April 15, 2015

The Board's Role with Risk

Five considerations to define a healthy balance within ERM

By Ronald Kral, CPA, CMA, CGMA
Managing Partner of Candela Solutions LLC

Where does the board's role begin and end regarding risk? A company's core objective is to create and increase wealth for its shareholders. Collectively, directors provide leadership toward this objective through two primary functions: 1) decision-making and 2) executive management oversight. Decision-making includes approving corporate policy, strategic goals, annual budgets, major expenditures, and the acquisition or disposal of material assets. It also includes evaluating and selecting the Chief Executive Officer (CEO) and approving the company's risk appetite. Risk appetite is the amount of risk the organization is willing to accept in pursuit of objectives. While it is typically the CEO who recommends a risk appetite to the board, it is the board that should render the ultimate decision on how much risk is appropriate.

The second primary board function involves a fine line regarding the degree of management oversight. Too much, and the board could be micro-managing the company thus infringing on the CEO's turf. Too little, and the board could lose its pulse on the status of the company's risk management efforts. Here are five considerations to define a healthy balance between board oversight and management responsibilities pertaining to Enterprise Risk Management (ERM):

1. **Defining Objectives**: ERM stems from the company's mission and objectives, as spelled out through strategic planning efforts. Risk and opportunity events flow from these objectives. The board needs to be comfortable with the alignment of the chosen objectives for ERM focus with approved strategic planning decisions. Since objectives drive the ERM process it is important to ensure that all relevant key objectives are covered.

2. **Identifying Events**: Identification of risks and opportunities is a core management responsibility in conducting ERM efforts. Risk is the possibility of an adverse event, while opportunity is the possibility of a favorable event. These two potential outcomes are inseparable as every decision to create or protect shareholder value (i.e., opportunities) involves risk. These events are typically very numerous, yet management only has a finite amount of resources to identify and respond to them. It is important for the board to be comfortable with this effort. In addition, this is a great opportunity for directors to contribute their thoughts on potential events based on their knowledge and expertise.

3. **Conducting the Assessment**: Risks and opportunities need to be analyzed in terms of their likelihood of occurrence and impact in reaching objectives. While this is the charge of executive management, the board should confirm that timely risk assessment activity is performed. A key consideration is the data and information used for the assessment. Decision-making improves when directors engage in open and frank discussions with management on presented

information, and even more important – information that is not presented. It is important for the board to gain comfort in the data and information supplied by management. An information audit to verify the timeliness, accuracy, and completeness of key information, including the supporting data elements and assumptions, is typically a wise investment.

4. **Deciding on Risk Responses**: Once the ERM analysis per the three previous steps is completed, management needs to ascertain risk responses. Should the company accept, avoid, reduce or share the risks? The response needs to be consistent with the company's risk appetite as recommended by management and approved by the board.

5. **Designing and Executing Controls**: Control activities are necessary to ensure that the ERM process is properly designed to effectively manage risks and opportunities. This is primarily done through carefully crafted policies and procedures. Perhaps even more important is confirming that management is following the established ERM policies and procedures through appropriate actions. This includes monitoring, tracking relevant information, and effective communication. The board should not assume that this is occurring, but rather conduct their own oversight activities to be comfortable that adequate controls are in place and operating effectively.

In summary, the management team is responsible for the heavy lifting pertaining to these five steps. So while it is the CEO who owns ERM, the board must be satisfied with management's performance consistent with the board's approval of objectives and risk appetite. How the board conducts their oversight duties is largely up to them, but for many organizations utilizing an independent internal audit function is a common choice. Otherwise, the board can bring in outside resources to conduct an ERM evaluation.

Despite having the utmost confidence in the integrity and ethics of the executive management team, an organization's ERM process should include a healthy dose of independent verification as directed by the board. It is not just a matter of trust, but also a matter of obtaining independent expertise to add value to the ERM process by providing different perspectives. Finally, the topic of risk oversight is important enough to merit a standing agenda item at every board and applicable committee meeting to help maintain an independent eye on the ERM process.

Defining the board's role on risk is vital through the corporate governance guidelines and committee charters. If the roles regarding ERM are not clearly spelled out and understood, then it is time to revisit the corporate governance guidelines and committee charters to add clarity. Once the roles are crafted and directors are educated on how to fulfill their duties, they must then have the collective discipline to follow-through on these duties. This is where the chairman of the board must insist on board accountability, as it is not simply management performance they should be concerned about, but also their own performance.

One effective way to assess board accountability is through periodic board and committee performance evaluations (refer to The Essentials of Boardroom Evaluations for a previous article on this topic). The scope of the board and committee evaluations should not simply entail ERM approval and oversight activities, but rather all board duties per corporate governance guidelines and committee charters. Without a robust assessment on their own activities, boards can be blinded to improvement opportunities. Effective boards must have the proper mindset rooted in a clear understanding of their duties to be productive and responsive to their duties.

*****

Ron Kral is the Managing Partner of Candela Solutions LLC, a public accounting firm with a national focus on governance, SEC compliance, and internal auditing. He is an educator, advisor, and internal auditor for boards and management teams. Ron is a member of 4 of the 5 COSO sponsoring organizations; the AICPA, FEI, IIA, and IMA. He can be reached at rkral@CandelaSolutions.com.

Candela Solutions LLC is a strategic CPA firm in providing services to US public companies that external auditors cannot due to independence concerns. Visit our website at www.CandelaSolutions.com

This is an article reprint from the Governance Issues™ Newsletter, Volume 2015, Number 2, published on April 15, 2015