

May 7, 2008

## Risk Management in the Boardroom

**By Ron Kral, CPA, CMA, CGMA  
Partner of Kral Usseyry LLC**

Shareholder confidence, client trust, stakeholder relations, and a company's reputation are typically built over decades, but can be lost overnight. Unexpected exposure to the subprime shakeout, over-priced acquisitions, regulatory actions, errant ERP conversions costing millions, and product liabilities, such as lead paint in toys, have become common news headlines. While a company can't anticipate everything that can go wrong, the board and management team must build a strong element of risk management into their culture to reasonably protect the company's interests.

Interestingly, many of the horror stories involve companies that supposedly had strong governance and risk management processes. Let's explore some common reasons these processes failed to protect companies, along with practical considerations for improvement, especially at the board level.

There is plenty of excellent information in today's marketplace evolving around Enterprise Risk Management (ERM) frameworks. ERM largely addresses the "what" and "how" of risk assessment and management processes. That's the relatively easy part. The difficult part is moving forward with the "why," "when," "whom," and "where" well defined. If these questions are not adequately addressed, the risk management process is virtually doomed. Let's address each of these four questions from a practical standpoint.

**Why?:** This should be the first question addressed and may sound like a slam-dunk; however, be careful. If the "why" is not understood by all and imbedded in the culture, forget it. There must be a compelling business case to justify the resources for this effort, which must be accepted by both the board and management. If the board and management team are not on the same page, action must be taken to address questions and reconcile significant differences prior to marching forward. This action will likely shed light on different perspectives regarding important strategic and operating issues.

The business case must be supported by a healthy return on investment (ROI). Be careful to factor the "risk-of-failure" into the equation, as traditional ROI analysis does not readily lend itself in quantifying these types of benefits. For example, the risk of being delisted by a stock exchange may lead to less credibility on Wall Street, shareholder disapproval, less liquidity and decreased access to capital markets. Factoring-in these considerations is critical to the ROI calculation. This is often where board of directors can contribute with their diverse and deep business expertise.

**When?:** Strong risk management practices call for an on-going review throughout an enterprise to achieve continuously improved operations, to leverage new opportunities, and to better manage non recurring events. In short, ERM is a process for identifying potential events, managing risk, and providing reasonable assurance on the achievement of objectives. The ERM process, unlike a "project", does not necessarily have beginning and ending points. This makes sense as risk management truly must be a 24



by 7 initiative, as developments and surprises can occur overnight with little or no warning. New information, if material to reaching objectives, must be added to the process and acted upon in a timely manner. It is important for the board to feel comfortable with the integrity of the information, as too many horror stories involve critical decisions being made on erroneous data and assumptions. The theme of “independence” plays an important role here and will be explored later.

For companies to adequately survive in their fast-paced environments, they must have the structure and discipline to address risk management from the long-term perspective to the very-short term. Consequently, healthy risk management processes are integral to longterm strategic planning initiatives, annual performance plans, and crisis situations. Risk management must be looked upon as both firm (i.e., we will do it) and flexible (i.e., we will quickly consider new developments and act swiftly).

Organizations must be flexible to respond to important decision making situations in a timely manner, while at the same time not sacrificing proper due-diligence. Escalation policies and procedures need to be clear and expert reinforcements lined-up in the event they are quickly needed. Boards can save a lot of time by pre-qualifying emergency outside resources in the areas of special reviews, IT controls, due-diligence, fraud investigations, and legal. Urgent situations happen, and not having resources identified in advance have cost many boards valuable time. Also, emergency board meetings should not be taken as a sign of crisis, but rather a sign of responsive risk management. However, make sure you have the resources lined-up to respond quickly.

**Whom?:** Clearly a company’s risk management process must be sponsored by the CEO with adequate resources approved by the board. While everyone on the executive management team has important roles, an individual needs to be assigned overall responsibility for risk management. Justifying a full-time Chief Risk Officer (CRO) will depend on a company’s size and risk management business case. Generally, companies north of \$1 billion in annual revenue should be able to justify a dedicated Risk Management Officer.

The role of the CRO is to coordinate and monitor risk management activities. Together with the CEO, the CRO is primarily responsible for the risk management program, which includes its initial development as well as its evolution. For smaller companies, primary risk management responsibilities may be assigned to the COO, CFO, General Counsel, Chief Compliance Officer, or other title. However, lead responsibility must be assigned!

Let’s not forget the board, as they serve an absolutely critical role to risk management. While management is directly responsible for operating activities, including ERM, these efforts must be held accountable by the board. By selecting the CEO, it is the board that is ultimately responsible for risk management. This is where it gets a little tricky. A root cause for many risk management failures is the lack of independence. The risk management function must have a healthy dose of independence to shield the process from biases. Easier said than done, as every company has their own silos and turfs controlled by managers. Managers are often incentivized on actual or perceived results over areas they control, thus creating natural biases.

Robust risk management can uncover previously unknown risks, weaknesses, and threats, which can refocus resources away from a specific manager’s interest. This includes the CEO as the chief manager and sheds light on why it is imperative for the board to have an active role. The board should routinely be kept apprised of the most significant risks and what management is doing to mitigate those risks. The board should also have a contributing role in establishing ERM objectives.



However, it is the independent verification of ERM components and action elements by the board that often is overlooked. Despite having the utmost confidence in the integrity and ethics of executive management, the board should always introduce some degree of independence into the process. This can be accomplished through a strong and independent Internal Audit function, procuring outside resources for a special review, or other independent channels to the board. Ideally, outside directors of the board, who do not have a management position inside the company, should oversee these efforts.

**Where?:** Let's tackle this one from an organizational unit perspective. All of a company's organizational units should be considered for ERM as this should not be viewed as simply an exercise at the headquarters office. Theoretically, risk management extends from the boardroom to the shop-floor. This includes units at the entity-level, division, subsidiary and departmental levels. This does not mean an extensive ERM effort needs to be rolled-out everywhere as one should never lose sight of the costs and benefits of risk management activities. Rather, a business case should be considered for all units of the company resulting in a risk management process that best accomplishes the company's key objectives in an efficient and effective manner. This is where ERM frameworks and relating tools can assist in ultimate success.

Finally, here are a couple of closing thoughts on risk management in the boardroom. First, leverage control activities to help ensure a successful risk management process. Keep in mind that "internal controls" are simply policies, procedures, and actions to help ensure board and management directives are carried out. Internal controls are not just for financial reporting and compliance, but also for meeting operational and strategic objectives. Second, the board must look at itself in the mirror in terms of their own performance on the risk management front. Boardroom evaluations that measure the board's on-going risk management efforts will help directors to best meet their fiduciary responsibilities.

\*\*\*\*\*

**Ron Kral** is a partner of [Kral Ussery LLC](#), a public accounting firm delivering advisory services, litigation support and internal audits. Ron is a highly rated speaker, trainer and advisor. He is a member of 4 of the 5 COSO sponsoring organizations; the AICPA, FEI, IIA, and IMA. Contact Ron at [Rkral@KralUssery.com](mailto:Rkral@KralUssery.com) or [www.linkedin.com/in/ronkral](http://www.linkedin.com/in/ronkral).

**Kral Ussery LLC** serves US public and private companies to protect and grow shareholder value, as well as non-profits and governments with internal controls and in combating fraud. We assist entities with governance and in all matters relating to financial reporting, including SEC compliance, internal controls testing and remediation, IT general controls, IPO readiness, M&A transactions, US GAAP compliance and implementation of new accounting standards. Visit us at [www.KralUssery.com](http://www.KralUssery.com).

**This is an article from the Governance Issues™ Newsletter, Volume 2008, Number 1, by Candela Solutions, which has since merged to form Kral Ussery LLC.**

© Kral Ussery LLC. Copyright: The Governance Issues™ Newsletter is meant to be distributed freely to interested parties. However, any use of this article must credit the respective author and Kral Ussery LLC as the publisher. All rights reserved. Use of the newsletter article constitutes acceptance of our [Disclaimer](#) and [Privacy Policy](#).

To automatically receive the newsletter, go to [www.KralUssery.com](http://www.KralUssery.com) and register. Or, send a request to [newsletter@KralUssery.com](mailto:newsletter@KralUssery.com) and we will register you.