The Role of the Board in Enterprise Risk Management

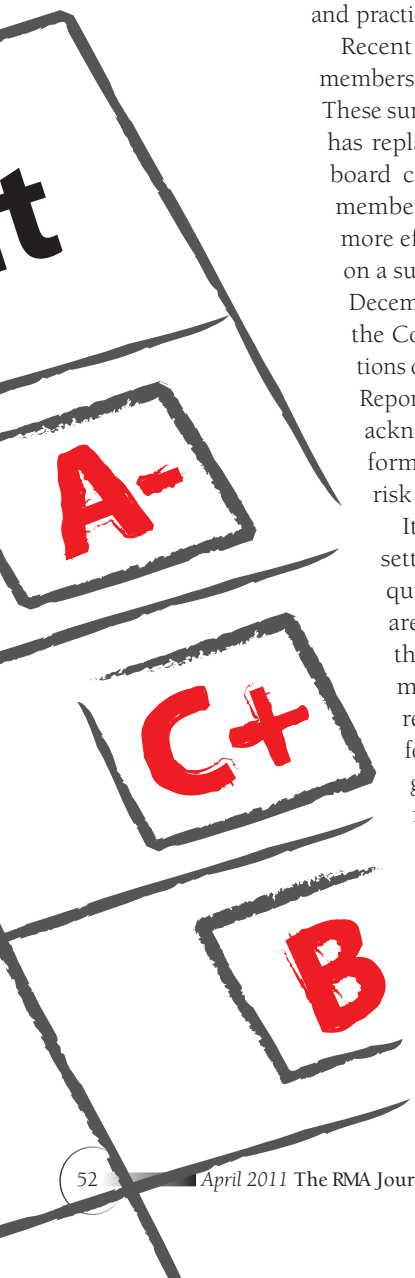
••The board of directors plays an essential role in ensuring that an effective ERM program is in place. Governance, policy, and assurance—GPA—are the key levers in this process.

BY JAMES LAM

A TRANSFORMATION IS under way at boards with respect to their role in enterprise risk management (ERM). In the wake of the global financial crisis, boards are taking a much more active role in risk oversight. They are reexamining governance structure and roles, risk policies and limits, and assurance and reporting processes.

This change is very significant and positive. Of the key groups that provide independent risk monitoring—boards, auditors, regulators, rating agencies, and institutional investors—the board of directors is the only group with both the direct responsibility and the greatest leverage in ensuring that sound risk management is in place.

At most organizations, corporate management would bend over backward to satisfy board demands. By asking tough questions and setting board expectations in regard to ERM, the board can set the "tone from the top" and effect significant change in the risk culture and practices of an organization.



Recent surveys have reported that board members recognize the importance of ERM. These surveys indicate that risk management has replaced accounting issues as the top board concern. More importantly, board members recognize that they can play a more effective role in risk oversight. Based on a survey of over 200 board members, a December 2010 report[1] commissioned by the Committee of Sponsoring Organizations of the Treadway Commission (COSO Report) indicated that 71% of respondents acknowledged that their boards "are not formally executing mature and robust risk oversight processes."

It's evident that board members are setting higher expectations and requirements for risk oversight. They are not alone. In December 2009, the Securities and Exchange Commission established new rules that require disclosures in proxy and information statements about the board governance structure and the board's role in risk oversight, as well as the relationship between compensation policies and risk management.

In July 2010, the Dodd-Frank Act was signed into law. The act requires that a board risk committee be established by all public bank holding companies (and public nonbank financial institutions supervised by the Federal Reserve) with over $10 billion in assets. The board risk committee is responsible for ERM oversight and practices, and its members must include "at least one risk management expert having experience in identifying, assessing, and managing risk exposures of large, complex firms."

Three Key ERM Levers

In academia, the acronym GPA means "grade point average." In the context of board risk oversight, the same acronym can be used to remember these key levers: governance, policy, and assurance. In brief, all boards must adopt these levers in their ERM oversight.

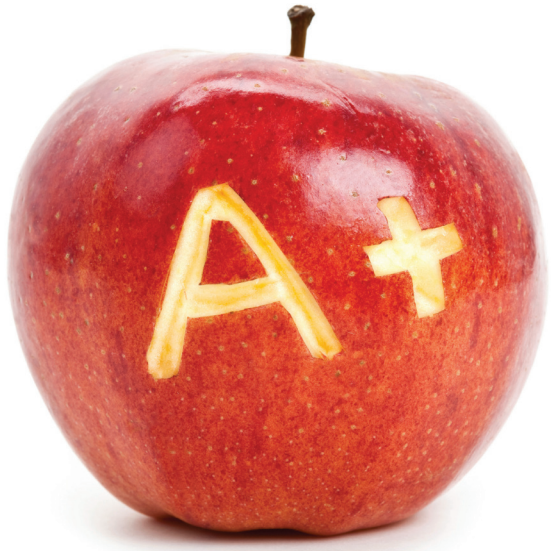
1. *Governance.* Establish an effective governance structure to oversee risk. How should the board be organized to oversee ERM? What is the linkage between strategy and risk management? How can the independence of the risk management function be strengthened?
2. *Policy.* Approve and monitor an ERM policy that provides explicit risk-tolerance levels for key risks. Do risk management policies and risk-tolerance levels effectively capture the board's overall risk appetite and ERM expectations? What is the linkage between risk policies and compensation policies?
3. *Assurance.* Establish assurance processes to ensure that an effective ERM program is in place. What are the performance metrics and feedback loops for ERM? How to improve the structure and content of board reports? How should that assurance be disclosed to investors, rating agencies, and regulators?

These key levers enable boards to play a constructive and effective role in ERM. Board members are not involved in day-to-day operations, and they have limited time to review materials and have discussions with management. But by using these levers, they can effectively oversee ERM and the key risks facing the organization.

Governance

A fundamental step in providing ERM oversight is to establish an effective risk governance structure at the board level. Beyond the organizational chart, risk governance establishes the oversight roles and decision points for the board and board committees, as well as the relationships with management and management committees. Common issues related to board risk governance include:

- Fragmented and/or ambiguous risk oversight responsibilities across the full board and various subcommittees.
- Insufficient risk experience and expertise among board members.
- Inconsistencies between the board and management governance structures or unclear separation of roles.



It's evident that board members are setting higher expectations and requirements for risk oversight.

Executive Management and Board Responsibilities for ERM

ERM Component	Executive Management	Board of Directors
Risk Governance	Establish management structure and roles	Establish board structure and roles
ERM Vision and Plan	Develop and implement	Support vision; track progress against plan
Risk-Tolerance Levels	Establish and conform	Debate and approve
Risk Policies	Develop and implement	Approve and monitor
Business and Risk Strategies	Formulate and execute	Challenge key assumptions; monitor execution
Critical Risks	Manage and measure; optimize risk/return	Provide input and oversight
Risk Reports	Provide context, analysis, and key points	Monitor key exposures, exceptions, and feedback loops
Risk Analytics	Provide qualitative and quantitative analyses	Obtain ERM assurance; conduct board assessments

- Lack of integration between strategy and risk management.
- Weak independence for the chief risk officer and/or the risk management functions.

To strengthen risk governance at the board level, organizations should consider adopting the following ERM practices:

- *Establish a risk committee.* While the full board generally retains overall responsibility for risk oversight, a growing number of organizations are establishing risk committees. Based on the COSO Report, 47% of board members at financial services organizations indicated that they had a risk committee, versus 24% at nonfinancial services firms. Given the Dodd-Frank Act and other regulatory reforms, it's likely that these percentages will increase in the next few years. Regardless of the committee structure, the risk oversight roles of the full board and subcommittees (for example, audit, governance, and compensation) should be clearly defined. Boards should also ensure that they can effectively challenge management on risk issues by appointing board members and/or board advisors with deep risk management expertise. General risk education should also be provided to all board members.
- *Align board and management structures.* The risk governance structures at the board and management levels should be fully aligned. This alignment includes committee charters, roles and responsibilities, reporting relationships, approval and decision requirements, and information flows. As boards become more active in establishing risk policies and risk appetite, the role of the board versus the role of management should be clearly differentiated. The table above provides an example of the separation between management and the board in terms of ERM responsibilities. Alignment and clarification of roles would prevent unnecessary tensions and encroachments between management and the board.
- *Integrate strategy and risk.* Monitoring the organization's strategy and execution has long been the purview of boards. As boards become more active in ERM, the integration of strategy and risk is a logical and desirable outcome. Independent research studies[2] have found that when publicly traded firms suffer a significant decline in market value, 60% of the loss events were caused by strategic risks, 30% by operational risks, and 10% by financial risks. While integrated strategy and risk oversight is arguably a key role for the board, this process is still in its early stage of development. According to the COSO Report, fewer than 15% of board members indicated

While risk governance provides the organization for risk management and oversight, the board needs an instrument for *communicating its expectations and requirements.*

that they were fully satisfied with the board's processes for understanding and challenging the assumptions and risks associated with the business strategy.

- *Strengthen risk management independence.* Independent risk management is a core tenet for ERM. The board must ensure that risk management is independent of the business and operational activities of the organization. This includes formalizing the reporting relationship between the chief risk officer and the board or board risk committee. Moreover, under exceptional circumstances (for example, excessive risk taking, major internal fraud, or significant business conflicts), the chief risk officer should be able to escalate risk issues directly to the board without concern about his or her job security or compensation.

Policy

While risk governance provides the organization for risk management and oversight, the board needs an instrument for communicating its expectations and requirements. Board-approved risk policies represent a critical tool in this regard. As shown in the table, management's responsibility is to develop and execute risk management policies. The board's role is to approve the policies and monitor ongoing compliance and exceptions. Common issues related to risk policies include:

- Absence of explicit limits or tolerance levels for key risks.
- Lack of standards across different policies for ERM, credit risk, market risk, operational risk, etc.
- Insufficient reporting and monitoring of policy exceptions and resolutions.
- Key policy components are missing, or obscured by detailed procedures.

To establish effective risk policies and address the above issues, the board should communicate its expectations and standards with respect to risk policy structure and content. For example, an ERM policy may include the following components:

- *Executive summary.* The executive summary provides a concise description of the purpose, scope, and objectives for ERM. It may also provide a high-level summary of the key risk limits and risk-tolerance levels.
- *Statement of risk philosophy.* The statement of risk philosophy discusses the overall approach to risk management. It should also include guiding risk principles that articulate the desired risk culture of the organization.
- *Governance structure.* The section on governance structure summarizes board committees and charters, management committees and charters, and roles and responsibilities. Moreover, the delegation of authority, including risk management and oversight responsibilities for key individuals, should be documented.
- *Risk-tolerance levels.* This section provides a statement of risk appetite, including specific limits or tolerance levels for critical risk exposures. It also provides exception management and reporting requirements.
- *Risk framework and processes.* This section summarizes the ERM framework, as well as key processes and specific requirements for overall risk management.
- *Risk policy standards.* This section discusses policy standards for all other risks so that the structure and content of risk policies are consistent across the organization.
- *Risk categories and definitions.* This section provides a taxonomy for commonly used risk terms and concepts, facilitating a common language for risk discussions.

While its role is to approve and monitor risk policies, the board should actively discuss (if not debate) the risk limits or risk-tolerance levels that are appropriate for the organization, including the risk/return trade-offs at various risk appetite levels.

The linkage between risk management and compensation policies should be a top board issue. As one board member remarked, "People don't do what you tell them to do; they do what you pay them to do." As such, the board should ensure that risk management performance is considered in a meaningful way (for example, a 20% weighting or more) in executive management performance evaluations and incentives. The criteria may be specific risk management goals or an ERM scorecard that includes various quantitative and qualitative indicators. By incorporating ERM into executive management incentives, the board can have a far-reaching impact not only on management actions, but also on the incentives and actions of all employees.

Assurance

While risk policies articulate board requirements for ERM, the board still needs information and feedback. How does the board know if risk management is working effectively? This question is perhaps one of the most critical facing board members today. The answer lies in the assurance processes established by the organization, such as board monitoring and reporting, independent assessments, and objective feedback loops. Common issues related to risk assurance include:

- Ineffective board communication and reporting.
- Lack of independent assessments of the ERM program.
- Use of subjective indicators to gauge ERM effectiveness.

To fulfill its mandate to oversee ERM, the board must rely on management to provide critical information through communications and reports. Board members often criticize the quality and timeliness of the reports they receive. The standards that they want but are not getting to their satisfaction include:

- A concise executive summary of business/risk performance, as well as external performance drivers.
- Streamlined reports, including a focus on key board discussion and decision points.
- An integrated view of the organization, versus functional or silo views.
- Forward-looking analyses, versus historical data and trends.
- Key performance and risk indicators shown against specific targets or limits.
- Actual performance of previous business/risk decisions, as well as alternatives to, and rationale for, management recommendations for board decisions.
- More time allotted for discussions and board input, versus management presentations.

Recently, James Lam & Associates worked with the board members and executive team of a large financial institution to improve its board communication and reporting. In addition to adopting the above standards, the financial institution developed an ERM dashboard that provides key risk exposures and trends, as well as drill-down capability to underlying data. Additionally, each board member was provided with an iPad with preloaded dashboard software to support efficient board communication and reporting.

Information provided to boards should include objective feedback loops that gauge the effectiveness of ERM. The common practice is to evaluate risk management performance based on the achievement of key milestones or the lack of policy violations, losses, or surprises. However, implementation milestones or "negative proves" are not sufficient. The board needs to work with management to establish performance metrics and feedback loops for ERM. In a previous *RMA Journal* article ("ERM Back to the Future," June 2010), the use of earnings-at-risk was discussed as a feedback loop on ERM. Regardless of the metric, the board should decide on the appropriate feedback loop for risk management.

On an annual basis, boards should conduct two ERM assessments. First, they should oversee an independent review of the ERM program. The final product of this review would be an assessment of the organization's ERM program relative to board expectations, ERM development milestones, and industry best practices. Second, boards should conduct a self-assessment of their role in ERM.

Risk assurance is important not only to boards, but also to investors, rating agencies, and regulators. And a key objective for any ERM program should be to enhance risk transparency not only to executives and board members, but also to key external stakeholders. Disclosures in proxy and financial statements should provide information about the organization's governance, policy, and assurance practices. Moreover, quantitative information such as risk-tolerance levels, earnings sensitivity of key performance and risk drivers, and performance indicators on ERM should be disclosed. After all, no one likes surprises—whether they are negative operational events, ERM gaps, or unexpected earnings volatility.

Conclusion

Board members are not involved in day-to-day business activities, but they have the ultimate responsibility to ensure that an effective ERM program is in place. What can they do to effectively oversee ERM and the key risks facing the organization? They have three key levers. First, a well-thought out governance structure should be put in place to organize risk management and oversight activities. Second, risk policies and risk-tolerance levels should be established to articulate the board's expectations and risk appetite. Finally, boards should establish assurance processes and feedback loops to gauge the effectiveness of the ERM program. In short, boards must increase their risk GPA. ❖

James Lam *is president, James Lam & Associates, and author of* Enterprise Risk Management: From Incentives to Controls. *He has worked directly with boards on ERM across a wide range of industries and is currently serving on several corporate and advisory boards. He can be reached at* james@jameslam.com.

Notes

1. The research study commissioned by COSO is "Board Risk Oversight: A Progress Report" by Protiviti, released in December 2010.

2. Three independent studies, by James Lam & Associates (2004), Deloitte Research (2005), and the Corporate Executive Board (2005), analyzed what caused public companies to suffer a significant decline in stock price. The studies used different research methodologies, sample sizes, and observation periods, but the key findings (as summarized above) were generally consistent.