UNDERSTANDING & MANAGING ENTERPRISE RISK MANAGEMENT-

Presentation by:

CPA Wanga John Boscow
Financial Controller, Salwa Kenya Limited

2019 Coast Branch Annual Summit, Mombasa

Definition of risk

What is Risk?

Definition of risk

Risk is the possibility of losing something of value. Values can be gained or lost when taking risk resulting from a given action or inaction, foreseen or unforeseen.

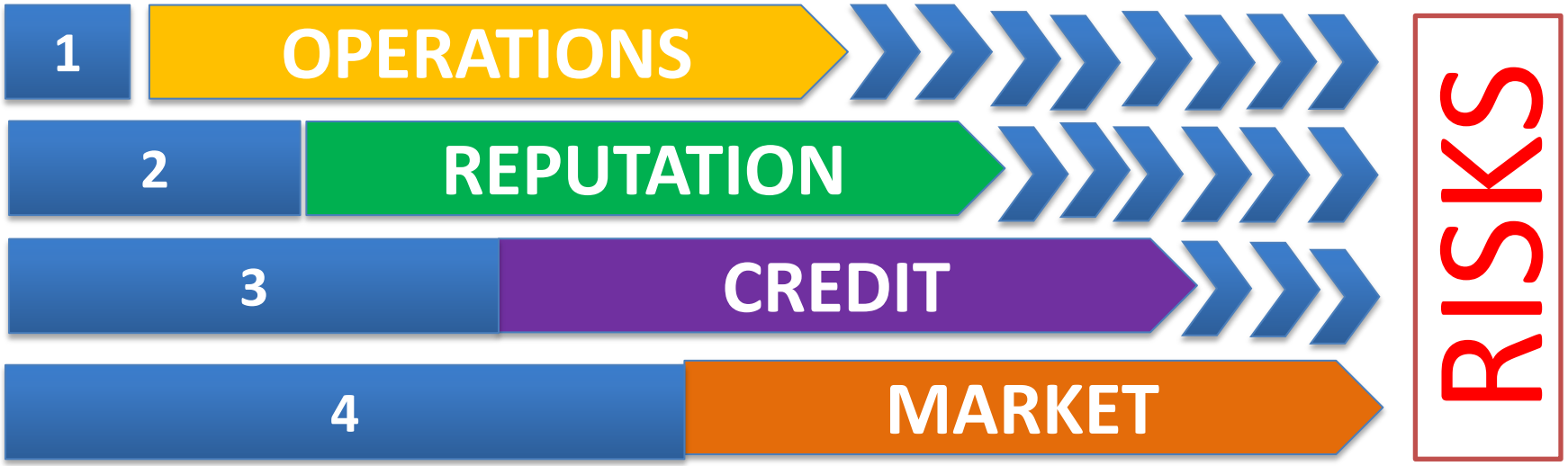
Risk can also be defined as the intentional interaction with uncertainty.

The Concept of ERM

"Enterprise risk management is 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 risk** to be within its risk appetite, to provide **reasonable assurance** regarding the achievement of entity objectives."

Focus of risk management

- Risk management applies a systematic and logical approach to uncertainties in:



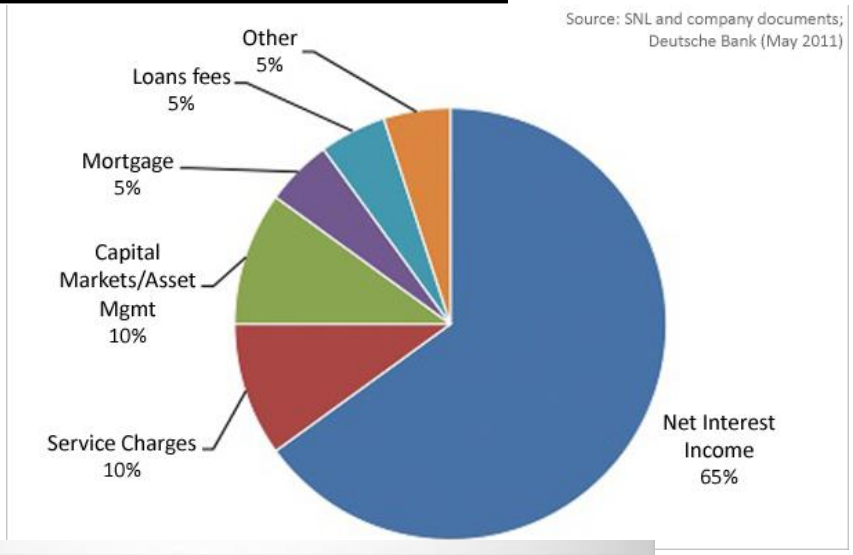
Why Risk Assessment is Necessary (Performance)

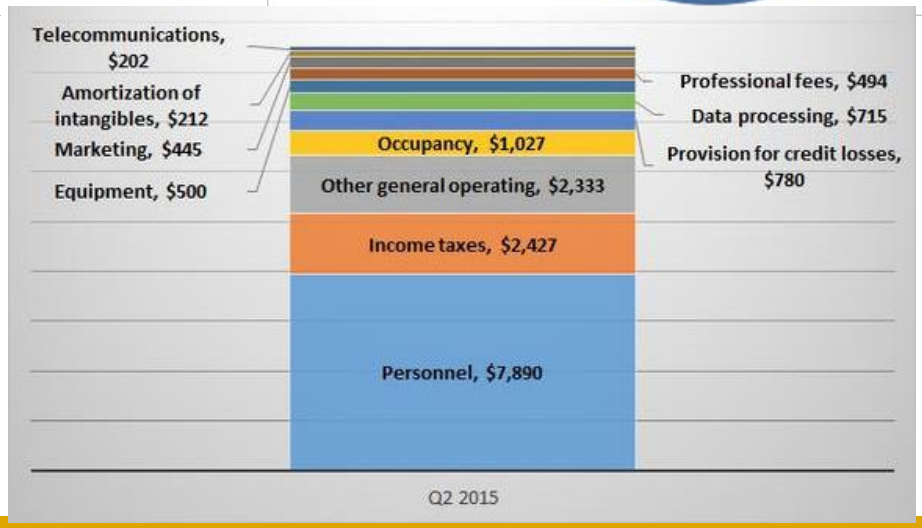
OTHER EFFECTS

Top line effects

Middle line effects

Bottom line effects

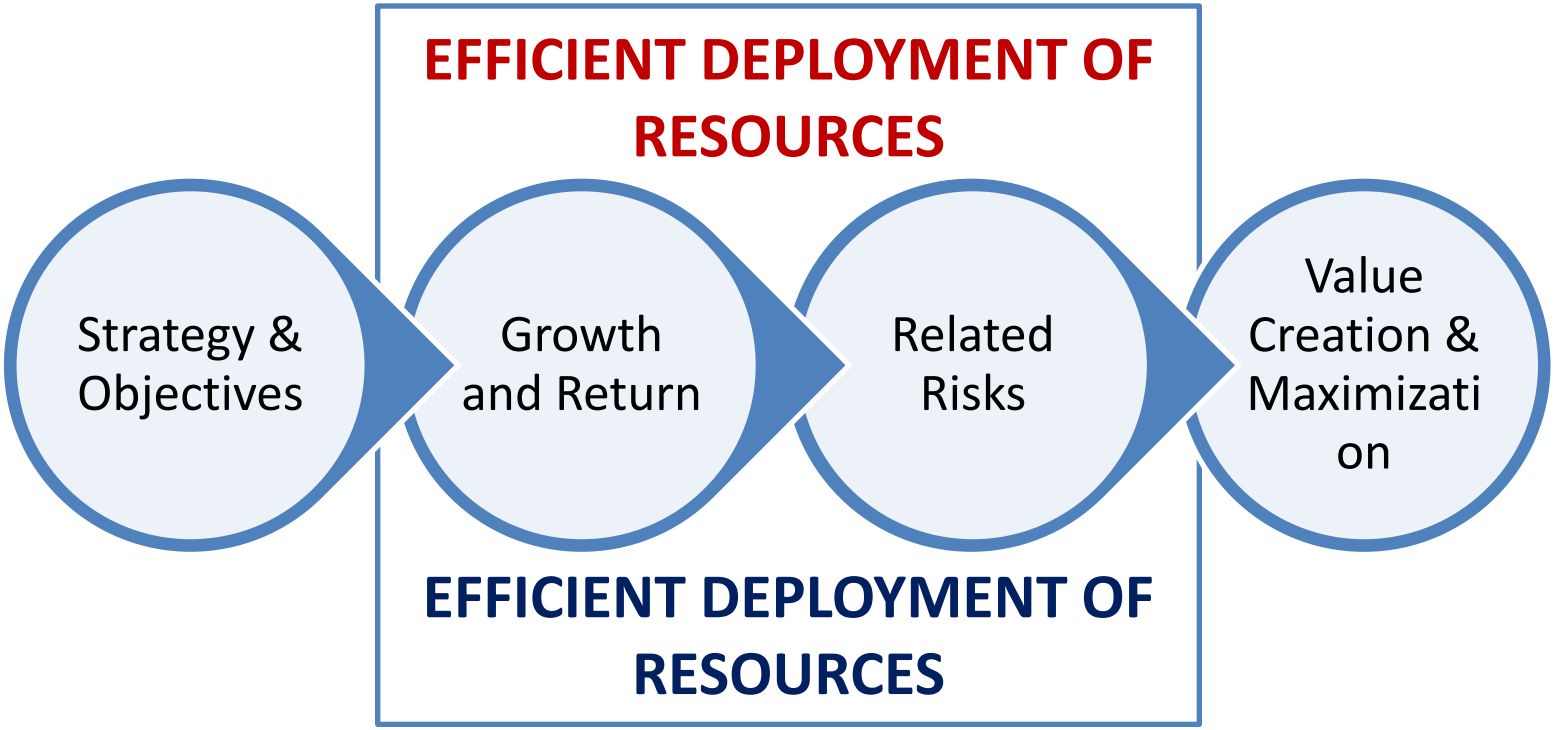




Why Risk Assessment is Necessary (Legal Requirement)

- Co. Act, Sec. 655, **Business review** to be included in certain directors' reports.
  - Sub-sec. (3): (a) (ii) a description of the principal risks and uncertainties facing the company
  - Sub-sec. (9) If directors of a company fail to comply with a requirement of this section, **each director of the company who is in default commits an offence** and on conviction is liable to a fine not exceeding five hundred thousand shillings.
- Sec. 656(1) - Directors not to disclose if information is likely to detrimentally affect the interests of the company.

ERM's Ultimate Goal



ERM Dispensation

Best-practice ERM delivers capabilities across 5 dimensions

- Clear understanding of firm's risk culture gaps
- Alignment of culture with the firm's risk strategy

- Prioritized risk heat map
- Insight into the big bets that really matter
- Cascading reports tailored to different management levels

- Organizational model tailored to business requirements
- Adequate resource levels to manage risks

- Clear definition of risk appetite, with matching operational levers
- Strategy informed by risk insights

- Managerial decisions optimized by embedding risk in processes
- Strong links between ERM function and key BUs and other functions

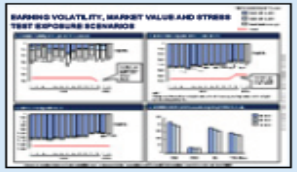
Source: McKinsey

Integrated system of risk reports

An integrated system of risk reports

Reporting "cascade" includes:

1. **Enterprise view of risk**
   - Enterprise risk heat map
   - Top 10 risks
   - Emerging risks
   - Current market outlook
   - Peer comparison



(10-20 pages providing an overview of enterprise-wide risk)

Board-level report

2. **Risk and BU syntheses**
   - Synthesis page for each risk
   - Synthesis page for each BU or function

(1 page per risk)
(10 – 15 pages overall)

3. **Detailed risk sections**
   - Provides a chapter containing overall synthesis and detailed support pages for each risk
   - Also includes reports on specific risks for each BU and function

(15-20 pages per chapter)
(10 – 15 chapters)

Best practice risk management

Principles for designing a best-practice risk management organization

1. Strong and visible commitment from all members of the top team
2. Central oversight of risk management across the enterprise (including subsidiaries and corporate functions)
3. Separation of duties between policy setting, monitoring, and control on the one hand; and risk origination and risk management execution on the other
4. Clearly defined accountability
5. Risk appetite and strategy clearly defined by top management (and the board)
6. Full ownership of risk and risk management at business-unit level
7. Business units formally involved and view risk function as a thought partner
8. Robust risk management processes reinforce organizational design (e.g., incentive systems incorporate risk-return considerations)

Source: McKinsey

Risk management in the corporate world

- Continuously provide oversight on identifying, assessing and to the extent possible, mitigating corporate risk.

BUT:
Oversight is somewhat passive and involves significant reliance on management.

Risk management in the corporate world

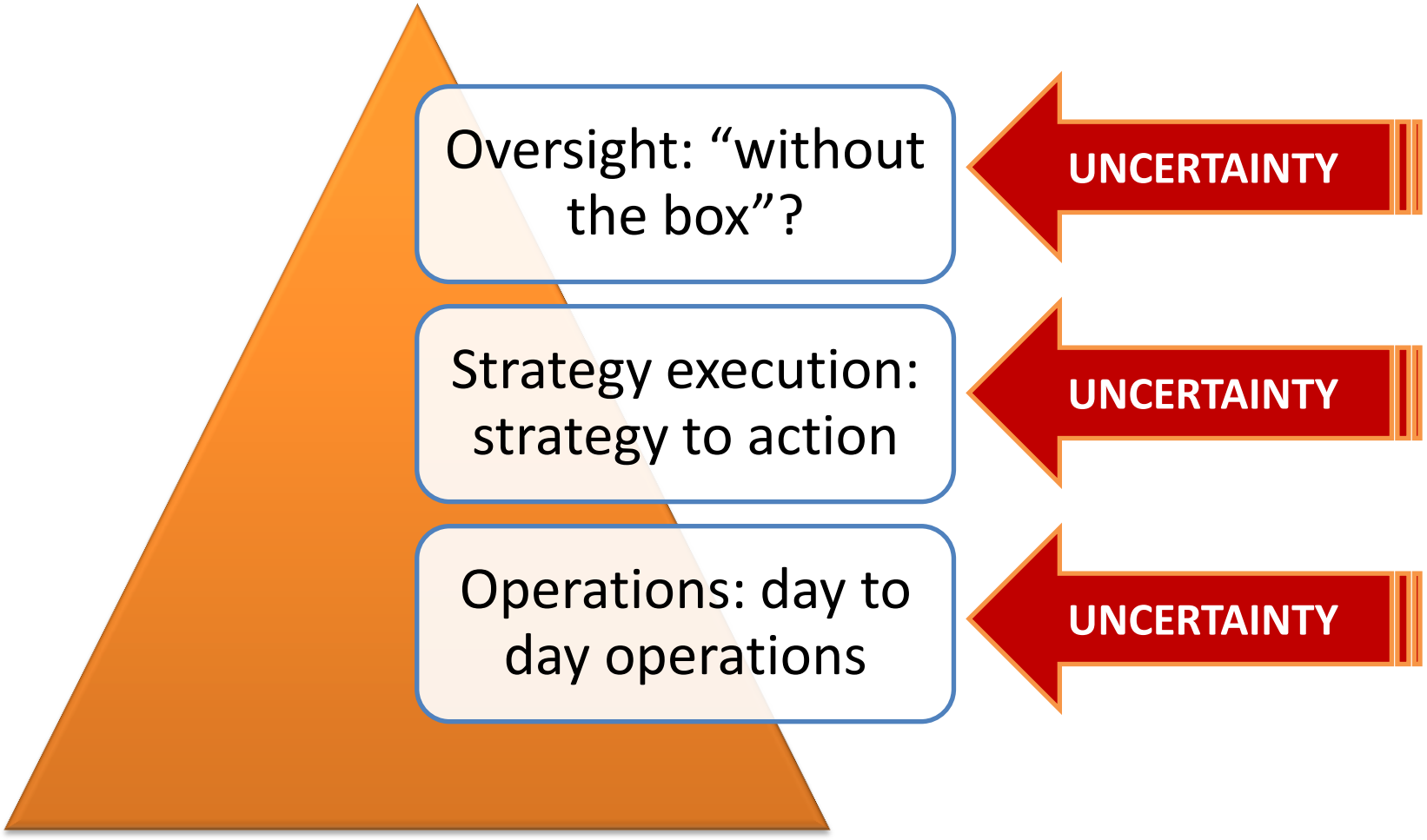
- **Risk oversight role:**

  Directors should be able to satisfy themselves that effective risk management processes are in place and functioning effectively.

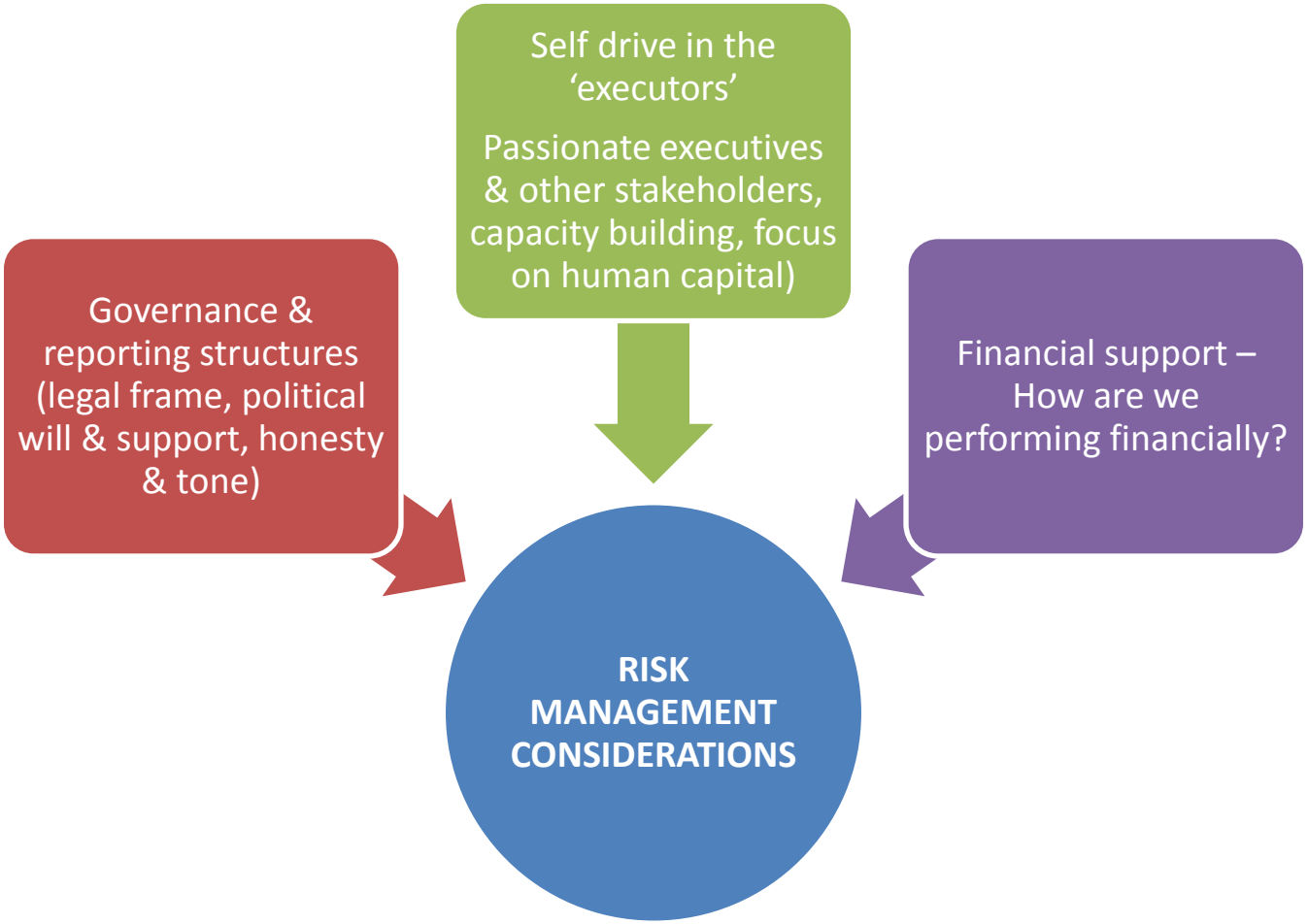
Board's oversight role: what to expect

- Company's material risks
- Understand and evaluate how the risks interrelate
- How the risks may affect the company
- How these risks are being managed.

Hierarchy of risks



Corporate world – key considerations



Dealing With Risks

Effective risk management and board oversight should not be premised on risk avoidance.

TOLERATE THE RISK

TREAT THE RISK

TRANSFER THE RISK

TERMINATE THE RISKY ACTIVITY

RM Process: Identifying risks

- Two phases:
  - Initial risk identification
  - Continuous risk identification

- Guided by an appropriate STRATEGY
  - External risks
  - Operational
  - Change risks

RM process: identifying risks

Human Resources
- Results of staff surveys
- Turnover rates
- Industrial action
- Time to fill vacancies

Org. Performance
Material variations from planned performance
- Failure to achieve objectives and targets
- Non-achievement of SASP targets

Finance
- Material variations for budget
- Number of financial write offs
- Unspent funding
- Number of adverse external audit findings
- Number of identified cases of fraud

Reputation & Image
- Number of adverse media stories
- Number of reviews by regulators
- Number of Ministerial /PAC questions

OH& S
- Number of reported incidents
- Number of compensable injuries
- Lost days due to illness/injury

Customer Impact
- Number of complaints from Students /stakeholders
- Number of loans processed beyond planned time
- Number of students serviced p.m.
- Time taken to provide service
- Length of waiting lists for services

Assessing risks

There are three important principles for assessing risk:

a) Ensure that there is a clearly structured process in which both likelihood and impact are considered for each risk;

b) Record the assessment of risk in a way which facilitates monitoring and the identification of risk priorities;

c) be clear about the difference between, **inherent** and **residual** risk

- **Risk required** – What you want to achieve
- **Risk capacity** – The appropriate level of risk
- **Risk tolerance** – How you feel about risk **[APPETITTE]**

http://www.imwealthmanagement.com/risk-profile

Reviewing and reporting risks

Why review and report:

- to monitor whether or not the risk profile is changing;
- gain assurance that risk management is effective, and to identify when further action is necessary.

Reviewing and reporting risks

Aspects to report in the "Risk Management" section:

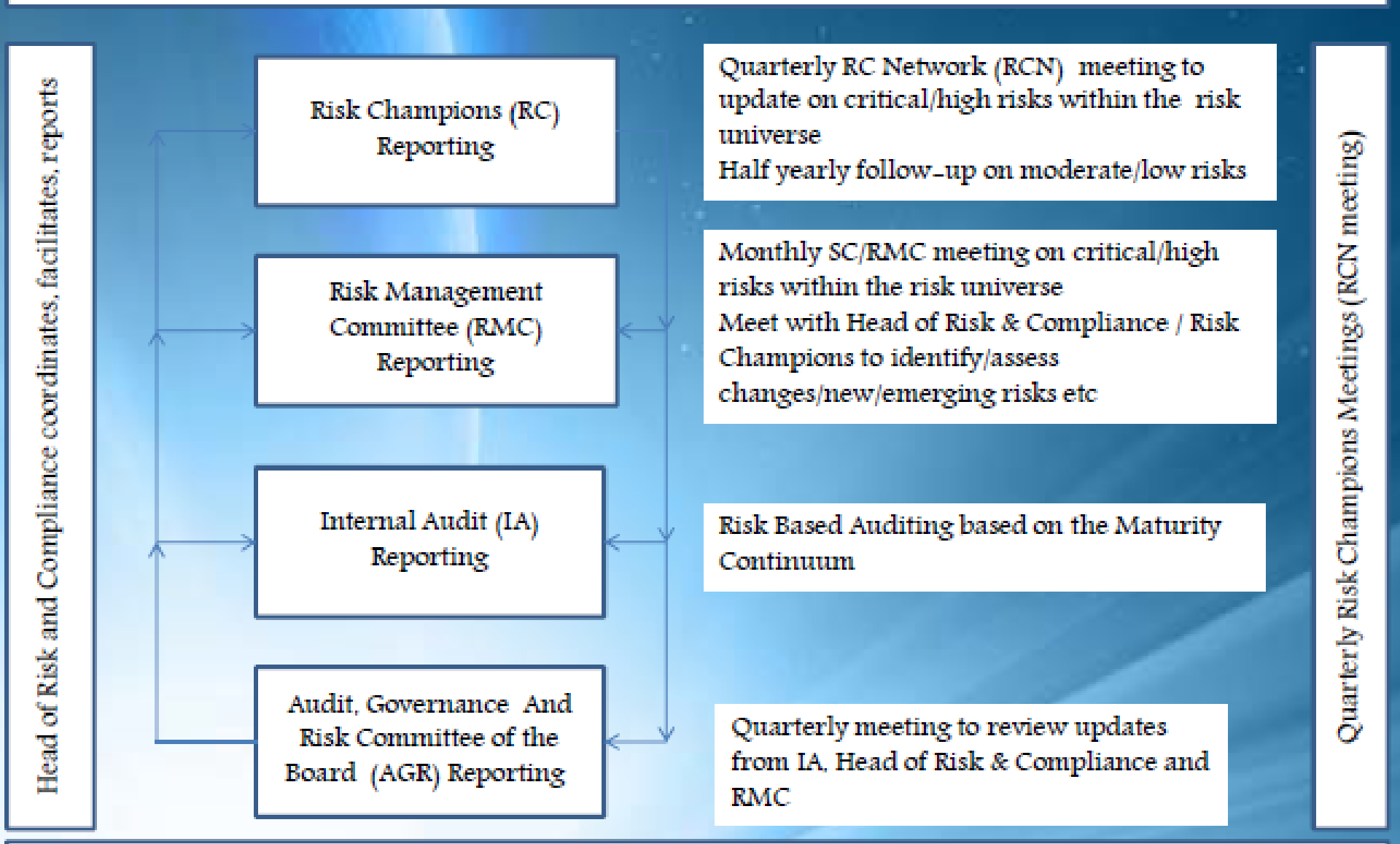
- Consider materiality
- Risk management approach and framework
- Risk management roles
- A brief on the specific risk categories – caution!
  - Information, market, compliance, reputation, credit, operational etc.
  - Highlight what the group has done to address each category
- Ethics and code of conduct
- Risk & innovation
- The group's future – plans in terms of risk management

Communication and learning

- A continuous process

- Runs through the whole risk management process.

Example –Risk Monitoring, Reporting and Communication Mechanism



Aligned with Strategic planning and Risk Management reporting cycle

Some [final] tips on risk management

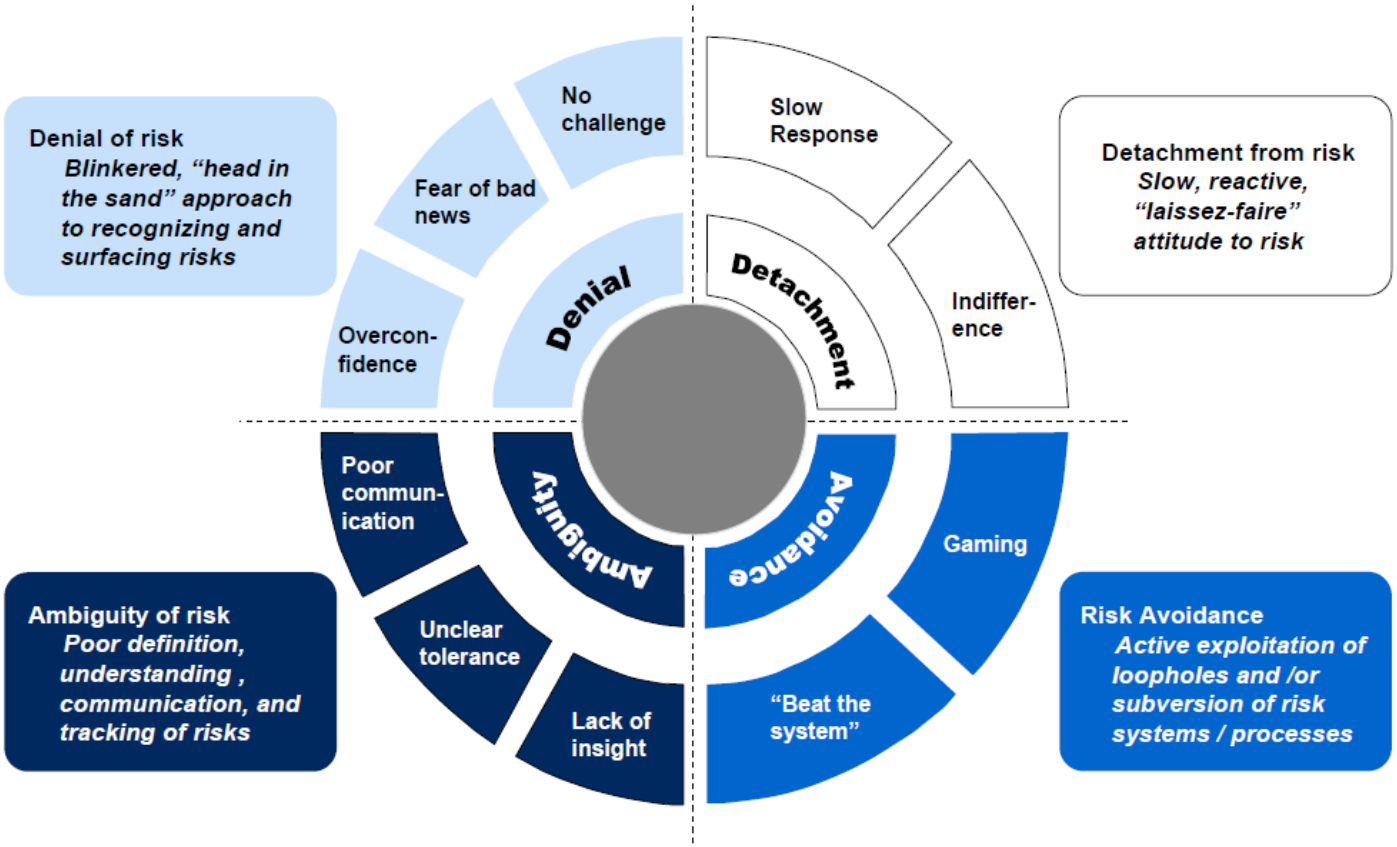
- Ensure that all aspects of the risk management process are reviewed at least once a year;
- Ensure that risks themselves are subjected to review with appropriate frequency (with appropriate provision for management's own review of risks and for independent review/audit);
- Make provision for alerting the appropriate level of management to new risks or to changes in already identified risks so that the change can be appropriately addressed.

Example of documented risk management

Fraud Risk Assessment as of [DATE]									
Identified Fraud Risks and Schemes	Likelihood [1-5]	Significance [1-5]	Fraud Risk Rating	People and/or Department	Existing Anti-Fraud Controls	Preventive [C] or Detective [D]	Controls Effectiveness Assessment [1-5]	Residual Risks	Fraud Risk Response
Fraudulent Disbursements - Check Tampering & Expense Reimbursement Schemes	5	5	25	Check tampering: Accounting & Finance staff *(including Treasury)* Contracting Purchasing Operations managers Senior executives *(e.g. Sales, Marketing, IT, Legal, General managers of remote locations, CEO, COO)* Expense Reimbursement: All staff *(especially sales personnel and management at remote locations)*	Physical access controls, dual signatures on checks, support for expenses, review by supervisor and requirement that any false statement made on any expense report could be grounds for dismissal Awareness of pressures/incentives at all levels that might drive inappropriate financial behavior as well as observation, inquiry, and other information that focus on lifestyle, family, and personal financial issues of personnel in these departments.	D	1	Medium (if by senior mgmt) Low (if by other employees)	Rotation of responsibilities in Accounting & Finance function, *(e.g. mandatory vacations)* Awareness of lifestyle and other personal issues such as divorce, illness, bankruptcies, and disgruntled employees who might want to get back at the organization
					Policy requires all				

Risk culture

Flaws in risk culture



Source: McKinsey

The integrated ERM: A Focused Framework

Governance & Culture

1. Exercises Board Risk Oversight
2. Establishes Operating Structures
3. Defines Desired Culture
4. Demonstrates Commitment to Core Values
5. Attracts, Develops, and Retains Capable Individuals

Strategy & Objective-Setting

6. Analyzes Business Context
7. Defines Risk Appetite
8. Evaluates Alternative Strategies
9. Formulates Business Objectives

Performance

10. Identifies Risk
11. Assesses Severity of Risk
12. Prioritizes Risks
13. Implements Risk Responses
14. Develops Portfolio View

Review & Revision

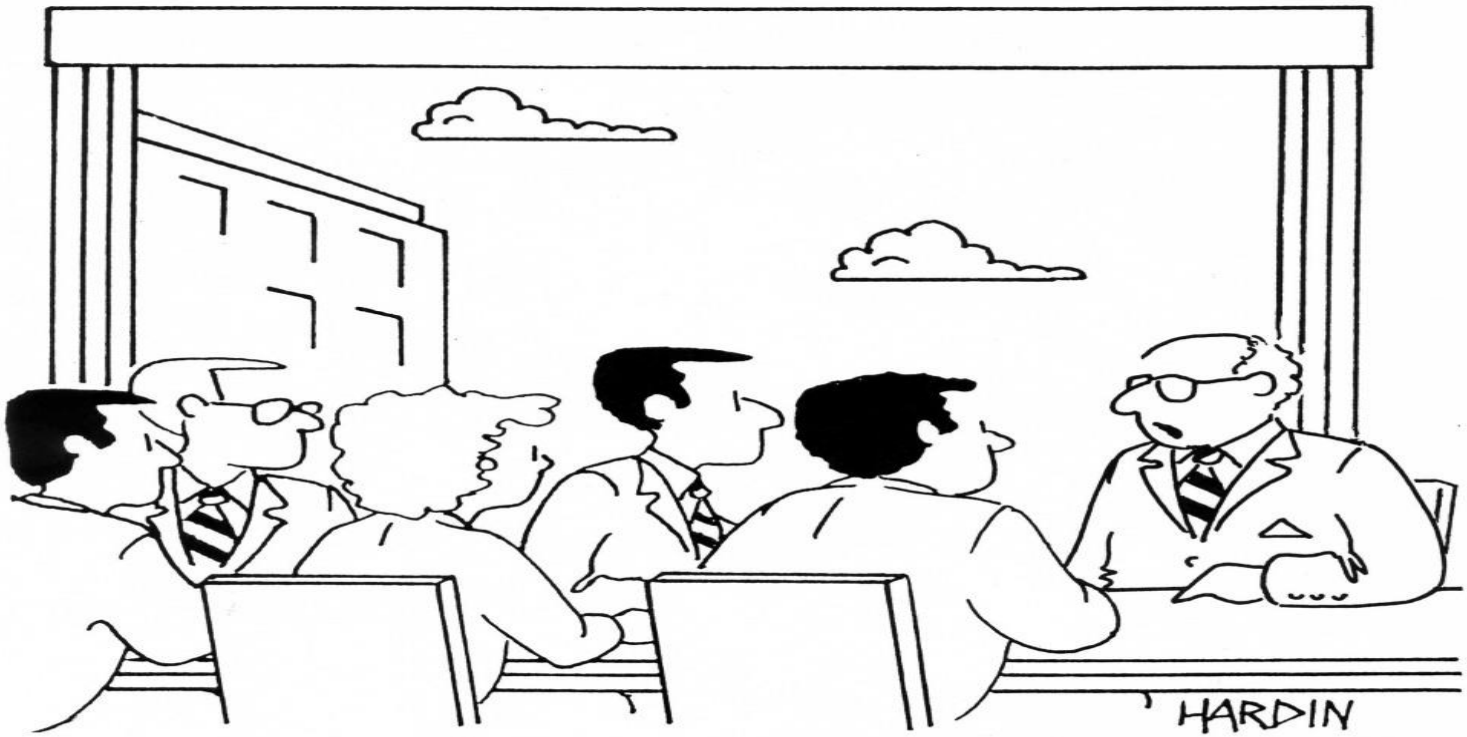
15. Assesses Substantial Change
16. Reviews Risk and Performance
17. Pursues Improvement in Enterprise Risk Management

Information, Communication, & Reporting

18. Leverages Information and Technology
19. Communicates Risk Information
20. Reports on Risk, Culture, and Performance

Source: COSO

Before we forget.....



Interactive Session