company's strategic direction and plan?
- **What are our principal business risks?**
- Are we taking the right amount of risk?
- **How effective is our process for identifying, assessing and managing business risks?**
- **Do people in this company have a common understanding of the term "risk"?**
- How do we ensure that risk management is an integral part of the planning and day-to-day operations of business units?
- **How do we ensure that the Board's expectations for risk management are communicated to and followed by all employees?**
- How do we best ensure that our executives and employees act in the best interests of this company?

# Governance and risk. What questions should board members be asking?

- **How is risk management coordinated across the company?**
- How do we ensure that the company is performing according to the business plan and within appropriate risk tolerance limits?
- How do we monitor and evaluate changes in the external environment and their impact on the organisation's strategy and risk management practices?
- How does the Board handle its responsibility for the oversight of opportunities and risk?
- How does the board ensure that at least some of its members have the requisite knowledge and experience in risk?
- **How do we, as a Board, help establish the "tone at the top" that reinforces the company's values and promotes a "risk aware culture"?**
- How satisfied are we that the Board is doing what it should in overseeing risk?

# The Effective GRC System - Key messages

- Integrate key ERM practices into the daily activities of business managers
- Aim to be viewed by the business as a facilitator of business value and innovation
- Integrate the ERM framework with the other risk and control oversight functions to create a unified view of risk
- Focus the ERM program on the threats to strategic and business objectives, including missed opportunities
- Use data and analytics to enhance your understanding of risk and to improve business decision making
- Understand the organization's culture and build an ERM program that evolves along with it.



# Contact us

**Daniel Karuga,**
Associate Director, Risk Consulting,
KPMG Advisory Services Ltd
E: dkaruga@kpmg.co.ke
Tel: 254 729 110 597
Fax: 254 (20) 221 5695