THE BOARD AUDIT COMMITTEE MASTERCLASS

Venue: Sarova Whitesands, Mombasa

Date: 24th February 2021

Presenter: CPA Phares Chege

Deputy Commissioner, Internal Audit, KRA

About CPA Phares Chege

Profession

- Audit & Risk management practitioner for 17 years
- Experience in public Sector – 70% of working life
- Experience in private Sector – 30% of working life

Some of the Organizations worked with:

- Kenya Revenue Authority
- Siginon Group Limited
- Higher Education Loans Board
- KPMG East Africa
- KeNHA
- Office of the auditor General

Qualifications

- MBA (Accounting)
- BA (Economics)
- Certified Public Accountant of Kenya
- Certified Internal Audit Quality Assessor
- Certified Information Systems Auditor (CISA)
- Certified in Risk and Information Systems Control (CRISC)
- Certified Operational Risk Practitioner (CORP)

Training experience

Since 2004 with focus on:

- Internal Auditing & QAIP
- Enterprise Risk Management
- Forensic Audits
- Data Analytics
- Strategic Management
- Financial Reporting

Phares is married to 1 beautiful wife and they have both been blessed with many children.

CONTENT

1	Introduction to Role of Audit Committees in effective Risk management practices to achieve value	25 MINUTES
2	Linking Risk Management to Strategy	10 MINUTES
3	Setting the right tone at the top for effective risk management	10 MINUTES
4	Critical steps in the implementation of the ERM Framework	15 MINUTES
5	Questions and discussions	30 MINUTES

1. Introduction to Risk governance

"Risk is like fire: If controlled it will help you; if uncontrolled it will rise up and destroy you."

- Theodore Roosevelt

VIDEO...

1. Introduction to Risk Governance–
Known past incidents - Globally

HIH Collapse – an Australian experience

Losses of $5.3Billion – the largest Australian company collapse in 2001:

Why?

- Dominant chief executive
- Ineffective chairman
- A board that did not ask questions
- Failure to grasp the concept of conflicts of interest
- Ad hoc executive remuneration
- Unusual accounting transactions
- Ineffective audit committee
- Compromised auditor independence

1. Introduction to Risk Governance–
Known past incidents - Kenya

UNDER RECEIVERSHIP , SOME ALREADY SOLD!

ICPAK
Credibility. Professionalism. Acc

ARM CEMENT LTD
(formerly Athi River Mining)

MUHORONI
SUGAR COMPANY LTD
(IN RECEIVERSHIP)

DEACONS
WE MAKE PEOPLE LOOK AND FEEL GOOD

1. Introduction to Risk Governance–
Known past incidents – Kenya…

WAS UNDER RECEIVERSHIP!! NOW SOLD OFF …

1. Introduction to Risk Governance–
Known past incidents – Kenya…

THE JUNCTION

NOTICE

TAKE NOTICE that Nakumatt Ho… …relinquished its rights over this premi… …Surrender dated 15th September, 2017

Th… …closed to the public from 1st October, 2017 …g will be permitted at the premises.

Nakumatt's directors and authorised agents and employees will however be permitted access to the premises for the purpose of removing the tenant's stock, items and property from the premises.

DATED THIS 1st Day of October 2017.

CLOSED INDEFINITELY!!

1. Introduction to Risk Governance–
Known past incidents – Kenya…

SCANDALS OF THE CENTURY!!

1. Introduction to Risk Governance–
Think about these scenarios…

1. Company workers die while having a team building event at Hell's gate after a heavy downpour
2. A company looses 8 out of its 10 top managers after a flight crash while enroute Arusha for a conference
3. Government delays grants disbursements to state corporations and county governments due to severe cash crunch
4. A strategic state corporation board term expired a year ago and a new one is yet to be constituted
5. A container full of counterfeit alcoholic drinks found with label of a local brewing company
6. Audit Committees of 5 County Governments resign citing hostile environment.

WHO IS NEXT?

WE HOPE IT WONT BE YOUR ORGANIZATION…

1. Introduction to Risk Governance – Lessons from Local cases

1. **Untamed conflicts of interest** – with rotten tone at the top, weak governance, poor oversight,
2. **Strategic plans** prepared without focus on key strategic risk and/ or weak or inexistent M&E of SPs hence risk crystalize without anyone's knowledge – Boards & management focusing on Crisis Management
3. **Weak governance** is a major ingredient of corporate failure- it is a common pitfall in risk management
4. **Risk management** – Regulatory requirement or intentional initiative by Boards?
5. Incompetent/ compromised **external auditor** can also be a critical point of failure for organizations
6. **Collusion** with external parties is a major contributor of corporate failures – vendors, customers, regulators

1. Introduction to Risk Governance – Menti.com

Arising from the cases we have gone through, what do you think in the MAIN contributor of corporate failures in Kenya?

1. Untamed conflicts of interest - Greed
2. Weak strategic plans without focus on key risks
3. Incompetence at the top – Ignorant oversight functions.
4. Compromised external auditors
5. Weak regulatory activities
6. Economic challenges
7. Unfavorable government policies

1. Introduction to Risk Governance–
Perception of risk makes all the difference

1

Perception of Risk

HINDERANCE

The internal audit syndrome

If my risks are known/high/reported – I am a bad performer

Am just too busy for risk management – professional issues managers

2

Perception of Risk

ENABLER

Risk owned by ALL staff

Freely reported and shared

Applied in decision making

1. Introduction to Risk Governance–
What is Risk and Risk management?

Risk : Effect of uncertainty on objectives

Risk Management: Coordinated activities to direct and control an organization with regard to risk.
- Aim achieve best balance of risk and opportunity and not to eliminate risk

RM Framework: A set of components that provide the foundations and organizational arrangements for designing, implementing, reviewing and continually improving risk management throughout the organization.

SOURCE: ISO 31000

1. Introduction to Risk Governance–
What is Risk Management?

"... a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."

SOURCE: COSO

Risk Management Policy

Risk management policy outlines the Institution's commitment to protecting the Institution against adverse outcomes, which may impact negatively on service delivery.

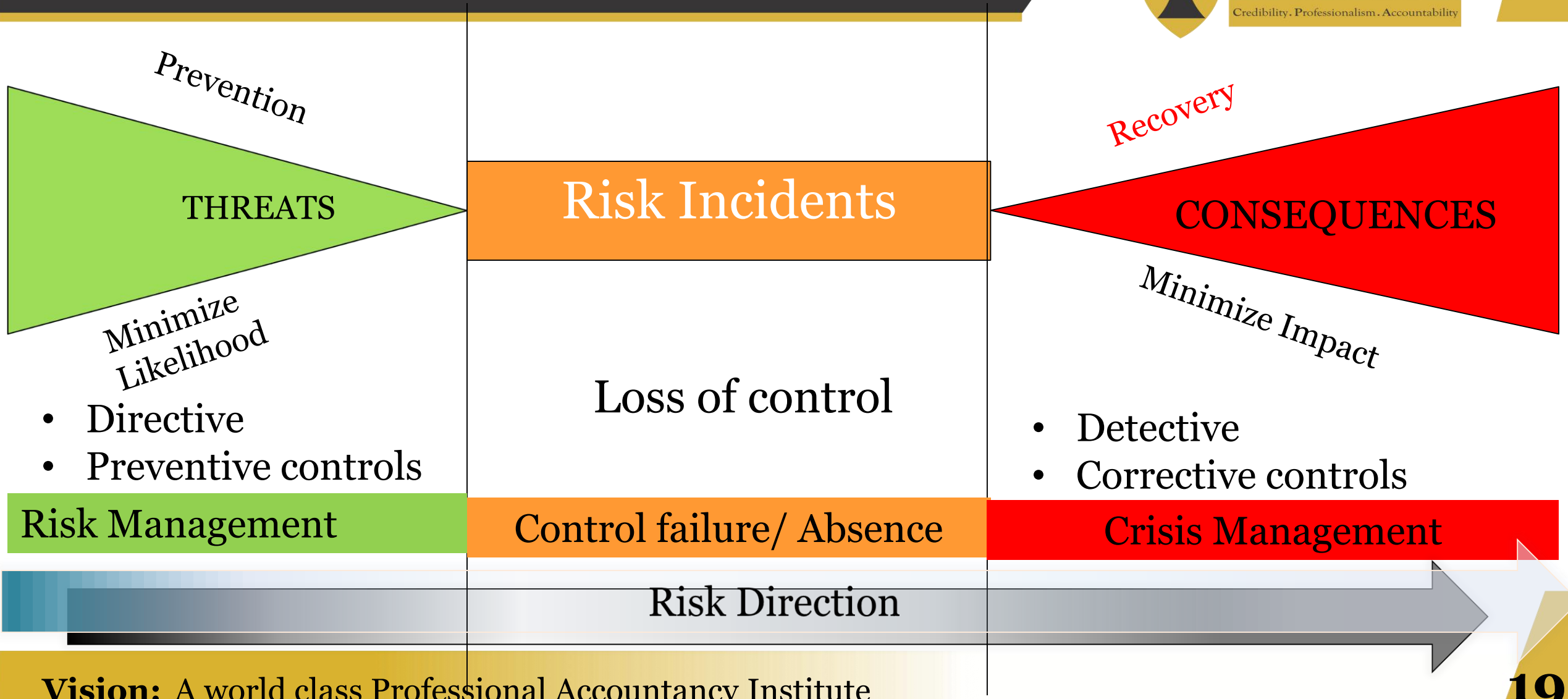
It is a brief statement about the Institution's commitment to risk management. Hardly 10 pages.

1. Introduction to Risk Governance

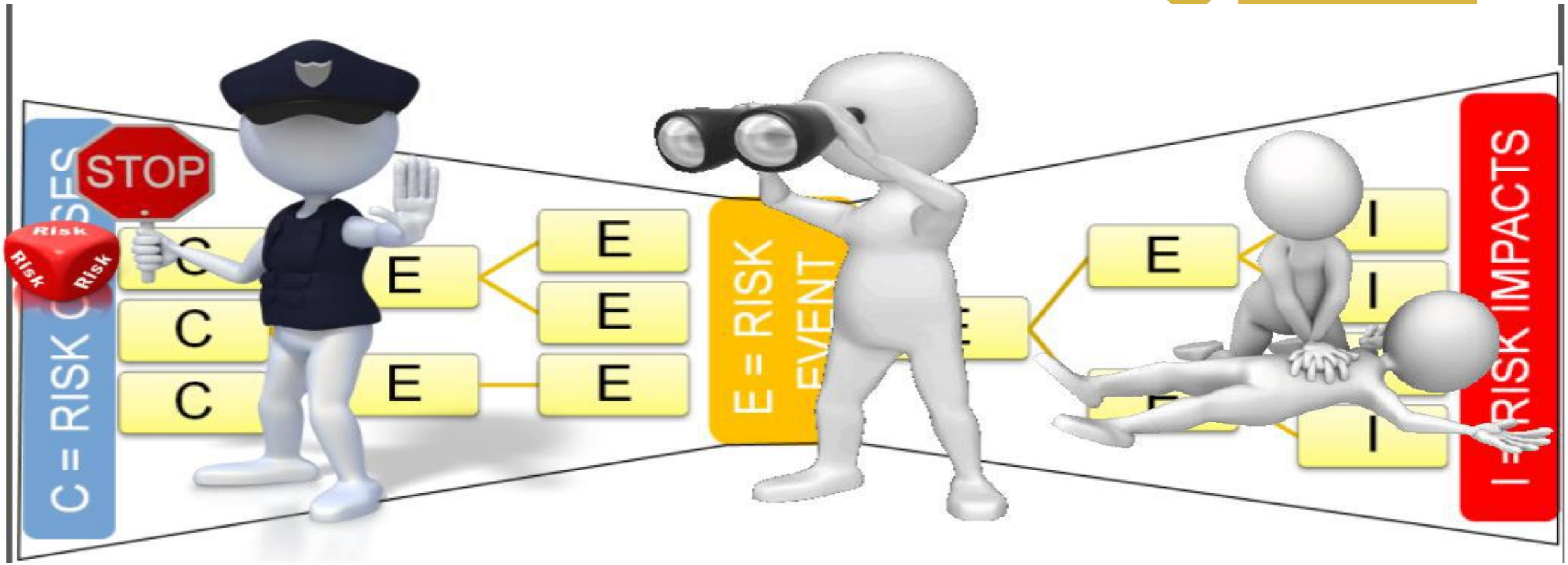
–Contents of a Risk Management Policy

1. Definition of terms
2. Purpose/ objectives of the policy
3. Scope
4. Effective date
5. Policy statement – Philosophy & RM approach
6. Responsibilities
   - Board of Directors
   - Audit & Risk Committee
   - Risk Management committee/HODs/CRO
   - Risk Champions Network
   - Employees
   - Internal & External Audit

1. Introduction to Risk Governance– Bow tie Concept



1. Introduction to Risk Governance–
Types of controls based on risk location

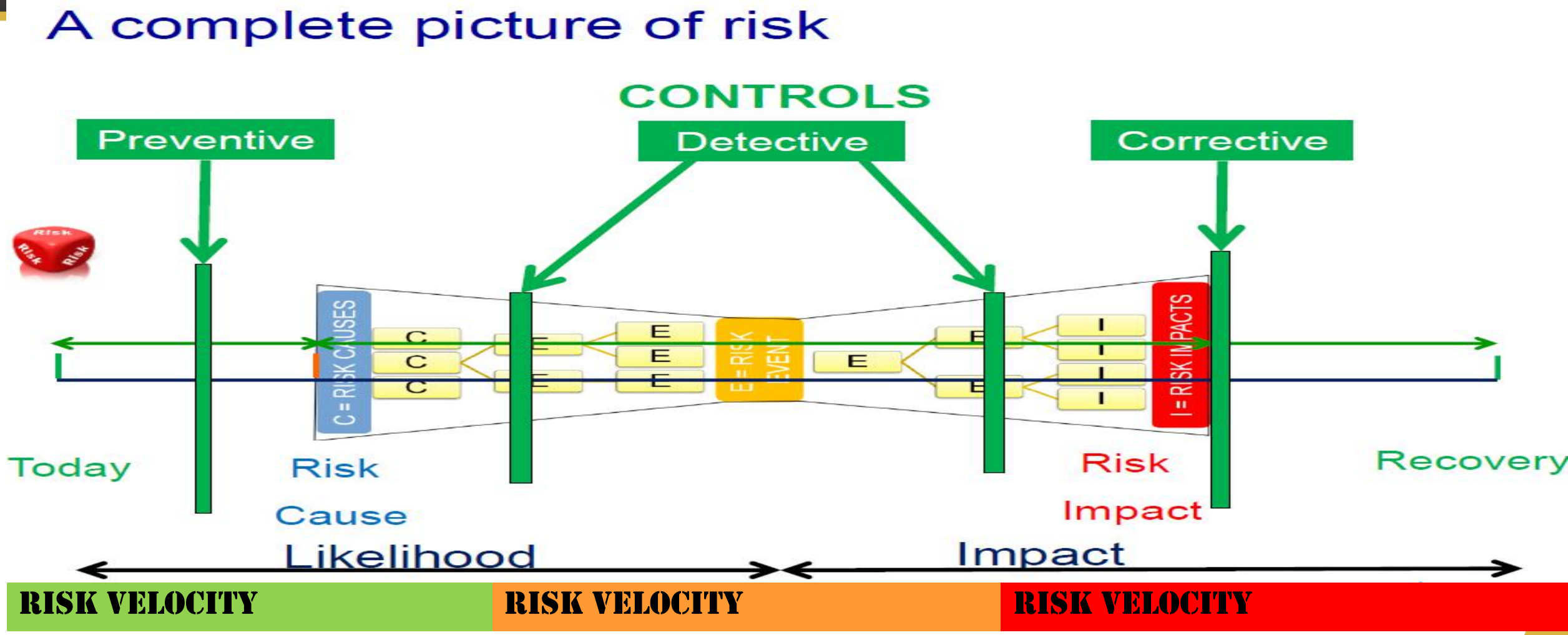


PREVENTATIVE

DETECTIVE

REACTIVE/ REMEDIAL

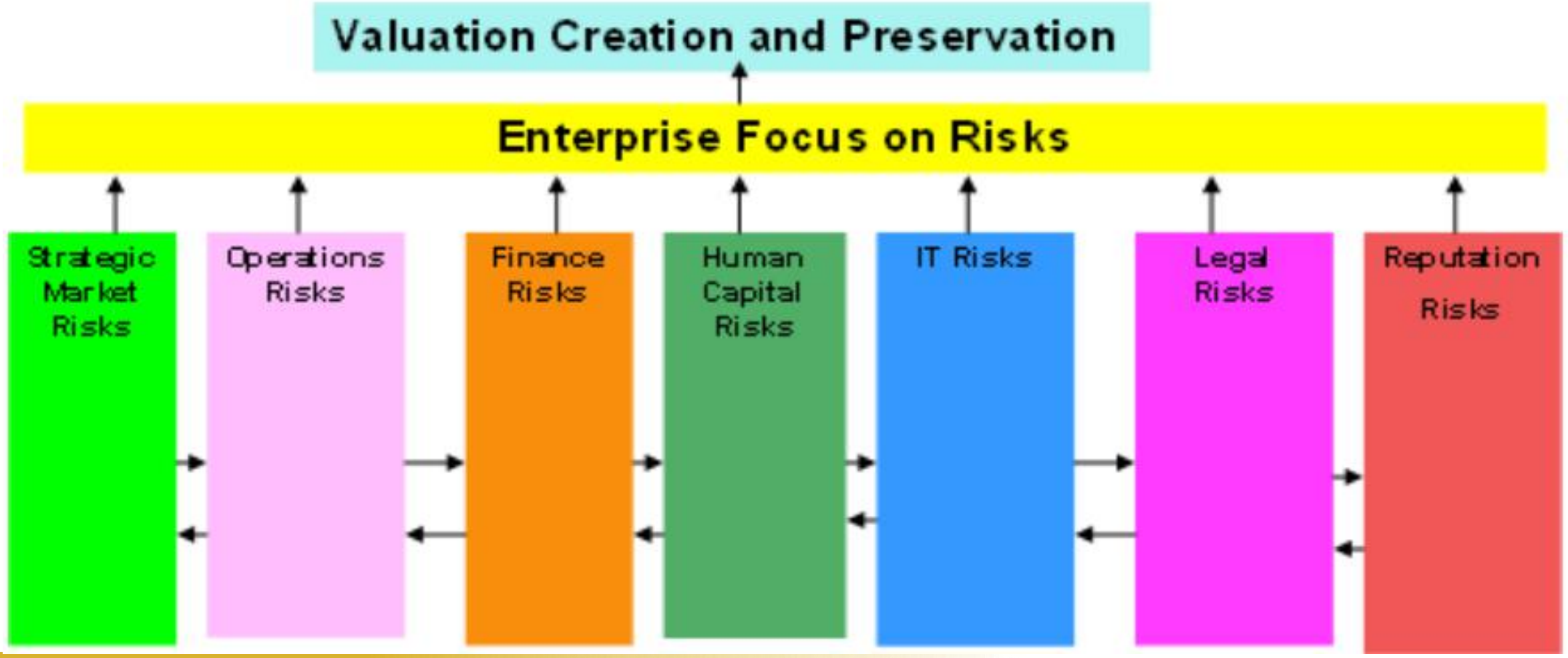
1. Introduction to Risk Governance–
Risk Velocity



1. Introduction to Risk Governance–
Silo Approach

"Silo" or "Stove-Pipe" Risk Management

1. Introduction to Risk Governance–
Anti-Silo Approach



1. Introduction to Risk Governance–
Risk management maturity continuum?

Initial	Repeatable	Defined	Managed	Optimized
Adhoc/ Naive	Intuitive/ Aware	Qualitative	Quantitative	Continuous feedback
• Institutional capacity lacking • Relies on initiative • Just do it • Reliance on Key people	• Processes established and repeatable • Common Language • Define tasks • Quality people assigned • Initial infrastructure component • Scattered silos	• Policies, processes and standards institutionalized • Firm wide • Rigorous methodologies • Remaining infrastructure components • Appetite defined	• Risk measured and managed • Risk aggregated firm wide • Rigorous measurement methodologies/ Analysis • Debate on risk/ reward	• Risk mgt is competitive advantage • Emphasis on taking and exploring risks • World-class processes • Knowledge management • RM embedded in processes

SOURCE: COSO

1. Introduction to Risk Governance–
RM maturity - Menti.com question

Where does your organization fit currently?

1. Initial
2. Repeatable
3. Defined
4. Managed
5. Optimized

Where do you want to be in the next 3 years?

1. Initial
2. Repeatable
3. Defined
4. Managed
5. Optimized

1. Introduction to Risk Governance – Category of risks

- Strategic
- Financial
- Operational
- Compliance
- Environmental

1. Introduction to Risk Governance–
2021 Top risks globally

1 — 41%

Business interruption
(incl. supply chain disruption)

2020: 37% (2)

2 — 40%

Pandemic outbreak
(e.g. health and workforce issues, restrictions on movement)[1]

2020: 3% (17)

3 — 40%

Cyber incidents
(e.g. cyber crime, IT failure/outage, data breaches, fines and penalties)

2020: 39% (1)

4 — 19%

Market developments
(e.g. volatility, intensified competition / new entrants, M&A, market stagnation, market fluctuation)[2]

2020: 21% (5)

5 — 19%

Changes in legislation and regulation
(e.g. trade wars and tariffs, economic sanctions, protectionism, Brexit, Euro-zone disintegration)

2020: 27% (3)

6 — 17%

Natural catastrophes
(e.g. storm, flood, earthquake, wildfire)

2020: 21% (4)

SOURCE: 10TH ALLIANZ SURVEY, 2021

1. Introduction to Risk Governance–
2021 Top risks globally

7 — 16%

Fire, explosion

2020: 20% (6)

9 — 13%

Climate change / increasing volatility of weather

2020: 17% (7)

8 — 13%

Macroeconomic developments

(e.g. monetary policies, austerity programs, commodity price increase, deflation, inflation)[3]

2020: 11% (10)

10 — 11%

Political risks and violence

(e.g. political instability, war, terrorism, civil commotion, riots and looting)

2020: 9% (11)

DOES THIS GLOBAL PICTURE RESONATE WITH KENYAN SITUATION?

1. Introduction to Risk Governance–
What is does risk governance entail?

Risk Governance:

- Is the architecture within which risk management operates in an organization.
- Defines the way in which a company undertakes risk management.
- Provides guidance for sound and informed decision-making and effective allocation of resources.

Successful Risk Governance is therefore contingent on how effectively the **Board and Management are able to work together** in managing risks.

SOURCE: PWC, 2012

1. Introduction to Risk Governance–
What is does risk governance entail?

Risk Governance:

- Board Oversight using Board Risk Committee or BAC
- Chief Risk Officer to provide executive oversight and co-ordination.
- Risk Committee of Management that ensures integrated approach and enterprise-wise approach to RM.
- Senior Management and Board meetings guided by risk profile. Areas of high risk are the main focus of such discussions
- Internal Audit that conducts risk based audits to provide assurance to Board that ERM framework is meeting its goals.

SOURCE: PWC, 2012

1. Introduction to Risk Governance–
What is does risk governance entail?

VIDEO...

2. Linking Risk Management to Strategy

"Risk is what an entrepreneur eats for breakfast. It's what she slips into bed with at night. If you have no appetite for this stuff, or no ability to digest it, then get out of the game right now."

- Heather Robertson

2. Linking Risk Management to Strategy – 5 Key steps towards this linkage

Step 1: Strategic objectives decomposition

- Start by taking a high-level objective and breaking it down into more tactical, operational key performance indicators (KPIs) and targets.
- This is a critical step to make sure risk managers understand the business logic behind each objective and helps make risk analysis more focused.
- While it should be management's responsibility to identify and assess risks, the business reality in your company may be that sometimes the risk manager should take the responsibility for performing risk assessment on strategic objectives and take the lead.

2. Linking Risk Management to Strategy – 5 Key steps towards this linkage

Step 2: Identifying factors associated with uncertainty

- Once the strategic objectives have been broken down into more tactical, manageable pieces, risk managers need to use the strategy document, financial model, business plan or the budgeting model to determine **key assumptions** made by the management.
- Most assumptions are associated with some form of **uncertainty [Risk]** and hence require risk analysis. Risk analysis helps to put unrealistic management assumptions under the spotlight.
- Risk managers should perform a classic risk assessment to determine whether all significant risks were captured in the management assumptions analysis.

2. Linking Risk Management to Strategy – 5 Key steps towards this linkage

Step 3: Performing risk analysis

- This step involves scenario analysis or simulation to assess the effect of uncertainty on the company's strategic objectives.
- When modelling risks it is critical to consider the correlations between different assumptions.
- One of the useful tools for an in-depth risk analysis and identification of interdependencies is a **bow-tie diagram**. Such analysis helps to determine the causes and consequences of each risk, improves the modelling of them as well as identifying the correlations between different management assumptions and events.

2. Linking Risk Management to Strategy – 5 Key steps towards this linkage

Step 4: Turning risk analysis into actions

- Risk managers should discuss the outcomes of risk analysis with the executive team to see whether the results are reasonable, realistic and actionable.
- If the results of the risk analysis are significant, then the management with the help from the risk manager may need to:
  - ✓ Revise the assumptions used in the strategy – **Terminate the risk**
  - ✓ Consider sharing some of the risk with third parties by using hedging, outsourcing or insurance mechanisms **- Transfer**
  - ✓ Consider reducing risk by adopting alternative approaches for achieving the same objective or implementing appropriate risk control measures **- Treat**
  - ✓ Accept risk and develop a business continuity / disaster recovery plan to minimize the impact of risks should they eventuate **- Take**
  - ✓ Or, perhaps, change the strategy altogether **- Treat**

2. Linking Risk Management to Strategy – 5 Key steps towards this linkage

Step 5: Monitoring strategic actions

- Monitoring is done at all levels from the operational to strategic level.
- The main question answered during monitoring is: Are the actions addressing the uncertainties associated with the strategic assumptions.
  - ✓ If the answer is yes, no further action is needed until the next monitoring cycle.
  - ✓ If the answer is no, management and Board must come up with compensating strategic actions that will ensure the goals are achieved.
- Operational and tactical level actions will change more often that the strategic level action to ensure stability of the organization.

2. Linking Risk Management to Strategy – 5 Key steps towards this linkage

Example:

Step 1: Objective: Increase sales by 300% by end of year 5

Step 2: Key assumptions: No legislative price controls will be imposed, Customers tastes and preferences will not significantly change, etc

Step 3: Risk Analysis

Changes in customer tastes & preferences – Causes: New products in the market, health concerns on existing products, new legislation, Consequences: Reduced demand, lower turnovers, lower profitability, staff layoffs

Step 4: Risk Response [strategic initiatives]: Product innovation, market research, acquisition of competition, etc

Step 5: Monitoring: Every 3 months the Board evaluates product innovations and how well they are addressing market needs.

2. Linking Risk Management to Strategy – Menti.com

Which of the statements BEST describe your organization integration of Risk into strategic planning?

a) Risk management is embedded into our Strategic planning process as described in the 5 steps.
b) Risk management is just a chapter in our strategic plan and there is no clear link with the objectives and strategies in the plan
c) Risk management is not expressly mentioned in our strategic plan but it is implied.
d) There is no mention of risk in our strategic planning document
e) My organization does not have a strategic plan

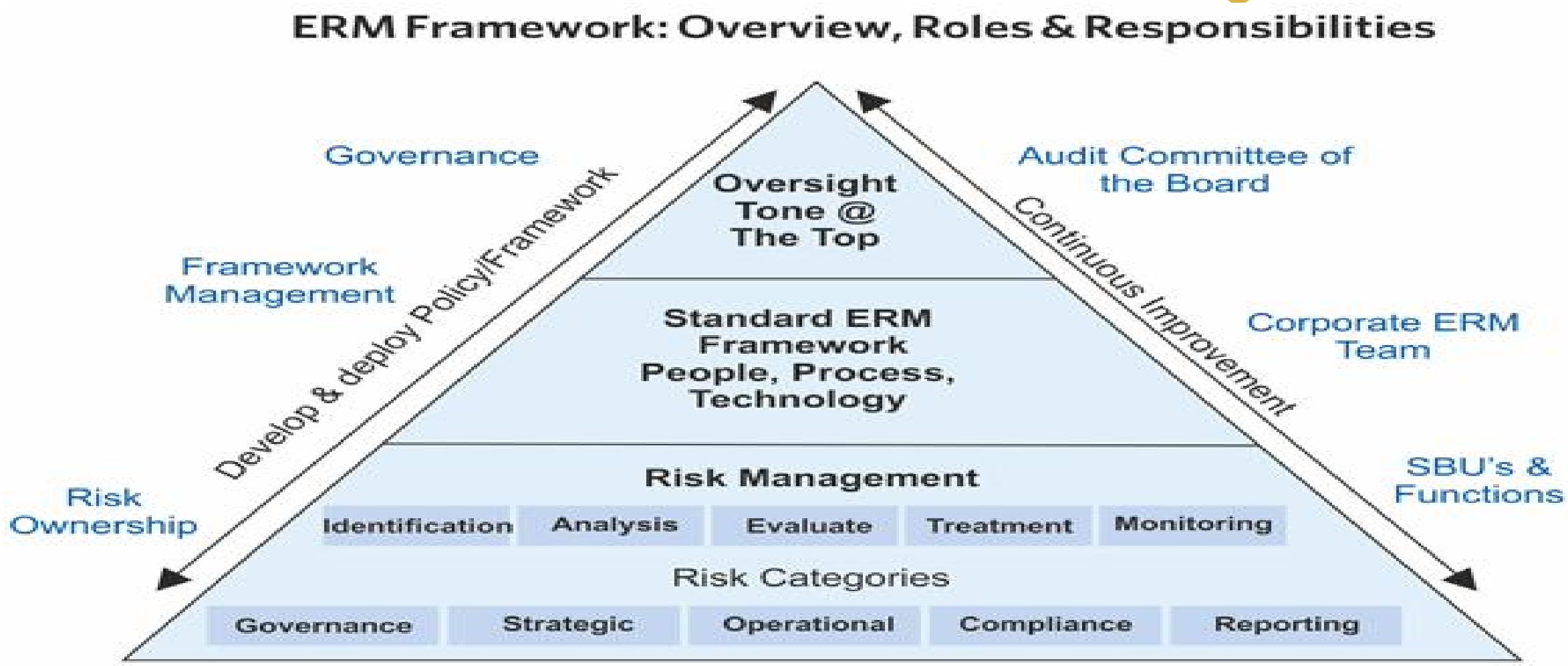
3. Setting the right tone at the top for effective risk management

"Boards must go a step further, and ensure that their company's ERM capabilities are optimized and are well adapted to the company's business culture and the nature of the risks it faces."

- Kevin B. et al, 2008

3. Tone at the top

– Responsibility for ERM



3. Tone at the top

– Responsibility for ERM

- The board has overall responsibility for ensuring that risks are managed.
- In practice, the board will delegate the operation of the risk management framework to the management team, who will be responsible for completing the risk management operational activities.
- There may be a separate function that co-ordinates and project-manages RM activities and brings to bear specialist skills and knowledge. In some organizations, Internal Audit Function coordinates RM activities.
- Everyone in the organization plays a role in ensuring successful enterprise-wide risk management but the primary responsibility for identifying risks and managing them lies with management.
- Internal Audit role with regard to ERM is to provide objective assurance to the board on the effectiveness of risk management.

3. Tone at the top

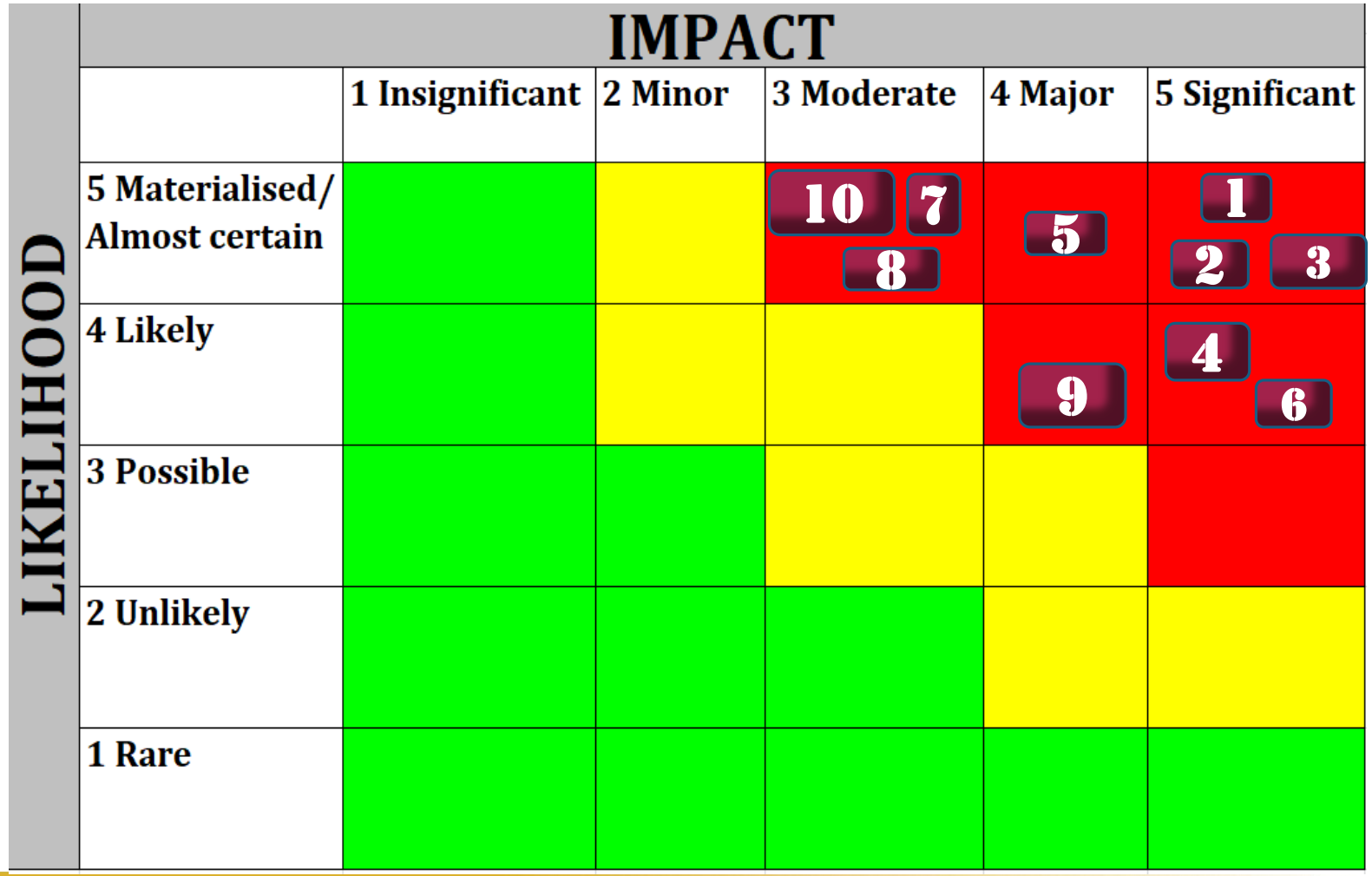
– Culture

- **Awareness** at Board level
- **Board Risk Committee** with clear risk roles
- **Risk Management committee** – clear roles
- Ownership of processes risks by **line managers**
- **Living risk aware culture** – Code of conduct. Management actions speak louder that words
- Incorporate risk roles in **JDs** and **staff annual scorecards**
- **Risk profile** should **ALWAYS** guide management and Board discussions

"One of the key implementation issues that must be addressed is how to overcome a corporate culture that is lacking or even negative toward risk management.""

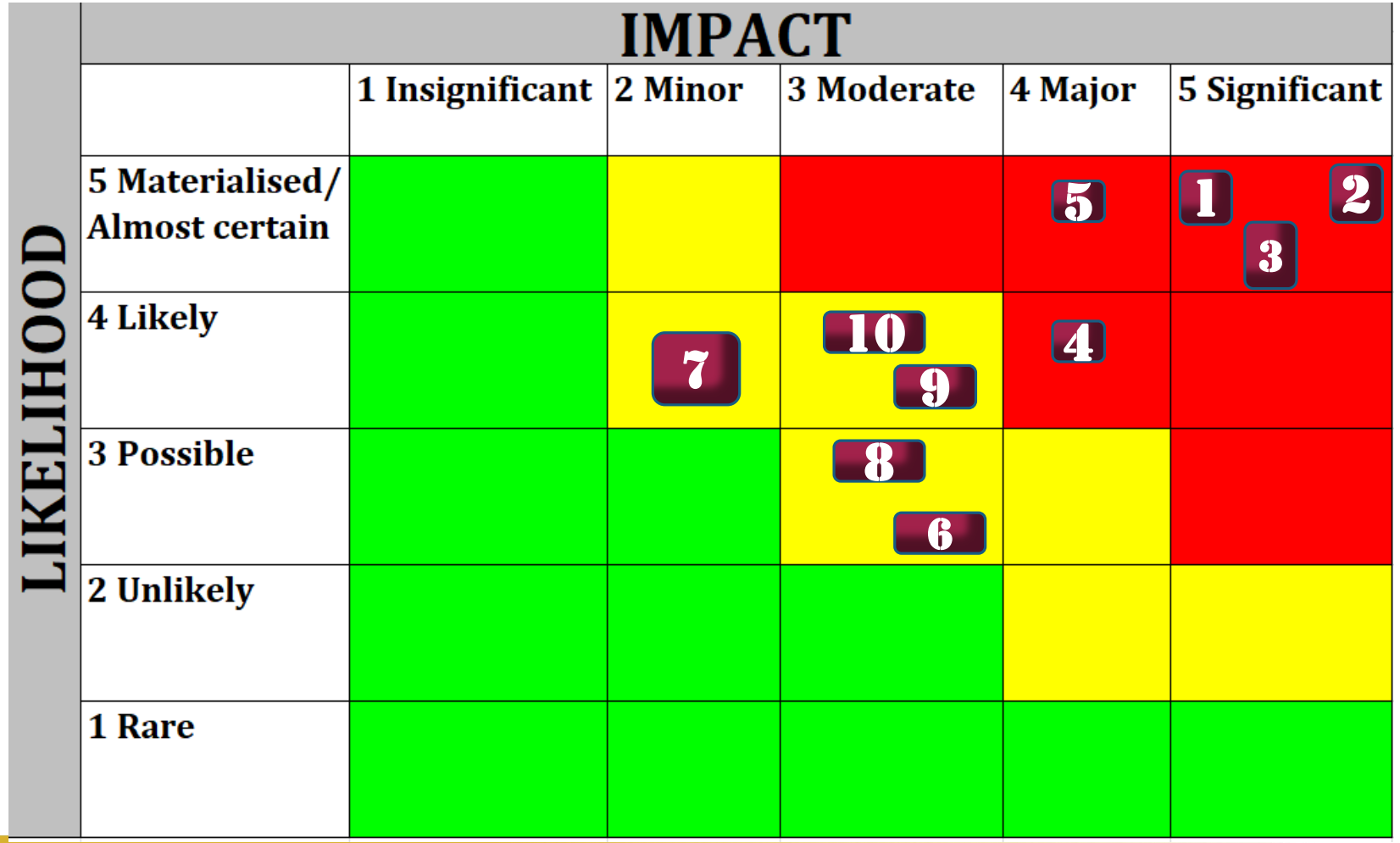
- Edmund Conrow

3. Tone at the top
– Risk Heat map - Inherent risk



#	RISK
1	Growth & Expansion risk
2	Competition
3	Asset under utilization
4	Growing energy cost
5	Financial – Debtors
6	People risk – Exit of Key staff
7	Technology risk - Integration
8	Physical Security
9	Human Safety
10	Legal & regulatory non compliance

3. Tone at the top
– Risk Heat map - Residual risk



#	RISK
1	Growth & Expansion risk
2	Competition
3	Asset under utilization
4	Growing energy cost
5	Financial – Debtors
6	People risk – Exit of Key staff
7	Technology risk - Integration
8	Physical Security
9	Human Safety
10	Legal & regulatory non compliance

3. Tone at the top – What is reported to the Board?

Source: Protiviti, 2010

The board receives the following risk information:

	Information Received:	Quarterly	2–3 times a year	Annually	Subtotal (at least annually)	Less than once a year	Ad hoc, e.g., as requested by board	Not at all
1	Periodic overview of management's methodologies used to assess, prioritize, and measure risk	19%	17%	29%	**65%**	3%	19%	13%
2	High-level summary of the top risks for the enterprise as a whole and its operating units	22%	18%	31%	**71%**	4%	16%	9%
3	Summary of emerging risks that warrant board attention	25%	21%	13%	**59%**	3%	25%	13%
4	Summary of significant gaps in capabilities for managing key risks and the status of initiatives to address those gaps	21%	12%	20%	**53%**	4%	23%	20%
5	Risk reports, such as trends in key risk indicators	30%	13%	15%	**58%**	5%	12%	25%
6	Report on effectiveness of responses for mitigating the most significant risks	28%	12%	16%	**56%**	3%	23%	18%
7	Summary of significant changes in the assumptions and inherent risks underlying the strategy and their effect on the business	21%	13%	22%	**56%**	4%	21%	19%
8	Summary of exceptions to management's established policies or limits for key risks	25%	11%	13%	**49%**	5%	21%	25%
9	Scenario analyses evaluating the impact of changes in key external variables impacting the organization	16%	10%	23%	**49%**	4%	20%	27%

3. Tone at the top

– Questions that BAC asks about ERM

1. Is the risk policy up to date? Are there any changes that need to be made based on changes in the legal or regulatory frameworks both locally and globally?
2. What are the top risks [inherent & residual] and how does that compare with the previous reporting? Is the organization still within **risk appetite** and **tolerable limits?** Are there key emerging risks not included in the risk register or newly added in the register?
3. Has management put adequate and effective controls to mitigate the risks?
4. What are the key findings [from internal & external audits], their impact to the objectives of the organization, respective audit recommendations and implementation status? Are any of these repeat findings and if so why are root causes not yet addressed? What do these audit findings mean to the organization risk profile?
5. What is the audit recommendations implementation status? Are there long outstanding recommendations with significant impact to the organization? Why have they remained unimplemented? Is board intervention required?

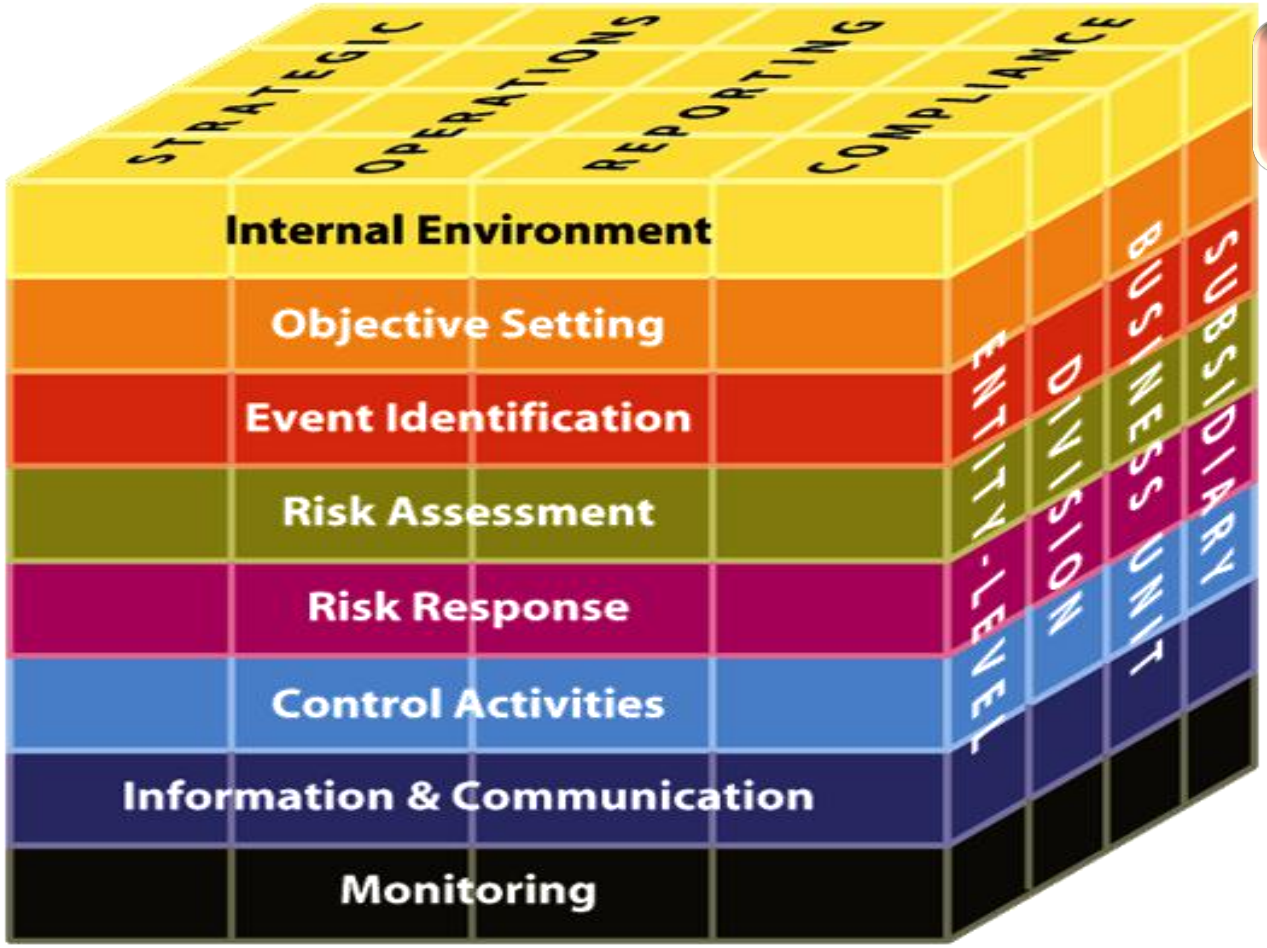
4. Critical steps in the implementation of the ERM Framework

1. ERM Framework Implementation
– RM Methodologies – Known frameworks

Similarities

1. Identify
2. Assess
3. Manage
4. Monitor

1. ERM Framework Implementation – RM Methodologies - COSO



Tone at the top as defined in RM policy

RM Policy + Framework

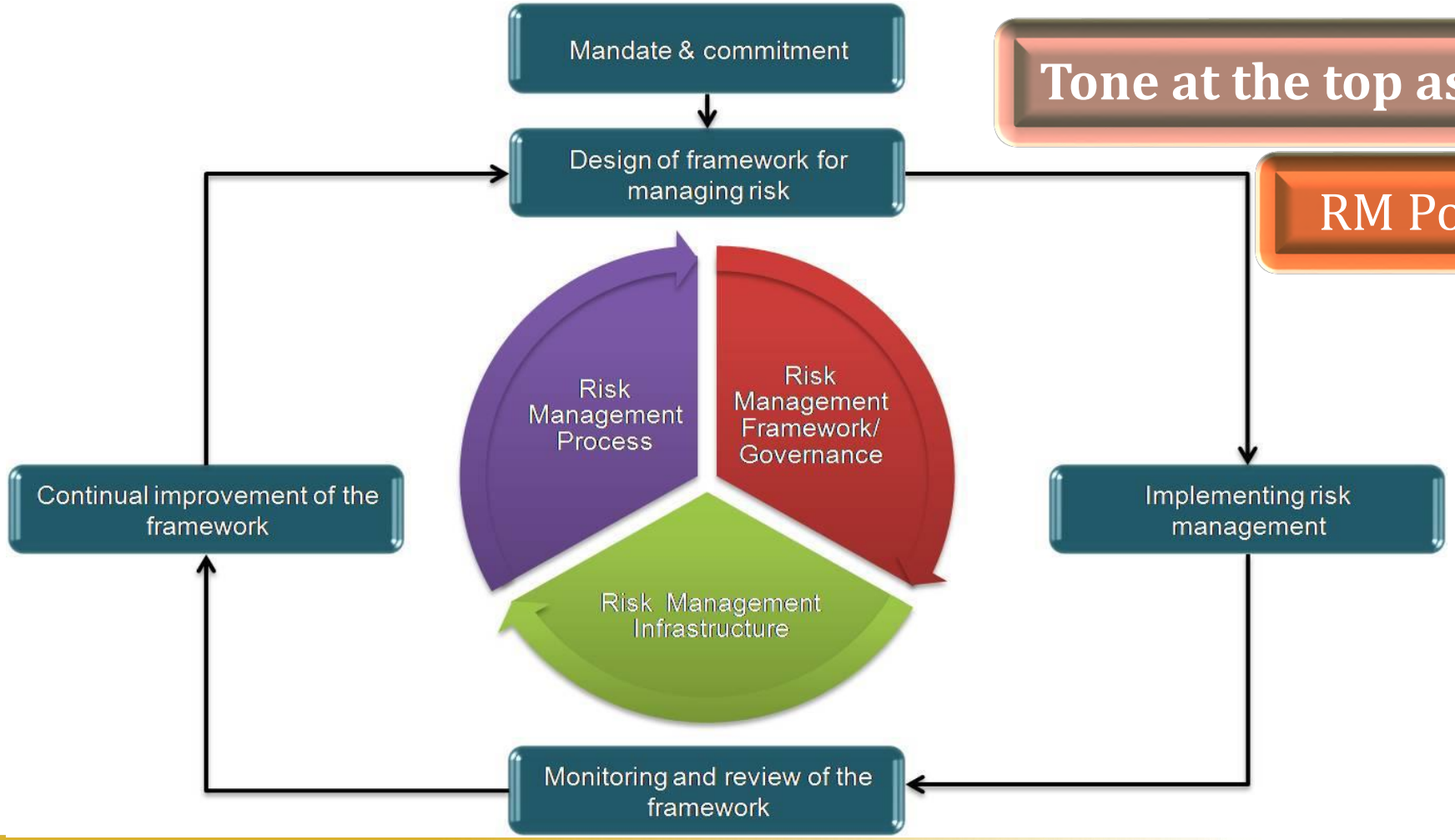
Identify

Assess

Manage

Monitor

4. ERM Framework Implementation – RM Methodologies – ISO 31000



Tone at the top as defined in RM policy

RM Policy + Framework

Identify

Assess

Manage

Monitor

4. ERM Framework Implementation – RM Practical approach – car analogy

Objective: Driving my Ferrari to work and back home

1. Future Risks	Service 
2. Current Risks	Gauges/ Lights 
3. Past Risks	Log book
4. Repairs	Repair schedule
5. Maintenance checks	Checklist
6. Police Checks	Inspection 

4. ERM Framework Implementation – RM Practical approach…

Objective: To sustainably give return to shareholders

1. Future Risks	RCSA
2. Current Risks	KRIs
3. Past Risks	Incidents Management
4. Improvements	Action tracking
5. Control Compliance	Compliance
6. Assurance	Internal Audit

4. ERM Framework Implementation
– Risk & Controls Self Assessment [RCSA]

Assessed Unit (Strategy, Dept, project, Activity etc)

1. Objectives

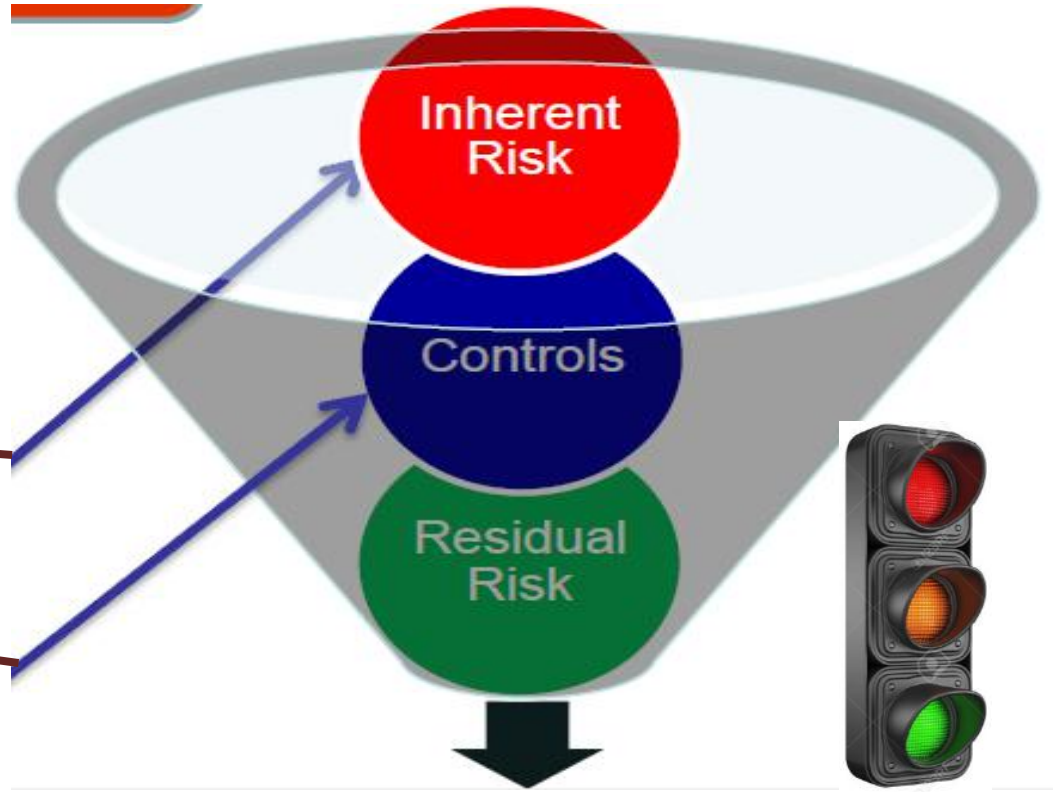
2. Critical Success Factors

3. Risks

4. Controls

5. Action

Desired level of risk



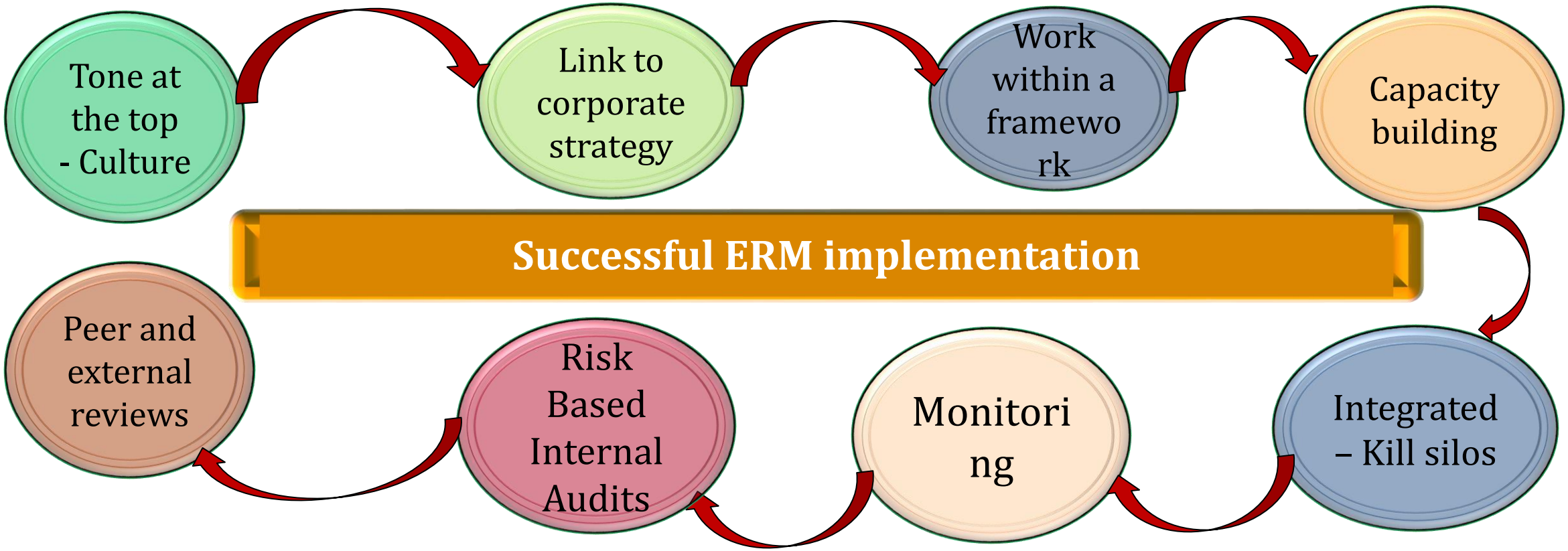
4. ERM Framework Implementation – RCSA Example

Assessed Unit - Financial reporting

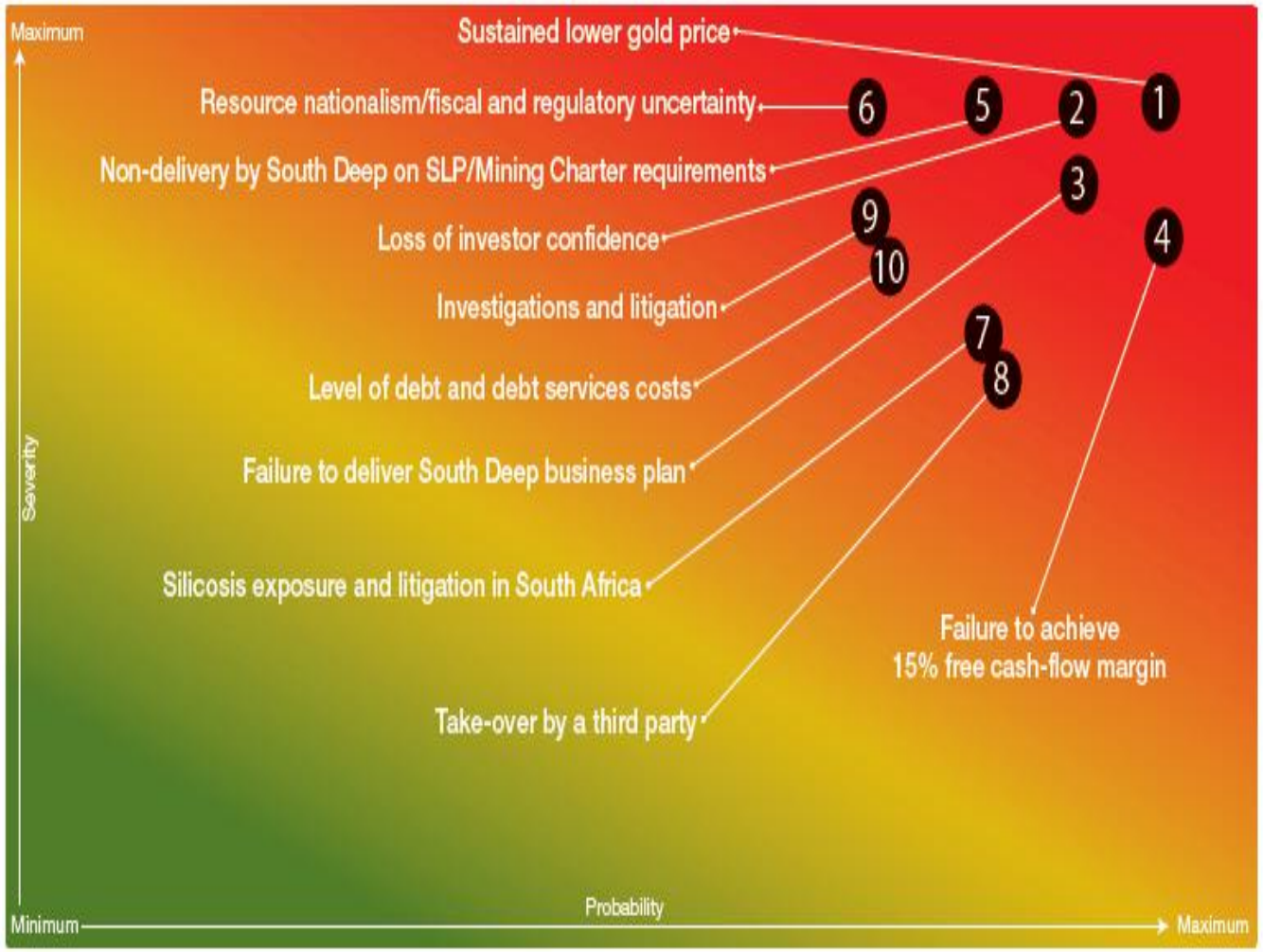
1. Objectives	1. To prepare accurate and timely financial statements for 2020-21.
2. Critical Success Factors	2. a) Financial reporting system [suitable, updated, integrated, available, secure]
3. Risks	3. a) Unauthorized data modification b) Data loss
4. Controls	4. a) Access controls b) Data back up
5. Action	5. a) Segregation of duties matrix b) Disaster recovery sire

Desired level of risk

4. ERM Framework Implementation
– Achieving an effective ERM



5. Questions and discussions




Thank
you

My contacts

Phares Chege

Deputy Commissioner – Internal Audit
Kenya Revenue Authority
Times Tower, 25th Floor
P.O. Box 40160-00100,
Nairobi – Kenya
T: +254 (0)20 281 7055
M: +254 721 411504/ +254 733 411504
Email: phares.chege@kra.go.ke