Risk Based Approach

Practice in financial institutions

ADVISORY / FINANCIAL SERVICES
Risk Management Models

COSO II - ERM Framework

ISO 31000

Lines of Defence
Risk Management Models – What is risk?

- **KPMG**
  - Risk relates to strongly adverse outcomes of uncertain (commercial) processes.

- **The Shorter Oxford Dictionary defines risk as:**
  - Hazard, danger, exposure to mischance or peril
  - The chance of hazard or commercial loss, specifically in the case of insured property or goods

- **Mathematician Bernoulli (1738):**
  - A risk is a random variable

- **Diekman**
  - Risk is an uncertain event causing non achievement of objectives set by an organisation
Enterprise Risk Management

“ERM is expected to become widely accepted by companies and other organisations and all stakeholders and interested parties”

COSO – Committee of Sponsoring Organizations of the Treadway Commission
(September 2004)
Risk Management Models - COSO

Risk Analysis

- Risk is a combination of the probability of an event and its consequence
- An event is the occurrence of a particular set of circumstances (e.g. market developments, acts of institutions or individuals, functioning of technical systems)
- A consequence may be positive or negative and may be expressed qualitatively or quantitatively
Risk Management Models - COSO

Risk response

- Insure
- Share (JV, alliances, partnership)
- Outsource
- Diversify/spread
- Hedge

- Stop activities
- Withdraw from market
- Divest
- Adapt objectives
- Decrease scale

To reduce risk adapt:
- Organisation
- People
- Governance
- Operational
- Monitor

- Just accept
- Finance consequences
- Build in back ups
ISO 31000

- New *(December 2009)* ISO Standard aimed at managing risk in a structured way

- Applicable on all kind of organisations

- ISO 31000 - a systematic and logical approach to Risk Management
ISO 31000

Systematic and logical approach

- Communication and consultation during the process
- Establishing an infrastructure for
  - Identification
  - Analysis
  - Evaluation
  - Treatment
- Focused monitoring and review of risk
- Recording and reporting of risk
ISO 31000

a) Creates value
b) Integral part of organizational processes
c) Part of decision making
d) Explicitly addresses uncertainty
e) Systematic, structured and timely
f) Based on the best available information
g) Tailored
h) Takes human and cultural factors into account
i) Transparent and inclusive
j) Dynamic, iterative and responsive to change
k) Facilitates continual improvement and enhancement of the organization

Principles (Clause 3)

Framework (Clause 4)

Process (Clause 5)
Risk Management

Overall Responsibility of the Board of Management

- Appropriate business processes
- Definition of business and risk strategies
- Assessment of risks
- Establish adequate internal control processes
- Measures to limit risks

The responsibility for the determination of strategies cannot be delegated!
Lines of Defence

Regulators

Audit Committee

1st line
Role:
• Strategy
• Execution
• Monitoring

2nd line
Role:
• Oversight and support
• Preparing standard setting (Legal, Compliance, Risk, Finance, HR)

3rd line
Role:
• (Internal) Audit
• Provide assurance to executive mgmt and audit committee

Senior Management
In charge of control functions

Executive Board

Stakeholders
GRC – A Holistic Model

Business Performance

GRC Measures

Integrated Reporting, Performance and Compliance

The presentation and the accompanying slides are provided solely for the benefit of the parties identified in the engagement letter and are not to be copied, quoted, or referred to in whole or in part without KPMG's prior written consent. KPMG accepts no responsibility to anyone other than the parties identified in the engagement letter for the information contained in this presentation. © 2010 KPMG Advisory N.V., registered with the trade register in the Netherlands under number 33263682, is a subsidiary of KPMG Europe LLP and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (‘KPMG International’), a Swiss entity. All rights reserved. Printed in the Netherlands.
KEY OBJECTIVES

Compelling reasons to drive towards an integrated GRC approach

• Proven tools and methodologies are available

• Major internal obstacles to overcome

• Early benefits are easy to realise
DISCUSSION OUTLINE

- What is governance, risk and compliance (GRC)
- Driving forces for change
- Barriers to implementation
- What we are seeing in the market
- Benefits – tactical and strategic
- Conclusions
GOVERNANCE, RISK AND COMPLIANCE (GRC)

**What it is**
- Starts with understanding strategic objectives, mission, business value and business model
- Comprehensive view of the oversight functions
- Converging risk related information from various oversight functions
- Encompasses people, processes and technology considerations

**What it is NOT**
- Not just a technology solution, but frequently involves technology enablement
- Not just another name for enterprise risk management
- Does not eliminate the need for or consolidate existing functions (e.g., compliance, audit, SOX)
- Not just conceptual – Must be practical
Board would like increased visibility into risk, compliance and governance process, especially given ongoing transformation efforts

Control environments are still heavily manual despite all our investment in technology. They are not taking advantage of ERP functionality and automated controls

Lack a centralised approach to managing and monitoring risks and controls within the organisation

Regulations are managed independently resulting in a cumbersome, redundant, and expensive approach

Ineffective, scattered approach to risk, compliance and governance

Looking for a solution that will bring down the amount of manual controls and increase automated controls

Rationalise information to drive business results
<table>
<thead>
<tr>
<th>Driving Forces - Changing Landscape</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overall business complexity</td>
<td>44%</td>
</tr>
<tr>
<td>Desire to reduce exposure of organisation to risks</td>
<td>37%</td>
</tr>
<tr>
<td>Desire to improve corporate performance</td>
<td>32%</td>
</tr>
<tr>
<td>Concern to avoid ethical and reputational scandals</td>
<td>32%</td>
</tr>
<tr>
<td>Expected regulatory intervention</td>
<td>21%</td>
</tr>
<tr>
<td>Concern about greater risk from non-compliance</td>
<td>20%</td>
</tr>
<tr>
<td>Increasing focus on governance from internal and external stakeholders</td>
<td>18%</td>
</tr>
<tr>
<td>Greater focus on corporate social responsibility</td>
<td>15%</td>
</tr>
<tr>
<td>Desire to reduce cost base</td>
<td>14%</td>
</tr>
<tr>
<td>Desire to improve agility in decision-making</td>
<td>10%</td>
</tr>
<tr>
<td>Increased use of outsourcing and off-shoring</td>
<td>8%</td>
</tr>
<tr>
<td>Increased technological complexity</td>
<td>8%</td>
</tr>
<tr>
<td>Increasing risk incidents</td>
<td>6%</td>
</tr>
<tr>
<td>More stringent requirements from rating agencies</td>
<td>6%</td>
</tr>
<tr>
<td>None of the above – we are not interested</td>
<td>1%</td>
</tr>
</tbody>
</table>

Source: The Convergence Challenge
Feb. 2010, Economist Intelligence Unit
DRIVING FORCES - DUPLICATION AND REDUNDANCY

73% of companies have seven or more separate risk functions

67% reported that they have overlapping risk coverage with two or more risk functions

50% of companies reported gaps in their coverage between risk functions

62% of companies believe they can get more risk coverage for less spend

Source: The future of risk, protecting and enabling performance
Economist Intelligence Unit, 2009
DRIVING FORCES - FRAGMENTATION PUZZLE

Operational Risk | Policy Management | Internal Audit | Enterprise Risk | Business Continuity

IT Governance | Compliance | Financial Controls | Corporate Responsibility | Fraud Management
Increasing (legal) requirements result in increasingly complex financial sector structures

- Business and risk management processes have multiples connections with the business and supporting departments
- Business is often asked to provide ad hoc information in different formats and different intervals
- Insufficient consistency and reliability between information derived from different silos in the organisation
### Significant barriers to greater GRC acceptance

<table>
<thead>
<tr>
<th>Barriers to Entry</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resistance to change</td>
<td>44%</td>
</tr>
<tr>
<td>Complexity of convergence process</td>
<td>39%</td>
</tr>
<tr>
<td>Lack of human resources/expertise</td>
<td>36%</td>
</tr>
<tr>
<td>Too many other priorities</td>
<td>34%</td>
</tr>
<tr>
<td>Lack of accountability</td>
<td>23%</td>
</tr>
<tr>
<td>Lack of clarity around potential benefits</td>
<td>23%</td>
</tr>
<tr>
<td>Lack of financial resources</td>
<td>14%</td>
</tr>
<tr>
<td>Lack of support from leadership</td>
<td>13%</td>
</tr>
<tr>
<td>Geographic dispersion of organisation</td>
<td>13%</td>
</tr>
<tr>
<td>Inadequate technology</td>
<td>9%</td>
</tr>
<tr>
<td>Concern about potential drawbacks</td>
<td>6%</td>
</tr>
<tr>
<td>Other, please specify</td>
<td>1%</td>
</tr>
</tbody>
</table>

Source: The Convergence Challenge
Feb. 2010, Economist Intelligence Unit
WHAT WE ARE SEEING IN THE MARKET
A GRC HOLISTIC MODEL

Source: KMPG LLP 2009
KPMG’s GRC Holistic Model®
WHAT WE SEE IN THE MARKET
COMMON SHARED CONTEXT

- Setting the organisation structure and legal environment
- Knowledge is organised into contexts
- Specialists usually organise GRC in a similar way
WHAT WE SEE IN THE MARKET
A COMMON GRAMMAR FOR RISK AND CONTROL

- Taxonomies for risk, control, and consequence

ROOT CAUSE
BROKEN SHOELACE

RISK
TRIP AND FALL

CONSEQUENCE
SPRAINED WRIST

DOWNSTREAM EFFECT
MEDICAL BILLS

COSO CONTROL
Control Environment
Monitoring
Info and Communication
Risk Management
Control Activity

COSO RISK EVENTS
Economic
Natural Environment
Political
Infrastructure
Personnel

COSO OBJECTIVES
Strategic
Operational
Financial
Compliance
WHAT WE SEE IN THE MARKET

CALIBRATED APPROACH

1. Identify/Assess Context
2. Assign Business Processes
3. Assess Process Risks
4. Manage Process Risks
5. Identify Issues
6. Create Action Plans
7. Assess KPI/KRI Results
8. Organisation/Process Certification

2. Identify critical processes in high risk orgs/accounts. Identify KPI’s.
3. Discover and rate process risks. Identify high risk issues. Identify KRI’s for high risks.
4. Identify and assess controls where high risks are mitigated. Create issues to remediate.
5. Do issues explain process performance gaps? If not, reassess risks and controls.

7. If KPI’s or KRI’s are outside range, update risks, controls and issues to explain gaps.
WHAT WE SEE IN THE MARKET
BEST PRACTICES

Change management requires an executive sponsor and individual champions

A phased in approach works best
- Start with 2-3 groups (e.g., audit, SOX ORM)
- Don’t try to forcefully win over skeptics but keep them informed or involved

Plan for quick wins (e.g., common issue tracking or calibrated risk assessment)

Consider entity-wide reporting requirements vs. siloed
- Board and senior management requirement

Don’t start with a technology solution
- Consider options throughout planning and scoping
- Enable processes with technology – keep it simple

Link to business performance
- Understand key performance indicators from a business perspective

Redefine GRC performance indicators and mission
- Measure the creation of knowledge and quantify benefits from collaboration
BENEFITS
MEASURING TACTICAL SUCCESS

• All reporting from a single data source – no inconsistencies or reconciliations

• Common grammar of risk and control makes knowledge searchable

• Common calibrated methodology allows professionals to collaborate and rely on each others work

• Reduced footprint on business

• Control testing is efficient – one test for multiple needs

• Control design efficiency – reduce redundant controls, better link to risk
BENEFITS
MEASURING STRATEGIC SUCCESS

- Transparent
- Reliable
- Timely
- Relevant
KEY TAKEAWAYS

Compelling reasons to drive towards an integrated GRC approach

- Reducing complexities, leveraging results, reducing duplication / redundancy, and improved reporting

- **Proven tools and methodologies are available**
  - Common risk and control models
  - Standardised workflows showing integration opportunities
  - Flexible and proven technologies (e.g., Paisley GRC)

- **Major internal obstacles to overcome**
  - Reluctance to change
  - Time and financial investment
  - Multi-year initiative

- **Early benefits are easy to realize**
  - Quick wins are available
  - Longer term value
Prof. Dr. Peter Diekman RA
Partner
KPMG Risk & Compliance
Diekman.Peter@kpmg.nl
Tel  +31 20 656 7958
Cell +31 651 52 7383