Strategic Risk Management: A Foundation for Improving Enterprise Risk Management and Governance

Mark L. Frigo and Richard J. Anderson

This article discusses the steps to success for organizations that want to improve their enterprise risk management. Management teams and boards of organizations of all types and sizes need to challenge themselves and their organizations to excel at strategic risk management. Developing strategic risk management processes and capabilities can become a strong foundation for improving risk management and governance.

Strengthening risk management and governance are major challenges for organizations following the global financial crisis. One of the lessons learned from the crisis was the necessity to clearly link strategy and risk management, and to be able to identify and manage risk in a highly uncertain environment. This article presents an overview of some of the latest developments in strategic risk management from the work we are doing with management teams and boards. The article also discusses research in the Strategic Risk Management Lab at DePaul University, along with collaborative research with the Committee of Sponsoring Organizations of the Treadway Commission (COSO) and other professional organizations. We describe the factors that are driving the need for strategic risk management and the underlying barriers, as well as some approaches to overcome those barriers. We present a definition of strategic risk management, a strategic risk assessment process, and recommendations for integrating risk management in strategy execution.

EVOLUTION OF RISK MANAGEMENT

Managing risk is certainly not a new concept to businesses and their management teams. But as the complexity and speed of the business environment have continued to evolve, a growing focus on risk management has emerged, including an expansion of the focus to the broader, enterprise-wide risks facing organizations. Risk management practices and processes have continued to develop, along with a growing awareness of risk on the part of boards and audit committees. However, there was until a few years ago no accepted framework or standard that could be used to establish or evaluate risk management activities.

To address that situation, COSO undertook a project to develop a framework that could be used by management teams to evaluate and improve their organizations' risk management activities. In 2004, COSO issued *Enterprise Risk*

Published online in Wiley Online Library (wileyonlinelibrary.com).
DOI 10.1002/jcaf.20677

Management—Integrated Framework to fill that gap. The COSO framework is a robust, enterprise-wide framework that is intended to encompass enterprise risk management (ERM) and be applied in both strategy and across the enterprise, "at every level and unit."

While the COSO ERM framework gained widespread recognition, its development and publication coincided with the implementation of the Sarbanes-Oxley Act of 2002 (SOX). For many organizations and their audit committees, dealing with the implementation and reporting requirements of SOX was overwhelming: it demanded virtually all their attention. Audit committees became very compliance-focused and had little time left to deal with strategic issues or enterprise-wide risks. Significant attention was placed on the COSO Internal Control Framework, which was extensively used by organizations in complying with the financial controls–related requirements of SOX. However, much less (if any) attention was given to the COSO ERM Framework, because SOX did not require or really even address ERM.

Following the period of SOX implementation, the past few years have seen an unprecedented series of economic losses and the destruction of stakeholder value as certain organizations have been negatively impacted by various events and risks. This situation has caused a renewed focus on risk and how boards and executives are managing the risks in their organizations. As a result, a number of countries, such as the United States, United Kingdom, and Australia, have now required boards and/or audit committees to focus more on risk and risk management. Recently, the International Organization for Standardization (ISO) issued ISO 31000:2009—Risk Management, which sets out principles, a framework, and a process for the management of risk that are applicable to any type of organization, whether in the public or private sector. Rating agencies, including Moody's and Standard & Poor's, have also indicated their interest and focus on risk management practices, including full ERM.

POSITIONING ERM AS STRATEGIC AND VALUE-CREATING[1]

ERM differs from a traditional risk management approach, frequently referred to as a "silo" or "stovepipe" approach, where risks are often managed in isolation. In those environments, risks are managed by business-unit leaders with minimal oversight or communication of how particular risk management responses might affect other risk aspects of the enterprise, including strategic risks. In contrast, ERM seeks to strategically consider the interactive effects of various risk events with the goal of balancing an enterprise's portfolio of risks to be within the stakeholders' appetite for risk. The ultimate objective is to increase the likelihood that strategic objectives are realized and that value is preserved and enhanced.

ERM seeks to strategically consider the interactive effects of various risk events with the goal of balancing an enterprise's portfolio of risks to be within the stakeholders' appetite for risk.

Several conceptual frameworks have been developed in recent years that provide an overview of the core principles for effective ERM processes. COSO defined ERM in its *Enterprise Risk Management—Integrated Framework* (see www.coso.org)[2]:

> Enterprise risk management is a process, effected by the 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 the risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.

Note that ERM is directly related to "strategy setting." For ERM to be value-creating, it must be embedded in and connected directly to the enterprise's strategy. Another part of this definition refers to the goal of ERM, which is to help the enterprise achieve its core objectives. So to be effective, ERM must be part of the strategic planning process and the strategy-execution processes.

The rise in the volume and complexities of risks is complicated by the fact that many of the techniques used by boards and senior executives are dated, lack sophistication, and are often *ad hoc.* Few boards and senior executives have robust key-risk indicators that provide adequate

DOI 10.1002/jcaf

data to recognize shifts in risk patterns within and external to their organizations, resulting in an inability to proactively alter strategic initiatives in advance of when risk events occur. In response to these changing trends, organizations are embracing ERM because it emphasizes a top-down, holistic approach to effective risk management for the entire enterprise. The goal of ERM is to increase the likelihood that an organization will achieve its objectives by managing risks to be within the stakeholders' appetite for risk. ERM done correctly should ultimately not only protect, but also create stakeholder value.

The term *governance, risk, and compliance* (GRC) has come into increasingly common use, particularly by consultants and vendors. However, there is not a good universal understanding of the term or its objectives. In some cases, the GRC term is associated with various technology tools, designed to assess risks or conduct automated tests of controls. In other cases, the GRC label is attached to a unit within the organization that is conducting controls testing across the organization. GRC should really be viewed as a holistic approach or framework, intended to enable a look across an organization's various risk and control units to align their unique roles around common objectives (e.g., protecting shareholder value) and then leverage common processes and knowledge to increase their efficiency and effectiveness. For example, an organization may have multiple risk and control units, each conducting separate risk assessments. The Strategic GRC Framework, which was presented in *Strategic Finance* in February 2009, includes a framework that is useful in explaining these concepts.[3]

THE ADVENT OF STRATEGIC RISK MANAGEMENT

Today, directors and executives are seeing increased expectations from shareholders, regulators, rating agencies, and other stakeholders that they understand and are managing strategic risks, and that there is transparency around that management process.

While ERM and risk management in general can encompass a wide range of risks, it appears that this re-emergence of risk management, when coupled with the catastrophic losses incurred by some organizations, has given rise to a focus on "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.

Despite rising to greater prominence in many companies, risk management has not generally attracted significant financial investment over the past year.

Strategic risk management is 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, then, is focused at the most consequential and significant risks to shareholder value—clearly an area deserving of the time and attention of executive management and the directors. A set of attributes for strategic risk management is contained in the 2008 announcement by Standard & Poor's and includes: "Management's view of the most consequential risk 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."[4]

As a recent study from the Economist Intelligence Unit concludes, "Strategic risk management remains an immature activity in many companies."[5] The study also found that there is "limited appetite for investment in the risk function. Despite rising to greater prominence in many companies, risk management has not generally attracted significant financial investment over the past year. Less than one-half of companies have invested in risk processes, while less than one-quarter have allocated funds to headcount or the training of managers in the central risk function. Ongoing cost constraints and company-wide budget freezes are undoubtedly helping to curtail investment, but care must be taken not to compromise the effectiveness of overall risk management." This situation presents a dilemma, where risk management remains immature and resource constraints present a barrier to further development.

In 2010, the Risk and Insurance Management Society, Inc. (RIMS) announced that it is increasing its focus on the evolving role of risk management with the creation of a strategic risk management development council. This development follows a comprehensive analysis by

 DOI 10.1002/jcaf

the RIMS strategic planning task force and board of directors to better equip RIMS member companies in tying their risk management programs to strategic goals.

STRATEGIC RISK MANAGEMENT (DEFINITION)

> Strategic Risk Management is a process for identifying, assessing and managing risk anywhere in the strategy with the ultimate goal of protecting and creating shareholder value. It is a primary component and foundation of Enterprise Risk Management; it is effected by boards of directors, management and other personnel; it requires a strategic view of risk and consideration of how external and internal events or scenarios will affect the ability of the organization to achieve its objectives; it requires an organization to define a tolerable level of risk or risk appetite as a guide for strategic decision making; and it is a continual process which should be embedded in strategy setting and strategy management.[6]

This definition is based on six principles of strategic risk management:

1. It is a process for identifying, assessing, and managing risk anywhere in the strategy, with the ultimate goal of protecting and creating shareholder and stakeholder value.
2. It is a primary component and foundation of enterprise risk management.
3. It is effected by boards of directors, management, and others.
4. It requires a strategic view of risk and consideration of how external and internal events or scenarios will affect the ability of the organization to achieve its objectives.
5. It requires an organization to define a tolerable level of risk or risk appetite as a guide for strategic decision making.
6. It is a continual process that should be embedded in strategy setting and strategy management.

Before management can effectively manage risks that might be identified by various scenario analyses, they need to define an overriding risk management goal.

THE RELATIONSHIP OF RISK AND STRATEGY

The first step in understanding strategic risk management surrounds defining the entity's use of the term "risk." Michael Porter's definition in his landmark book *Competitive Advantage* is useful:

> Risk is a function of how poorly a strategy will perform if the 'wrong' scenario occurs.[7]

Strategic risk management begins by identifying and evaluating how a wide range of possible events and scenarios will impact a business's strategy execution, including the ultimate impact on the valuation of the company. Before management can effectively manage risks that might be identified by various scenario analyses, they need to define an overriding risk management goal. Risk appetites can vary across industries and entities.

The Return Driven Strategy framework has been used as an effective tool for integrating strategic goals and risk management goals.[8] The framework is the result of more than a decade of research and application, involving the study of thousands of companies and the identification of strategic activities that separate the best performers from the worst. The Return Driven Strategy framework describes the hierarchy of strategic activities of best-performing companies in terms of financial impact and shareholder value.

The Return Driven Strategy is composed of eleven core tenets and three foundations that together form a hierarchy of interrelated activities that companies must perform to deliver superior financial performance. These tenets and foundations summarize the common activities of high-performance companies and identify flawed strategies of marginal performers.[9] As boards and management teams use the framework to evaluate strategies, they start to hone in on the risk areas, thereby using it as a *de facto* strategic risk assessment framework.

STRATEGIC RISK MANAGEMENT AS A CORE COMPETENCY FOR MANAGEMENT AND THE BOARD

In their 1990 *Harvard Business Review* article, C.

DOI 10.1002/jcaf

K. Prahalad and Gary Hamel introduced the concept of *core competence*, which has some striking applications to strategic risk management. A key concept is that "core competence is about harmonizing. . . ."[10] Harmonizing risk management capabilities and processes is critical for advancing risk management. Another dimension relating to strategic risk management as a core competency relates to avoiding the silo problem, which is prevalent in risk management and analogous to the concept: "core competence is communication, involvement and deep commitment to working across organizational boundaries" as a central theme of core competencies.[11]

At the board level, strategic risk management is also a necessary core competency. In his recent book, *Owning Up: The 14 Questions Every Board Member Needs to Ask,* one of the questions Ram Charan asks is "Are we addressing the risks that could send our company over the cliff?"[12] 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.[13]

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."[14]

STRATEGIC RISK ASSESSMENT

A strategic risk assessment is a systematic and continual process for assessing significant risks facing an enterprise.[15] Conducting an initial assessment is a valuable activity for senior management and the board of directors. 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 that the process can be embedded and owned by management. If the risk assessment and management processes *aren't* embedded and owned by management as an integral part of their business processes, then the risk management process will rapidly lose its impact and not add to or deliver on its expected role. To help you conduct strategic risk assessments, we have shown key strategic risk management tools and diagnostics at their appropriate points in the process. Here are the seven steps for conducting a strategic risk assessment:

Harmonizing risk management capabilities and processes is critical for advancing risk management.

1. Achieve a deep understanding of the strategy of the organization.
2. Gather views and data on strategic risks.
3. Prepare a preliminary strategic risk profile.
4. Validate and finalize the strategic risk profile.
5. Develop a strategic risk management action plan.
6. Communicate the strategic risk profile and strategic risk management action plan.
7. Implement the strategic risk management action plan.

These steps define a basic, high-level process and allow for a significant amount of tailoring and customization in their execution to reflect the maturity and capabilities of an organization. They also show that Strategic Risk Assessment is an ongoing process, not just a one-time event. Reflecting the dynamic nature of risk, the seven steps constitute a circular, or closed-loop, process that should be an ongoing and continual process within the organization.

INTEGRATING RISK MANAGEMENT IN STRATEGY EXECUTION

A strategic risk management action plan should consider how risk assessment and risk management can be integrated into strategy-execution processes. This would include integrating risk management into strategic planning and performance measurement systems. The Kaplan-Norton Strategy Execution Model[16] describes six stages for strategy execution and provides a useful framework for visualizing where risk management can be done.

- **Stage 1—Develop the Strategy**: This stage includes developing mission, values,

DOI 10.1002/jcaf

and vision; strategic analysis; and strategy formulation.

At this stage, a strategic risk assessment could be included that could use 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 in developing risk-based objectives and performance measures for balanced scorecards and strategy maps. It would also be useful for analyzing risks related to strategic expenditures. You could also consider developing a risk scorecard at this stage.

- **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 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.

- **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.

- **Stage 5—Monitor and Learn**: This stage includes strategy reviews 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.

The strategic risk assessment can complement and leverage the strategy-execution processes in an organization toward improving risk management and governance.

- **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 discussion on integrating risk management in the strategy-execution model and a discussion of risk scorecards, see Robert S. Kaplan, "Risk Management and Strategy Execution Systems," *Balanced Scorecard Report*, November–December 2009.[17]

CRITICAL STEPS FOR VALUE-ADDED STRATEGIC RISK MANAGEMENT

Strategic risk management is increasingly being viewed as a core competency at both the management and board levels. In fact, board members are increasingly focused on strategic risk management, asking executives such questions as "Of the top strategic business risks the company faces, which ones are you looking at, and what countermeasures are you devising?" The Strategic Risk Management Lab in the Center for Strategy, Execution, and Valuation at DePaul University is sharing with management teams and boards emerging best practices gleaned from its research. Here is a working list of practices worth striving toward.[18]

- *Communicate and share information across business and risk functions—and externally.* This is considered by some to be the ultimate risk management "best practice."
- *Break down risk management silos.* Establish interdisciplinary risk management teams so that each functional area can understand where it fits into the entire company strategy and how it affects other areas.
- *Identify and, where possible, quantify strategic risks* in terms of their impact on revenue, earnings, reputation, and shareholder value.
- *Make strategic risk assessments part of the process of developing strategy, strategic plans, and strategic objectives.* Again, this requires

DOI 10.1002/jcaf

a combination of skills that can be achieved by creating interdisciplinary teams.
- *Monitor and manage risk through the organization's performance measurement and management system*, including its balanced scorecard.
- *Account for strategic risk and embed it within the strategic plan and strategic plan management process.* Wherever scenario planning is included in the strategic plan, there should also be a discussion of countermeasures in the event that a risk event occurs.
- *Use a common language of risk throughout your organization.* Everyone must understand the organization's particular drivers of risk, its risk appetite, and what management considers acceptable risk levels.
- *Make strategic risk management, like strategy management itself, a continual process.* Risk is inherently dynamic, so risk management and assessment must evolve from being an event to being a process—and must include regular analysis and critical risk information refreshes. Strategic risk management reviews should be conducted as part of regular strategy reviews.
- *Develop key risk indicators (KRIs) to continuously monitor the company's risk profile.* Like the balanced scorecard with its measures, targets, and initiatives, the risk management system should include KRIs, thresholds, and trigger points, as well as countermeasures to mitigate or manage the risk.
- *Integrate ERM into strategy-execution systems.* This means integrating ERM into the entire management system. This will require strategic risk management as a core competency in organizations and a commitment to continuously monitor and manage risk in the strategy and its execution.

MOVING FORWARD WITH STRATEGIC RISK MANAGEMENT

Management teams and boards need to challenge themselves and their organizations to move up the strategic risk management learning curve. Developing strategic risk management processes and capabilities can become a strong foundation for improving risk management and governance. The keys to success for improving ERM as described in a recent COSO report[19] are very applicable in strategic risk management, which include building ERM in incremental steps and focusing on the top risks of an organization, the strategic risks.

NOTES

1. See Beasley, M. S., & Frigo, M. L. (2007, May). Strategic risk management: Creating and protecting value. *Strategic Finance*, pp. 25–31, for more information. Also see Beasley, M., Hancock, B. V., & Branson, B. C. (2009). Strengthening enterprise risk management for strategic advantage. Retrieved from http://www.coso.org/documents/COSO_09_board_position_final102309PRINTandWEBFINAL.pdf.
2. Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2004). *Enterprise risk management—Integrated framework.* Retrieved from http://www.coso.org/ERM-IntegratedFramework.htm.
3. Frigo, M. L., & Anderson, R. J. (2009, February). A strategic framework for governance, risk, and compliance. *Strategic Finance.* Retrieved from http://findarticles.com/p/articles/mi_hb6421/is_8_90/ai_n31912096/.
4. Standard and Poor's. (2008, May 7). Enterprise risk management, Standard & Poor's to apply enterprise risk analysis to corporate ratings. S&P press release. Retrieved from http://www2.standardandpoors.com/spf/pdf/events/CRTconERM5908.pdf.
5. Economist Intelligence Unit. (2010). Fall guys: Risk management in the front line. Retrieved from http://www.businessresearch.eiu.com/fall-guys.html.
6. Frigo, M. L., & Anderson, R. J. (2010). *Strategic risk management: A primer for directors and management teams.* Chicago, IL: Strategy and Execution.
7. Porter, M. E. (1985). *Competitive advantage: Creating and sustaining superior performance.* New York: Free Press, p. 476.
8. Beasley, M. S., & Frigo, M. L. (2007, May). Strategic risk management: Creating and protecting value. *Strategic Finance*, pp. 25–31.
9. Frigo, M. L., & Litman, J. (2008). *Driven: Business strategy, human actions and the creation of wealth.* Chicago, IL: Strategy and Execution.
10. Prahalad, C. K., & Hamel, G. (1990). The core competence of the corporation. *Harvard Business Review*, 68(3), 79–91, p. 82.
11. Ibid.
12. Charan, R. (2009). *Owning up: The 14 questions every board member needs to ask.* Hoboken, NJ: Wiley.
13. Ibid., p. 23.
14. Ibid., p. 28.
15. Frigo, M. L., & Anderson, R. J. (2009, December). Strategic risk assessment: A first step for improving risk management and governance. *Strategic Finance.* Retrieved from http://www.imanet.org/PDFs/Public/SF/2009_12/12_09_frigo.pdf.
16. Kaplan, R. S., & Norton, D. P. (2008). *The execution premium.* Boston, MA: Harvard Business Press.
17. Kaplan, R. S. (2009, November–December). Risk management and strategy execution systems. *Balanced Scorecard Report.* Boston, MA: Harvard Business Publishing.
18. See article by Frigo, M. L. (2009, January–February). Strategic risk management: The new core competency. *Balanced Scorecard Report.* Boston, MA: Harvard Business Publishing.
19. Frigo, M. L., & Anderson, R. J. (2011). Embracing enterprise risk management: Practical approaches for getting started. Retrieved from http://www.coso.org/documents/EmbracingERM-GettingStartedforWebPostingDec110.pdf.

 DOI 10.1002/jcaf

Mark L. Frigo, PhD, CPA, CMA, is the director of the Center for Strategy, Execution and Valuation and the Strategic Risk Management Lab in the Kellstadt Graduate School of Business and the Ledger & Quill Alumni Foundation Distinguished Professor in the School of Accountancy at DePaul University in Chicago. He is an advisor to management teams and boards in the area of strategic risk management and strategy development and execution. You can reach him at mfrigo@depaul.edu. **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. You can reach him at rander37@depaul.edu.

This article is adapted from the book *Strategic Risk Management: A Primer for Directors and Management Teams* by Mark L. Frigo and Richard J. Anderson, and from the forthcoming book, by the same authors, *Strategic Risk Management: Creating and Protecting Value in an Uncertain World.*

DOI 10.1002/jcaf