Board Perspectives: Risk Oversight

Ensuring Risk Management Success

Issue 73

A fundamental role of the board in discharging its risk oversight responsibilities is to ensure the success of the independent risk management function. Below we discuss five fundamental tenets to attaining this success.

Given that there is no one-size-fits-all solution for risk and the risk management function, how risk is governed varies across industries and organizations. However, there are five interrelated principles that underlie effective risk management within all organizations in both good times and bad: integrity to the discipline of risk management, constructive board engagement, effective risk positioning, strong risk culture, and appropriate incentives.

Integrity to the Discipline of Risk Management

Integrity to the discipline of risk management means having a firm grasp of business realities and disruptive market forces. It also means engaging in straight talk with the board and within executive management about the related risks in achieving the organization's objectives and the capabilities needed to reduce those risks to an acceptable level.

Integrity to the discipline is tied to strong "tone at the top" – what the C-suite stands for, how senior executives provide leadership with respect to the appropriate governance and behavior around doing the right things in the right way consistently over time, and ensuring the affairs of the business are conducted in a fair and transparent manner and at arm's length.

If tone at the top is lacking, the executive team is not likely paying attention to the warning signs, and the organization's affairs may be so complex that few can understand them. Risk management then faces an almost insurmountable challenge to making a difference.

Consider the following common examples, some strategic and some tactical, of integrity failures:

- **Not grasping business realities clearly –** The global financial crisis is a good example of what can happen when the inherent risks associated with aggressive, growth-oriented market strategies are discounted, ignored or never considered. Breakdowns in time-tested underwriting standards, failures to consider concentration risks, and excessive reliance on third-party assessments of structured products were among the root causes of the crisis.
- **Not integrating risk with strategy-setting –** When risk is an afterthought to strategy, risk management fails to reach its full potential as a discipline. The critical assumptions underlying the corporate strategy must be understood at the highest levels of the institution, and the external environment must be monitored to ensure that these assumptions remain valid over time.
- **Not tying risk tolerance to performance –** Risk is often an appendage to performance management. How does an organization even know that it is doing an efficient job of managing risk when it hasn't delineated its risk appetite and risk tolerances at

the level at which decisions are made? Performance and risk must be integrated; to that end, defining thresholds is essential.

- **Limiting risk management to a compliance activity –** Integrity to the discipline means knowing that undertaking initiatives to manage uncertainty (risk) in the pursuit of business objectives is not strictly a regulatory compliance measure. Viewing risk management as a "regulatory" check-the-box matter restrains its value proposition.

These examples illustrate that integrity must permeate every aspect, every level and every action related to managing risk within the organization. Hoping that risks are managed sufficiently while knowing that business realities are not actively monitored, risk is not really understood, tolerance levels are not set, and risk management is addressed solely to meet regulatory guidelines is a clear indicator that integrity to the discipline is lacking.

Constructive Board Engagement

Effective board risk oversight begins with defining the role of the full board and its standing committees with regard to the oversight process and working with management to understand and agree on the types (and format) of risk information the board requires. Directors need to understand the company's key drivers of success, assess the risks in the strategy, and encourage a dynamic dialogue with management regarding strategic assumptions and critical risks.

The scope of the board's risk oversight should consider whether the company's risk management system – including people and processes – is appropriate and has sufficient resources. The board should pay attention to the potential risks in the company's culture and monitor critical alignments in the organization – strategy, risk, controls, compliance, incentives and people. Finally, the board should consider emerging and interrelated risks (i.e., what's around the next corner?).[1]

Effective Risk Positioning

While positioning of the risk management function is not a one-size-fits-all prescription, there are fundamental principles that make it work. The board's and executive management's expectations for the chief risk officer (CRO) or equivalent executive and the risk management function must be carefully considered and, given those expectations, the function positioned for success. To this end, six key success factors increase the function's chances of success:

- The CRO (or equivalent executive) is viewed as a peer with business-line leaders in virtually all respects (e.g., compensation, authority, and direct access and reporting to the chief executive officer) and likewise down through the business hierarchy and across the organization.
- The CRO has a dotted reporting line to the board or a committee of the board and faces no constraints of any kind in reporting to the board.
- The board, senior management and operating personnel believe that managing risk is an organizational imperative and everyone's job.
- Management values risk management as a discipline equal to opportunity pursuit.
- The CRO is clearly viewed as undertaking a broader risk focus than compliance.
- The CRO's position, and how it interfaces with senior line and functional management, is clearly defined.

While these attributes may not be exhaustive, they represent a significant step toward ensuring that the risk management function makes a strong impact, and setting the tone for effectively functioning risk management. Taking one or more of these elements away should send up a red flag indicating that the risk management function may be unable to fulfill its expected role and lacks real authority or influence. Depending on the expectations, the function may be set up to fail.

[1] *Report of the NACD Blue Ribbon Commission – Risk Governance: Balancing Risk and Reward,* National Association of Corporate Directors, October 2009, Chapter 4, pages 14-19.

Strong Risk Culture

An actionable risk culture helps to balance the inevitable tension between (a) creating enterprise value through the strategy and driving performance on the one hand and (b) protecting enterprise value through risk appetite and managing risk on the other hand. While risk culture has gained traction in terms of relevancy in financial services institutions in the post-global financial crisis era, the decision-making preceding the occurrence of reputation-damaging risk events and lack of response readiness when those events occur have made risk culture a topic of interest in other industries as well.

Culture is influenced by many factors. We've discussed two – the tone at the top and the quality of the board's risk discussions. Other factors include:

- **Accountability –** Successful risk management requires employees at all levels to understand the core values of the institution and its approach to risk, be capable of performing their prescribed roles, and be aware that they are held accountable for their actions in relation to expected risk-taking behaviors.
- **Effective challenge –** A sound risk culture encourages an environment in which decision-making processes allow expression of a range of views, manage the effect of bias and facilitate reality testing of the status quo.
- **Collaboration and open communications –** A positive, freely open and collaborative environment engages the most knowledgeable people and leads to the best decisions.

Incentives that encourage risk awareness help shape risk culture, as discussed below.

Appropriate Incentives

Performance and talent management should encourage and reinforce maintenance of the organization's desired risk behavior. The old saying, "What gets rewarded, gets done," is as true with risk management as it is with any other business process. Disconnects in the organization's compensation structure and an excessive near-term focus can lead to the wrong behaviors, neutralizing otherwise effective oversight by the board, CRO and other executives.

For example, if lending officers are compensated based on loan volumes and speed of lending without regard for asset quality, reasonable underwriting standards and process excellence (e.g., their compensation is not adjusted for borrower and collateral riskiness, portfolio concentrations, and the likelihood of unexpected losses), the financial institution may be encouraging the officers to game the system to drive up their compensation – thus exposing the company to unacceptable credit risk.

This principle requires more than focusing on C-suite executive compensation and upper management. Just as important is an understanding of the incentive plans driving behavior in the sales force and on the "factory floor" where production takes place, as this is where the individual "moments of truth" occur that add, subtract or neutralize the buildup of risk within the organization's processes, each and every day.

Questions for Boards

The following are some suggested questions that boards of directors may consider, based on the risks inherent in the entity's operations:

- Has the board articulated its risk oversight objectives and evaluated the effectiveness of its processes in achieving those objectives? If there are any gaps that may impede risk oversight effectiveness, is the board taking steps to address them?
- Are there any elements of ineffective positioning of the risk management function present in the organization? Is the CRO (or equivalent executive) viewed as a peer with business-line leaders? Does the board leverage the CRO in obtaining relevant and insightful risk reports? Does the CRO have a direct reporting line to the board?
- Does executive management openly support each line of defense (e.g., the primary risk owners [business-line leaders and process owners whose activities create risk], independent risk and compliance management functions, and internal audit) to ensure it functions effectively and that there is timely consideration of escalated matters by executive management and the board?

- Do primary risk owners identify and understand their respective risks and risk appetites? Do they escalate issues to executive management in a timely manner? Is the board of directors engaged in a timely manner on significant risk issues?
- Is risk management a factor in the organization's incentives and rewards system? Is risk/reward an important factor in key decision-making processes? Do information systems provide sufficient transparency into the entity's risks?

How Protiviti Can Help

Protiviti assists directors in public and private companies with identifying and managing their organization's key risks. We provide an experienced, unbiased perspective on issues separate from those of company insiders and an analytical assessment approach that is aligned with the unique characteristics of the risks the company faces.

About Protiviti

Protiviti (**www.protiviti.com**) is a global consulting firm that helps companies solve problems in finance, technology, operations, governance, risk and internal audit, and has served more than 60 percent of *Fortune* 1000® and 35 percent of *Fortune* Global 500® companies. Protiviti and our independently owned Member Firms serve clients through a network of more than 70 locations in over 20 countries. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies.

Named one of the 2015 *Fortune* 100 Best Companies to Work For®, Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

Protiviti is partnering with the National Association of Corporate Directors (NACD) to publish articles of interest to boardroom executives related to effective or emerging practices on the many aspects of risk oversight. As of January 2013, NACD has been publishing online contributed articles from Protiviti, with the content featured on www.nacdonline.org/Magazine/author.cfm?ItemNumber=9721. Twice per year, the six most recent issues of *Board Perspectives: Risk Oversight* will be consolidated into a printed booklet that will be co-branded with NACD. Protiviti will also post these articles at **Protiviti.com.**

protiviti®
Risk & Business Consulting.
Internal Audit.