

# RISK BASED AUDITING

**Theme: Ensuring objectivity and completeness of  
Internal Audit Planning**

**Risk Maturity**

**25<sup>th</sup> - 26<sup>th</sup> Aug 2021**

**CIA, CPA Muonde Daniel,  
CFE, CISA**

# Outcomes



1. Risk Maturity
2. Risk Assessment Tools



# Background



If you don't invest in risk management, it doesn't matter what business you're in, it's a risky business.

— Gary Cohn —

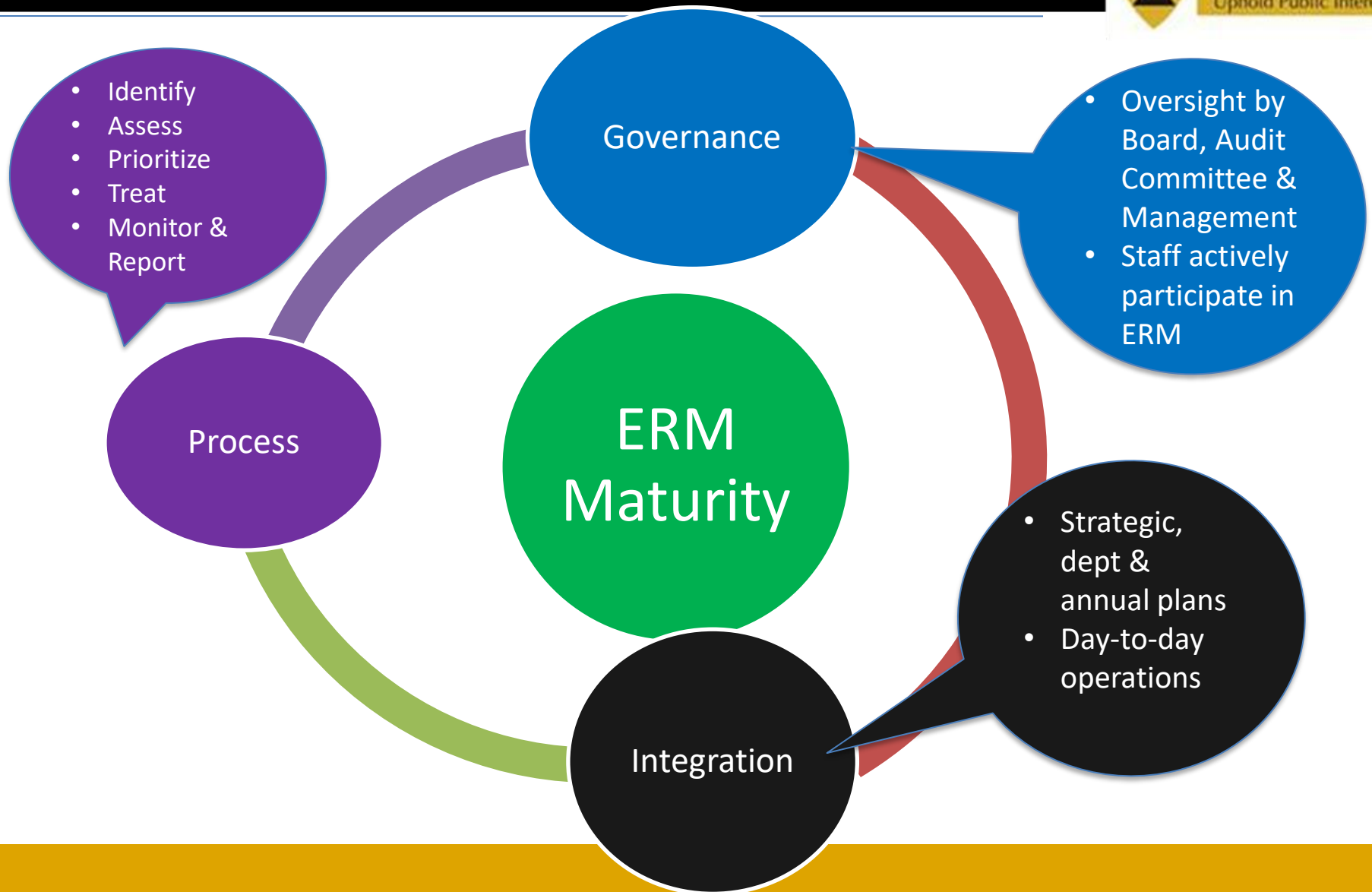
# Linkage With Other Topics



1. Overview of the COSO Risk Management Framework and ISO 31000:2019—we use the a framework to benchmark our maturity
2. ERM Risk Management--we assessing maturity is the 1<sup>st</sup> step in establishing a risk management process
3. Risk Based Internal Audit Plan—maturity of risk management is key in determining how to develop a risk based plan



# Assessment Pillars



# Risk Governance



1. **Risk intelligent culture**—definition of risk, attitude & behaviour.
2. **Risk Management oversight**—monitoring and reporting to Board, Audit Committee and Management
3. **Risk Management Responsibility**—defined for Board, Board Committees, Management and Staff and key external parties. Capacity building
4. **Inter-functional risk management** — is it Silo
5. **Risk Management communication**—top-down (messaging) and bottom-up (feedback)



# Risk Integration



1. **Strategic plan**—aligned to mandate, vision & mission.
2. **Operational plan**—supports achievement of strategic plan
3. **Organizational structure**—supports strategy (not strategy developed to support the structure)
4. **Risk Appetite**—strategy aligned to risk appetite
5. **Strategic risks**—linked to strategic objectives. Opportunities and threats
6. **Operational risks**—linked to operational objectives, threats and opportunities, linked to strategic risks





# Risk Process



1. Risk policy and procedures—
  - Manual in place and reviews regularly,
  - Consistently applied in the entire organization
  - Risk logs or registers
  - Business Continuity Plan
  - Disaster Recovery Plan
2. Risk management infrastructure
3. Risk management assurance—audit of the risk management process, continuous improvement



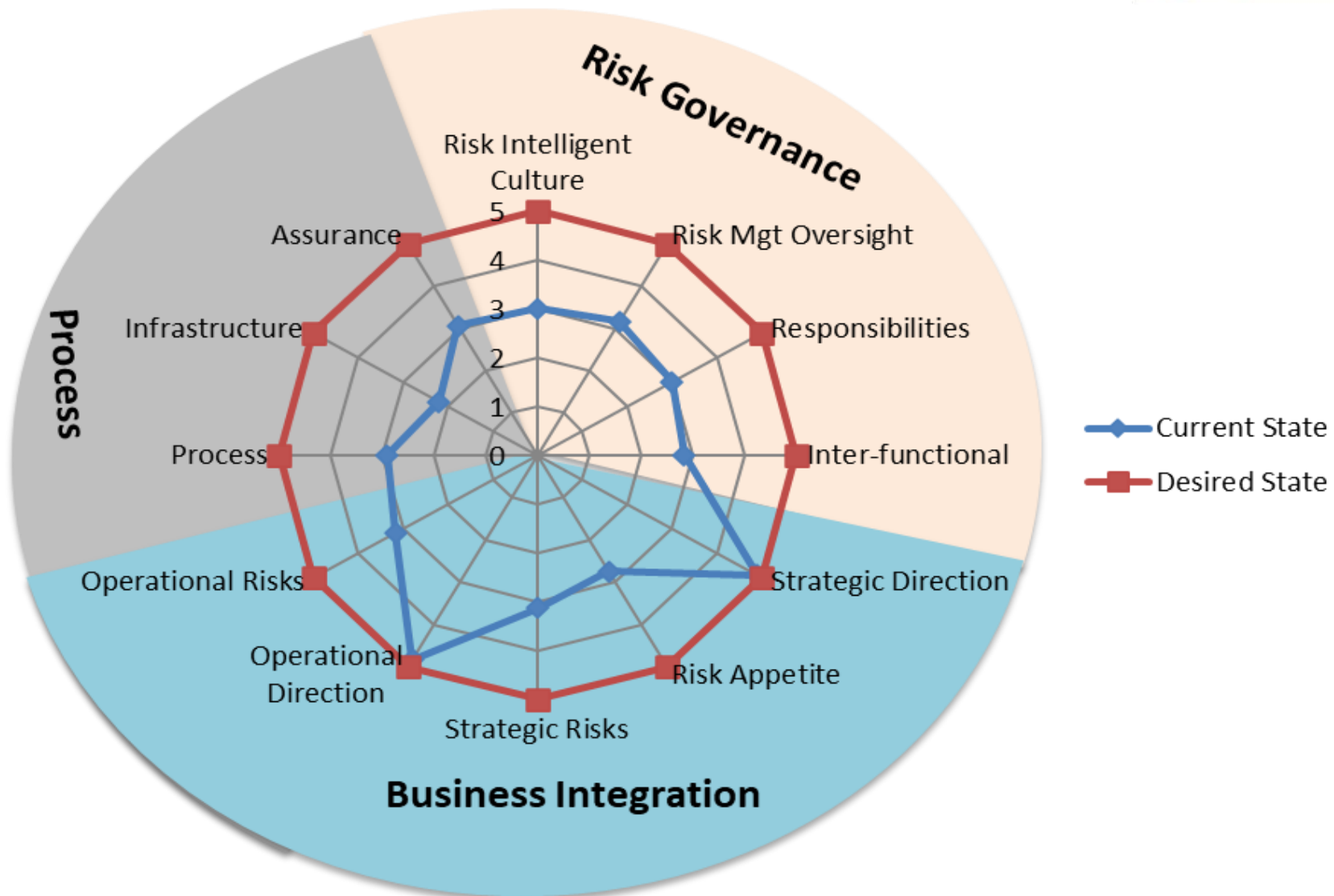


# Assessment Criteria



Category	Foundation (Ad-hoc)	Fragmented	Top-Down	Systematic (Managed)	Risk Intelligent
Risk Governance	<ul style="list-style-type: none"> <li>Limited awareness &amp; capacity</li> <li>Depends on individual</li> </ul>	<ul style="list-style-type: none"> <li>Fragmented/silos.</li> <li>No uniform definition of risk and risk management.</li> <li>Limited or no alignment to objectives.</li> <li>Compliance-based</li> </ul>	<ul style="list-style-type: none"> <li>Top-bottom Approach (management know it all)</li> <li>Risk management Policy &amp; Procedures</li> <li>Focus on top risks only/key projects</li> <li>Mitigation focus</li> </ul>	<ul style="list-style-type: none"> <li>Standardized across the organization</li> <li>Risk appetite</li> <li>Risk management tools developed and in use</li> <li>Threats and opportunities.</li> <li>Regular communication</li> </ul>	<ul style="list-style-type: none"> <li>Good risk culture</li> <li>Integrated with development and implementation of plans</li> <li>Effective risk indicators</li> <li>Linked to performance management</li> <li>Risk modelling</li> </ul>
Business Integration					
Risk Management Process					
Scoring	1	2	3	4	5

# Maturity Score-Overall



# Maturity Score-Pillar



## Risk Management Pillar Maturity Rating

Risk Governance

**Top Down**

3.00

Business Integration

**Top Down**

3.76

Risk Management Process

**Fragmented**

2.72

# Tools-Risk Identification



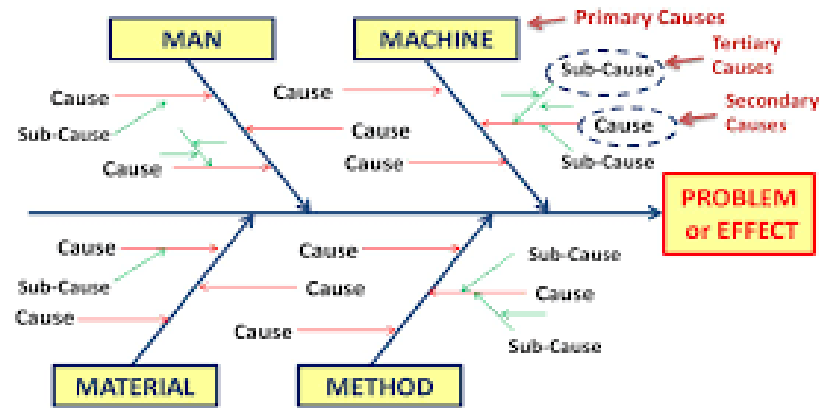
1. **Vulnerability assessment**—points of failure/opportunity arise.
2. **Scenario planning**—scenario modelling & possible outcomes/risks
3. **Brain storming**—listing of possible risks (no wrong risks)
4. **Questionnaire/survey**
5. **Checklist**—example of risks to consider
6. **Benchmarking**—industry, similar organization



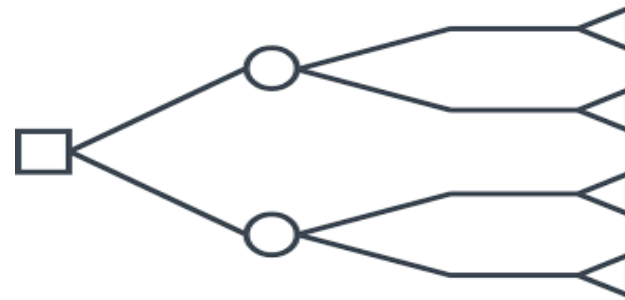
# Tools-Risk Assessment



## CAUSE AND EFFECT DIAGRAM



## Fishbone Analysis

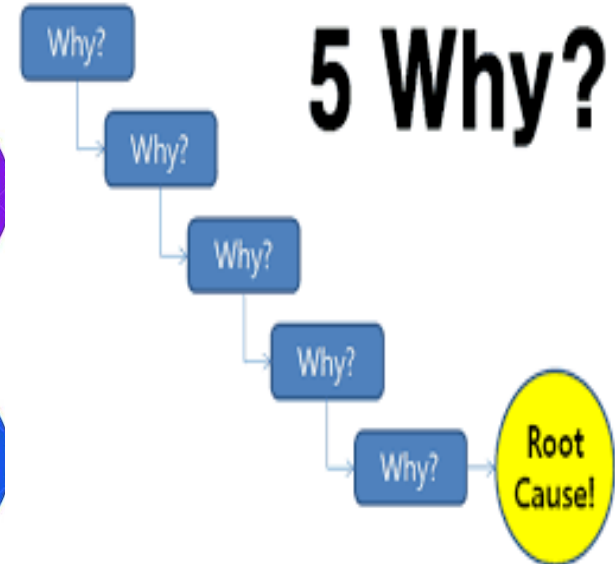


## Logic Tree/ Fault Tree

**Failure Mode Effects Analysis--** potential undesired outcomes & their causes (similar to vulnerability analysis)



## FMEA



## 5 Why?

END



*Thank  
you*



# RISK BASED AUDITING

**Theme: Ensuring objectivity and completeness of  
Internal Audit Planning**

**Risk Maturity**

**25<sup>th</sup> - 26<sup>th</sup> Aug 2021**

**CIA, CPA Muonde Daniel,  
CFE, CISA**