Best Practices for a Board’s Role in Risk Oversight

Summary

Moody’s views a board of directors’ risk oversight role as critical to the sound running of an institution — especially for financial institutions and for other companies with significant market and credit risk exposures. In particular, Moody’s sets high expectations for boards’ role in shaping a firm’s risk appetite and ensuring a proper risk management framework is in place. (By board, Moody’s typically refers to the board of directors. In those jurisdictions with a dual board structure, we refer to the role of the supervisory board.)

In Moody’s view, the board has five central functions with respect to risk:

1. Approve the firm’s risk appetite as a component of its strategy
2. Understand and question the breadth of risks faced by the company
3. Ensure robust oversight of risk at the board committee and senior management levels
4. Promote a risk-focused culture and open communication across the organization
5. Assign clear lines of accountability and encourage an effective risk management framework

This special comment describes how Moody’s views best practices for the role of boards of directors in risk oversight.1 Moody’s evaluates the extent to which issuers have adopted these best practices during our reviews of the quality of corporate governance within each company, and will emphasize this aspect of our analysis further in the future.

1. This special comment complements Moody’s Risk Management Assessment methodology (July 2004, 87539) and Moody’s U.S. and Canadian Corporate Governance methodology (August 2003, 78666)
#1. APPROVE THE FIRM’S RISK APPETITE AS A COMPONENT OF ITS STRATEGY

Moody's has noted in previous research that directors in North America are becoming more involved in strategic planning at early stages, rather than just reviewing and signing off on a strategy after it has been fully developed by management. Boars are similarly more engaged in reviewing large capital commitments and investments. But as boards become more engaged, they must walk a fine line between a healthy level of oversight and intervention, and counter-productive micro-management. Nonetheless, we believe they have a legitimate, indeed necessary, role in shaping strategy.

Too often, though, board strategy sessions appear to be not sufficiently rich in discussion about the key risks facing the company, or inherent within the construct of the strategy. More broadly, we believe that explicit discussions surrounding a firm’s overall risk appetite are perfunctory, and sometimes non-existent. Yet, any strategy and return profile is intrinsically linked with a given risk profile. It is important that the board is comfortable not only about a certain return target and strategy, but also with the level of risk that that return target entails.

Therefore, Moody’s views it as important that the board understands and approves the firm’s risk appetite, and be clear on how the level of risk taken by the company is measured and how it relates to the firm’s strategy.

- **Risk appetite.** The board implicitly approves the risk appetite of the firm as part of the annual or multi-year business plan. Best practice calls for the risk appetite to be clearly and explicitly identified in terms of the types of risks that the firm is ready to retain, and the total exposure it is comfortable with (e.g., as a percent of earnings or equity). The risk-return trade-off should be transparent.

- **Alignment of strategy, risks and financial objectives.** The board should make sure that the financial objectives of the firm (earnings, ROE, ROA, etc.) are compatible with the level of risk embedded in the business plan and the constraints faced by the firm, such as maximum leverage or operational limitations.

- **Drivers of risk.** The board should be aware of the relationships between various risks and revenue drivers. This implies that the board is regularly presented with alternative scenarios for the future financial results of the firm. At a minimum there should be three scenarios (worst case, expected case and best case), but some firms have implemented more topical simulations following the model of financial institutions. These simulations can be based on historical events or hypothetical developments. In all cases, directors should be aware of the assumptions embedded in the scenarios (such as diversification among businesses).

#2. UNDERSTAND AND QUESTION THE BREATH OF RISKS FACED BY THE COMPANY

Moody's analysts ask non-executive directors regularly for their views on the key risks facing their respective companies. The responses run the gamut, from the mundane (“competition is our biggest risk”) to the specific (“management’s judgments that are built into our reserve calculations are critical”). We believe the responses provide insight as to the quality of board dialogue with management on key risks, and highlight any differing priorities between the board and management.

Assessing the board’s understanding of risks is important, albeit hard to quantify. Directors need to understand both the nature of the risks to which the firm is exposed and their potential impact to engage forcefully with executive management on strategic and tactical matters. Key components of expanding a board’s knowledge of key risks include:

- **Identification of risks.** The board should have a good grasp of the total bundle of risks faced by the firm (e.g., market, credit, operational, business, liquidity, reputational, litigation). Because these risks change over time, it is important that the board be updated regularly on the key risks faced by the organization and, more broadly, on the firm’s risk profile, including a quantification of the risk, even if it is rough approximation (operational risks, for instance).

- **Communication.** The board should engage regularly in communications with management on risks. These communications should include high level reports on all types of risks, as well as private sessions with the senior risk professionals (typically a chief risk officer in financial institutions) at least on a quarterly basis. The board should also ensure that communications from the risk professionals provide an integrated and coherent picture of the risks facing the business and the quality of the firm’s control environment when set alongside reports from other control functions, such as audit, compliance and legal.

- **Training.** Communication without understanding is of limited value. Often risk oversight requires an understanding of the technicalities of risk measurement, monitoring and mitigation. Directors should receive ongoing updates on trends in risk management and in new risks facing the business or embedded in new products. Training is particularly important in enabling boards to use the risk information shared with the board by management, some of which can be onerous in terms of its detail and complexity.

---

2. See Moody’s Findings on Corporate Governance in the United States and Canada (October 2004, 89113).
#3. ENSURE ROBUST OVERSIGHT OF RISK AT THE BOARD COMMITTEE AND SENIOR MANAGEMENT LEVELS

Broad risk matters, such as setting the firm’s risk appetite and ensuring its fit with strategy are matters for the full board. However, in most cases, the detail of risk oversight is undertaken in a committee setting, where other major agenda items are not vying for attention. A committee setting also provides a positive environment for interactions among board members and risk professionals.

Key components of effective committee-level risk oversight include:

- **Skilled directors.** The technical nature of risk oversight requires a good understanding of risk management techniques and trends. Training can facilitate a deeper understanding. However, Moody’s believes that risk-focused committees are most effective when they are staffed, at least in part, with directors whose backgrounds include risk or financial management; this is particularly important for financial institutions.

- **Sufficient time allotted to coordinated risk oversight.** Boards have adopted various approaches to ensure sufficient committee time is allocated to risk oversight; each approach has its own benefits and challenges as highlighted in the table below.

### Table One: Committee Approach to Risk Oversight

<table>
<thead>
<tr>
<th>Committee assignment of risk oversight</th>
<th>Benefits</th>
<th>Challenges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit committee</td>
<td>• Ultimately, major risks find their way into the financial reports • This committee plays a central role in ensuring robust internal controls and compliance procedures</td>
<td>• Ensuring sufficient time is allotted to risk matters, particularly given the significant burden placed on such committees in recent years</td>
</tr>
<tr>
<td>Risk committee (sometimes called investment or credit committees)</td>
<td>• Promotes routine, focused oversight of risk, broadly defined</td>
<td>• Coordinating its work with that of the audit committee, e.g., through overlapping membership</td>
</tr>
<tr>
<td>Specialized committee focused on primary risk (e.g., an R&amp;D committee in pharmaceuticals focused on pipeline for new drugs)</td>
<td>• Promotes routine, focused discussion on the primary risk facing the company</td>
<td>• Ensuring other risks are sufficiently addressed • Coordinating its work with that of the audit committee, e.g., through common membership</td>
</tr>
</tbody>
</table>

#4. PROMOTE A RISK-FOCUSED CULTURE AND OPEN COMMUNICATION ACROSS THE ORGANIZATION

The support of the board is key to creating an overall culture that promotes decision-making at all levels of the firm that is sensitized to risk matters and risk-adjusted performance. This culture feeds from well-established business and ethical principles emphasizing openness in communication and the right to fail. (Otherwise risk managers tend to care more about their career and reputational risks than about doing the right thing for the firm.) Key elements of promoting such a culture include:

- **“Tone at the top.”** Many directors speak of the “tone at the top” as a key ingredient of a strong, open culture. Moody’s agrees. However, it is not so clear that directors have first-hand understanding of the tone across the firm, other than through their interactions with senior executives. In several major corporate governance failures of recent years, boards either did not understand the culture within the organization, including the attitude towards risk-taking, or ignored the culture and instead focused on short-term corporate performance. In our view, it is critically important that directors establish their own lines of communications with employees across the organization, unhindered by the CEO or other executives. These connections provide valuable context for the ongoing dialogue with management as to the firm’s culture and approach to risk.

- **Communications with risk professionals.** Risk-focused committees should establish routine, robust and frank lines of communication with the key risk professionals, much as audit committees do with audit professionals. Board members should have direct access to risk professionals and, conversely, risk professionals should have unhindered access to the board.
Moody’s Risk Management Assessment methodology sets out four pillars of a robust risk structure: (1) risk governance; (2) risk management; (3) risk analysis and quantification; (4) risk infrastructure and intelligence. In order for a board to assess whether these aspects are addressed diligently, a few core fundamentals should be in place:

- **Risk management policy, product approvals.** The board should approve a risk management policy that outlines the objectives of risk management, its own key responsibilities in the risk process, as well as the mechanisms to delegate responsibilities and to elevate issues and conflicts. The policy should highlight clearly how the board or risk-focused committee(s) would monitor action plans that are put in place to remedy deficiencies in the key risk framework, controls and risk systems of the firm, where these are required.

  As part of the risk management policy, boards of financial institutions should ensure the establishment of a formal process by which families of new products can be reviewed and approved and ensure that they are aware of how families of new products affect the firm’s overall risk profile. At non-financial firms, the board or the risk-focused committee should be empowered to approve the list of traded products (e.g., futures, options, structured trades) and ensure that the firm is adequately prepared to handle the risks inherent in these products.

- **Clear delegations of authority.** Boards should adopt policies that spell out when full board approval is required for key corporate decisions such as investments, acquisitions or refinancing (often called “delegations of authority”). In reviewing these policies in U.S. and Canadian companies, Moody’s has found that, for the most part, investment or transaction thresholds for required submission to the board are relatively conservative in the context of the size of companies reviewed. Almost regardless of the company’s size, these thresholds have been below $100 million, and in many cases markedly so. Only a handful of companies we assessed have adopted thresholds above $150 million. Beyond corporate actions, however, it is important that the board approve a set of cascading delegation of authorities for risk matters; this is particularly important for financial institutions.

- **Integration of risk insights into other functions’ planning processes.** The board or the appropriate board committees should ensure that other control functions within the organization use the intelligence on key risks from the risk management function in their planning processes. For example, internal audit should use these insights as a major input into their risk-based audit plan.
Related Research

Rating Methodologies:
Risk Management Assessments, July 2004 (87539)
U.S. and Canadian Corporate Governance Assessment, August 2003 (78666)

Special Comments:
U.S. Executive Pay Structure and Metrics, June 2006 (97887)
Risk Disclosures of Banks and Securities Firms, May 2006 (97366)
The Downside of Incentive Pay for Directors, April 2006 (97174)
Lessons Learned in Moody’s Experience in Evaluating Corporate Governance in Major North American Issuers, April 2006 (97104)
Assessing Corporate Governance As A Ratings Driver For North American Financial Institutions, April 2006 (97279)
Emerging Best Practices for Operational Risk Management at European Banks, October 2004 (89510)
Moody’s Findings on Corporate Governance in the U.S. and Canada, October 2004 (89113)

To access any of these reports, click on the entry above. Note that these references are current as of the date of publication of this report and that more recent reports may be available. All research may not be available to all clients.