Enterprise Risk Management: From Theory to Practice
Executive Summary

Enterprise Risk Management (ERM) is a structured and disciplined business tool aligning strategy, processes, people, technology, and knowledge with the purpose of evaluating and managing the uncertainties that enterprises face. It is a holistic, integrated, future-focused, and process-oriented approach that helps an organization manage key business risks and opportunities with the intent of enhancing shareholder value for the enterprise as a whole. This is accomplished by taking an “enterprise-wide” view of risk through the removal of traditional business unit, segment/division, functional, departmental or cultural barriers to open and honest risk communication.

Still, as with any important business tool, a large gap exists between inception, adoption, and implementation. KPMG has assisted many organizations with adopting ERM and has conducted a series of surveys related to the current state of ERM. This survey—Enterprise Risk Management: From Theory to Practice—targeted an array of companies from different industries in the U.S. and asked a range of questions designed to see what current practices they are using and just how far they had progressed with the practical implementation of ERM.
Key Findings

Our survey explored current risk management practices and five themes emerged:

**Governance Structure and Reporting Lines**

Leading practice is cited for risk oversight to reside with a Risk Committee of the Board and for the CRO to report directly to the CEO. Interestingly, current practices appear to differ:

- A significant majority (70 percent) of respondents provide ERM updates to their Audit Committees, while less than half (40 percent) report that updates are provided directly to the Board of Directors or a separate Board-level Risk Committee on a quarterly basis.
- Three quarters of respondents say they have a CRO who reports to the CFO.

**Emerging Risk Identification**

In response to the financial crisis and increased rating agency focus, there is increased emphasis on the identification of emerging risks:

- More than a third (37 percent) of the companies surveyed reviewed emerging risk as part of their periodic risk identification/assessment process, while a similar percentage of companies reported having a defined emerging risk identification process in place.
Risk Appetite

As a company’s risk maturity evolves, developing a risk appetite is becoming an increasing area of focus. Many companies are working on defining their risk appetite at both corporate and business unit level specifically, and cascading the corporate-wide risk appetite down into regions, business units, and products lines in a meaningful way.

- Nearly thirty percent of companies surveyed do not yet have a corporate risk appetite statement articulated. Forty seven percent of the respondents noted that their corporate risk appetite statement is expressed in both descriptive and quantitative terms.

Use of Scenario Analysis and Economic Capital models

Although the financial crisis brought the use of scenario analysis and models front and center, the key is sufficient management review and thought as outputs are used to make business decisions:

- More than two-fifths (42 percent) of the respondents perform scenario analysis for enterprise level risks.
- A solid majority (86 percent) of respondents are using an economic capital model (ECM) in a variety of ways in their business. At least half use it for strategic decision-making or capital management. Approximately 40 percent use it for capital planning and determining risk appetite/risk tolerances.
Risk Aware Culture

One of the areas companies are focusing on is increasing their employees’ awareness of risk management and making better risk-based decisions. One of the key elements to successfully doing this is to educate or train the appropriate levels in the organization. Not all companies have currently implemented such awareness or education yet.

- Respondents were evenly split on whether there is a formal risk training/education process in their companies.

Conclusion

This paper highlights similar risk management practices across 21 companies in financial services and other regulated industries that we surveyed in 2009 (see the survey methodology on page 20). Specifically, it highlights the fact that what may be considered “leading practices” are not necessarily “common” or “current” practice for the majority of respondents. It appears that some of the practices in place may be used as they are practical and work effectively for that particular company’s culture, and that leading practices would not be effective or efficient. Despite the apparent progress with regard to the application of ERM, the following key questions remain:

- Is ERM embraced and understood throughout the organization and at the board level?
- Is ERM positioned or structured in a way to promote value throughout the organization as opposed to being a compliance exercise?
- Are risk management and performance management integrated in order to promote an overall return in accordance with an organization’s established risk appetite?

Risk management practices must be tailored to meet a company’s maturity, culture, and risk profile. In addition, in order to derive real value from ERM, risk management must be integrated into a company’s business decision processes as well. Ultimately, ERM practices must be integral to how a company operates instead of simply being viewed as a compliance exercise.

The companies in KPMG’s survey acknowledge the need for ERM and have created the governance structure to implement it throughout the organization. In order to evaluate the effectiveness of ERM, however, a key next step is determining the appropriate metrics to measure both how well ERM mitigates an organization’s risk and emphasizes opportunities to increase rewards.
Detailed Findings

Board Oversight and Reporting

To which committee(s) are Enterprise Risk Management updates provided?

<table>
<thead>
<tr>
<th>Committee</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit Committee</td>
<td>70%</td>
</tr>
<tr>
<td>Board of Directors</td>
<td>40%</td>
</tr>
<tr>
<td>Risk Committee</td>
<td>26%</td>
</tr>
<tr>
<td>Finance Committee</td>
<td>15%</td>
</tr>
<tr>
<td>Other</td>
<td>10%</td>
</tr>
</tbody>
</table>

Multiple selections allowed.

Note on the charts: Since survey respondents were able to select multiple responses, percentages do not add up to 100 percent.

A significant majority (70 percent) of respondents provides ERM updates to the Audit Committee, while less than half (40 percent) report that updates are provided directly to the Board of Directors or a separate Board-level Risk Committee. It is currently considered a leading practice to send the risk management report to the Board-level Risk Committee, and the proposed Shareholder Bill of Rights Act of 2009 (see sidebar) recommends that each issuer be required to have a Board-level risk committee, comprised entirely of independent directors, responsible for the risk management practices of the issuer. But this is not currently common practice, as only 35 percent of companies surveyed actually reported to the Board-level Risk Committee.

The Shareholder Bill of Rights Act of 2009

The Senate’s Shareholder Bill of Rights Act was proposed in May of 2009 by Senator Charles Schumer (D-NY). Among other things, the Act calls for more board accountability for a public company’s risk management process, including the establishment of an independent board-level risk committee.

Currently risk management is typically the responsibility of a public company’s Audit Committee, which can comprise both outside and inside directors. But the Act calls specifically for public companies being required to have a risk committee of independent directors responsible for the establishment and evaluation of risk management practices. By creating separate risk committees, boards will not be able to claim they did not understand the risks that the firms they oversee were taking.

Upon passage of the Act, a substantial challenge for many organizations may be finding enough independent directors with the necessary technical risk management skills required to qualify them for their positions.
A significant majority (72 percent) of respondents provide ERM updates to the Audit Committee and/or Board of Directors on a quarterly basis as opposed to 22 percent reporting that updates occur annually. Both become important if the proposed SEC Rules on Proxy Disclosure and Solicitation Enhancements are enforced (see sidebar). Companies may need to revisit structure reporting lines, composition, and oversight of risk management activity.

**Potential Impact on Risk Management: SEC Rules on Proxy Disclosure and Enhancements**

Organizations should be aware of how the recently approved SEC Rules on Proxy Disclosure Enhancements\(^1\) may impact future public disclosure regarding the risks associated with compensation, director qualifications, and governance. The following excerpts are from the recently approved SEC proxy rule change:

- **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 included.

- **Director Qualifications**: Additional detail regarding disclosure relative to directors and nominee qualifications, including skills (e.g., risk assessment skills) that qualify the person to be a director and participate in related committees served will need to be included.

- **Governance 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. The board’s role in risk management would also need to be addressed (e.g., how risk oversight is allocated amongst the full board vs. board committees and which committees are responsible for risk oversight).

---

Committees get a lot of information ... but is it focused and insightful?

What level of report detail is provided?

<table>
<thead>
<tr>
<th>Level of Detail</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Additional Detail Provided</td>
<td>67%</td>
</tr>
<tr>
<td>Summary Dashboard</td>
<td>61%</td>
</tr>
<tr>
<td>Detailed Risk Profile</td>
<td>17%</td>
</tr>
</tbody>
</table>

Note on the charts: Since survey respondents were able to select multiple responses, percentages do not add up to 100 percent.

More than 60 percent of the survey respondents offer a summary dashboard and 67 percent offer additional detail, compared to only 17 percent that provide a detailed risk profile. This means that the survey respondents are speaking to the Audit Committee, but there needs to be a balance between relevant and focused information and striking the right balance on additional details provided. The key is focused and insightful information. However, the Board of Directors’ role in overseeing risk will change in 2010 as a result of the recently approved SEC proxy rule.
Internal Governance Structure: Use of the ERM Steering Committee

What is the role of the Enterprise Risk Committee?

- Understand Key Risk and Mitigation: 69%
- Make Risk Decisions: 63%
- Identification of emerging risks: 42%
- Other: 11%

Multiple selections allowed.

Note on the charts: Since survey respondents were able to select multiple responses, percentages do not add up to 100 percent.

According to 89 percent of respondents, understanding risk and mitigation is the role of the Enterprise Risk Committee. Almost two-thirds (63 percent) include making risk decisions as part of their role, while less than half of the respondents indicate that identifying emerging risks is part of their responsibility.

Composition of the ERM Committee

Who chairs ERM committee/council?

- CRO: 55%
- CFO: 20%
- CEO: 10%
- Internal Audit: 5%
- Other: 5%
- Do not have committee: 5%

About half (55 percent) of respondents indicate that the CRO chairs the ERM Committee. The next largest group responded that the CFO (20 percent) chairs the committee, followed by the CEO (10 percent). This may say something about the increased level of responsibilities for the CRO as ERM issues are elevated and discussed at companies.
Are there representatives from Legal, HR, IT or Compliance as members of the Risk Committee?

Legal 100%
Compliance 82%
IT 76%
Other 71%
HR 65%

Note on the charts: Since survey respondents were able to select multiple responses, percentages do not add up to 100 percent.

Not surprisingly, 100 percent of respondents say that Legal is represented on the Risk Committee. There is also strong representation from Compliance (82 percent), Information Technology (76 percent), and Human Resource (65 percent).

A majority of companies have a centralized ERM department, with the CRO reporting to CFO.

Who does the CRO report to?

- CFO 61%
- CEO 22%
- Other 17%

Nearly two-thirds of the survey respondents say that the CRO reports to CFO, while about a quarter say the CRO reports directly to the CEO. Although the former is a more common practice, the leading practice, especially in European companies, is the CRO reporting directly to the CEO. Having the CRO report directly to the CEO may also raise the corporate appreciation of the importance of risk management, moving it from balance sheet risk to corporate risk.
Three quarters of the respondents say they have a CRO and centralized ERM department. In another survey question, there is nearly a 50/50 split on whether Business Units have risk management resources. Since KPMG surveyed larger companies, it appears the trend is to have a centralized ERM department, while smaller companies may not have the dedicated resources to follow a similar plan.

**Identification and Assessment of Emerging Risks**

How formalized is emerging risk management?

<table>
<thead>
<tr>
<th>Process Type</th>
<th>Percentages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defined process in place</td>
<td>37%</td>
</tr>
<tr>
<td>Part of Risk identification/assessment on a regular basis</td>
<td>37%</td>
</tr>
<tr>
<td>Informal process</td>
<td>28%</td>
</tr>
<tr>
<td>Ad hoc monitoring of events/trigger</td>
<td>21%</td>
</tr>
<tr>
<td>Not considered</td>
<td>0%</td>
</tr>
</tbody>
</table>

Multiple selections allowed.

*Note on the charts: Since survey respondents were able to select multiple responses, percentages do not add up to 100 percent.*

Less than half (37 percent) have a defined emerging risk process in place while another 37 percent include it as part of the periodic risk identification/assessment process. Companies are also using informal processes and *ad hoc* monitoring of events. This is a focus area that ratings agencies such as Standard & Poors are looking at as part of their ratings reviews for all public companies.
Companies appear to be taking steps to identify emerging risks and trying to determine whether to create a new process or add it into current risk identification methods. Emerging risks are being identified in two buckets—internal and external. Internal risks are being monitored through customer touch points, surveys, discussions with business unit leadership, and assessing “near-miss” events. The other is external emerging risks being driven by events over which the company does not have full control and may need to react to and comply with. We have noticed that many defined processes are external facing, such as media scanning or tracking proposed legislation.

**Quantification**

**What level of scenario analysis/stress testing is being performed?**

- Designed and implemented for entity-wide risks: 42%
- Ad Hoc: 32%
- Designed at corporate level and implemented at BU level: 21%
- Designed and implemented at BU level: 16%
- Not used: 5%

Multiple selections allowed.

*Note on the charts: Since survey respondents were able to select multiple responses, percentages do not add up to 100 percent.*

Scenario analysis/stressing testing is being performed most often (42 percent of respondents) for entity-wide risks. In addition, one-third of respondents indicate that it is performed on an *ad hoc* basis, while more than a third (37 percent) indicate that scenario analysis/stressing testing is implemented at the business unit level.
The Economic Capital Model is used in many different ways

What is the Economic Capital model used for?

- Strategic decision-making: 55%
- Capital allocation: 50%
- Determining risk appetite/risk tolerances: 40%
- Capital planning: 40%
- Other (please specify): 20%
- Not used: 15%

Multiple selections allowed.

Note on the charts: Since survey respondents were able to select multiple responses, percentages do not add up to 100 percent.

A solid majority of respondents (85 percent) are using an economic capital model (ECM) in a variety of ways as a tool to aid in risk management. At least half use it for strategic decision-making and/or capital management. Some 40 percent use it for capital planning and determining risk appetite/risk tolerances. In addition, nearly two-thirds of the survey’s respondents indicate that the outputs of ECM are used for medium- to long-term risk-based planning as well as short-term decision making. The survey results suggest that ECM is being used in a variety of instances to support risk management, but financial services companies are using it more than non-financial services companies (such as utilities).

As ERM matures and becomes a more strategic tool, the linkage of ECM and ERM becomes more intertwined. ECM then becomes one of the techniques used to provide more quantitative insight in areas shown in the chart above.
Risk Appetite and Strategy

Taking ERM to the next level and managing a company’s risk requires setting and articulating the company’s risk appetite/risk tolerance and establishing risk limits. Without this approach, there are no guidelines linked to the company’s strategy for how much or how little risk to take. As companies evolve, developing a risk appetite/risk tolerance is becoming an increasing area of focus (see sidebar).

What is Risk Appetite?

- Risk appetite is the total impact of risk an organization is prepared to accept to achieve its strategic objectives.
- Considerations in defining risk appetite may include how an organization wishes to be perceived by key stakeholders—shareholders, employees, regulators, rating agencies and customers.
- The amount of risk an organization accepts will vary from organization to organization.
- Factors, such as the external environment, people, business systems and policies can influence an organization’s risk appetite.

What Does Risk Appetite Look Like?

Characteristics of a well-defined risk appetite are:

- Reflective of strategy, including all key aspects of the business—organizational objectives, business plans and stakeholder expectations
- An acknowledgement, willingness and capacity to take on risk
- Documented as a formal risk appetite statement
- Considerate of the skills, resources and technology requirements to manage and monitor risk exposures in the context of risk appetite
- Inclusive of a tolerance for loss or negative events that can be reasonably quantified
- Periodically reviewed and reconsidered with reference to evolving industry and market conditions
- Reviewed by the Board

Of the companies we surveyed, many have taken the first step and articulated a risk appetite at the entity level, and then only half of those have articulated this to the business unit level. The key trend here is that most companies are working on developing a risk appetite, and the first step is to develop a corporate-wide risk appetite.
Almost a third (29 percent) of companies surveyed do not yet have a corporate risk appetite statement. The second step is tougher; specifically, how companies enhance cascading the corporate-wide risk appetite down into regions, business units, and products lines in a meaningful way. Indeed, there is nearly a 50/50 split on whether risk appetites have been defined for different business units or product types.

How is your risk appetite statement expressed?

- Descriptive and Quantitative 41%
- Don’t have risk appetite statement 29%
- Quantitative 24%
- Descriptive 0%

What considerations influence the setting of risk appetite?

- Business objectives 65%
- Rating 65%
- Stakeholder groups 59%
- Other 18%

Note on the charts: Since survey respondents were able to select multiple responses, percentages do not add up to 100 percent.

There are multiple considerations in setting risk appetite. As seen in the chart above, in over half of respondents, considerations include business objectives, rating agency evaluations, and stakeholder groups.
Our survey respondents said that risk-adjusted return measures are incorporated into many strategic objectives. These included investment objectives (92 percent), product changes (77 percent), and growth and risk mitigation strategies (62 percent). Slightly more than half of respondents indicated that market changes and acquisitions are also reflected in risk-adjusted measurements.
The more risk identification and management is integrated as part of the daily processes and procedures, the better chances the organization has of improving the risk culture since risk management will then be considered as part of corporate processes instead of an additional step.

**Are ERM results/risk considerations incorporated into the following processes?**

<table>
<thead>
<tr>
<th>Process</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Investments</td>
<td>88%</td>
</tr>
<tr>
<td>Strategic Planning</td>
<td>81%</td>
</tr>
<tr>
<td>Budgeting</td>
<td>69%</td>
</tr>
</tbody>
</table>

*Note on the charts: Since survey respondents were able to select multiple responses, percentages do not add up to 100 percent.*

Survey respondents said that ERM results and risk considerations are incorporated by strong majorities in the investment (88 percent), strategic planning (81 percent), and budgeting processes (69 percent).

**Risk Aware Culture**

Respondents were evenly split on whether there is a formal risk training/education process in their companies (See chart on next page). The evidence from the survey shows that companies are making progress at integration. But what the survey does not show, and what the 2008–2009 financial crisis highlighted, was whether risk management was effective enough in helping companies avoid the types of risks that would have greatly impacted their financial results.

The other key component of building risk awareness and risk management is the level of awareness and training provided to all levels of the organization. The trend is that more organizations are formally providing risk training and education to various levels of these organizations.
Do you have a formal Risk training/education or awareness program for various levels in organization?

- Yes 50%
- No 50%

One of the most challenging aspects of driving and embedding risk management into companies is educating all levels of the organization on what risk management is, how it should be approached, and what that means for daily decision-making. The key success factor is training and education, but interestingly enough, of those surveyed only 50 percent have a formal risk training program. So the question is for those companies that don’t have a formal risk training program: Do they really consider and evaluate risk consistently across the organization?
Appendix

ERM Survey Questions

Board and Senior Management Involvement and Oversight
1. To which committee(s) are Enterprise Risk Management updates provided?
2. How often are Enterprise Risk Management updates provided to the Audit Committee/Board of Directors?
3. What level of report detail is provided?

Internal Governance Structure
4. Who chairs ERM committee/council?
5. Are there representatives from Legal, HR, IT or Compliance as members of the Risk Committee?
6. What is the role of the Enterprise Risk Committee?
7. Does your organization have a CRO and Central ERM department?
8. Do Business Units (BUs) have a BU CRO or Risk Manager?
9. Who does the CRO report to?

Risk Identification and Assessment
10. How formalized is emerging risk management?
11. Is operational risk focused on and evaluated as other main risk categories (e.g. insurance, credit, market)?
Quantification

12. Is capital or resources allocated accordingly based on risk exposure?
13. What is the Economic Capital model used for?
14. What are the outputs of the model used for?
15. What level of scenario analysis/stress testing is being performed?

Risk Appetite and Strategy

16. What considerations influence the setting of risk appetite?
17. How is your risk appetite statement expressed?
18. Have different levels of risk appetites been defined for different product types or business lines?
19. Which type of strategic objectives incorporate risk-adjusted return measures?
20. How is risk-adjusted capital determined as part of the defined corporate risk appetite?
21. Do executive management and the board use risk-adjusted return metrics in strategic planning?
22. Are ERM results/risk considerations incorporated into the following processes?

Risk Aware Culture

23. Do you have a formal Risk training/education or awareness program for various levels in organization?
Survey Methodology

During the summer of 2009, KPMG surveyed 21 companies in regulated industries such as insurance, banking, and utilities regarding their current ERM practices. As advisors, we are frequently asked about the common practical ERM procedures that other companies are using. As a result, we asked questions in this survey about the practical applications of ERM, such as Board and management governance, reporting, risk appetite, and the extent and use of quantification techniques. For a full list of the questions, please see the Appendix. All responses were submitted anonymously, with the understanding that results would be published in the aggregate groups of ten or greater.

Acknowledgements

We would like to thank the following contributors from KPMG LLP: Bruce Hager, Heather Ingram, Leslie Marlo, John Farrell, and Kreg Weigand.
Contact

For more information about this survey or to discuss the challenges associated with ERM, please contact one of the following KPMG professionals:

**Angela Hoon**
Principal
Advisory Services
267-256-1970

**Matt Smyth**
Principal—Leader Insurance Advisory
Advisory Services
212-872-6414

**Scott Weinstein**
Principal
Advisory Services
404-222-3594