BAILEY | CAVALIERI

ENTERPRISE RISK MANAGEMENT: AN IMPORTANT STRATEGIC DISCIPLINE

Every wave of business failures or scandals leaves a legacy of lessons learned. For example, the dot.com debacle in the late 1990s taught investors not to ignore lack of profitability or business fundamentals and to avoid irrational exuberance. The Enron era emphasized the importance of financial reporting integrity, transparency and accountability. More recently, the stock option backdating claims demonstrated that "everyone does it" is not an excuse for wrongful behavior.

Although far from over, one of the primary lessons from the current subprime and credit crisis is the importance of effective risk management. In too many instances, companies and their shareholders have been surprised at how vulnerable they were to predictable events. With the benefit of hindsight, it is now obvious that many financial institutions blindly chased the high returns from high risk loans, seemingly without regard to the institution's total risk profile. A comprehensive and effective risk management program should prevent that type of disconnect between risk and reward.

Virtually all public companies have some type of risk management department or function. However, in many companies, formal risk management is delegated to a lower level department which is limited to purchasing insurance and implementing routine loss prevention programs for certain high frequency exposures. In contrast, an "enterprise risk management" ("ERM") program is far more comprehensive and focuses on the financial, reputational, operational and strategic risks throughout the entire company, whether or not insurable. An ERM program seeks to identify, quantify and manage those risks and to align business decisions with approved risk tolerances.

In recent years, a number of companies, including most financial institutions, began embracing the concept of ERM by, among other things, appointing a chief risk officer ("CRO") to oversee the risk management function. Some of these efforts have been quite successful, but it is now obvious that many were not. In recognition of those failings, some rating agencies are now including within their debt rating analysis and scoring for companies an evaluation of the companies' risk management culture and governance. For example, S&P now grades the risk management programs and culture of financial institutions, insurance companies and energy-trading companies. S&P reportedly will be expanding this analysis to non-financial companies, focusing on how well those companies have integrated risk management processes throughout their enterprises. This analysis evaluates how companies view consequential risks, how often and in what ways they identify their risks and how risk management affects overall strategic decisions. According to S&P, companies are expected to adopt a coherent, systematic risk management program, and a "crammed-together collection of long-standing and disparate practices" will be frowned upon.

From a directors and officers liability perspective, implementing and maintaining an effective risk management program is consistent with one's fiduciary duty of care. Among other things, directors and officers are expected to reasonably manage and guide the company, which includes making informed decisions regarding acceptable levels of risks and prudent management of risk exposures.

Many of the shareholder derivative lawsuits now being prosecuted against directors and officers of financial institutions in connection with the subprime crisis allege the defendants breached their fiduciary duties by improperly managing the company's risks. A sample of such allegations includes the following excerpt:

> Defendants failed in good faith to supervise, and to exert internal controls over, and consciously disregarded responsibilities involving the Company's derivatives portfolio, and allowed [the Company] to ignore many red flags and warnings that existed and that should have caused Defendants to limit or reduce the Company's exposure to risk and loss and ultimately to tens of billions of dollars of unreserved losses.

The following summarizes some of the key components to an effective ERM program and highlights some of the ERM deficiencies which contributed to recent corporate losses.

1. Executive Leadership. Senior management and the Board must embrace the importance of enterprise risk management. An independent and highly vocal chief risk officer should be appointed who reports directly to the CEO and the Board. The CRO should have the respect of other senior leaders within the company so that his opinions and input will be heard. As a result, the CRO should be highly experienced and have a thorough understanding of the company's industry, business and operations. When circumstances require, the CRO must be prepared and equipped to express strong concern and disagreement with senior management and persuasively defend his or her views to the Board.

   The CRO should also have the skills and structural authority to collaborate with and have access to all departments and divisions within the company. No one person or small group of persons can possibly know enough to identify and evaluate all significant risks, and therefore the CRO must rely upon cooperation and input from a wide array of other executives, managers and employees within the company. In addition, the CRO must be supported with sufficient staff and budget to perform through internal and external resources the necessary investigations and analysis.

   Board involvement in the ERM process is essential both because the Board's strategic input can be invaluable and because that senior-level visibility creates better credibility and accountability. Most frequently, the ERM function reports

to the audit committee of the Board, which typically has responsibility for risk oversight. In fact, the New York Stock Exchange's Final Corporate Governance Rules require audit committees to discuss policies with respect to risk assessment and risk management. Those rules contemplate the audit committee discussing guidelines and policies to govern the process by which the company's exposure to risk is assessed and managed.

2. Risk Assessment Prioritization. It is obviously not practical to manage every risk faced by a large company. Instead, the ERM program should focus on defining the most important areas of risk exposure, and then seek to identify and evaluate the most important risks in each of those areas. It is tempting to limit this analysis to financial and operational risks, but a variety of other business and strategic risks should be addressed as well. For example, risks related to the company's industry, customers or competitors, as well as brand erosion and technology development, can have an enormous impact on a company.

   For each identified risk area, the highest priority should be given to the mission-critical or key strategic risks rather than less important exposures. That identification and prioritization process needs to be constantly updated to reflect the most recent dynamics within and outside the company. Not only do existing risks need to be assessed and addressed, but future or emerging risks need to be anticipated.

   Once identified and prioritized, the risks need to be assigned to "risk owners" who are responsible for managing the risk and aligning the risk with the company's broader strategic objectives. That delegation of responsibility must report up to the CRO and ultimately the Board to assure consistent and comprehensive risk management throughout the company.

3. Qualitative Information. The effectiveness of an ERM program is highly dependent upon receiving current, relevant and accurate information to perform the risk/reward analysis. Various good software programs are available to assist in this analysis. But, not surprisingly, the value of the information that comes out of that process is a direct function of the quality of the information that goes into the process. As a result, senior leadership within the company must be committed to devoting sufficient resources to develop the necessary information for this process.

   The single biggest barrier to an effective ERM program is the lack of awareness of certain risks. Therefore, those involved in the ERM program need to create new and more effective methods for gathering correct and current information, which then allows the risk management team to recognize, quantify and evaluate the magnitude and likelihood of risks. Because each company has different risks and risk appetite, one must resist the temptation to duplicate programs created by

other companies. Instead, creativity in designing the program is as important as the diligence in implementing the program.

Timely and current information is critical. For example, the subprime crisis highlighted the fact that many rating agencies do not adjust their ratings in "real time" but frequently base their rating decisions on stale information several months or more old. As a result, many who relied on those external ratings in assessing risks were making ill-informed risk decisions.

A necessary part of an ERM program is the creation of effective management and Board dashboards, which can be used by senior officers and directors to regularly see key qualitative and quantitative risk indicators, similar to the use of dashboards for key performance indicators.

4. Integrated Culture of Risk Management. Many companies naturally create risk silos pursuant to which certain operations or risks are removed from other operations and risks for purposes of assessment and management. This approach is inconsistent with the notion of enterprise risk management and ignores the companywide implications to many risk factors. For example, many companies manage through separate departments the IT, legal, financial, human capital, operational and strategic market risks, with little or no coordination between those departments. An ERM program consolidates the oversight of risks arising from these multiple exposures.

   Ultimately, a corporate culture should be developed in which corporate decisions at all levels are strongly influenced by risk tolerances established by the CRO and approved by the CEO and Board. For example, risks associated with corporate decisions such as new product development should be evaluated against overall enterprise risk tolerances, and a robust culture of communications relating to these risk issues should be nurtured.

   The goal of a good ERM program should be to create a risk-aware culture throughout the organization without creating a risk-averse culture. Like many management challenges, attaining that desired balance is very important yet very difficult. Companies are not well served by seeking to eliminate all high risks, since lower risks typically generate lower rewards. A proper risk/reward balance in one context may be improper in another context, which highlights the need for an integrated system which applies common criteria in defining the appropriate balance in each unique situation.

5. Emphasize Upside. If an ERM program is perceived as merely telling people they cannot do what they want to do, the program will constant struggle for the credibility and respect which is necessary to effectively fulfill its goals. Instead, executives should view the program as a means to better align strategy and performance, and should project an image of maximizing profits rather than

minimizing losses. A risk/reward analysis will identify areas where the company should increase its commitments, not just reduce activities.

An acceptable risk tolerance can be achieved not just through avoiding risky behavior, but also through transferring or insuring some of the risk. If the risky behavior is strategically important to the company and can be contained through external means, an ERM program should support that behavior. In other words, the goal of ERM is not risk reduction but risk management, so that risk can be wisely used to achieve the company's strategic objectives.

When properly viewed in that light, a quality ERM program can help create a corporate environment where managers at all levels seek to increase business activities using prudent risk tolerance objectives.

Now more than ever, companies should create a companywide senior-level risk management program which is designed to identify potential events that may affect the company and manage those risks within the approved risk appetite for the company. As is evidenced by numerous corporate failures in the subprime context, companies literally risk their very existence if they fail to implement this type of essential governance structure.

About the Author:

Dan A. Bailey is the Chair of the Firm's Directors & Officers Liability Practice Group and represents and consults with directors and officers, corporations, insurance companies, and law firms across the country. In addition to advising Boards and drafting most of the D&O insurance policies in the market, he has represented clients or served as an expert witness in many of the largest D&O claims for more than 30 years. He is co-author of Liability of Corporate Officers and Directors, a leading treatise on the topic, has published dozens of articles and speaks at more than 20 seminars a year on the subject.

He can be reached at (614) 229-3213, or dbailey@baileycav.com.