Putting Board Risk Committees To Work

by John Bugalla, Janice Hackett, James Kallman and Kristina Narvaez

Despite all of the new regulatory, legal and investor demands that boards give better oversight to risk, any effort is doomed to fail without an effective board-level risk oversight mechanism. How do best-practice corporate risk management systems operate? How does the board build itself into this system? Why are boards now considering a risk management committee when there is no legal requirement?

Risk management is officially on the board agenda, at least for publicly traded companies. The status was affirmed in February 2010 when Securities and Exchange Commission Rule 33-9089 became effective. The rule includes a provision for disclosure information about the board's role in risk oversight.

The Dodd-Frank Act, which became law in July, mandates that financial bank holding companies, some publicly traded non-bank financial companies and other "systemically important" public companies have a board-level "risk committee."

Both the SEC rule and Dodd-Frank will reshape disclosures and practices pertaining to the board's responsibility for risk management.

The financial meltdown was the primary driver in any discussion about the SEC action and risk disclosure. The SEC expressed their thinking when issuing the final rule: "We were persuaded by commenters who noted that risk oversight is a key competence of the board, and that additional disclosure would improve investor and shareholder understanding of the role of the board in the organization's risk management practices… This disclosure requirement gives companies the flexibility to describe how the board administers its risk oversight function, such as through the whole board, or through a separate risk committee or the audit committee, for example."

While it is too early to measure the impact of Dodd-Frank, the impact of the SEC rule has been immediate. ermINSIGHTS, an enterprise risk management (ERM) consulting firm, conducted an informal review of the 30 companies comprising the Dow Jones Industrials. The focus was to examine how the companies monitor, measure and manage risk.

Of the 25 Dow companies issuing their proxy statements after February, 76 percent included a section addressing the board's role in risk oversight. Sixty-four percent mentioned "enterprise risk management" or an enterprise approach to risk. Twenty percent said that they had a chief risk officer in place.

There are an assortment of approaches and board committees involved with risk management, but "board risk management committees" are now found at some companies.

One of the key words in the new SEC rule is flexibility. The various responses shown in this year's corporate proxy statements indicates that there are an assortment of approaches and board committees involved with risk management. As more proxy statements are analyzed, we should observe that a standard approach will develop by leading companies. We also think a greater number of boards will follow and adopt the informal best practices.

We believe the new standard will consist of three pieces:

- ☐ A board-level risk committee where required by Dodd-Frank, or an executive risk committee at companies not subject to Dodd-Frank.
- ☐ A chief risk officer who will chair either of these committees.
- ☐ A detailed operating charter.

John Bugalla, Janice Hackett, *and* **James Kallman** *are principals of ermINSIGHTS risk management consulting.* **Kristina Narvaez** *is president of ERM Strategies.*
[www.erminsights.com] [www.erm-strategies.com]

Bringing Risk Management Into The Boardroom

Owens-Illinois' Risk Management Committee Charter

Purpose

The Risk Management Committee (the "committee") shall provide assistance to the board of directors in fulfilling its responsibility to the shareholders, potential shareholders and investment community by:

☐ Assessing, and providing oversight to management relating to the identification and evaluation of, major strategic, operational, regulatory, information and external risks inherent in the business of the company (the "risks") and the control processes with respect to such risks;

☐ Overseeing the risk management, compliance and control activities of the company;

☐ Overseeing the integrity of the company's systems of operational controls regarding legal and regulatory compliance; and

☐ Overseeing compliance with legal and regulatory requirements, including, without limitation, with respect to the conduct of the company's business.

The committee shall not have responsibility for matters subject to the jurisdiction of another committee of the board of directors pursuant to that committee's charter.

Membership

The committee shall be composed of at least three directors. The members of the committee shall be appointed by the board and shall serve until such member's successor is duly elected and qualified or until such member's earlier resignation or removal. The members of the committee may be removed, with or without cause, by a majority vote of the board.

Chairman

Unless a chairman is elected by the board, the members of the committee shall designate a chairman by majority vote of the full committee membership. The chairman will chair all regular sessions of the committee and set the agendas for committee meetings.

Meetings

The committee shall meet at least two times annually, or more frequently as circumstances dictate. The chairman of the board or any member of the committee may call meetings of the committee. All meetings of the committee may be held telephonically.

All directors that are not members of the committee may attend meetings of the committee but may not vote. Additionally, the committee may invite to its meetings any director, management of the company and such other persons as it deems appropriate in order to carry out its responsibilities. The committee may also exclude from its meetings any persons it deems appropriate in order to carry out its responsibilities.

Responsibilities and Duties

The following functions shall be the common recurring activities of the committee in carrying out its purposes outlined above. These functions should serve as a guide with the understanding that the committee may carry out additional functions and adopt additional policies and procedures as may be appropriate in light of changing business, legislative, regulatory, legal or other conditions. The committee shall also carry out any other responsibilities and duties delegated to it by the board from time to time related to the purposes of the committee outlined above.

☐ Review and evaluate management's identification of all major risks to the business and their relative weight;

☐ Assess the adequacy of management's risk assessment, its plans for risk control or mitigation, and disclosure;

☐ Review the company's disclosure of risks in all filings with the Securities and Exchange Commission (including the Form 10-K Annual Report); and

☐ Together with the audit committee, review, assess and discuss with the general counsel, the chief financial officer and the independent auditor (as defined in the company's certificate of incorporation): any significant risks or exposures; the steps management has taken to minimize such risks or exposures; and the company's underlying policies with respect to risk assessment and risk management.

Structure and Operation

The committee shall have authority to retain outside counsel, risk management consultants or other experts, including authority to approve the fees payable to such advisors and any other terms of retention. The company will provide for appropriate funding, as determined by the committee, for payment of compensation to any advisors employed by the committee.

In fulfilling its responsibilities, the committee shall be entitled to delegate any or all of its responsibilities to a subcommittee of the committee.

The committee will make regular reports to the board and will propose any necessary action to the board. The committee will review and reassess the adequacy of this charter annually and recommend any proposed changes to the board for approval.

A review of the biographies of directors on most boards at this time does not mention risk management expertise.

☐ *Board/executive risk committees.* Board-level risk committees, while not yet common, are now in place at some companies. The Dodd-Frank board risk committee mandate is aimed at financial companies, yet-to-be determined public non-bank financials, and other companies with more than $10 billion in assets. However, any company will be well served by forming a new board-level risk committee.

Dodd-Frank contains three key components which will have long range implications (keeping in mind that the rules to carry out this requirement will take time to develop). The first component is that the risk committee be "responsible for oversight of the enterprise-wide risk management practices." Dodd-Frank has mandated the practice of ERM, which will likely spread to additional companies as a best practice.

The second key component is the requirement that the risk committee will contain a yet-to-be determined number of "independent directors."

The third component requires that at least one member of the committee be a risk management expert with experience in "identifying, assessing, and managing risk exposures of large, complex firms." This provision is very intriguing and bears watching because a review of the biographies of directors on most boards at this time does not mention risk management expertise.

We encourage the formation of an executive-level risk committee at all public companies, especially with the continued expansion of ERM. The responsibilities of this risk committee composed of senior executives (the C-suite), is not risk oversight, but risk management. One of the functions will be to assist the board with their risk oversight responsibilities. The focus of this committee should be strategic risks, as well as emerging and unanticipated risks that require greater analysis.

The benefits of a high-level executive risk committee include a broader picture of risk, enhanced understanding of risk relationships, and appreciation for the positive and negative correlations that can multiply the impact of risk on the company. Analyzing and recognizing which risks (or combination of risks) could have the greatest impact on the company gives senior leadership an internal warning system of what could be on the horizon, thereby avoiding surprises that impact earnings or other performance measures.

The executive risk committee's membership is crucial, because they must demonstrate and transmit two critical messages throughout the organization. First, risk management is not an unnecessary constraint on management imposed by outsiders. Second, cross-functional collaboration at the top should continue at all other levels. This is because the executive risk committee should not be expending its efforts dealing with routine risks that properly should be addressed at the operating levels.

Executive management has greater insights on recognizing risk correlations, including emerging and unanticipated risks.

Executive management should be working in concert with the board to set risk appetites and tolerances. They have authority to see beyond pure numbers to also consider such critical issues as organizational reputation and brand building. Executive management also has greater insights and a longer view for recognizing multiple risk correlations, including emerging, unanticipated risks that by their very nature are difficult to predict or quantify.

Operations leaders or mid-level managers are not usually in a position to have a broad, strategic risk perspective. They are heavily engaged in the day-to-day operational issues within individual profit centers. Mid-level managers are also on the operational front lines of regulatory and compliance issues. This provides the C-suite with results and assurances that they are operating in compliance with company standards. Mid-level managers do not set strategic risk management policy. Instead, they implement the operational and tactical actions required by the risk committee.

Cross functional collaboration should continue during the project risk analysis and interpretive process that will likely take place between senior and middle level management. This entails measuring a risk or a portfolio of risks, and calculating their potential impact both independently and (more importantly) in the aggregate.

Part of the mid-level manager's performance evaluation should include an analysis of both their skills in managing the risks and their ability to collaborate on responses with others. It is the only way for the importance of risk management and the concept of risk intelligence to become embedded in the organizational DNA.

There is still a great deal of debate about the skills required for the chief risk officer position. Multiple skills are needed, depending on the company's business.

☐ *Chief risk officer.* The chief risk officer (CRO) is a kind of risk ombudsman, and a relatively recent addition to the C-suite. CROs started appearing in companies whose industry dynamics held the potential for a great deal of volatility. Examples are financial institutions, energy marketers, insurance companies, and utilities.

The CRO should chair the executive level risk committee or serve as its chief of staff, and have duel reporting lines to both the CEO and a board-level committee. A less desirable alternative is to not affix responsibility for risk to a single person, but have the risk committee report to another board committee, such as governance, compensation, or audit.

There is still a great deal of debate about the skills required for the CRO position. Various polls taken by different organizations seem not to agree on any one background, but multiple skills depending on the business of the company. No matter the background, a CRO has to: know the business cold; have the ability to assemble a cross functional team of executives and subject matter experts; and actually make ERM work.

☐ *Risk committee charters.* The risk committee should create a charter that sets out a vision, mission, and a straightforward policy. Include a statement about strategic and operational risk positions in the aggregate. Risk positions may be expressed in both financial terms as well as qualitative outcomes.

Collecting data and information about known and emerging risks is essential. However, the company must also have an ongoing process to correctly organize, access, analyze, interpret and present the information in order to enable senior management to make critical decisions. Therefore, as the risk committee charter is being drafted, include the organizational capability to create an internal "risk intelligence" process and practice.

Risk intelligence is both a process and a product. It consists of the organizational ability to collect and collate data, statistics and information on risk and volatility. This is followed by the systematic analysis, interpretation and presentation of the information. The end goal is decision making that produces the most favorable outcome under existing circumstances.

The purpose of risk intelligence is to provide senior leadership and the board with facts, options, assessments of those options, and views as to what lies beyond the readily observable. Superior risk intelligence underlies the most effective responses and most efficient deployment of resources for addressing material and critical risks. It provides a competitive advantage to companies that understand risk intelligence and employ it effectively.

One of the key goals of the risk committee is to prevent a risk intelligence gap. Some examples where gaps occurred are the risk intelligence of the failed or rescued financial institutions.

Another example is found where former directors of some now-bankrupt or rescued firms claim they did not receive information necessary to perform their fiduciary oversight responsibilities. They assert that if they had been made aware of the impending doom, they would have immediately taken action to avoid or limit financial disaster.

Another problematic situation is if critical information is known by the CEO, but is not conveyed to the board. As a matter of organizational governance, a

risk intelligence gap between the CEO and the board of directors cannot be allowed.

Aside from the vision, mission, and policy provisions of the risk committee charter, a statement that the risk committee is adopting enterprise risk management (ERM) should be a priority. A review of proxy statements indicates a clear majority of companies are adopting some form of ERM to serve as the process to manage risks across the entire business enterprise.

There is a debate about which of the major ERM frameworks to adopt. Two commonly used frameworks are those of the Committee of Sponsoring Organizations (COSO), and the newer ISO31000.

While there are differences between the two, there are also similarities. Most of the American companies practicing ERM adopted the COSO framework several years ago in response to financial compliance issues. The COSO framework has a financial reporting, audit and compliance emphasis. The ISO31000 framework was created to be a worldwide guide. Thus, a global company practicing two different ERM approaches seems inefficient.

ISO31000 accepts the traditional view that risk management's primary function is to protect people, preserve assets, and ensure compliance (value protection). However, there is also a broader recognition that there is an upside to risk—value creation. Value is measured in different ways depending on the business, but value creation is a universal goal. One place to insert ERM is within strategic planning where growth values are a primary goal.

The risk committee charter should also detail how and how often the board will receive a report detailing risk information. Some companies will need monthly reporting, while others may be satisfied with quarterly reports. In either case the board must see a summary of the key risks and current risk management activities. Internal audit should review and report on the current risk management strategies to assure that they work as desired.

In conclusion, both the SEC rules and Dodd-Frank will reshape corporate governance, compensation and risk management for decades. The SEC has provided a solid foundation in protecting investors in public companies, and put risk oversight clearly in the hands of board members. Dodd-Frank provides a tactical approach to implement the SEC rule, and should serve as a model for best practices in risk management.

Risk committees need a mandate that includes a risk intelligence system that informs the board and C-suite about the key risks that are inherent in the business. A well-designed risk management system is essential in today's interconnected and interdependent global economy. If risk intelligence is present in the decision making process, the strategic and tactical actions that follow will enhance the company's chances of success in creating value. ■

Governing Risk

Board Risk Management Recommendations

- ☐ Form a high-level risk committee composed of the senior leadership team.
- ☐ Assure that the board of directors knows and understands the company's critical risks. The executive risk committee must report to a board level committee.
- ☐ Initially, the board or executive risk committee should focus on the strategic, emerging, and unanticipated risks critical to company governance, compensation, and risk oversight as required by the SEC for public companies.
- ☐ Consider the value of having a Chief Risk Officer, or designating an existing officer with the responsibility of a CRO.
- ☐ Create a charter for the risk committee that provides operational details including a vision/mission/policy statement that clearly addresses the issue of risk appetite and tolerances.
- ☐ Include a risk intelligence mandate within the risk committee charter.
- ☐ Adopt an ERM approach to risk.