Board Perspectives: Risk Oversight

Strengthening Your Risk Culture

Issue 57

Risk culture is an enigma. We agree it is important when someone asserts its significance – even though we may not be sure exactly what it is, much less what to do about it if it requires improvement. The dichotomy of risk culture is, despite its importance, often either given lip service or simply ignored. This is a mistake.

Key Considerations

Risk culture is the "set of encouraged and acceptable behaviors, discussions, decisions and attitudes toward taking and managing risk within an institution."[1] Developed in conjunction with research Protiviti conducted with the Risk Management Association (RMA), this definition applies to all organizations, whether public or private, for-profit or not-for-profit. Risk culture is the glue that binds all elements of risk management infrastructure together because it reflects the shared values, goals, practices and reinforcement mechanisms that embed risk into an organization's decision-making processes and risk management into its operations. In effect, it is a look into the soul of an organization to ascertain whether risk/reward trade-offs really matter.

Whether management realizes it or not, risk culture may be a formidable hurdle to improving risk management performance. Because risk culture often evolves as the organization evolves, it may make sense for a company to use self-assessment techniques, internal surveys, focus groups and other methods to understand its current state by considering the following:

- **Tone of the organization –** This term refers to the collective impact of the tone at the top, tone in the middle, and tone at the bottom on risk management, compliance and responsible business behavior. Communications from the top have little impact if the organization's employees see and hear a different message every day from the managers to whom they report. The greater the number of management layers in the organization, the greater the risk of incongruities in the respective tones at the top, middle and bottom; likewise, the greater the risk of executive management being unaware of serious financial, operational and compliance risks that may be common knowledge to one or more middle managers and rank-and-file employees. Information is often distorted as it moves up and down the management chain, creating disconnected leaders.[2]
- **Physical mechanisms driving risk culture –** These tangible mechanisms influence the tone of the organization and include many things comprising the risk governance structure (e.g., corporate value statements, code of conduct and ethics programs; policies and procedures; risk committee oversight activities; incentive programs; risk assessment processes; key risk indicator reporting and performance reviews; and reinforcement processes, among other things).

[1] "Risk Culture: From Theory to Evolving Practice," *The RMA Journal,* December 2013–January 2014, Risk Management Association and Protiviti: www.protiviti.com/en-US/Documents/RMA%20Journal.pdf.

[2] "Boards Should Monitor the Tone at the Bottom," Dr. Larry Taylor, NACD Directorship, October/November 2011: www.directorship.com/boards-should-monitor-the-tone-at-the-bottom/.

They also include the risk appetite dialogue of the executive team and board, and the decomposition of risk appetite into risk tolerances and limit structures used day-to-day in executing the corporate strategy.

- **Internal attributes driving risk culture –** These attributes include the attitudes, belief systems and core values that drive behavior and guide daily activities and decision-making throughout the organization, particularly with respect to entrepreneurial pursuits. While not as easily "seen and touched" as physical mechanisms, they warrant careful attention. For example, behaviors around risk management and internal control accountabilities often manifest themselves in how people clear audit issues, address control deficiencies, escalate issues and resolve issues reported. The timeliness in which such activities are carried out provides powerful "tells" regarding an organization's risk culture, as does executive management's reaction to warning signs provided by independent, back office risk management functions.
- **External attributes driving risk culture –** These attributes include regulatory requirements and expectations of customers, investors and others. The extent to which an organization seeks out these requirements and expectations and aligns business processes through actionable improvements reveals a lot about its resiliency.
- **Subcultures that might have an impact on risk management –** Multiple subcultures permit an institution to be more agile in response to a changing business environment to solve problems, share knowledge and serve customers that a so-called unitary culture may not address. On the other hand, they can also lead to rogue risk-taking behavior that can ultimately harm the organization.[3]
- **Relationship to overall culture –** Risk culture does not operate in a vacuum. The overall organizational culture influences it in many ways, and some argue they are one and the same.

As risk is about uncertainty in facing the future, it would seem logical that a desirable risk culture would position the organization to be proactive as an early mover that quickly recognizes a unique opportunity or risk and uses that knowledge to evaluate its options, either before anyone else or along with other firms that likewise seize the initiative. Such a culture would give management the advantage of time, with more decision-making options before market shifts invalidate critical assumptions underlying the strategy. Another example of a desirable risk culture might be one that maintains a healthy tension between the organization's entrepreneurial activities for creating enterprise value and its activities for protecting enterprise value so that neither one is too disproportionately strong relative to the other.

Once an initial assessment of the current risk culture is completed, executive management should consider whether any organizational changes are needed and take steps to implement those changes, as directed by the board. In transitioning to a desired risk culture:

1. **Embed it in the organization –** Risk culture should be effected through the firm's overall risk governance process; otherwise, it becomes either a nebulous appendage or a theoretical concept. To illustrate, accountabilities for risk management and desired risk management behaviors should be reinforced through committee charters, policies, job descriptions, limit structures, procedures and escalation protocols.
2. **Make it a priority at the highest levels –** Executive management must support the desired risk culture by demonstrating the appropriate behaviors through its actions and decisions over time, as well as periodically communicating the value contributed by the organization's risk culture. For example, promoting a warrior culture, fostering a "star system" with little or no accountability, "shooting" the bearers of bad news, ignoring the warning signs escalated by the risk management function, and making decisions that everyone can see are inconsistent with the desired risk culture all send the wrong message.

[3] "Risk Culture: From Theory to Evolving Practice," *The RMA Journal*.

3. **Undertake an integrated approach –** Standing alone, programs such as periodic policy communications, awareness campaigns and training strategies are mere window dressing. When baked into a comprehensive program that aligns performance expectations, roles, responsibilities and compensation structures to appropriate risk-taking behaviors, they reinforce critical aspects of the desired risk culture for employees.
4. **Periodically evaluate progress –** Monitor employee behavior for new trends, attitudes or perceptions requiring attention. Track quantitative and qualitative measures of an effective risk culture using such indicators as:
   - Level of executive management sponsorship
   - Line-of-business (LOB) ownership of risk management as the "first line of defense"
   - Effectiveness of risk committee and governance processes
   - Evidence of key business decisions taking risk and solvency into consideration
   - Quality of board discussions on risk issues and escalated matters
   - Use of risk appetite statement, tolerances and limit structures in decision-making
   - Alignment and incorporation of risk into strategic planning and direction
5. **Be alert for signs of change, for better or worse –** As noted earlier, employee surveys and focus groups are examples of tools that can provide insights when evaluating risk culture. Reports from the independent risk management function and internal audit are other sources. Consider the effects of changes in strategy and the organization, as well as the occurrence of external events, including regulatory developments, when evaluating whether changes are necessary to strengthen risk culture.

Every organization is different. That is why it is important to evaluate risk culture and make necessary adjustments to shape it over time in response to change.

Questions for Directors

Following are some suggested questions that boards of directors may consider, in the context of the nature of the entity's risks inherent in its operations:

- Does executive management openly support each line of defense to ensure it functions effectively, for example, the primary risk owners (LOB leaders and process owners whose activities create risk); independent risk and compliance management functions; internal audit; and timely consideration of escalated matters by executive management and the board?
- Do primary risk owners identify and understand their respective risks and risk appetite? 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 the risk culture consistently applied throughout the organization, or are there subcultures that also exist? If subcultures exist, do they contribute to effective risk management behaviors? If not, do they present exposure to excessive risk-taking across the organization?
- Is risk management a factor in the organization's incentives and rewards systems? Is risk/reward an important factor in key decision-making processes? Do the organization's information-for-decision-making systems provide sufficient transparency into its risks?
- What types of risk culture training, awareness programs or support are available within the organization?

How Protiviti Can Help

Protiviti assists directors and executive management in public and private companies to identify and manage the organization's key risks. We work closely with companies to assess the entity-level control environment, organizational structure and cultural issues that can impact the effectiveness of risk management. We provide an experienced, unbiased perspective on issues separate from those of company insiders and an analytical assessment approach that focuses on strengthening the organization's risk culture.

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 40 percent of FORTUNE 1000® and FORTUNE Global 500® companies. Protiviti and its independently owned Member Firms serve clients through a network of more than 70 locations in over 20 countries. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies.

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.directorship.com/author/jim-deloach/ in the "Blogs & Opinion" section. A compilation of blog posts and articles is maintained and categorized by author's name. 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.