Compliance & Ethics PROFESSIONAL

Vol. 8 / No. 6
12 / 2011

TOP STORIES INSIDE

Meet Patrick W. Kelley

Assistant Director, FBI Office of Integrity and Compliance

Society of Corporate Compliance and Ethics

Risk Management: What's a (smaller) public company board to do?

By Jeffrey M. Tilton, CFE, CICA; and Nancy D. Lieberman, JD

Ultimately, a company's board of directors is responsible for the oversight of the various risks the company faces. SEC rules require that all public companies disclose in their annual proxy statement the extent of the board of directors' role in risk oversight. Enhanced disclosure rules were approved on December 16, 2009, focusing on corporate governance and compensation matters that require specific disclosures in the proxy and financial statements on, among other things, the relationship of a company's compensation policies and practices to risk management, board leadership structure, and the board's role in risk oversight.

Every board of directors should ensure that their company adopts procedures to effectively identify and monitor risks so that the company may operate more effectively and can make appropriate and accurate disclosure in its SEC filings.

As a result of the adoption of the Dodd-Frank Wall Street Reform and Consumer Protection Act (also known as the Wall Street Reform Act), many smaller public companies have diverted their attention from focusing on risk management. Dodd-Frank was adopted on July 21, 2010, and established a permanent exemption from Section 404(b) of the Sarbanes-Oxley Act of 2002 (SOX) for public companies with less than $75 million in market capitalization. Section 404(b) requires that companies obtain an external audit and attestation regarding their internal controls over financial reporting; boards of smaller public companies need to understand that Dodd-Frank does not. The Startup Expansion Investment Act, introduced on September 15, 2011 by Rep. Ben Quayle (R, Ariz.), which proposes to temporarily exempt companies with market capitalizations below $1 billion from the requirements of Section 404(b), will not exempt them from their obligation to manage the risks faced by their companies. It merely exempts their companies from the obligation to obtain an external audit and attestation of certain controls. Consequently, notwithstanding budget and personnel constraints, smaller public companies must find a way to formally identify and monitor risk in order to discharge their obligation to manage risk.

The board must take action it reasonably believes to be appropriate in the exercise of its reasonable good faith business judgment. Appropriate action would be to institute policies and procedures designed to identify and monitor risks, including thoroughly documented testing. It is this documentation that will help establish that the board is affirmatively identifying and monitoring risk.

One way for a board to establish and document this responsibility is to expand the company's existing SOX and other regulatory programs into to a consolidated governance, risk management and compliance (GRC) program. GRC is the umbrella term covering an organization's approach across these three closely related concerns: governance, risk management and compliance. A GRC program has the added benefit of being designed to be integrated and aligned in order to avoid conflicts, wasteful overlaps, and gaps. GRC also addresses the personnel constraints that are common at smaller companies by establishing a program that applies across various risk functions using a company's existing organizational structure, to the extent feasible.

CONTINUED ON PAGE 10

GRC aims to eliminate expensive corporate silos and to integrate organizational management, protect against fraud, and monitor regulatory adherence. GRC provides a framework for risk management, which typically involves identifying particular events or circumstances relevant to the organization's objectives (risks and opportunities), assessing them in terms of likelihood and magnitude of impact, determining a response strategy, and monitoring progress. In addition, by identifying and proactively addressing risks and opportunities, business enterprises protect and create value for their stakeholders, including owners, employees, customers, regulators, and society overall. GRC is evolving to address the needs of various stakeholders, who want to understand the broad spectrum of risks facing organizations to ensure the risks are appropriately managed. Regulators and debt rating agencies have increased their scrutiny on the risk management processes of companies.

Governance

There are various policies that are typically classified as "corporate governance" which can assist a board in managing risk.

A board comprised of a majority of independent (non-management and non-affiliated) directors can assist in effectively managing risk. Governance experts, as well as proxy advisory firms, have stated that having a majority of the board consist of independent directors is advisable to reduce the risk that directors will fail to act in the best interests of the stockholders. Having independent directors, particularly directors from varying backgrounds, can also be expected to have value, due to the differing expertise and connections that independent directors bring to the boardroom, outweighing the increase in board fees paid by companies. Majority-independent boards are required for companies listed on the New York, American or NASDAQ stock exchanges. Companies that are not exchange-listed are not subject to exchange governance requirements. Nevertheless, SEC rules require that a non-listed issuer apply an exchange definition of independence and disclose whether its directors are independent under that standard.

In order to appropriately manage board-level risk, in addition to establishing a majority-independent board, generally a board should also establish board committees. Again, stock exchange listing rules generally require that the board establish committees of independent directors or provide that if a company does not establish such committees, require that decisions that would typically be made by those committees be made by a majority of the company's independent directors. For example, New York Stock Exchange rules require that its listed companies establish an Audit Committee, Compensation Committee, and Nominating/Corporate Governance Committee, while NYSE-Amex and NASDAQ rules mandate that companies have an Audit Committee and, if they fail to establish Compensation and Nominating Committees, require that actions that would typically be made by those committees be made by a majority of the company's independent directors. Committee charters should address certain basic subjects and should provide for the committee's ability to retain independent advisers.

In connection with managing financial reporting risks, every public company should also establish a Disclosure Committee, including, at a minimum, the CFO, CEO, and General Counsel (GC) (whether in-house or outside). The role of a Disclosure Committee is to ensure that an issuer has established effective "disclosure controls and procedures" as required by Section 13a-15 of the Securities and Exchange Act of 1934 (Exchange Act). "Disclosure controls and procedures" are procedures designed to ensure that the information required to be disclosed by an issuer in the company's reports is accumulated and communicated to management to allow timely decisions regarding required disclosure. Companies need to remember that, notwithstanding the exemption from Section 404(b)

of SOX contained in Dodd-Frank, Section 13a-14 of the Exchange Act continues to require that a company's CFO and CEO certify in every Form 10-Q and 10-K as to the effectiveness of an issuer's disclosure controls and procedures and internal controls over financial reporting. "Internal controls over financial reporting" are procedures designed to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles. It is the monitoring and testing of a company's various financial, IT, and operational risks, including as part of a GRC program, that enable its CEO and CFO to make such certification. In addition, the documented monitoring and testing of such controls is what enables the auditors of larger public companies to attest to those internal controls.

Another committee that is not required by exchange-listing rules, but many consider advisable, is a Finance Committee. The Finance Committee provides assistance to the board with respect to its oversight of the company's capital structure, corporate finance strategy, and activities; share redemption and purchase activities; treasury function, investment management, and financial risk management; defined benefit and contribution plan investment planning; insurance plans; and major acquisitions.

Generally, the GC (in-house or outside) should attend meetings of the board and its committees in order to enable the GC to advise regarding legal issues that arise at such meetings, to ensure that any issues that are required to be reported in the company's Exchange Act reports are adequately and accurately reported, and to ensure that records of actions taken at the meetings are adequately and accurately memorialized.

Risk management and compliance

Management should perform an evaluation to identify the risks facing their organization by utilizing company personnel or a consultant who can assist the company's managers or other staff as required. The initial risk functions companies may identify would include, but should not be limited to:

Strategic planning identifies external threats and competitive opportunities, along with strategic initiatives to address them.

Compliance and ethics monitors compliance with codes of conduct and directs fraud investigations.

Accounting and financial reporting compliance directs the Sarbanes-Oxley Section 302 and 404 assessment, which identifies financial reporting risks.

Disaster recovery oversees policies and procedures related to recovery of technology infrastructure critical to an organization after a natural or human-induced disaster.

Internal Audit evaluates the effectiveness of each of the above risk functions and recommends improvements.

Treasury ensures cash is sufficient to meet business needs, while managing risk related to commodity pricing or foreign exchange.

Credit ensures any credit provided to customers is appropriate to their ability to pay

Legal manages litigation and analyzes emerging legal trends that may impact the organization

Insurance maintains the proper insurance coverage for the organization

Marketing understands the target customer to ensure product/service alignment with customer requirements

Operational quality assurance verifies operational output is within tolerances.

Operations management ensures the business runs day-to-day and that related barriers are surfaced for resolution.

Customer service ensures customer complaints are handled promptly and root causes are reported to operations for resolution.

After the initial risks have been identified and related policies and procedures have been written, they should be reviewed and approved

CONTINUED ON PAGE 13

by the board. Management should then establish a system to monitor, inquire, and test the risk program quarterly for any required changes to the program and prepare a report to the board, which should again approve any required changes to the program.

Boards should understand that any risk assessment and monitoring program has limitations. Limitations can result from various issues, such as human judgment in decision-making that can be faulty; responses to risk functions and controls that may breakdown because of human failures, such as simple errors or mistakes; controls that can be circumvented by collusion of two or more people; and management's ability to override enterprise risk management decisions. Although these types of limitations preclude a board and management from having absolute assurance as to achievement of a GRC program's objectives, regular testing can often reduce their impact.

Boards and management of smaller public companies must not lose sight of the fact that, notwithstanding budget and personnel constraints, the board must manage and monitor risk and disclose in SEC filings the board's role in risk oversight. Although not the only way, a GRC program is one way for smaller companies to manage and monitor risk and eliminate silos to increase reporting effectiveness and reduce cost. Ensuring that a company has an effective risk management program enables a board to discharge its obligation to manage risk and make appropriate SEC disclosure. ✳

Editor's note: Jeffrey M. Tilton is the President of JMT Consulting Solutions, LLC in Woodmere, New York. He may be contacted by phone at 516-967-3179 or by e-mail at jmtconsolllc@aol.com.

Nancy D. Lieberman is a Corporate and Securities Partner at Farrell Fritz, PC in Uniondale, New York. She can be contacted by phone at 516-227-0638 or by e-mail at nlieberman@farrellfritz.com.