Board Perspectives: Risk Oversight

The Five Lines of Defense – A Shareholder's Perspective

Issue 51

As the board of directors focuses its attention on risk oversight, there are many questions to consider. One topic the board should examine is how the organization safeguards against breakdowns in risk management and compliance management.

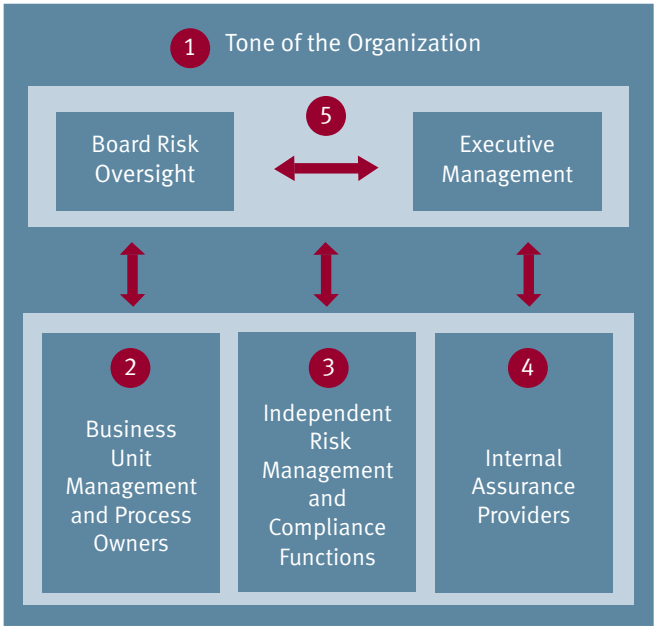
It goes without saying that organizations exist to create enterprise value. That is universally understood and accepted. However, when executive management ignores warning signs posted by the risk management function, fails to address critical compliance requirements when considering a new product or service, or resists contrarian information suggesting the corporate strategy is not working, the board must step up. Otherwise, the organization may learn tough lessons about the importance of protecting enterprise value. If management does not involve the board with strategic issues and important policy matters in a timely manner, the result of a breakdown in risk management or inattention to compliance imperatives can be the loss of enterprise value that took decades to build – tragic lessons from the financial crisis and the recent spate of high-profile compliance breakdowns.

An effectively designed and implemented lines-of-defense framework can provide strong safeguards against these breakdowns.

Key Considerations

Much more than "segregation of incompatible duties" and "checks and balances," the lines-of-defense model emphasizes a fundamental concept of risk management: *From the boardroom to the customer-facing processes, managing risk, including compliance risk, is everyone's responsibility.* A widely accepted view of the lines-of-defense model is three lines of defense where business unit management and process/risk owners comprise the first line, independent risk and compliance functions are the second line, and internal audit is the third line. While this point of view has considerable merit, we also see a broader perspective from

The Five Lines of Defense



the vantage point of shareholders and other external constituencies (the external stakeholders' view) – five lines of defense that support the execution of the organization's risk management and compliance management capabilities (see *The Five Lines of Defense* graphic on the previous page).[1]

Tone of the organization – This phrase is intended to describe 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. While tone at the top is important and provides a vital foundation, the reality is that although leaders communicate the organization's vision, mission, core values and commitment to appropriate ethical behavior, what really drives behavior is what the organization's employees see and hear every day from the managers to whom they report.

Tone of the organization is the first line of defense because of the significant influence it has on the organization's risk culture. Executive management initiates the proper tone by driving an "everyone is responsible for risk management" perspective throughout the organization and positioning each of the other lines of defense, as discussed below, to function effectively. The board must be vigilant to ensure there is nothing constraining the independent risk management and compliance functions (third line of defense) and internal audit (fourth line of defense) from reporting to it when critical risk and compliance issues arise. Periodic executive sessions with the appropriate functional leaders and the chief audit executive can help in this regard. As for a formalized escalation process, even in circumstances where the CEO (or preferably, an executive risk committee or equivalent group) resolves disputes between the second and third lines of defense, the board should be informed to the extent such disputes are about significant matters or close calls. All of these actions help set the proper tone of the organization.

Business unit management and process owners – Those responsible for the units and processes that create risks must accept the ultimate responsibility to own and manage the risks their units and processes create, as well as establish the proper tone for managing these risks consistent with the tone at the top. As the principal owners of risk, these managers set objectives, establish risk responses, train personnel, and implement and reinforce risk response strategies. They implement and maintain effective internal control procedures on a day-to-day basis and are best positioned to integrate risk management capabilities with the activities that create the risks. They must accept and cooperate with the oversight activities of risk management and compliance functions and the assurance activities of internal audit; it is a bright red warning flag if they don't.

Independent risk management and compliance functions – Effective risk and compliance management requires an independent, authoritative voice to ensure that an enterprisewide framework exists for managing risk, risk owners are doing their jobs in accordance with that framework, risks are measured appropriately, risk limits are respected and adhered to, and risk reporting and escalation protocols are working as intended. Depending on the industry, these functions may include compliance, environmental, financial control, health and safety, inspection, legal approval, quality assurance, risk management, security and privacy, and supply chain. While these functions collaborate with unit managers and process owners to develop and monitor controls and other processes that mitigate identified risks, they also may conduct independent risk evaluations and alert management and the board to emerging risk and compliance issues.

To be truly objective and effectively positioned within the organization, risk management and compliance functions should be insulated from and independent of business unit operations, lines of business, and front-line, customer-facing processes of the business. The expectations of the CEO and the board set the tone in determining whether these functions constitute a robust third line of defense. For example, if these

[1] For more about the five lines of defense, see "Applying the Five Lines of Defense in Managing Risk," *The Bulletin*, Volume 5, Issue 4, Protiviti: www.protiviti.com/en-US/Pages/The-Bulletin.aspx.

functions lack the necessary veto and/or escalation authority to serve as a viable line of defense, they may be relegated to serving as mere champions, facilitators or reporters.

Internal assurance providers – The fourth line of defense provides assurance that the other lines of defense are functioning effectively. Accordingly, it should use the lines-of-defense framework as a way of sharpening its value proposition by focusing its assurance activities more broadly on risk management. Internal audit reviews internal controls and risk management procedures; identifies risks, issues and improvement opportunities; makes recommendations; and keeps the board and executive management informed of the status of open matters.

Board risk oversight and executive management – The board of directors and executive management play separate and distinct roles in providing the final line of defense. The ability to act on escalated risk information is vitally important. "Blind spots" spawned by such dysfunctional behavior as myopic short-term focus on "making the numbers," lack of transparency, an unbalanced compensation structure and other tone-at-the-top issues can obstruct action at the crucial moment. A leadership failure to act will almost always undermine even the strongest risk management capabilities, regardless of the various lines of defense in place.

Under the oversight of the board of directors, executive management must manage the inevitable tension between business unit managers and independent risk management and compliance functions of the organization by ensuring these activities are balanced appropriately, such that neither one is too disproportionately strong relative to the other. Executive management must align governance processes, risk management capabilities and internal control toward striking the appropriate balance to optimize this natural tension between value creation and value protection. More important, they must act on risk information on a timely basis when it is escalated to them and involve the board in a timely manner when necessary. In this regard, executive management and the board's risk oversight comprise the last line of defense, when significant issues are escalated upward.

The five-lines-of-defense model provides a powerful line of sight to the board's risk oversight process in terms of what to look for and expect. It is an integrated approach through which an organization responds to risk. It provides direction to executive management and the board of directors as to how the organization should approach risk management and reminds them that, when significant issues are escalated to their attention, it is ultimately up to them to strike the appropriate balance between creating and protecting enterprise value. Their action or inaction at the crucial decision-making moment could significantly influence the organization's viability going forward.

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:

- Is the board satisfied that executive management has its finger on the pulse of the tone of the organization, including how it influences the manner in which the organization's personnel perceive and manage risk? How does executive management evaluate the organization's risk culture?
- Are the line-of-business leaders and process owners designated as the ultimate owners of risk and held accountable for results? If so, do they act as risk owners?
- Do the independent risk management and compliance functions have clearly defined roles? Do those roles, as defined, constitute effective lines of defense? Are these functions positioned within the organization to carry out their respective roles effectively? Do they have access to the board or to a committee of the board?
- Has internal audit broadened its value proposition to encompass risk management? Does it have access to the audit committee?
- Are directors satisfied that executive management involves the board with significant risk management and compliance issues on a timely basis?

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 and compliance. We provide an experienced, unbiased perspective on issues separate from those of company insiders and an analytical assessment approach that focuses on strengthening the five lines of defense.

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. Through our network of more than 70 offices in over 20 countries, we have served more than 35 percent of FORTUNE 1000® and FORTUNE Global 500® companies. We also work 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.