



# **New York IIA Chapter - Workshop**

## ***Enterprise Risk Management (ERM) and Governance: Leading Practices***

January 15, 2010

**ADVISORY SERVICES**

# Discussion Topics

## Risk Management

- ◆ Enterprise Risk Management: Importance of Fundamentals
- ◆ Areas Presenting Challenge and Gaining Focus – Leading Practices

## Risk Governance

- ◆ Emerging Ideas in Risk Governance
- ◆ Linking Enterprise Risk Management to the Internal Audit Function

## Linking ERM to the Internal Audit Functions

## Linking ERM to Governance, Risk and Compliance (GRC)

### Appendix

#### A. Board vs. Management View – Survey Highlights

# ***Enterprise Risk Management: Importance of Fundamentals***

# Enterprise Risk Management: Importance of Fundamentals Drivers

## ERM Drivers

Governance

Strategy

Performance

### Governance

- Meet NYSE listing requirements that the audit committee must discuss policies with respect to risk assessment and risk management
- Meet SEC requirements: 10-K description of “Risk Factors” in plain English
- Meet credit rating agencies’ expectations with regards to risk, to ensure “no surprises” culture
- Meet proposed SEC proxy rules regarding the disclosure of risk decisions made in connection with compensation policies, director qualifications and governance structure
- Meet Shareholder Bills of Rights regulation, which has proposed for more board accountability, including the establishment of a board-level risk committee

### Strategy

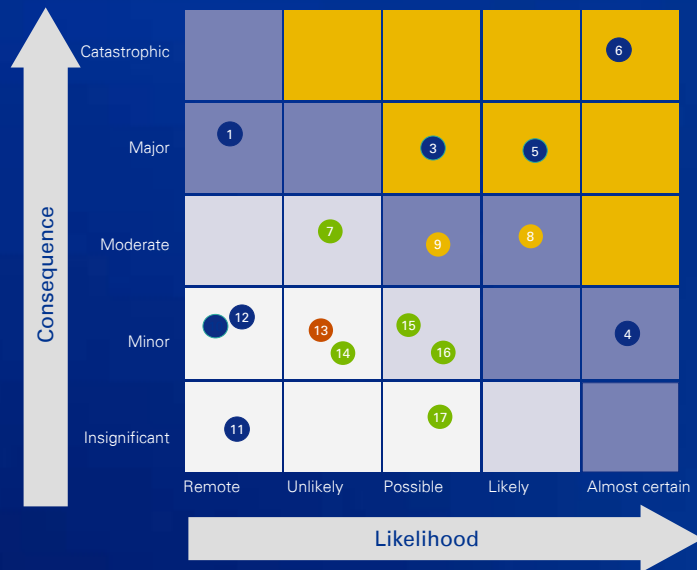
- Beyond regulation: provides a competitive advantage versus industry peers
- Re-align strategy through evaluation of prioritized risks
- Link to risk: cannot develop strategy without understanding enterprise risks

### Performance

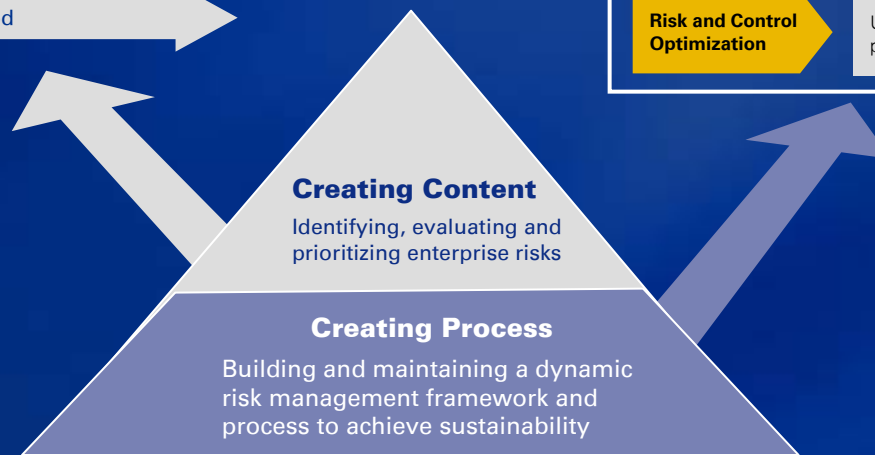
- Improve accountability and transparency through coordinated enterprise risk monitoring and reporting, including risk mitigation strategies
- Reduce cash flow volatility using derivatives, insurance or improved controls
- Reduce costs through risk consolidation and cross-functional efficiencies

# Enterprise Risk Management: Importance of Fundamentals

## The Basics



KPMG ERM Framework	
Framework Element	Description
Risk Governance	Establishment of approach for developing, supporting, and embedding the risk strategy and accountabilities
Risk Assessment	Identifying, assessing, and categorizing risks across the enterprise
Risk Quantification and Aggregation	Measurement, analysis, and consolidation of enterprise risks
Risk Monitoring and Reporting	Reporting, monitoring, and assurance activities to provide insights into risk management strengths and weaknesses
Risk and Control Optimization	Using risk and control information to improve performance



***Risk Management:  
Areas Presenting Challenge  
and Gaining Focus – Leading Practices***

# Risk Management: Areas Presenting Challenge and Gaining Focus – Leading Practices

ERM Capabilities	Trend
<b>I</b> <b>Identifying, focusing and responding to the right risks</b> <ul style="list-style-type: none"> <li>Identifying and responding to the most significant risks</li> <li>Focusing attention on areas needing mitigation or optimization</li> </ul>	<ul style="list-style-type: none"> <li><i>Linking Risk to Strategic Planning</i></li> <li><i>Using Scenario Analysis to Focus on Emerging Risks</i></li> </ul>
<b>II</b> <b>Right level of controls (Control Portfolio Optimization)</b> <ul style="list-style-type: none"> <li>The right level of controls executed by the right people with the right information from the right system</li> </ul>	<ul style="list-style-type: none"> <li><i>Aiming to Contribute to Improved Business Performance</i></li> <li><i>Understanding Risk Appetite and Thresholds: The Cornerstone of Risk Management</i></li> </ul>
<b>III</b> <b>Risk management structure and governance</b> <ul style="list-style-type: none"> <li>Accountability and assurance</li> <li>Reporting to management and Board</li> </ul>	<ul style="list-style-type: none"> <li><i>Clearly Defining Roles and Responsibilities in Risk Governance</i></li> <li><i>Consideration for a Risk Executive or Equivalent</i></li> <li><i>Reconciling Compensation Policies with Risk Taking</i></li> </ul>
<b>IV</b> <b>Risk culture</b> <ul style="list-style-type: none"> <li>The organization's culture facilitates and embraces the sharing of risk information</li> </ul>	<ul style="list-style-type: none"> <li><i>Understanding Risk Culture and Its Impact on a Risk Management Program</i></li> <li><i>Targeted Risk Management Communication, Awareness and Training Programs</i></li> </ul>
<b>V</b> <b>Value added risk and compliance processes</b> <ul style="list-style-type: none"> <li>Structuring the risk and compliance activities to obtain more value and be more cost effective</li> <li>Reducing redundancy and costs and increase efficiency</li> </ul>	<ul style="list-style-type: none"> <li><i>An Approach to Valuing ERM</i></li> <li><i>Considering the Convergence of Governance, Risk and Compliance</i></li> </ul>



# Identifying, Focusing and Responding to the Right Risks

## Linking Risk to Strategic Planning: Example

**Example Only**

Strategic Objective or Significant Change	Risks that Threaten Strategic Objectives	Risk Category	Risk Direction	Management Plan (e.g., avoid, reduce likelihood, reduce impact, transfer, retain)	Outcomes / Impacts						Accountability for Actions to Manage Risks				
					Cash Flow	Profit and Loss	Legal and Regulatory Matters	Innovation	Quality	Reputation	Communication	Measurement	Standardization	Process	
1) Acquire attractive business line	a) Lack of due diligence leads to a misunderstanding of the acquired company's operating results and metrics	Finance and Treasury	↑	Avoid			√		√	√		AB	AB	AB	
	b) Limited market share growth to the overall company as a result of the acquisition	Strategic	→	Retain	√	√				√		CD		XY	
	c) Inability for Company X to finance the acquisition due to uncertain liquidity and current liquidity reserves	Finance and Treasury	→	Reduce Likelihood	√	√	√			√		AB			
	d) More stringent laws and regulations in mergers and acquisitions may lead to reputational impact and regulatory sanctions	Compliance	→	Reduce Likelihood			√	√		√				XY	
	e) Increase in competition to acquire a company may lead to potential overbidding and long-term financial loss	Finance and Treasury	→	Transfer	√	√	√			√		XY			CD
2) Integrate acquired business into existing organization	a) Lack of innovation and new product development decreases market share and stakeholder confidence	Operating	→	Reduce Impact	√	√		√	√	√					CD
	b) Inability of management of acquired company to adapt to Company X business culture	Operating	→	Reduce Impact			√	√	√	√		CD		CD	AB
	c) Inability to succeed at transforming a company with low profit margins at the time of acquisition	Operating	↑	Retain	√	√				√		XY	XY		AB

# Right Level of Controls (Control Portfolio Optimization)

II

## *Understanding Risk Appetite and Thresholds: The Cornerstone of Risk Management*

### Quantitative Risk Appetite Measurement Examples

- ◆ Capital adequacy
- ◆ Earnings volatility
- ◆ Credit rating
- ◆ Other external ratings
- ◆ Market capitalization

### Qualitative Risk Appetite Measurement Examples

- ◆ Reputational impact
- ◆ Management effort
- ◆ Regulatory compliance

1. Organizational Strategic Objectives

2. Align risk profile to business and capital management plans

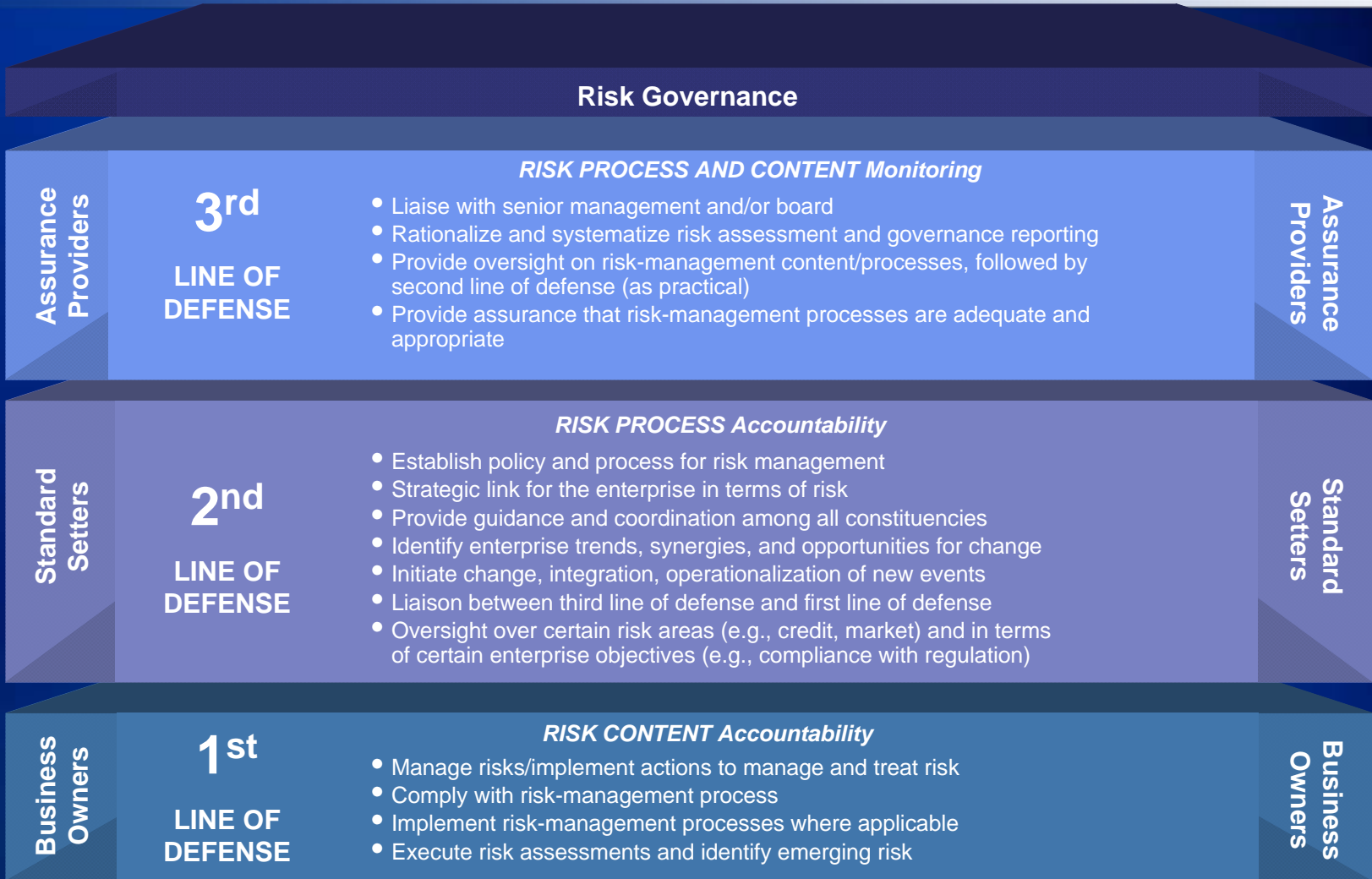
3. Determine risk thresholds

4. Formalize and ratify a risk appetite statement



# Risk Management Structure and Governance

## *Clearly Defining Roles and Responsibilities in Risk Governance*



## Risk Culture

### IV

## *Understanding Risk Culture and Its Impact on the Risk Management Program*

The first step to asserting and understanding the importance of risk culture is to begin a dialogue within the organization on the topic. Below are some key questions that can be asked and discussed with management:

- What's the true 'tone at the top' – and 'in the middle'?
- Is there effective and continuous communication around ethics and risk?
- Are employees incentivized to 'do the right thing'?
- Is risk formally considered during decision-making?
- How does your risk culture extend beyond your organization?
- Does your organization consider risk in its hiring process?
- Does your organization understand the geopolitical structure and dispersion of the various businesses?

V

# Value Added Risk and Compliance Processes

## *An Approach to Valuing ERM*

### *Common approaches for valuing ERM programs or program components*

**Assessing  
capital costs**

**Identifying  
avoided losses  
from industry or  
company risk events**

**Assessing  
total compliance  
program costs**

**Assessing  
earnings variability  
before and after  
risk mitigation**

**Assessing hedging  
or insurance costs**

**Identifying the “flip-  
side” of risk (or the  
investment  
opportunities for  
each risk)**

# ***Emerging Ideas in Risk Governance***

# Emerging Ideas in Risk Governance

## *Recent Developments*

- ◆ **The finalized SEC rule amendments to an organization's proxy statement for 2010 include:**
  - Compensation Policies: If the risks arising from a company's compensation policies or practices could have a material effect on the company's overall risk exposure, adequate disclosure around overall compensation policies, compensation incentives that affect risk-taking, adjustment of compensation in light of risk issues, and the company's assessment of such risks will need to be disclosed.
  - Director Qualifications: Additional detail regarding disclosure relative to directors qualifications, including skills (e.g., risk assessment skills) that qualify the person to be a director will need to be included.
  - Leadership Structure: Adequate disclosure of a company's leadership structure (e.g., separation of Chairman of the Board and CEO) and why such structure is the best arrangement for the company needs to be included.
  - Board Oversight: A description on the board's role in risk oversight would be required (i.e., risk management is the responsibility of management, subject to the oversight and direction of the Board).
- ◆ **The Shareholder's Bill of Rights, which has been recently introduced in the Senate, calls for more board accountability, including the establishment of a board-level risk committee, and directly links failures in corporate governance with the financial crisis.**

# Emerging Ideas in Risk Governance

## 1 Structure – Risk Content

- ◆ Full Board may have overall oversight responsibility. Standing committees may assist in addressing risk content inherent in their respective areas of oversight (e.g., financial risk allocated to audit committee).

## 2 Structure – Risk Process Sustainability

- ◆ A board level committee (e.g., Audit Committee) may add value to oversee the ERM process. It may regularly review the oversight objectives and oversight processes, which facilitate risk information flow / frequency and understand the related information types / sources to foster proper risk oversight and meaningful challenge. Alternatively, organizations may nominate a a board level risk committee comprised of independent directors and align with the proposed Shareholder’s Bill of Rights.

## 3 Process – Monitor Critical Alignments (Strategy – Risk – Performance)

- ◆ Board may regularly monitor management’s process to identify and link changes between strategy, risks / controls and incentives with consideration for company culture / performance.

## 4 Process – Risk Appetite

- ◆ Board oversight may include a clear understanding, agreement and approval of management’s risk appetite.

## 5 Competencies

- ◆ Board skills may be evaluated commensurate with the risk complexity and company agility and composition or skill enhancement / education considerations are made accordingly.

# Emerging Ideas in Risk Governance

## Risk Governance

### Responsibilities

Oversight of:

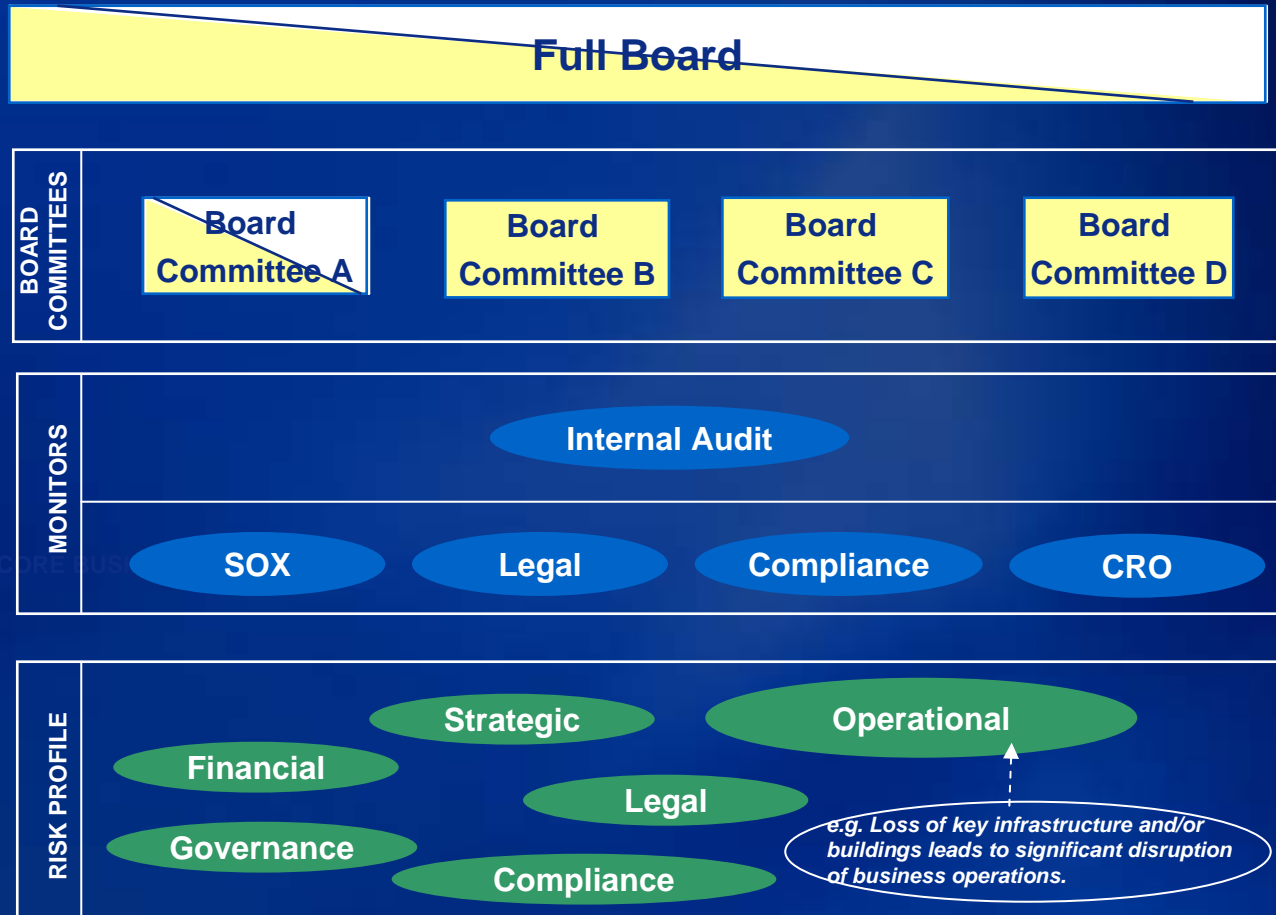
Risk Content

Risk Process

Provide **Assurance**

- over:
- Achieving business objectives
  - Mitigating/Managing risks
  - Controls operating effectively

Risk Owners manage and identify the risks



# Emerging Ideas in Risk Governance

## Reporting Risk Management Progress to Facilitate Board Challenge

No.	Risk Description	Risk Inter-relationship-Scenario Analysis	Strategy Link (Strategy Objective#)	Risk Direction	Overall Current Score (*)	Risk Ownership	Board Oversight
1	Failure to develop new products in a highly competitive market may inhibit the future growth and success of the company	6,10	Product Innovation	↑	Green	Strategy	Com A
2	Past and future acquisitions and integrations within the industry may result in a loss of assets and increase pressure on the company	6, 10	Capital Growth	↑↑	Green	Strategy	Com B
3	Inability to control patterns and behaviors of consumer spending	8, 9, 13	Cost Reduction	↓	Yellow	Strategy	Com B
4	Loss of key infrastructure and / or buildings leads to significant disruption of business operations	16, 22	Capital Growth	↑	Yellow	Operations	Com A
5	Inability to attract and retain key talent	15	Global Expansion	↑	Red	HR	Com B
6	Dependency on key vendors for timely and effective sourcing of products may reduce quality of products received	1,2	Global Expansion	→	Green	Operations	Com B
7	Unanticipated fluctuations in foreign currency may have an adverse affect on the company's financial results	11, 12	Financial Stability	↓	Red	Legal	Com C
8	Changes in, or interpretations of, accounting principles, laws, regulations, or government policies, especially in the Internet and e-commerce, could result in unfavorable accounting charges	3, 25, 30	Compliance	→	Yellow	Legal	Com D
9	Lack of legal and/or technical protections for the company's intellectual property rights may adversely affect the company's results	3, 15, 21, 25	Innovation	→	Green	Finance	Com D
10	Defective products may expose the Company to increased liability in excess of its insurance coverage and may lead to financial loss and reputation damage	1, 2, 18	Innovation	↑	Yellow	Finance	Com D

**Example Only**

✓ Stress tested

Definitions of Risk Direction:	
→	No change in risk direction
↑	Risk is increasing
↓	Risk is decreasing

(*)	Risk Score
Red	Needs Improvement
Yellow	Minor improvements
Green	Adequately managed



# ***Linking Enterprise Risk Management to the Internal Audit Function***

# Overview of Risk Oversight and Monitoring Roles and Responsibilities

## Board/ Related Committee(s) *Monitor Effectiveness*

### Internal Audit

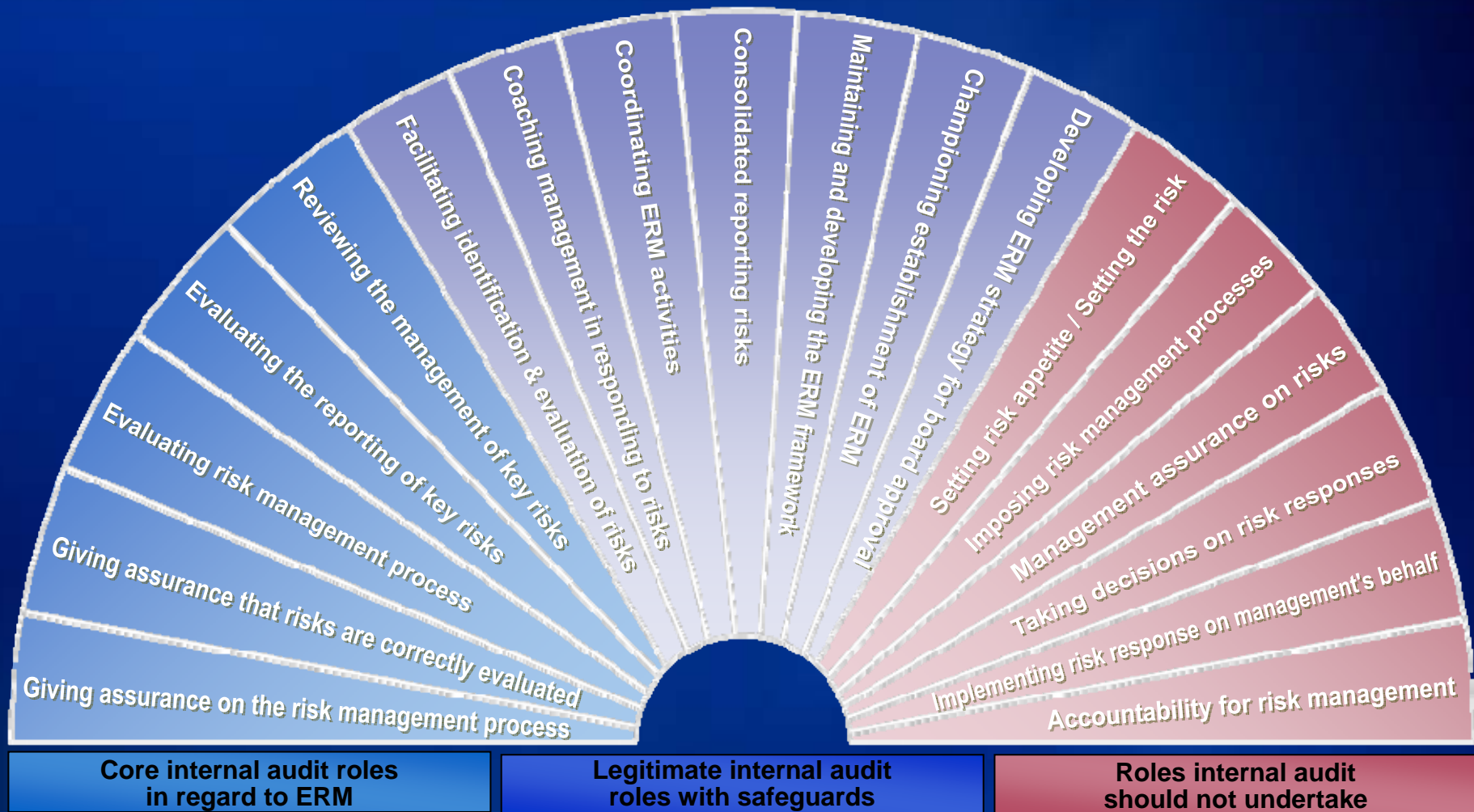
#### *Provide independent evaluation*

- Feedback mechanism as to whether all key risks have been identified, accurately measured and effectively controlled
- Monitoring and evaluating effectiveness of ERM process
- Align internal audit plan and procedures with top risks
- Oversight on risk and control for audit committee
- Role evolves as ERM iteratively takes shape

**Risk Management Process Accountability**  
*(Risk Sponsor and Risk/Management Committee)*  
**Oversee completeness and quality of risk management framework and policy activities**

**Risk Content Accountability**  
*(Risk Owners)*  
*(e.g., Legal / Compliance / Finance / HR / Operations)*  
**Implement and report on risk management actions**

# Internal Audit's Role in ERM

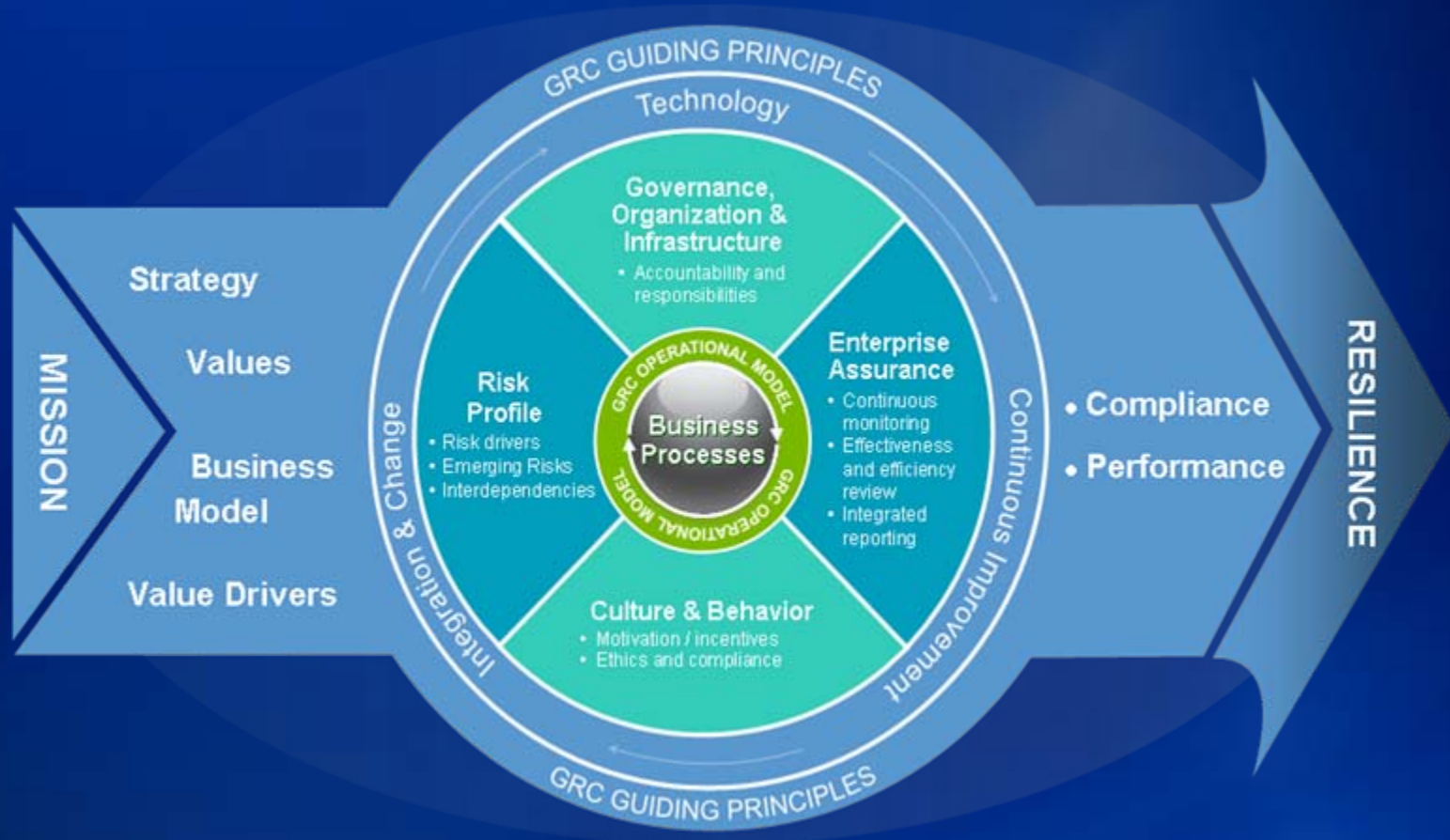


Source: IIA UK and Ireland

# Linking ERM to Governance, Risk and Compliance (GRC)

# KPMG's Holistic Model for GRC

KPMG's Holistic Model for GRC provides an integrated approach for developing and establishing a successful and sustainable GRC Framework within the organization.



# Appendix

# Appendix A: Board vs. Management View – Survey Highlights\*

## 1 Board / Audit Committee Driving Risk Management Program

- More than a third (38%) of internal audit respondents cited the key driver to adopt their risk management program to be the Board / Audit Committee interest and recommendation

## 2 Lack of Training

- One-third of respondents said their senior executives have had no training or formal guidance around risk management
- Only 16% receive frequent (i.e., at least annual) training

## 3 Little Understanding of how to Assess Risk Exposures

- More than half of respondents (58%) said their employees had little or no understanding of how risk exposures should be assessed for likelihood and impact

## 4 Lack of Technology

- Only a quarter of respondents apply technology into their risk management program
- Just a quarter of respondents said they were considering technology

## 5 Redundancies in Risk Assessments

- One third of internal audit respondents have made no efforts to reduce potential redundancies in competing risk assessments
- Just 13% of internal audit respondents have consolidated risk assessments;
- Only 14% have established one governance and oversight function (i.e., risk committee), or use templates with common assessment questions across organizations

*\*KPMG conducted the surveys at the 2008 National Association of Corporate Directors Conference, and at the 2008 Institute of Internal Auditors International Conference. The approximately 130 respondents included a mix of senior internal audit executives and board members across all industries*

## Presenter's Contact Details

**Deon Minnaar**  
**Partner, KPMG LLP**  
**(212) 872-5634**  
**[deonminnaar@kpmg.com](mailto:deonminnaar@kpmg.com)**

*All information provided is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.*