Enterprise Risk Management (ERM)

You can provide value to your organization by effectively managing business risks.

Overview of ERM presentation

- What is ERM?
- Why is it important?
- Risk oversight objectives and principles
- Steps in ERM process
- ERM process: What does ERM look like?
- KPMG’s ERM vision
- ERM questions to ask your organization
- Q&A
What is ERM (Enterprise Risk Management)?

“ERM 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”


ERM fundamental concepts (COSO)

Enterprise Risk Management is:
- A process, ongoing and flowing through an entity
- Effected by people at every level of an organization
- Applied in strategy setting
- Applied across the enterprise, at every level and unit, and includes an entity-level portfolio view of risk
- Designed to identify potential events that, if they occur, will affect the entity, and to manage risk within its risk appetite
- Able to provide reasonable assurance to an entity’s management and board of directors
- Geared to achievement of objectives in one or more separate but overlapping categories.
Why is ERM important?

Assessment and management of risks is vital in order to:

- Protect reputation and brand
- Anticipate emerging risk
- Meet regulatory and governance requirements
- Meet market constituents needs
- Enhance risk awareness and accountability, and facilitate decision making in connection with risks
- Provide a platform to understand ALL risk types (strategic, operational, compliance, investment, emerging) and their interrelationships, and therefore, manage them more effectively.

Bottom line:

“Every organization faces various business risks each day and they have limited time and resources to address them, so the organization needs a risk management strategy and an ongoing process to identify, evaluate and effectively mitigate those risks.”

Why are organizations focused on ERM?

Standard & Poor’s seven questions for companies

1. What are the company’s top risks, how big are they, and how often are they likely to occur? How often is the list of top risks updated?
2. What is management doing about the top risks?
3. What size of quarterly operating or cash loss has management and the board agreed is tolerable?
4. Describe the staff responsible for risk management programs and their place in the organization chart. How do you measure the success of risk management activities?
5. How would a loss from a key risk affect incentive compensation of top management and planning/budgeting?
6. What discussions about risk management have taken place at the board level or among top management when strategic decisions were made in the past?
7. Give an example of how your company responded to a recent “surprise” in your industry. How did the surprise end up affecting your company differently than others?”
National association of corporate directors risk oversight objectives

While objectives vary from entity to entity, every organization should satisfy itself that:

- Expected risks are commensurate with expected rewards
- The risk appetite implicit in the organization’s business strategy is appropriate
- Management has implemented a system to manage risk, and the system is appropriate given the strategy
- The risk management system operates to inform those charged with governance of the major risks facing the organization
- An appropriate culture of risk-awareness exists throughout the organization
- There is a recognition that management of risk is essential to the execution of the organization’s strategy.

NACD: 10 principles of effective risk oversight

1. Understand the organization’s key drivers of success.
2. Assess the risk in the organization’s strategy.
3. Define the role of those charged with governance with regard to risk oversight.
4. Consider whether the organization’s risk management system—including people and processes—is appropriate and has sufficient resources.
5. Work with management to understand and agree on the types (and format) of risk information those charged with governance require.
6. Encourage a dynamic and constructive risk dialogue between management and those charged with governance, including a willingness to challenge assumptions.
7. Closely monitor the potential risks in the organization’s culture and its incentive structure.
8. Monitor critical alignments—of strategy, risk, controls, compliance, incentives, and people.
9. Consider emerging and interrelated risks: What’s around the next corner?
10. Periodically assess risk oversight processes: Do they enable the organization to achieve its risk oversight objectives?
Steps in ERM process: Developing an enterprise risk inventory

The risk inventory is developed for the entity by:

- Interviewing key management officials
  - Operational, legal, risk management, financial, internal audit, etc.
- Interviewing stakeholders
  - Regulators, bankers, suppliers, vendors, customers, auditors, etc.
- Reading external assessments/reports
  - Rating agency reviews, analyst reports, independent auditors’ reports, regulatory reports, etc.
- Preparing risk inventory
  - Identify risks and group similar risks

Steps in ERM process: Assessing and quantifying enterprise risks

Once risks are inventoried and grouped, they are assigned a risk value (rating scale of 1–5) from two perspectives:

1. **Magnitude of the risk consequence**
   - Insignificant (1)
   - Minor (2)
   - Moderate (3)
   - Major (4)
   - Catastrophic (5)

2. **Likelihood of risk occurrence**
   - Remote (1)
   - Unlikely (2)
   - Possible (3)
   - Likely (4)
   - Almost certain (5)
Steps in ERM process: Evaluating, prioritizing, mitigating and monitoring enterprise risks

After risks have been assigned a risk value:

- Evaluated and prioritized
  - Risks are ranked, plotted to visualize impact, and highlighted on dashboard
- Determined whether they are discrete versus ongoing and controllable or uncontrollable
- Mitigated through risk action plans
  - Improving/enhancing internal controls, purchase insurance/self-insured, implementing various risk management techniques, etc.
- Scenario planning for emerging risks
- ERM is then integrated into strategic and operating plans.
- ERM activities are monitored and optimized to improve performance.
  - Going from project to process to cultural change within the organization

ERM process highlights

Creating Process
Building and maintaining a dynamic risk management framework and process to achieve sustainability

Creating Content
Identifying, evaluating and prioritizing enterprise risks

KPMG ERM Framework

<table>
<thead>
<tr>
<th>Framework Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Governance</td>
<td>Establishment of approach for developing, supporting, and embedding the risk strategy and accountabilities</td>
</tr>
<tr>
<td>Risk Assessment</td>
<td>Identifying, assessing, and categorizing risks across the enterprise</td>
</tr>
<tr>
<td>Risk Quantification &amp; Aggregation</td>
<td>Measurement, analysis, and consolidation of enterprise risks</td>
</tr>
<tr>
<td>Risk Monitoring &amp; Reporting</td>
<td>Reporting, monitoring, and assurance activities to provide insights into risk management strengths and weaknesses</td>
</tr>
<tr>
<td>Risk &amp; Control Optimization</td>
<td>Using risk and control information to improve performance</td>
</tr>
</tbody>
</table>

Top Risks (those that threaten)

1. Strategic Priorities
2. Business Model
3. Corporate Existence

Likelihood
Remote Unlikely Possible Likely Almost certain

4 1 8 9 6

Insignificant Minor Moderate Major Catastrophic

12 11 13 14 15 16 17 10
ERM process: What does ERM look like?

Creating content – Risk categories
Discrete v. ongoing and controllable v. uncontrollable

Risk Category
Catastrophic
Major
Moderate
Minor
Insignificant

Likelihood of Risk Occurrence
Remote
Unlikely
Possible
Likely
Almost certain

Risk Consequence

1. Loss of building, together with key staff or technology infrastructure
2. Adverse changes in law and government affecting the company’s business model
3. Loss of market share or revenue through competition or regulation
4. Introduction of competing products and technologies by other companies
5. Inability to attract and retain key employees
6. Failure to develop global management and information systems
7. Exposure to litigation related to the company’s products/services
8. Insufficient products/services provided resulting in loss of reputation
9. Inability to react to changes in overseas legal, economic, or regulatory environment
10. Increased pricing pressure from competitors and/or customers

Top Ten Risks
1. Loss of building, together with key staff or technology infrastructure
2. Adverse changes in law and government affecting the company’s business model
3. Loss of market share or revenue through competition or regulation
4. Introduction of competing products and technologies by other companies
5. Inability to attract and retain key employees
6. Failure to develop global management and information systems
7. Exposure to litigation related to the company’s products/services
8. Insufficient products/services provided resulting in loss of reputation
9. Inability to react to changes in overseas legal, economic, or regulatory environment
10. Increased pricing pressure from competitors and/or customers

Key to assessment of current actions to manage risks:
(0) Exceed Requirement – The risk management processes have been over-engineered for the level of risk involved.
(1) Meet Requirement – The risk management processes are appropriate for the level of risk identified.
(2) Need Strengthening (Minor) – Minor improvements in the risk management processes are necessary to reach “meet requirements.”
(3) Need Strengthening (Important) – Risk management processes need to be strengthened in important ways to reach “meet requirements.”
(4) Need Strengthening (Critical) – Risk management processes are clearly deficient in critical ways.
(5) Unestablished – Risk management processes have not yet been established. This will most likely be the situation in the case of a new business initiative.
ERM process: What does ERM look like?
Creating content – Dashboard view

<table>
<thead>
<tr>
<th>Risk description</th>
<th>Risk category (M, C, O, I)</th>
<th>Overall current score</th>
<th>UC</th>
<th>DC</th>
<th>DD</th>
<th>Risk direction</th>
<th>Monitoring schedule (IA/compliance)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1) Introduction of competing products and technologies by other companies</td>
<td>S</td>
<td>U</td>
<td>O</td>
<td>D</td>
<td>4</td>
<td>2010</td>
<td></td>
</tr>
<tr>
<td>2) Inadequate production/operations resources or procedures</td>
<td>S</td>
<td>U</td>
<td>O</td>
<td>D</td>
<td>8</td>
<td>2011</td>
<td></td>
</tr>
<tr>
<td>3) Fraud with compensation results in adverse change (e.g., loss of customers)</td>
<td>S</td>
<td>U</td>
<td>O</td>
<td>D</td>
<td>2010</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4) Loss of building together with key staff or technology infrastructure</td>
<td>O</td>
<td>U</td>
<td>D</td>
<td>2012</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5) Inability to attract and retain key talent</td>
<td>O</td>
<td>U</td>
<td>D</td>
<td>2012</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6) Losses associated with currency fluctuations and inability of effectively hedge the company’s exposure</td>
<td>F</td>
<td>U</td>
<td>O</td>
<td>D</td>
<td>2011</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7) Exposure to litigation related to the company’s production/services</td>
<td>F</td>
<td>U</td>
<td>O</td>
<td>D</td>
<td>2012</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8) Reversal change in tax and government affecting the company’s business model</td>
<td>L</td>
<td>U</td>
<td>O</td>
<td>D</td>
<td>6</td>
<td>2011</td>
<td></td>
</tr>
<tr>
<td>9) Inability to react to changes in overseas legal, economic or regulatory environment</td>
<td>L</td>
<td>U</td>
<td>O</td>
<td>D</td>
<td>6</td>
<td>2011</td>
<td></td>
</tr>
<tr>
<td>10) (*) Assessment of actions of manage risk</td>
<td>Exceed Requirement – The risk management processes have been over engineered for the level of risk involved.</td>
<td>Meet Requirement – The risk management processes are appropriate for the level of risk identified.</td>
<td>Need strengthening (Minor) – Minor improvements in the risk management processes are necessary to reach “meet requirements.”</td>
<td>Need strengthening (Important) – Risk management processes need to be strengthened in important ways to “meet requirements.”</td>
<td>Need strengthening (Critical) – Risk management processes are clearly deficient in with critical ways.</td>
<td>Unestablished – Risk management processes have not yet been established. This will most likely be the situation in the case of a new business process.</td>
<td></td>
</tr>
</tbody>
</table>

E.R.M. process: What does ERM look like?
Creating content – Scenario analysis for emerging risks

Purpose: To identify trends and macro-level scenarios that may impact the company and lead to emerging risks and develop action plans to address related potential unfavorable outcomes.

<table>
<thead>
<tr>
<th>Scenario/ Emerging risk</th>
<th>Impact type</th>
<th>Velocity</th>
<th>Materiality</th>
<th>Reputational impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>1) Significant Regulatory Changes</td>
<td>Short-term</td>
<td>Long-term</td>
<td>Immediate</td>
<td>Trend</td>
</tr>
<tr>
<td>2) Systems Failure</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>3) Forced Major (change occurrence beyond your control)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>4) Supply Disruption/Quality</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>5) Employees Related</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>6) Economic Factors</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>7) Technology Breakthrough</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>8) Strategic Business Partner</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>9) Environmental</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>10) Ethical Behavior/Fraud</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
ERM process: What does ERM look like?
Creating process – Risk maturity continuum

<table>
<thead>
<tr>
<th>Framework Element</th>
<th>BASIC</th>
<th>MATURE</th>
<th>ADVANCED</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Remain in Compliance</td>
<td>A Management Process</td>
<td>A Strategic Tool</td>
</tr>
<tr>
<td>Governance</td>
<td>A central risk management policy to support external requirements</td>
<td>A risk management structure with clear accountabilities to support risk management objectives</td>
<td>Risk management accountability integrated with performance management</td>
</tr>
<tr>
<td>Assessment</td>
<td>Annual risk assessment with limited analysis and interpretation</td>
<td>Frequent risk assessment in line with normal management reporting and including analysis</td>
<td>Risk and control activities embedded in business processes</td>
</tr>
<tr>
<td>Quantification and Aggregation</td>
<td>Quantification of market and credit risks</td>
<td>Quantification of operational risk; advanced quantification of market and credit risk</td>
<td>Entitywide aggregation across all risk areas</td>
</tr>
<tr>
<td>Monitoring and Reporting</td>
<td>Business risk reporting designed to support external requirements</td>
<td>Extensive reporting to the board and audit committee on current risk levels and future risk issues</td>
<td>Alignment of all risk reporting to provide a comprehensive single view of risk</td>
</tr>
<tr>
<td>Risk and Control Optimization</td>
<td>Fewer surprises through management of key risks</td>
<td>Greater stakeholder confidence and improved risk mitigation strategies</td>
<td>Risk-adjusted strategy with performance evaluation</td>
</tr>
</tbody>
</table>

ERM process: What does ERM look like?
Creating process – Risk maturity continuum (continued)

KPMG Risk Maturity Continuum

<table>
<thead>
<tr>
<th>Risk Governance</th>
<th>Risk Assessment</th>
<th>Risk Quantification &amp; Aggregation</th>
<th>Risk Monitoring &amp; Reporting</th>
<th>Risk and Control Optimization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic</td>
<td>Mature</td>
<td>Advanced</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remain in Compliance</td>
<td>A Management Process</td>
<td>A Strategic Tool</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Example
ERM process: What does ERM look like?
Creating process – Ownership and oversight

Responsibilities
- Oversight of risk content and process
- Oversight of risk content
- Provide Assurance over:
  - Achieving business objectives
  - Mitigating/Managing risks
  - Controls operating effectively
- Risk Owners manage and identify the risks

Full Board

Board Committees
- Board Committee A
- Board Committee B
- Board Committee C
- Board Committee D

Monitors
- SOX
- Compliance
- Internal Audit

Risk Profile
- Financial
- Legal
- Governance
- Strategic
- Compliance

- e.g., Loss of key infrastructure and/or buildings leads to significant disruption of business operations.

KPMG’s vision – Governance, Risk & Compliance (GRC) holistic model

Four key components that must be in balance to enable resilience:
- Risk profile – Understanding and quantifying risks that the organization faces
- Culture and behavior – Embedding risk management within everyday behavior
- Governance, organization, and infrastructure – Overseeing business processes and decision making
- Enterprise assurance – Evaluating, monitoring, and reporting on the effectiveness of controls
Questions to ask for assessing your risk management approach

<table>
<thead>
<tr>
<th>Overview question</th>
<th>Some further questions to ask</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is there a clear set of risk management objectives?</td>
<td>How is risk management defined in your organization?</td>
</tr>
<tr>
<td></td>
<td>What do you want risk management to achieve now/in the future in your organization?</td>
</tr>
<tr>
<td>Does the executive take risk management seriously?</td>
<td>What is the risk appetite of your organization?</td>
</tr>
<tr>
<td></td>
<td>How do you know managements is taking the right level of risk?</td>
</tr>
<tr>
<td></td>
<td>How does risk management align with the rest of your organization?</td>
</tr>
<tr>
<td></td>
<td>What risks have occurred recently which you knew about but still seriously affected your</td>
</tr>
<tr>
<td></td>
<td>organization?</td>
</tr>
<tr>
<td>Does ownership for risk management reside in the</td>
<td>How does risk management align with other management activities?</td>
</tr>
<tr>
<td>business?</td>
<td>How do you measure the performance of individual risks?</td>
</tr>
<tr>
<td></td>
<td>How do you use the risk information collected to develop your business?</td>
</tr>
<tr>
<td>Is there a structure for strong oversight and</td>
<td>Who has oversight of risk management in your organization?</td>
</tr>
<tr>
<td>challenge?</td>
<td>How sustainable is the process to identify, manage, and escalate risk?</td>
</tr>
<tr>
<td></td>
<td>When and how is risk reporting undertaken?</td>
</tr>
<tr>
<td></td>
<td>Whom do you report risk information to? How often is this done?</td>
</tr>
<tr>
<td></td>
<td>How have the actions undertaken to manage the risks been evaluated for effectiveness?</td>
</tr>
<tr>
<td>Is general risk awareness visible?</td>
<td>How aware are management and employees of their risk management roles and responsibilities?</td>
</tr>
<tr>
<td></td>
<td>What monitoring plan is in place for those charged with governance?</td>
</tr>
</tbody>
</table>

Questions directors should ask… and management should answer

<table>
<thead>
<tr>
<th>Overview question</th>
<th>Some further questions to ask</th>
</tr>
</thead>
<tbody>
<tr>
<td>How was the information collected?</td>
<td>Interviews, questionnaires, or a single view? Other stakeholders?</td>
</tr>
<tr>
<td></td>
<td>Was a management team consensus reached? Risk committee deployed?</td>
</tr>
<tr>
<td></td>
<td>Were topdown and bottomup views consolidated to create the group risk profile?</td>
</tr>
<tr>
<td></td>
<td>How frequently?</td>
</tr>
<tr>
<td>How meaningful are the risk descriptions?</td>
<td>Are they aligned and relevant to the organization’s strategic objectives?</td>
</tr>
<tr>
<td></td>
<td>Is there clarity over causes and consequence?</td>
</tr>
<tr>
<td></td>
<td>Are those charged with governance aware of the relationships between risks and revenue</td>
</tr>
<tr>
<td></td>
<td>drivers?</td>
</tr>
<tr>
<td></td>
<td>How do we know that the information we get is accurate and reliable?</td>
</tr>
<tr>
<td>What is the organization’s risk tolerance and appetite?</td>
<td>Are risks quantified?</td>
</tr>
<tr>
<td></td>
<td>Is the organization taking the right amount of risk?</td>
</tr>
<tr>
<td></td>
<td>Is there clarity over the group risk appetite vs. appetite for different categories of risk,</td>
</tr>
<tr>
<td></td>
<td>e.g., fraud versus business continuity?</td>
</tr>
<tr>
<td>How sustainable is the risk management process?</td>
<td>What is the frequency/caliber of the risk reporting and monitoring (e.g., dash board)?</td>
</tr>
<tr>
<td></td>
<td>How is risk awareness embedded in the organization? (e.g., policies, training, performance</td>
</tr>
<tr>
<td></td>
<td>goals)</td>
</tr>
<tr>
<td></td>
<td>How are emerging risks identified?</td>
</tr>
<tr>
<td></td>
<td>Is the overall ERM program steadily improving?</td>
</tr>
</tbody>
</table>
Questions directors should ask… and management should answer (continued)

<table>
<thead>
<tr>
<th>Overview question</th>
<th>Some further questions to ask</th>
</tr>
</thead>
<tbody>
<tr>
<td>What are the risk improvement actions?</td>
<td>☐ How has the management action effectiveness been evaluated? By whom?</td>
</tr>
<tr>
<td></td>
<td>☐ Are there any actions planned against the key risks?</td>
</tr>
<tr>
<td></td>
<td>☐ Who is accountable? Timing?</td>
</tr>
<tr>
<td></td>
<td>☐ How is risk coordinated across the organization? Is there one risk owner or many?</td>
</tr>
<tr>
<td></td>
<td>☐ How do we evaluate changes in the external environment and their impact on the organization?</td>
</tr>
<tr>
<td></td>
<td>☐ Is there a clear monitoring plan for those charged with governance?</td>
</tr>
</tbody>
</table>

Q & A

Contact information:

Rod Filliben, partner
KPMG LLP
1225 17th Street, Suite 800
Denver, CO 80202
303295-8843
rfillibe@kpmg.com
The information contained herein 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 of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2013 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.

The KPMG name, logo and “cutting through complexity” are registered trademarks or trademarks of KPMG International.