Strategic Risk Assessment

A first step for improving risk management and governance.

By Mark L. Frigo and Richard J. Anderson

ILLUSTRATION: TIM LEE/WWW.LEEILLO.COM

The recent economic environment and negative events of 2008 and 2009 that significantly impacted many organizations have created a new or renewed emphasis on risk and risk management. In particular, boards of directors are focusing on risk and the related risk management practices of their organizations and are asking management tough questions about how those organizations identify, assess, monitor, and manage their risks. CFOs and management teams are being challenged to respond by actively participating in risk assessments and risk management initiatives. This trend has been especially evident in nonfinancial companies as shown by the expanded focus of rating agencies, such as Standard & Poor's, on risk management activities in nonfinancial companies. This new focus has spawned a variety of activities, including risk assessments, enterprise risk management (ERM) initiatives, or governance, risk, and compliance (GRC) initiatives. For many directors and management teams, this heightened focus on risk is new and somewhat daunting. Of particular concern is the question of where to start. Where should the valuable time of directors and senior management be directed to generate the maximum benefit for the organization?

Focusing on Strategic Risk

Based on our interactions with directors and senior executives, we believe the right place for a board to start is to focus on the identification and management of strategic risks—those risks that are most consequential to an organization's ability to execute its strategy, achieve its business objectives, and build and protect value. This strategic focus isn't intended to identify every risk facing the organization but to identify those that are most significant to its ability to achieve and realize its core business strategy and objectives. Accordingly, these should be the risks that are of most concern to senior management and directors and most deserving of their time and attention. This focus on strategic risk will also reinforce the direct relationship and critical link connecting the organization's strategy, strategy execution, and risk management processes.

The starting point is a Strategic Risk Assessment designed to identify an organization's strategic risks and related action plans to address those risks.

Strategic Risk Assessment

A Strategic Risk Assessment is a systematic and continual process for assessing significant risks facing an enterprise. Conducting an initial assessment is a valuable activity for senior management and the board of directors. Current thought leadership on corporate governance and board responsibilities is virtually unanimous that a key board responsibility is to understand an organization's strategies and associated risks and to ensure that management's risk management practices are appropriate. For example, *Key Agreed Principles to Strengthen Corporate Governance for U.S. Publicly Traded Companies*, published by the National Association of Corporate Directors (NACD), indicates that: "For most companies, the priority focus of board attention and time will be understanding and providing guidance on *strategy and associated risk*…and monitoring senior management's performance in both carrying out the *strategy and managing risk*." [emphasis added]

How to Conduct a Strategic Risk Assessment

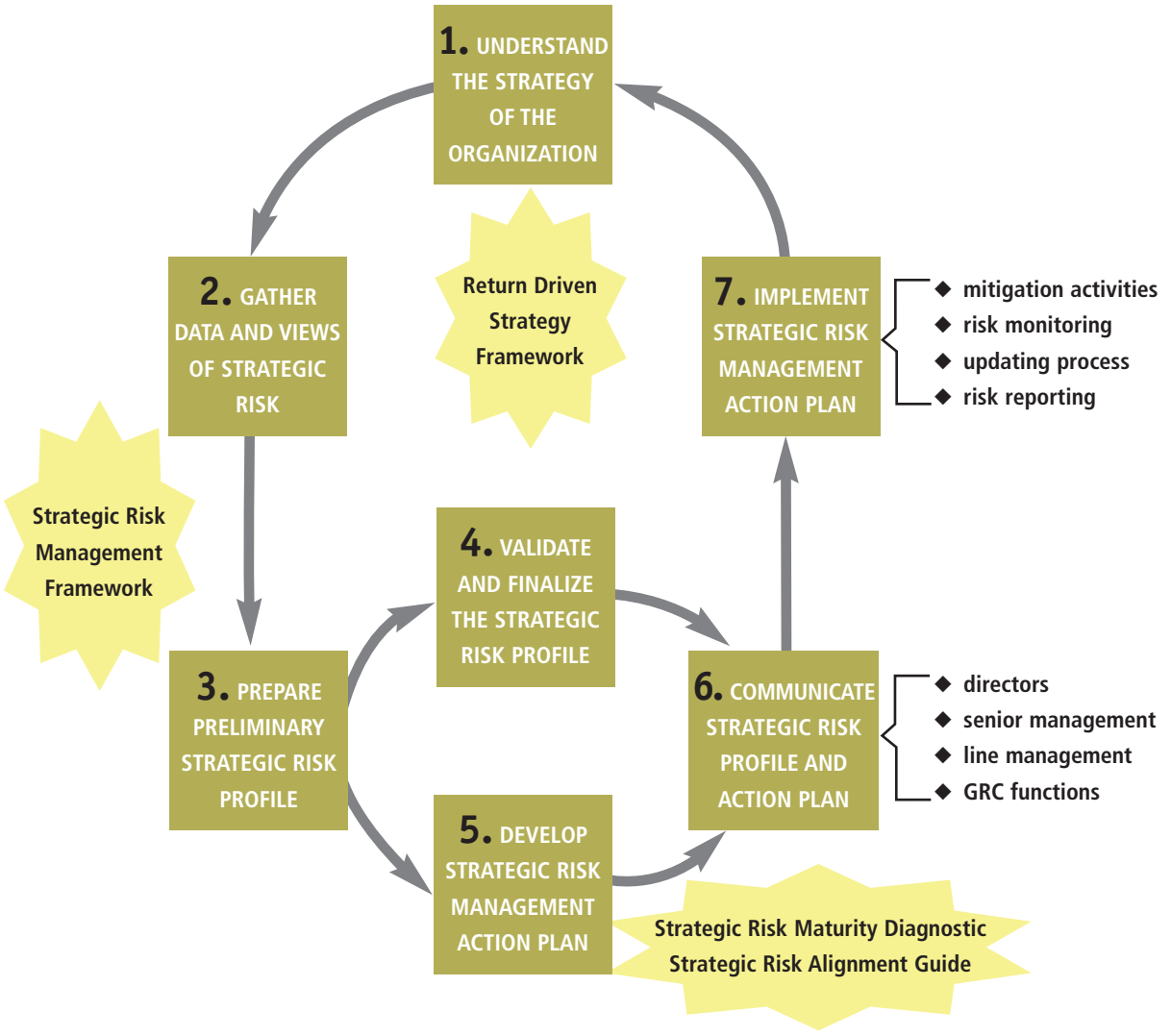
The Strategic Risk Assessment process we describe is designed to be tailored to an organization's specific needs and culture. To be most useful, a risk management process and the resultant reporting must reflect and support an enterprise's culture so the process can be embedded and owned by management. 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 (see "Strategic Risk Management Tool Kit" on p. 31 for helpful references).

Here are the seven steps for conducting a Strategic Risk Assessment:

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, and
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 the organization. They also show that Strategic Risk Assessment is an ongoing process, not just a one-time

Figure 1: Strategic Risk Assessment Process



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 (see Figure 1).

Typically, the Strategic Risk Assessment is performed by management with input and validation by the directors. In this process, it's important to link the assessment of risk directly into the organization's strategies and strategy execution processes. The exact format of the assessment and the resulting Strategic Risk Profile are dependent on the level of maturity of the organization's risk management processes. For example, organizations that are in the early development of risk management processes may find basic lists or matrices of risks useful for presentation, and organizations with more-mature risk management processes may find more-detailed or quantitative profiles more useful.

Step 1: Achieve a Deep Understanding of the Strategy of the Organization

The first step in the process is to develop a thorough understanding of the organization's strategy and its key components. The focus here is to identify the specific risks associated with the core strategy, so it's important to have this deep understanding of the strategy and its key elements. The Return Driven Strategy (RDS) framework has been a useful tool for facilitating and giving structure to this step. This framework provides a lens to deconstruct and analyze the strategy and to identify, classify, and link its critical elements according to the tenets and foundations of the RDS framework. In later steps, this process will allow a more-detailed assessment of the risks associated with each tenet.

For example, one of the supporting tenets of the RDS framework is to "Partner Deliberately," so the assessment

Figure 2: Strategic Risk Management Framework

needs to consider and identify any key initiatives in the organization's strategy where partnering is to be conducted. These initiatives can take many forms, including joint ventures, offshoring, outsourcing, or other alliances. An organization may have many partnering arrangements, some of which are relatively low risk—for example, running the cafeteria—while others, such as outsourcing information technology, can present much higher risk. Accordingly, the key question is which partners or partnering arrangements are critical to the execution of the strategy. Those are the arrangements we're trying to identify.

Much of the information for this step can be obtained from corporate and business unit plans, strategy summaries, and management and board materials. At the end of this step, the board and management should have a clear understanding of the key elements of the organization's strategy and how they are linked within the RDS framework.

Step 2: Gather Views and Data on Strategic Risks

In this step, the objective is to gather data and views from management and directors on the key strategic risks associated with the core business strategy. There are several ways to do this, such as executive interviews, surveys, or focus groups. Here the culture of the organization should be considered. Some organizations are very receptive to surveys, but others aren't. If management is spread out geographically, individual interviews may be difficult, so teleconferencing or phone interviews are good options. Key members of management, including business-line leaders, should be asked to participate. It may also be useful to obtain the views of some members of the board, especially the audit committee members, and the organization's internal and external auditors.

In gathering data, a company should consider, review, and leverage information already available within the organization—for example, risk assessments performed by internal groups such as legal, compliance, or internal audit or assessments performed related to Sarbanes-Oxley Act (SOX) compliance. The required risk disclosures for public companies also should be reviewed carefully.

In conducting these assessments, we've found that, rather than simply asking an open-ended question about what an individual considers strategic risks to be, providing a structure or areas of focus can make the interviews more productive. Here, the Strategic Risk Management (SRM) framework is useful. The components of the SRM framework (Figure 2) correspond to the tenets of the RDS framework. Discussions and questions may be built from risk areas of the SRM framework related to the strategy classifications defined in Step 1.

Participants should also be encouraged to identify external risks they believe would inhibit the organization's ability to achieve its strategic and business objectives. These external factors could include systemic risks,

Figure 3: Example of Strategic Risk Maturity Diagnostic

1. RISK MANAGEMENT CULTURE AND GOVERNANCE

a. Does the company have a risk management program?

1—WEAK	2—ADEQUATE	3—ENHANCED	4—LEADING PRACTICE
◆ No formal ERM program, framework, or structure in place. ◆ Ad hoc/limited coordination and/or communication between risk and control functions.	◆ Early-stage ERM program, framework, or structure in development. ◆ Modest coordination and/or communication between risk and control functions.	◆ Formal, independent ERM program, framework, or structure in place and functioning on a repeatable basis. ◆ Regular coordination and/or communication among risk, control, and planning functions. ◆ Common risk criteria and definitions used across the organization. ◆ Communications on risk and risk management to all levels of the organization.	◆ Board-approved risk policy establishes clear roles and accountabilities. ◆ Risk management acknowledged as part of the organization's culture. ◆ Formal, independent ERM program, framework, or structure in place and evaluated/validated by credible third party. ◆ Extensive collaboration, coordination, and/or communication among risk, control, and planning functions.

emerging risk areas, or other external factors such as regulation. Participants can also rate the possible severity or impact of the risks they identify.

Step 3: Prepare a Preliminary Strategic Risk Profile

The information obtained in the first two steps is now used to prepare a preliminary Strategic Risk Profile. The format and complexity of the risk profile should be tailored to match the risk maturity and capabilities of the organization. Enterprises just starting to formalize their risk management processes should keep this profile straightforward and simple. As this information is intended to spur discussion and understanding at executive and board levels, excess detail or amounts of data may be counterproductive. Many organizations find graphical presentations helpful—for example, heat maps using colors to convey levels of risk. Others start with basic lists and then add detail and complexity as their risk processes mature.

Companies also find it useful to communicate the potential level of exposure or impact associated with a risk area or type. Traditionally, they used probability and impact analyses. Recently, however, there has been concern about exposure to high-impact/low-probability risks ("black swan" events based on the 2007 book, *The Black Swan: The Impact of the Highly Improbable*, by Nassim Nicholas Taleb), such as systemic risks that frequently have been overlooked because of their very low probability. For these types of risks, some organizations are adding new dimensions, such as the velocity of the risk or their organization's preparedness for the risk, to their traditional risk measures. Again, the level of detail and complexity of the Strategic Risk Profile should mirror the maturity of the organization's risk management processes.

Step 4: Validate and Finalize the Strategic Risk Profile

(Note: We present Steps 4 and 5 in sequence, but it's best to execute them in tandem.) The preliminary Strategic Risk Profile must be validated with key participants to ensure that it reflects their views of the most critical strategic risks. Again, which participants are involved and the exact process that's used to validate the Strategic Risk Profile may depend on the culture of the enterprise. Some organizations circulate the preliminary profile for comments, others conduct follow-up interviews, and others use small group presentations and discussions. This validation process may include all stakeholder participants or only a portion of the group. Possible risk profile

Figure 4: Example of Strategic Risk Management Alignment Guide

RISK CATEGORY (1)	RISK OWNER (2)	RISK APPETITE METRICS (3)	MONITORING (4)	ACTION PLANS (5)	BOARD OVERSIGHT (6)	COMPANY OVERSIGHT (7)
REPUTATION	CEO	POLICY APPROVED XX/XX/XX	CORPORATION AFFAIRS	APPROVED & UPDATED XX/XX/XX	FULL BOARD	EXECUTIVE COMMITTEE
OPERATIONAL	COO	METRICS IN PLACE FOR ALL OPERATING DIVISIONS	OPERATIONS MANAGEMENT DAILY MONITORING AND REPORTING	PLANS IN PLACE FOR EACH TRIGGER POINT	RISK COMMITTEE	RISK MANAGEMENT INTERNAL AUDIT

(1) Strategic risk categories as defined and used on an enterprise-wide basis
(2) Member of management responsible for each risk category
(3) Risk appetite or limit approved by management and the board
(4) Monitoring activities performed for the risk category
(5) Existence and status of action plans to address deterioration in the risk category
(6) Board unit responsible to oversee management of the risk category
(7) Company unit responsible for assurance or oversight of the risk activities of the category

reporting formats can also be circulated to get input and views on the various formats. Remember, though, that it's critically important to the entire assessment process that enough participants validate the profile and the risks highlighted.

Companies then can use input and comments from this validation step to make any needed revisions to the risk profile and report format. This validation is also an opportunity to build further buy-in to the entire Strategic Risk Assessment process and the value to be obtained from the information gathered during the assessment.

Step 5: Develop a Strategic Risk Management Action Plan

Once the strategic risks are identified, senior management and the directors will be quick to ask about plans to mitigate or monitor them, so we suggest that companies develop and implement initial action plans as a core part of the assessment and not later as a separate initiative. Again, the specific actions to be taken will depend on the maturity of the organization's risk management practices.

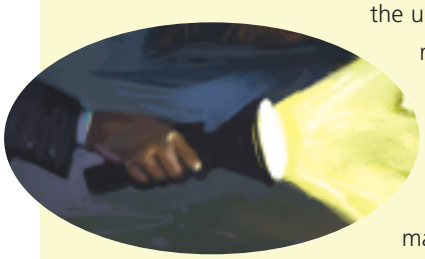
Based on our work in the Strategic Risk Management Lab at DePaul University and various studies, it appears that many organizations are approaching risk management through a series of incremental steps rather than moving directly to some desired end state. Accordingly, organizations can use the Strategic Risk Maturity Diagnostic (Figure 3) and the Strategic Risk Management Alignment Guide (Figure 4) as tools to facilitate this step. (See "Strategic Risk Management Tool Kit," which describes these tools.)

The specific actions to take will depend on the exact situation of the organization. Typically, actions will encompass some of these areas:

- Mitigation activities and strategies to reduce some of the risks identified.
- Risk-monitoring activities to determine if risks are increasing or decreasing. This may include tools such as balanced scorecards and strategy maps.
- Plans for integrating strategic risk management tools in the strategy execution processes such as the Kaplan-Norton Six-Stage Execution Process (see "Strategic Risk Management Action Plan and Strategy Execution" on p. 32).
- A process to periodically update the Strategic Risk Profile.
- Various types of reporting activities.
- Processes directed at the identification of new or emerging risks.

This step creates another opportunity to increase the sharing of information and risk across the organization's various risk and control functions. The action plans should address needed actions across the organization, not just within one risk or control function. This enterprise-wide focus is another step in building a risk management culture across the organization.

Strategic Risk Management Tool Kit



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 (ERM); is effected by boards of directors, management, and other personnel; requires a strategic view of risk and consideration of how external and internal events or scenarios will affect the ability of an organization to achieve its objectives; requires an organization to define a tolerable level of risk or risk appetite as a guide for strategic decision making; and is a continual process that should be embedded in strategy setting and strategy management. Here are five tools you can use in a Strategic Risk Assessment.

1. Return Driven Strategy Framework: This framework is used in Step 1 to analyze the elements of an organization's strategy. It provides a systematic way and a common language for articulating and clarifying that strategy. It also provides a lens for seeing how various elements of the strategy link together and drive value creation, and it offers perspective on identifying risk areas in the strategy.

For more information, see Mark Frigo, "Return Driven: Lessons from High-Performance Companies," *Strategic Finance*, July 2008, and Mark Frigo and Joel Litman, *Driven: Business Strategy, Human Actions, and the Creation of Wealth*, 2007.

2. Strategic Risk Management Framework: This framework is used to assess strategic risk and has been vetted by directors, management teams, and thought leaders in ERM and GRC (governance, risk, and compliance). It provides a way to identify, link, and prioritize an organization's strategic risks, which can encompass a broad spectrum, including customer risk, innovation risk, operations risk, brand and reputation risk, partnering risk, supply chain risk, employee engagement risk, fraud risk, governance risk, financial markets risk, financial reporting risk, sustainability risk, and unique capabilities (Genuine Assets) at risk.

For more information, see Mark Beasley and Mark Frigo, "Strategic Risk Management: Creating and Protecting Value," *Strategic Finance*, May 2007; Mark Frigo, "When Strategy and ERM Meet," *Strategic Finance*, January 2008; and Mark Frigo and Venkat Ramaswamy, "Co-Creating Strategic Risk-Return Management," *Strategic Finance*, May 2009.

3. Strategic Risk Maturity Diagnostic: This diagnostic is based on several streams of leading practices in risk management and provides a way to assess the maturity and development of risk management processes and capabilities in an organization. It includes diagnostic questions for self-assessment.

For more information, see Chapter 8 in the forthcoming book, *Strategic Risk Management: A Primer for Directors and Management Teams*, by Mark Frigo and Richard Anderson.

4. Strategic Risk Management Alignment Guide: This guide provides a way to determine how well risk management is covered within an organization, allowing for identifying where gaps and redundancies exist.

See Chapter 8 of the Frigo and Anderson book.

5. Strategic GRC Framework: This framework provides an overview for aligning risk and control units in an organization.

For more information, see "A Strategic Framework for Governance, Risk, and Compliance," Strategic Management column, *Strategic Finance*, February 2009.

Strategic Risk Management Action Plan and Strategy Execution

The 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 (see Robert S. Kaplan and David P. Norton, *The Execution Premium*, Harvard Business Press, 2008) 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, 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.

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.)

Step 6: Communicate the Strategic Risk Profile and Strategic Risk Management Action Plan

At this stage of the assessment, an organization should have a validated Strategic Risk Profile and initial action plans to address the strategic risks identified. Communication and building a common view of risk are widely accepted as leading practices in risk management. In fact, "Information and Communication" is one of the eight core components of enterprise risk management, according to the *Enterprise Risk Management—Integrated Framework* of the Committee of Sponsoring Organizations of the Treadway Commission (COSO).

This step challenges management to develop and execute communication across and into the enterprise to convey the organization's view of its strategic risks and the importance of executing the related action plans. Communication must also flow upward to the directors because this is a topic requiring their attention and interaction. As COSO states, "The better the communications, the more effective a board will be in carrying out its oversight responsibilities—acting as a sounding board for management on critical issues, monitoring its activities, and providing advice, counsel, and direction. By the same token, the board should communicate its information needs to management and provide feedback and direction."

A company should also consider its communication to external stakeholders, such as regulators, rating agencies, and shareholders. A recent progress report by Standard & Poor's on its initial reviews of enterprise risk management in nonfinancial companies indicated that, "There appears to be a link between transparency and disclosure and companies' confidence about ERM; many companies have been willing and able to provide considerable detail about risk management practices."

Here, again, the communication process represents an opportunity to build or reinforce an organization's risk culture. Information about the organization's key risks should be shared across the enterprise. Employees should receive communications about the organization's risk activities, policies, and overall guidance. In particular, there should be communications and information sharing between the organization's various risk and control units and the business units. It should be emphasized that successful communication is an iterative process and needs constant attention and reinforcement.

Step 7: Implement the Strategic Risk Management Action Plan

At the end of the day, the true value of the Strategic Risk Assessment process lies in the resulting actions that an organization takes. These actions are also intended to build the company's ongoing Strategic Risk Management processes and "complete the circle." As noted above, the dynamic nature of risk requires ongoing processes to monitor and mitigate it. Action plans should enable or enhance these types of processes.

An organization should also consider how it reports and updates the status of the actions, including to the board. As its Strategic Risk Management processes continue to mature, it should consider the next round of incremental steps to enhance its overall risk management processes. Again following the COSO ERM framework, other major risk categories, such as operations and compliance, could be fruitful areas for subsequent risk initiatives.

Moving Forward

CFOs and management teams have a great opportunity to help boards of directors and senior management build an organization's risk management processes so they are focused on strategic risks and on aligning ERM and GRC initiatives based on an ongoing assessment of those risks. The Strategic Risk Assessment we've described can provide a valuable foundation and first step for risk management and governance that will clarify and define the path to developing risk management capabilities for how risk is assessed, monitored, and managed. **SF**

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 in the School of Accountancy 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, and he is an IMA member. You can reach Mark at mfrigo@depaul.edu.

Richard J. (Dick) Anderson, 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. You can reach Dick at rander37@depaul.edu.