Director Notes

Strategic Risk Management: A Primer for Directors

by Mark L. Frigo and Richard J. Anderson

Recent significant risk events, including catastrophic weather events, cybercrime, macroeconomic issues, and supply chain interruptions, have resulted in an increased focus on risk and risk management by boards of directors. One of the board's key oversight roles is to understand the organization's strategic risks and the relationship between risk and strategy. This Director Notes describes the factors that are driving the need for strategic risk management, outlines a strategic risk assessment process, and offers recommendations for integrating risk management in strategy execution and measurement.*

As noted by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), "In the aftermath of the financial crisis, executives and their boards realize that ad hoc risk management is no longer tolerable and that current processes may be inadequate in today's rapidly evolving business world."[1] However, especially for non-financial companies that may be relatively new to these topics, enhancing risk management can be a somewhat daunting task.

This article focuses on two key aspects of the relationship between risk and strategy: (1) understanding the organization's strategic risks and the related risk management processes, and (2) understanding how risk is considered and embedded in the organization's strategy setting and performance measurement processes. These two areas not only deserve the attention of boards, but also fit closely with one of the primary responsibilities of the board—risk oversight.

* This *Director Notes* is adapted from Mark L. Frigo and Richard J. Anderson, *Strategic Risk Management: A Primer for Directors and Management Teams* (2012).

No. DN-V4N15
JULY 2012

THE CONFERENCE BOARD
Trusted Insights for Business Worldwide

The Advent of Strategic Risk Management

Enterprise risk management ("ERM") and risk management in general can encompass a wide range of risks that face any organization. Some risks may reflect exposures that, although harmful, will not threaten the overall health of an organization or its ability to ultimately meet its business objectives. For example, a temporary data center outage can result in a short-term problem or customer dissatisfaction, but once recovered, the organization can quickly be back on track. Other more significant risk events can be catastrophic, resulting in losses that can not only impair an organization's ability to meet its objectives, but may also threaten the organization's survival. The recent credit crisis is an example of this type of risk. These more significant risk exposures have given rise to a focus on "strategic risks" and "strategic risk management." "Strategic risks" are those risks that are most consequential to the organization's ability to execute its strategies and achieve its business objectives. These are the risk exposures that can ultimately affect shareholder value or the viability of the organization. "Strategic risk management" then can be defined as "the process of identifying, assessing and managing the risk in the organization's business strategy—including taking swift action when risk is actually realized." Strategic risk management is focused on those most consequential and significant risks to shareholder value, an area that merits the time and attention of executive management and the board of directors.

Standard & Poor's included the following attributes for strategic risk management in its 2008 announcement that it would apply enterprise risk analysis to corporate ratings:

> Management's view of the most consequential risks the firm faces, their likelihood, and potential effect; The frequency and nature of updating the identification of these top risks; The influence of risk sensitivity on liability management and financial decisions, and The role of risk management in strategic decision making.[2]

Clearly the potential impact of strategic risks is significant enough to deserve the attention of the board and its directors.

Strategic Risk Management and the Role of the Board

At the board level, strategic risk management is a necessary core competency.[3] In Ram Charan's book, *Owning Up: The 14 Questions Every Board Member Needs to Ask,* one of the questions posed is "Are we addressing the risks that could send our company over the cliff?"[4] According to Charan, boards need to focus on the risk that is inherent in the strategy and strategy execution:

> Risk is an integral part of every company's strategy; when boards review strategy, they have to be forceful in asking the CEO what risks are inherent in the strategy. They need to explore 'what ifs' with management in order to stress-test against external conditions such as recession or currency exchange movements.[5]

Regarding risk culture, Charan provides the following insight: "Boards must also watch for a toxic culture that enables ethical lapses throughout the organization. Companies set rules—but the culture determines how employees follow them."[6] We believe that corporate culture plays a significant role in how well strategic risk is managed and must be considered as part of a strategic risk assessment.

Understanding an Organization's Strategic Risks and Related Risk Management Processes

A necessary first step for boards to understand their strategic risks and how management is managing and monitoring those risks is a strategic risk assessment. A strategic risk assessment is a systematic and continual process for assessing the most significant risks facing an enterprise.[7] It is anchored and driven directly by the organization's core strategies. As noted in a 2011 COSO report, "Linkage of top risks to core strategies helps pinpoint the most relevant information that might serve as an effective leading indicator of an emerging risk."[8]

Conducting an initial assessment can be a valuable activity and should involve both senior management and the board of directors. Management should take the lead in conducting the assessment, but the assessment process should include input from the board members and, as it is completed, a thorough review and discussion between management and the board. These dialogues and discussions may be the most beneficial activities of the assessment and afford an opportunity for management and the directors to come to a consensus view of the risks facing the company, as well any related risk management activities.

The strategic risk assessment process is designed to be tailored to an organization's specific needs and culture. To be most useful, a risk management process and the resultant reporting must reflect and support an enterprise's culture so the process can be embedded and owned by management. Ultimately, if the strategic risk assessment process is not embedded and owned by management as an integral part of the business processes, the risk management process will rapidly lose its impact and will not add to or deliver on its expected role.

The Strategic Risk Assessment Process

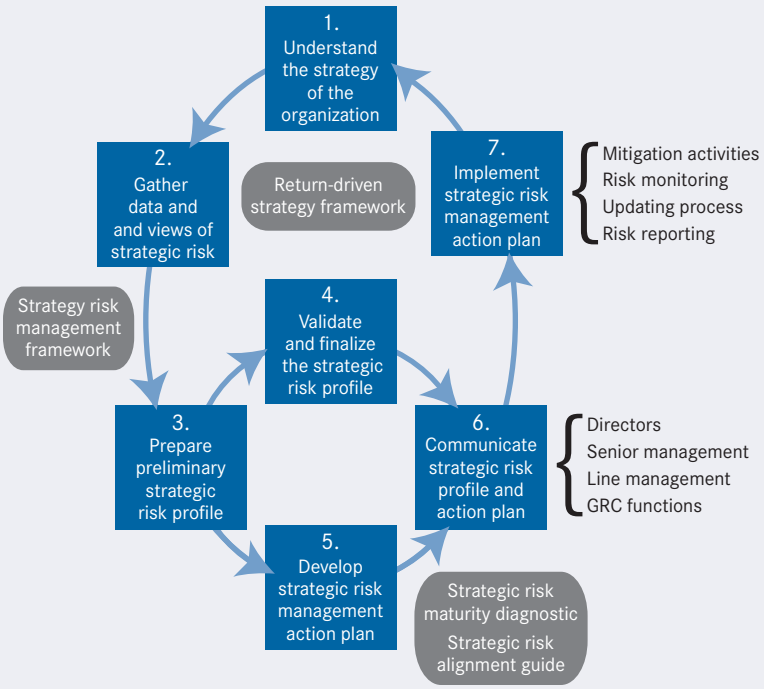
There are seven basic steps for conducting a strategic risk assessment:

1 **Achieve a deep understanding of the strategy of the organization** The initial step in the assessment process is to gain a deep understanding of the key business strategies and objectives of the organization. Some organizations have well-developed strategic plans and objectives, while others may be much more informal in their articulation and documentation of strategy. In either case, the assessment must develop an overview of the organization's key strategies and business objectives. This step is critical, because without these key data to focus around, an assessment could result in a long laundry list of potential risks with no way to really prioritize them. This step also establishes a foundation for integrating risk management with the business strategy. In conducting this step, a strategy framework could be useful to provide structure to the activity.[a]

2 **Gather views and data on strategic risks** The next step is to gather information and views on the organization's strategic risks. This can be accomplished through interviews of key executives and directors, surveys, and the analysis of information (e.g., financial reports and investor presentations). This data gathering should also include both internal and external auditors and other personnel who would have views on risks, such as compliance or safety personnel. Information gathered in Step 1 may be helpful to frame discussions or surveys and relate them back to core strategies. This is also an opportunity to ask what these key individuals view as potential emerging risks that should also be considered.

Figure 1

Strategic Risk Assessment Process



3 **Prepare a preliminary strategic risk profile** Combine and analyze the data gathered in the first two steps to develop an initial profile of the organization's strategic risks. The level of detail and type of presentation should be tailored to the culture of the organization. For some organizations, simple lists are adequate, while others may want more detail as part of the profile. At a minimum, the profile should clearly communicate a concise list of the top risks and their potential severity or ranking. Color-coded reports or "heat-maps" may be useful to ensure clarity of communication of this critical information.

4 **Validate and finalize the strategic risk profile** The initial strategic risk profile must be validated, refined, and finalized. Depending on how the data gathering was accomplished, this step could involve validation with all or a portion of the key executives and directors. It is critical, however, to gain sufficient validation to prevent major disagreements on the final risk profile.

5 **Develop a strategic risk management action plan** This step should be undertaken in tandem with Step 4. While significant effort can go into an initial risk assessment and strategic risk profile, the real product of this effort should be an action plan to enhance risk monitoring or management actions related to the strategic risks identified. The ultimate value of this process is helping and enhancing the organization's ability to manage and monitor its top risks.

6 **Communicate the strategic risk profile and strategic risk management action plan** Building or enhancing the organization's risk culture is a communications effort with two primary focuses. The first focus is the communication of the organization's top risks and the strategic risk management action plan to help build an understanding of the risks and how they are being managed. This helps focus personnel on what those key risks are and potentially how significant they might be. A second focus is the communication of management's expectations regarding risk to help reinforce the message that the understanding and management of risk is a core competency and expected role of people across the organization. The risk culture is an integral part of the overall corporate culture. The assessment of the corporate culture and risk culture is an initial step in building and nurturing a high performance, high integrity corporate culture.

7 **Implement the strategic risk management action plan** As noted above, the real value resulting from the risk assessment process comes from the implementation of an action plan for managing and monitoring risk. These steps define a basic, high-level process and allow for a significant amount of tailoring and customization to reflect the maturity and capabilities of the organization. As shown by Figure 1, strategic risk assessment is an ongoing process, not just a one-time event. Reflecting the dynamic nature of risk, these seven steps constitute a circular or closed-loop process that should be ongoing and continual within the organization.

[a] For a sample framework, see Mark L. Frigo and Joel Litman, *DRIVEN: Business Strategy, Human Actions and the Creation of Wealth* (Strategy & Execution, LLC 2008).

Integrating Strategic Risk Management in Strategy Setting and Performance Measurement Processes

The second step for an organization is to integrate strategic risk management into its existing strategy setting and performance measurement processes. As discussed above, there is a clear link between the organization's strategies and its related strategic risks. Just as strategic risk management is an ongoing process, so is the need to establish an ongoing linkage with the organization's core processes to set and measure its strategies and performance. This would include integrating risk management into strategic planning and performance measurement systems. Again, the maturity and culture of the organization should dictate how this performed. For some organizations, this may be accomplished through relatively simple processes, such as adding a page or section to their annual business planning process for the business to discuss the risks it sees in achieving its business plan and how it will monitor those risks. For organizations with more developed performance measurement processes, the Kaplan-Norton Strategy Execution Model described in *The Execution Premium* may be useful.[9] This model describes six stages for strategy execution and provides a useful framework for visualizing where strategic risk management can be embedded into these processes.

Stage 1: Develop the strategy This stage includes developing the mission, values, and vision; strategic analysis; and strategy formulation. At this stage, a strategic risk assessment could be included using the Return Driven Strategy framework to articulate and clarify the strategy and the Strategic Risk Management framework to identify the organization's strategic risks.

Stage 2: Translate the strategy This stage includes developing strategy maps, strategic themes, objectives, measures, targets, initiatives, and the strategic plan in the form of strategy maps, balanced scorecards, and strategic expenditures. Here, the strategic risk management framework would be used to develop risk-based objectives and performance measures for balanced scorecards and strategy maps, and for analyzing risks related to strategic expenditures.[10] At this stage, boards may also want to consider developing a risk scorecard that includes key metrics.

Stage 3: Align the organization This stage includes aligning business units, support units, employees, and boards of directors. The Strategic Risk Management Alignment Guide and Strategic Framework for GRC (Governance, Risk and Compliance) would be useful for aligning risk and control units toward more effective and efficient risk management and governance, and for linking this alignment with the strategy of the organization.[11]

Stage 4: Plan operations This stage includes developing the operating plan, key process improvements, sales planning, resource capacity planning, and budgeting. In this stage, the strategic risk management action plan can be reflected in the operating plan and dashboards, including risk dashboards. One organization we worked with developed a "resources follow risk" philosophy to make certain that resources were appropriately and efficiently allocated. This philosophy focused on ensuring that resources used in risk management are justified economically based on the relative amount of risk and cost-benefit analysis.

Stage 5: Monitor and learn This stage includes strategy and operational reviews. "Strategic risk reviews" would be part of the ongoing strategic risk assessment, which reinforces the necessary continual, closed-loop approach for effective strategy risk assessment and strategy execution.

Stage 6: Test and adapt This stage includes profitability analysis and emerging strategies. Emerging risks can be considered part of the ongoing strategic risk assessment in this stage. The strategic risk assessment can complement and leverage the strategy execution processes in an organization toward improving risk management and governance.

For more information about integrating risk management in the strategy execution model and a discussion of risk scorecards, see "Risk Management and Strategy Execution Systems."[12]

Final Thoughts: Moving Forward with Strategic Risk Management

Management teams and boards must challenge themselves and their organizations to move up the strategic risk management learning curve. Developing strategic risk management processes and capabilities can provide a strong foundation for improving risk management and governance. Boards may want to consider engaging independent advisors to advise and educate themselves on these matters. For organizations that are early in this process, the seven keys to success for improving ERM as described in a 2011 COSO Thought Leadership Paper may be useful, and are applicable in strategic risk management:

1. Support from the top is a necessity
2. Build ERM using incremental steps
3. Focus initially on a small number of top risks
4. Leverage existing resources
5. Build on existing risk management activities
6. Embed ERM into the business fabric of the organization
7. Provide ongoing ERM updates and continuing education for directors and senior management[13]

However the board decides to proceed, their leadership, direction, and overall oversight will be critical to the success of a strategic risk management process.

About the Authors

Mark L. Frigo, Ph.D., CMA, CPA, is director of the Center for Strategy, Execution and Valuation and the Strategic Risk Management Lab in the Kellstadt Graduate School of Business and Ledger & Quill Alumni Foundation Distinguished Professor at DePaul University in Chicago. He also is an advisor to management teams and boards in the area of Strategic Risk Management and strategy development and execution. He can be reached at mfrigo@depaul.edu or at www.markfrigo.com.

Richard J. (Dick) Anderson, MBA, CPA, is a Clinical Professor in the Center for Strategy, Execution and Valuation and the Strategic Risk Management Lab at DePaul University and a retired partner of PricewaterhouseCoopers LLP. With PwC, he was a regional leader in the Financial Services Advisory practice, consulting with major financial services organizations on internal auditing practices, risk management, and audit committee activities. He can be reached at rander37@depaul.edu.

Endnotes

1. "Effective Enterprise Risk Oversight: The Role of the Board of Directors," COSO 2009, p. 1.
2. "Enterprise Risk Management, Standard & Poor's to Apply Enterprise Risk Analysis to Corporate Ratings" Standard & Poor's press release, May 7, 2008 (www.standardandpoors.com).
3. Mark L. Frigo, "Strategic Risk Management: The New Core Competency," *Balanced Scorecard Report*, 11, no. 1, January–February 2009.
4. Ram Charan, *Owning Up: The 14 Questions Every Board Member Needs to Ask* (San Francisco: John Wiley & Sons 2009).
5. Charan, *Owning Up: The 14 Questions Every Board Member Needs to Ask*, p. 23.
6. Charan, *Owning Up: The 14 Questions Every Board Member Needs to Ask*, p. 28.
7. Mark L. Frigo and Richard J. Anderson, "Strategic Risk Assessment: A First Step for Improving Risk Management and Governance," *Strategic Finance*, December 2009.
8. Mark S. Breasley, Bruce C. Branson and Bonnie V. Hancock, "Developing Key Risk Indicators to Strengthen Enterprise Risk Management," COSO, 2011 p.2.
9. Robert S. Kaplan and David P. Norton, *The Execution Premium* (Cambridge, MA: Harvard Business Press, 2008).
10. Mark L. Frigo and Richard J. Anderson, "Strategic Risk Management: A Primer for Directors and Management Teams," 2012.
11. Mark L. Frigo and Richard J. Anderson, "A Strategic Framework for Governance, Risk and Compliance," *Strategic Finance*, February 2010.
12. Robert S. Kaplan, "Risk Management and Strategy Execution Systems," *Balanced Scorecard Report*, Vol. 11, No. 6, November-December 2009.
13. Mark L Frigo and Richard J. Anderson, "Embracing Enterprise Risk Management: Practical Approaches for Getting Started," COSO, 2011.

About Director Notes

Director Notes is a series of online publications in which The Conference Board engages experts from several disciplines of business leadership, including corporate governance, risk oversight, and sustainability, in an open dialogue about topical issues of concern to member companies. The opinions expressed in this report are those of the author(s) only and do not necessarily reflect the views of The Conference Board. The Conference Board makes no representation as to the accuracy and completeness of the content. This report is not intended to provide legal advice with respect to any particular situation, and no legal or business decision should be based solely on its content.

About the Series Director

Matteo Tonello is managing director of corporate leadership at The Conference Board in New York. In his role, Tonello advises members of The Conference Board on issues of corporate governance, regulatory compliance, and risk management. He regularly participates as a speaker and moderator in educational programs on governance best practices and conducts analyses and research in collaboration with leading corporations, institutional investors and professional firms. He is the author of several publications, including *Corporate Governance Handbook: Legal Standards and Board Practices,* the annual *U.S. Directors' Compensation and Board Practices* and *Institutional Investment reports, Sustainability in the Boardrooom,* and the forthcoming *Risk Oversight Handbook*. Recently, he served as the co-chair of The Conference Board Expert Committee on Shareholder Activism and on the Technical Advisory Board to The Conference Board Task Force on Executive Compensation. He is a member of the Network for Sustainable Financial Markets. Prior to joining The Conference Board, he practiced corporate law at Davis Polk & Wardwell. Tonello is a graduate of Harvard Law School and the University of Bologna.

About the Executive Editor

Melissa Aguilar is a researcher in the corporate leadership department at The Conference Board in New York focusing on issues of corporate governance, regulatory compliance, and risk management. Prior to joining The Conference Board, she was a contributor for more than five years at *Compliance Week,* where she reported on a variety of corporate governance topics, including proxy voting developments, executive compensation, risk management and shareholder activism. Her work has also appeared in Bloomberg's Bloomberg Brief Financial Regulation newsletter. Previously she held a number of editorial positions at SourceMedia Inc. Aguilar is a graduate of Binghamton University.

About The Conference Board

The Conference Board is a global, independent business membership and research association working in the public interest. Our mission is unique: to provide the world's leading organizations with the practical knowledge they need to improve their performance and better serve society. The Conference Board is a nonadvocacy, not-for-profit entity, holding 501(c)(3) tax-exempt status in the United States.

For more information on this report, please contact:
Melissa Aguilar, researcher, corporate leadership at 212 339 0303 or melissa.aguilar@conferenceboard.org

THE CONFERENCE BOARD, INC. www.conferenceboard.org
AMERICAS +1 212 759 0900 / customer.service@conferenceboard.org
ASIA-PACIFIC +65 6325 3121 / service.ap@conferenceboard.org
EUROPE/AFRICA/MIDDLE EAST +32 2 675 54 05 / brussels@conferenceboard.org
SOUTH ASIA +91 22 23051402 / admin.southasia@conferenceboard.org

THE CONFERENCE BOARD OF CANADA +1 613 526 3280 / www.conferenceboard.ca

© 2012 by The Conference Board, Inc. All rights reserved. Printed in the U.S.A.
The Conference Board® and the torch logo are registered trademarks of The Conference Board, Inc.