ENTERPRISE RISK MANAGEMENT CONFERENCE

Continental Beach Resort, Mombasa
Thursday, 06 August 2015

The Board approach to ERM; Connecting Shareholders and Board Members Expectations

Presented by:

CPA Phares Chege, MBA, CISA, CORP
Head of Internal Audit, HELB

Directors versus Shareholders

The board has duties to the corporation and its shareholders. Why? Because of the **fiduciary relationship** between the board and shareholders. When directors breach their duties, shareholders can bring a derivative suit against the directors because they are the ultimate beneficiaries of the corporation's growth and increased value.

- **Douglas Y. Park**

Content

1 Risk and the Board - Introduction

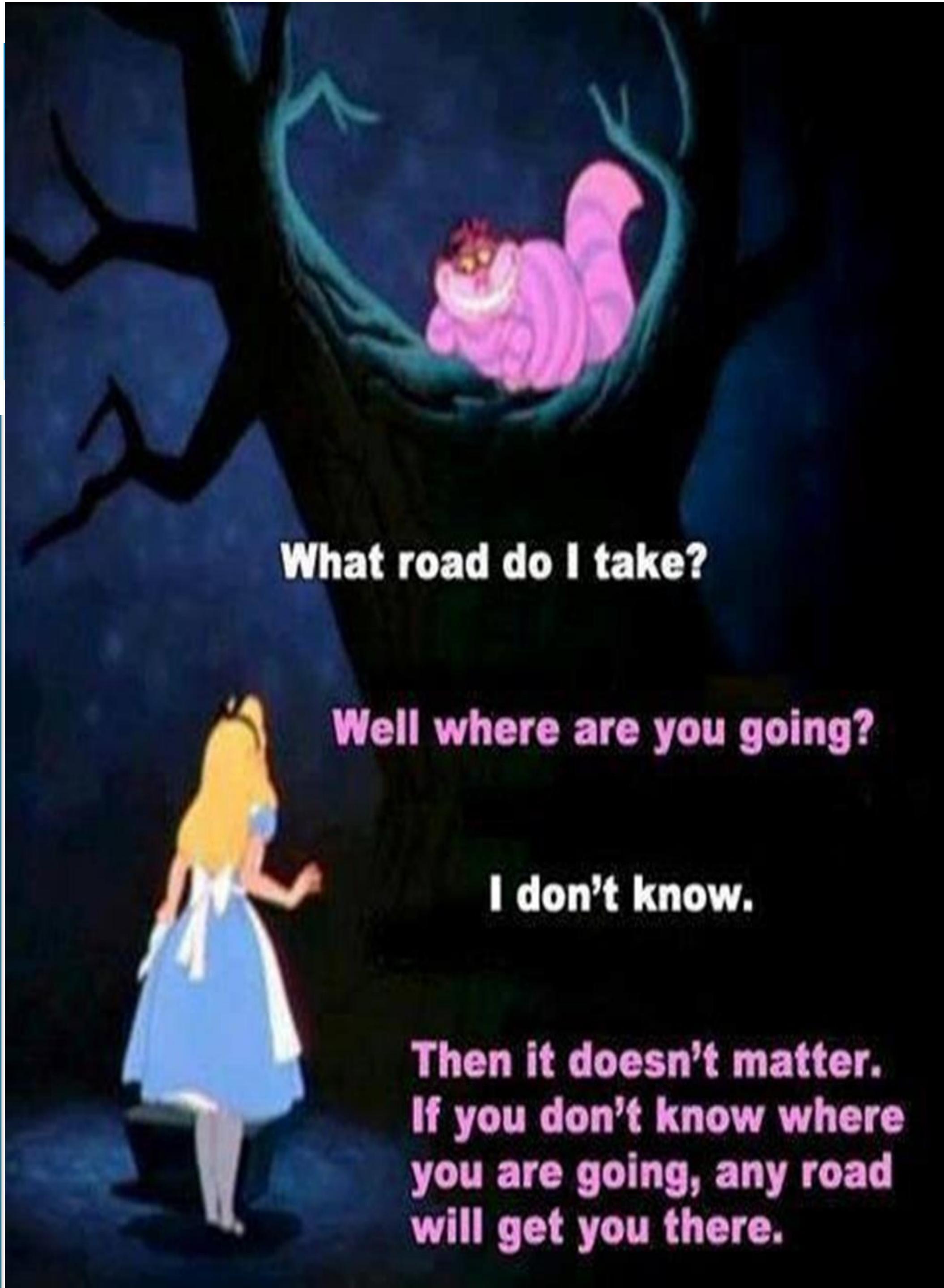
2 Provisions of COSO Framework on Risk and Board – Survey highlights

3 What therefore should be reported to Board about ERM

DISCUSSION & CLOSE

1. Risk and the Board

McKinsey study



ERM framework

Risk Management Framework

Governance & Oversight

Board / Executive Team

Business Strategy | Risk Strategy | Risk Appetite | Risk Profile

Lines of Defense

First Line

Business Lines & Support Functions

- Product, process, risk, & control ownership & management
- Business strategy execution
- Revenue generation & support

Second Line

Independent Risk Oversight Functions:

- ERM, ORM, Regulatory Compliance, Credit Review, etc.
- Risk Management Framework; Alignment Monitoring; Challenging 1st Line; Facilitation

Third Line

- Internal & External Audit
- Independent validation and reporting of risk management program design & effectiveness
- Leverage information

Risk Management Process Lifecycle

Identify

- Where is Risk?
- Internal & External threat-sources
- How Risk Arises
- Business Context
- Scenarios/What-if

Assess

- Inherent/Residual
- Likelihood/Impact
- Volatility/Speed
- Rating scales
- Top-Down/Bottom-Up
- Qualitative/Quantitative
- RCSAs & Modeling

Decision

- Accept, Reject, Reduce
- Manual/Automated
- Decision Escalation based on Risk Tolerances & Delegated Authorities

Treat

- "Right" People
- Policies, Procedures, Controls, Incentives
- Risk Transfer (Insurance & Hedging)
- Risk Reserves & Risk Based Pricing

Monitor

- Risk Profile
- Biz Changes
- KRIs, KCIs, KPIs
- Losses, near miss, external events
- Outstanding Issues
- Model output

Culture, Communications & Training

Tolerances & Authorities

Risk and the Board: What ERM is not…

- A silver bullet to prevent risks from occurring
- A methodology or a checklist of items that need to be completed that guarantee results
- The only way organizations can take a more proactive approach to managing risk

Risk and the Board

Directors in organizations are encouraged to embrace entrepreneurial risks and pursue risk-bearing strategic opportunities.

Because of this, it is widely recognized that corporate directors are responsible for **reviewing** and **approving** the company's ERM program.

Risk and the Board …Cont'd

Boards must go a step further, and ensure that their company's ERM capabilities are at the level of **best practices** and are well **adapted** to the company's business culture and the nature of the risks it faces. Best practices has **five** ERM dimensions.

\- Kevin B. et al, 2008

Risk and the Board …Cont'd

Source: McKinsey

Risk and the Board …Cont'd

- 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

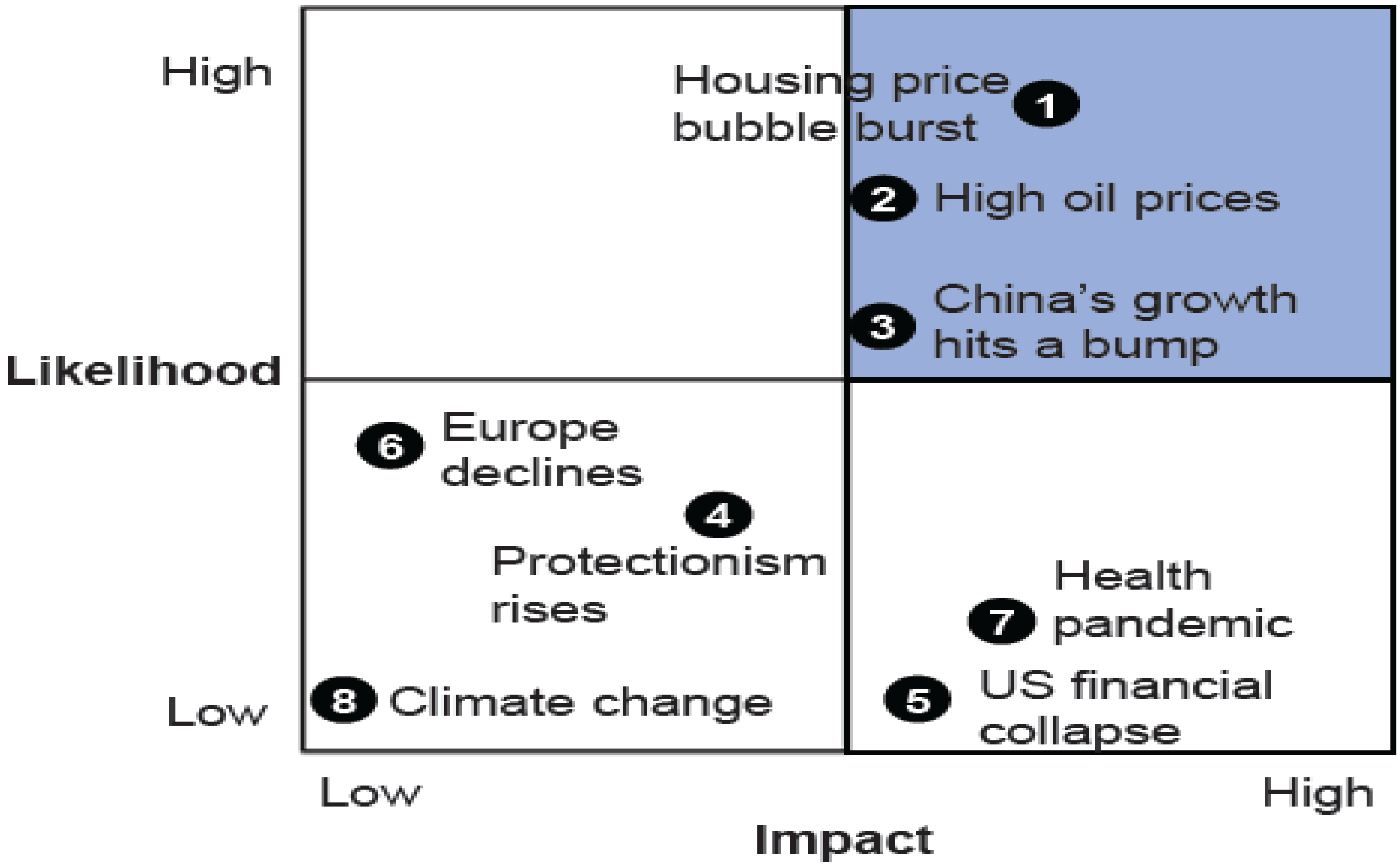
- Organizational model tailored to business requirements
- Adequate resource levels to manage risks

- 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

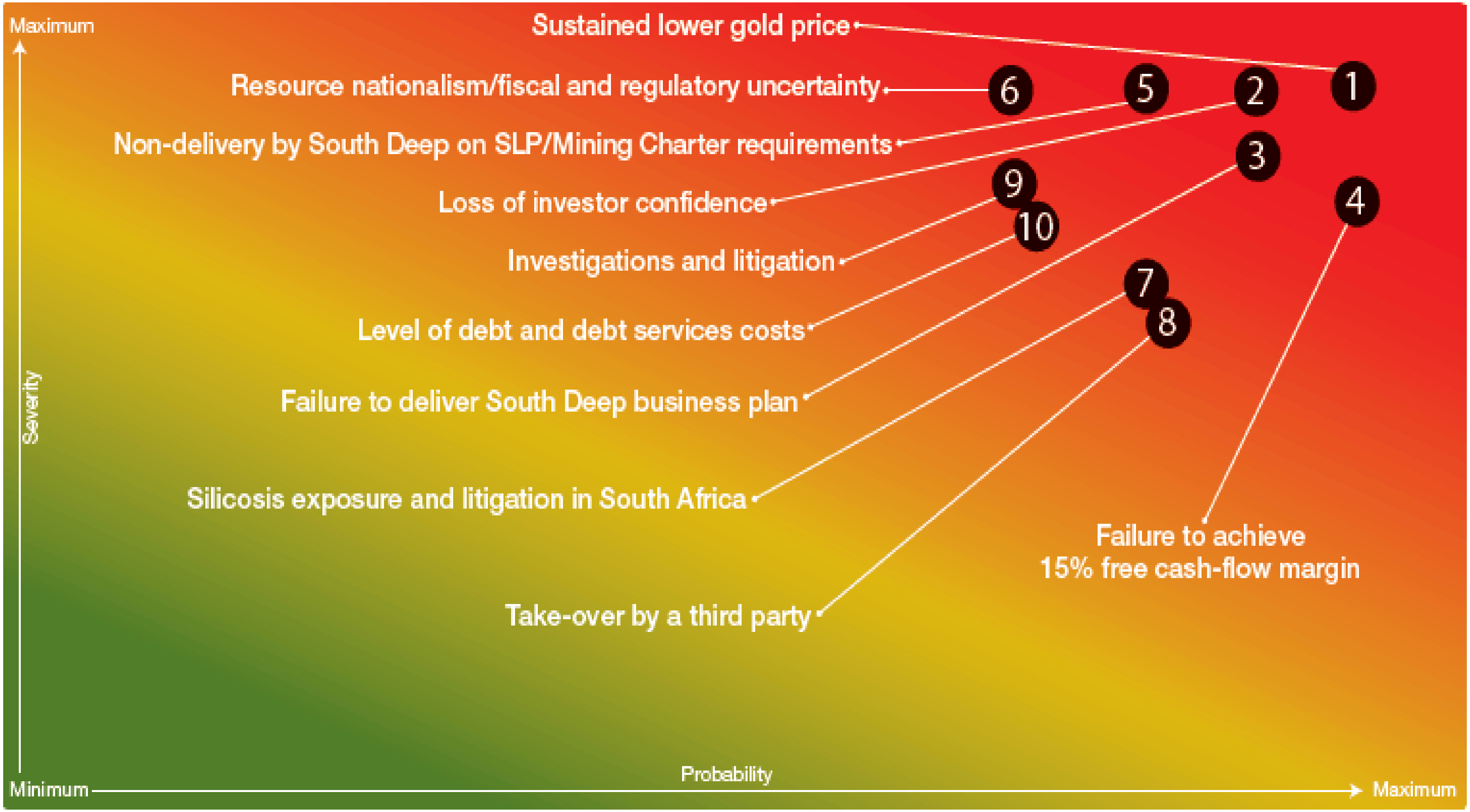
Risk and the Board …Cont'd
Heat Map



Source: McKinsey

Risk and the Board ...Cont'd

Heat Map



Source: Gold Fields Integrated Annual Review 2013

Board responsibility for risk oversight

Risk oversight is one of the core responsibilities of boards. The best boards have all their members take responsibility for risk oversight.

They ensure that the company has an ERM organizational model that is **optimized** for the kinds of risk a company encounters.

Within the board, where does responsibility for risk oversight lay?

Board responsibility for risk oversight …Cont'd

In many companies, directors will say it rests with the **board's audit committee**.

This is likely a mistake, and might result from a deep-seated underestimation of the value and importance of risk oversight to the company's performance and health.

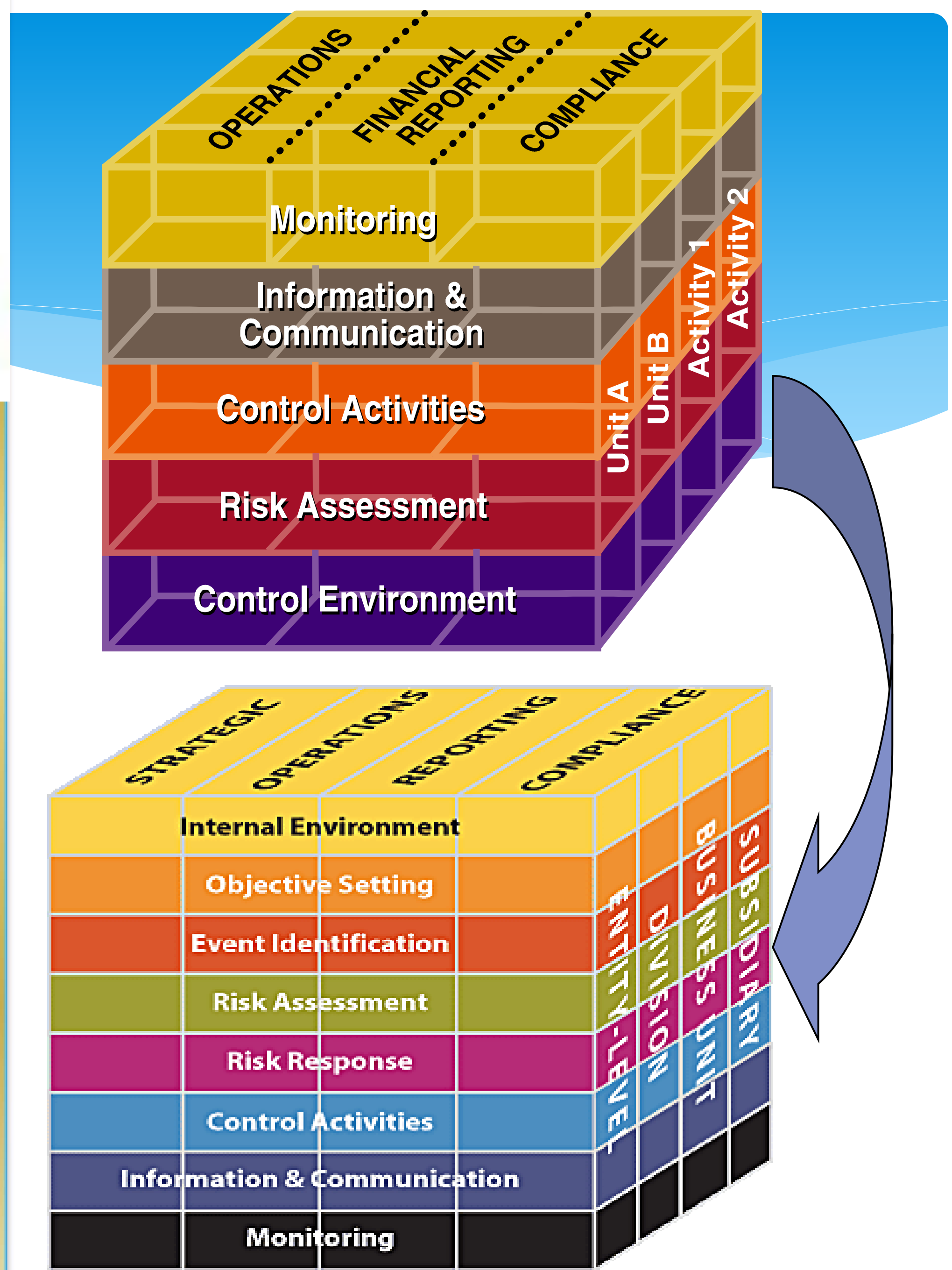
Best-performing boards involve **all their directors** in the evaluation of risks and they do so at least semiannually during a full-board, dedicated discussion of risk.

Board responsibility for risk oversight …Cont’d

In some circumstances a separate **risk committee** can be useful, to ensure that risk is given proper attention. But at the end of the day, risk oversight remains the full board’s responsibility.

To be effective in this role, the board must have the right composition. For instance, having a <u>mix of backgrounds</u> ensures a variety of perspectives on risk issues. Equally important is a board **culture** that promotes dialogue and constructive challenge.

2. COSO study on Board Risk Oversight – Key highlights and lessons learnt



So, what should you report to the Board?

The short answer is:

The larger picture of risk with a connection directly to the front-line…

Your board needs to understand the sources of uncertainty that could impair continuing operations or reaching your organization's strategic goals. This is Board Risk Oversight.

What does this reporting mean?

COSO Research on Board Risk Oversight

COSO commissioned a study in 2010 on Board Risk Oversight and found mixed signals about the effectiveness of board risk oversight across organizations.

While many boards of directors **believe** they are performing their risk oversight responsibilities diligently and achieving a high level of effectiveness, a **strong majority** indicate that their boards are <u>not formally executing mature and robust risk oversight processes</u>. Only half of the respondents rated their risk oversight process in their organizations as effective.

Results of COSO study on reporting to Boards on risk - 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%

COSO Research on Board Risk Oversight-Key highlights

The results of this study revealed a number of areas for improving board risk oversight. These improvements would enable boards to advance the maturity of the risk oversight process. These areas are:

1. Improve the **robustness** of the Risk Oversight Process – Need for **more structured** process for monitoring and reporting key risks to the board
2. Enhance Risk Reporting to the Board – Include **scenario analyses**; a summary of exceptions to management's established policies or limits for key risks; and a summary of significant gaps in capabilities for managing key risks and remediation's for the gaps

COSO Research on Board Risk Oversight-Key highlights

3. Improve the **Risk appetite Dialogue** - While respondents generally indicated they have routine discussions regarding risks that are acceptable for the organization to take, just **14** percent reported that this activity is **sufficient for the board's purposes.**
4. Improve Monitoring of the **Risk Management Process** - According to the results of the study, nearly **two-thirds** of the respondents noted that board monitoring of the organization's risk management process is <u>not done at all</u> or is carried out in an <u>ad hoc</u> manner.

COSO Research on Board Risk Oversight-Key highlights

5. Do more to appraise the Board of **Significant Risk** Matters - Based on the survey's findings, there are opportunities to improve processes to notify the board when the organization has <u>exceeded its risk limits</u>, and to ensure that <u>risk issues are addressed</u> in an appropriate and timely manner
6. Boards to **self-evaluate** the Risk Oversight Process Better and More Frequently - Almost <u>one-third</u> of the respondents noted that the board <u>does not self-evaluate</u> its risk oversight processes to determine if it is meeting its oversight responsibilities, while an additional <u>one-third</u> only do so on an <u>ad hoc</u> basis

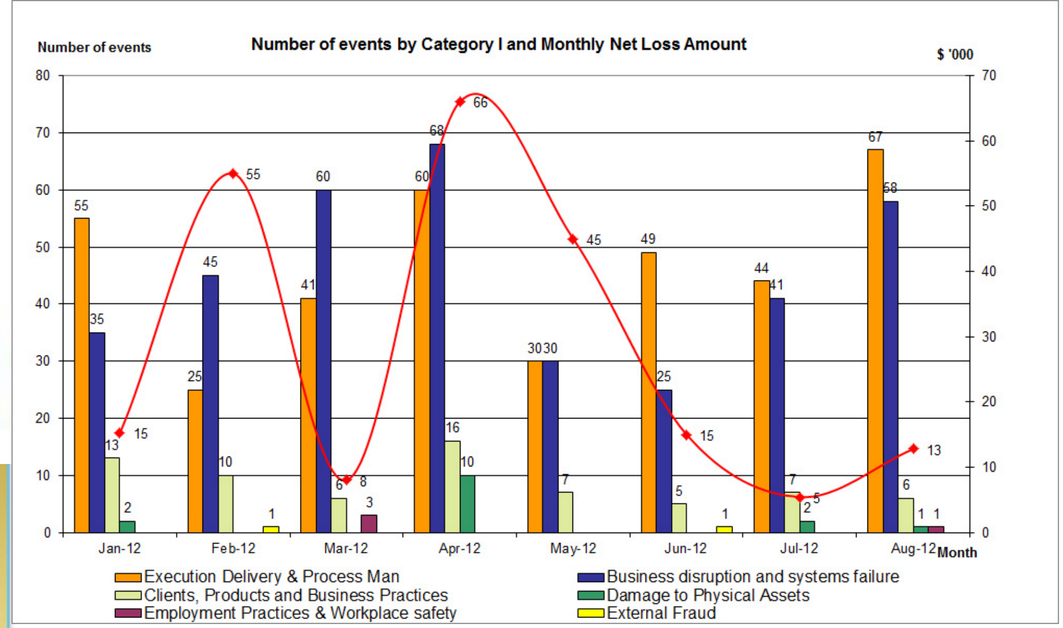
COSO Research on Board Risk Oversight-Key highlights

Conclusion about the study

While many board members perceive that their board's risk oversight process is operating effectively, particularly those directors from larger publicly held organizations, there are opportunities for improvement for most organizations as well as several noted obstacles to be considered.

As Members, we challenge ICPAK to carry out a similar survey for Kenyan organizations to provide a basis of continual improvement that we need on risk oversight.

3. What therefore should be reported to Board about ERM?



What then should board be concerned about with regard to effectiveness of their ERM?

Ensuring best ERM practices is a journey that management and boards need to take together. I will highlight **twelve** specific actions that all boards should consider taking when aiming for best practice.

1. Require from management the establishment of a **top-down ERM program** that addresses key risks across the company and elevates risk discussions to the strategic level
2. Require a **risk heat map** that identifies and collates exposures across the company, reveals linkages between exposures, and identifies fundamental risk drivers
3. Require an in-depth, prioritized analysis of the **top three to five risks** that can really make or break the business—the company's "big bets" and key exposures

What then should board be concerned about with regard to effectiveness of their ERM? …Cont'd

4. Require integrated, multi-factor **scenario analysis** that includes assumptions about a wide range of economic and business-specific drivers
5. Establish a board-level risk review process and require from management insightful risk reports
6. Establish a clear understanding of **risk capacity** based on metrics that management can measure and track
7. Produce a strategy statement that clarifies risk appetite, risk ownership, and the strategy to be used for the company's key risks
8. Require management to formally **integrate risk thinking** into core management processes, e.g., strategic planning, capital allocation, and financing

What then should board be concerned about with regard to effectiveness of their ERM? …Cont'd

9. Clarify **risk governance** and risk-related committee structures at board level, and review board composition to ensure effective risk oversight
10. Define a **clear interaction model** between the board and management to ensure an effective risk dialogue
11. Require that management conduct a <u>diagnostic</u> of the organization's <u>risk culture</u> and formulate an approach to address gaps
12. Review top management's compensation structure to ensure <u>performance</u> is also <u>measured</u> in light of <u>risks taken.</u>

4.0 Discussions (Q & A) and close

My Contacts

Phares Chege
Head of Internal Audit
Higher Education Loans Board
18th Floor, Anniversary Towers University Way –
Nairobi, Kenya
P.O. Box 69489-00400
Cell: **+254 721 411 504/ +254 733 411 504**
Email: pchege@helb.co.ke
Website: http://www.helb.co.ke

Thank you
for your participation!

COFFEE/ TEA BREAK