Compliance & Ethics Professional

January 2014

A PUBLICATION OF THE SOCIETY OF CORPORATE COMPLIANCE AND ETHICS

www.corporatecompliance.org

Congratulations, Brian!

an interview with Brian Patterson

the 6,000th person actively certified by the CCB

See page 14

by Greg Dickinson

Rethinking your third-party risk management initiatives and responsibilities: Part 1

» Consider risk management and governance in terms of their impact on specific stakeholders, such as senior management, board members, and corporate and external counsel.

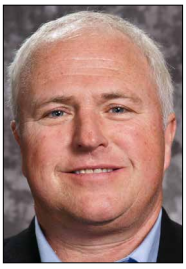
» Consider how procurement can impact your governance initiatives and define the roles and responsibilities in proactive vendor/third-party relationship measurement and monitoring.

» Your board members need to understand how risk can impact their company's regulatory requirements and shareholder value.

» Consider implementing processes and procedures that will help to identify critical risks and ensure analytical and reporting transparency.

» Technology, while not the entire solution, is necessary in helping management and board members develop and oversee corporate risk management initiatives.

Compliance issues are no longer just the concern of Compliance departments and risk management officers. Recent federal legislation on risk governance and management directly involves the board of directors, requiring at least one board member to be accountable for compliance issues.



Dickinson

We recognize that compliance/risk management officers are under pressure as they respond to new mandates, work to figure out how to stay within regulatory frameworks, and work with their boards to comply with new laws. These rules currently impact companies in the financial sector, but the writing is on the wall for many industries. In light of the sweeping and ongoing reforms, Wall Street and boards of directors are forced to operate under a heightened level of uncertainty related to the shifting legislation impacting their businesses.

The perspectives below answer some hard questions I posed as to how companies can deal with the latest legislation by working it into their existing risk management strategies. The experts who provided information and insight for these questions are D'Anne Hurd, a strategy and risk mitigation expert and faculty at the National Association of Corporate Directors' Board Advisory, and William Wise, Chief Ethics Officer of the Ethics and Compliance Officers Association.

GD: Risk management is not a new issue. However, boards seem to be paying greater interest to this topic. Do you agree? What do you think is driving this change?

DH: Many of the changes are the result of deficiencies in risk management in the banking industry and the recent financial crisis. There are two key indicators of changes with respect to risk management. The first is a company's Form 10K; the second is recent

proposed regulatory changes from the Federal Reserve Board.

Reporting on risk factors has been a part of a public company's annual filing for many years and, therefore, something that board members routinely review. However, the discussion of risk factors, as reported on Form 10K, is getting lengthier and more complex and companies are now reporting on a new risk factor—the risks associated with their third-party relationships. Third parties include vendors, suppliers, partners, or any other party whose success is critical for a company to produce and sell their product or service.

A new proposal from the Federal Reserve Board (under the Dodd-Frank Act) mandates the formation of a board of directors' level risk management committee. The risk committee must be chaired by an independent director and must have at least one member with risk management expertise. The legislation currently only affects companies in the financial sector, but it is an indication of a trend. It also blurs the lines between management and the board. Previously the chief compliance officer reported risk factors to the board. Now the board must have its own risk committee and include someone with risk management expertise.

A new proposal from the Federal Reserve Board (under the Dodd-Frank Act) mandates the formation of a board of directors' level risk management committee.

GD: Proposed legislation from the Federal Reserve and the Dodd-Frank Wall Street Reform and Consumer Protection Act (with regard to board of directors and risk management) applies to companies in the financial services sector. How does this legislation affect companies in other industries?

WW: Currently the legislation itself only applies to financial services companies. However, companies outside financial services should be thinking about these changes in terms of best practices with the possibility of them expanding to other sectors.

One approach is to consider what keeps board members up at night. The answer should be "absolutely nothing!" The board should be handling issues of strategy and governance. However, it's management's job to give the board the fullest confidence that they have policies, procedures and tools in place to manage and identify risk and can avoid risk to the extent that is possible.

GD: If changes in risk management are occurring at the board level, what changes need to occur at the management level?

DH: The operational management of risk is the responsibility of a company's management team. It needs to be included in their job descriptions and baked into their roles, responsibilities, objectives, and day-to-day functions. All departments need to have a stake in the role of risk reduction.

Taking the Foreign Corrupt Practices Act as one area of risk management, it is essential for the board to know that every member of its management team is aligned with identifying, eliminating, or mitigating risks associated with bribery of foreign officials to obtain or retain business.

GD: Is third-party risk management the responsibility of the chief compliance officer or of other members of the management team?

WW: Even if a company has a CCO, he/she is not the person responsible for the day-to-day management of risk. The CCO should be advising, supporting, and maybe establishing appropriate policies and procedures, but execution and oversight must be the purview of individual managers. It should be part of the fabric of what a manager thinks about on a day-to-day basis.

One example is the Mexican subsidiary of an American multinational operating in the food industry, which interacted with publicly-employed veterinarians to get proper clearances and permits for a food processing plant. It turns out that the company was bribing these officials as well as employing their wives in no-show jobs. The issue, therefore, is who has the responsibility to prevent, discover, and manage these matters? Where is appropriate due diligence occurring? Is it in compliance, manufacturing, plant management, sales, marketing, human resources? The list is extensive.

One example is the Mexican subsidiary of an American multinational operating in the food industry, which interacted with publicly-employed veterinarians to get proper clearances and permits for a food processing plant.

GD: If the lines between the responsibility of the board and management are blurring, does that mean that the board is now responsible for day-to-day or operational risk management?

DH: The board has a very clear role with respect to risk. There are two areas where the board should be concerned and neither of them has to do with operational risk. Operational risks need to be reported to the board, but the board should not be taking on day-to-day responsibilities. The two areas are:

- **Governance risk**—The focus is on board leadership and board composition. Who is on the board? Are the people on the board doing the right things? Are they executing against their fiduciary duties?
- **Strategic risk**—Boards should be concerned with anything that might affect the strategy of the company, such as diversification of product lines or overseas expansion.

Operationally, board members need to have confidence in the ability of management to manage risk and to provide them with accurate, comprehensive, and appropriate reporting.

GD: If the board is responsible for strategic risk (versus operational risk), does that include risk associated with a company's third parties?

DH: Management of third parties should be one of the controls that a company has in place and reports at every board meeting. Board members need to understand what management is doing to identify, assess, mitigate, and monitor third-party risk. This is particularly important for companies doing business and expanding their business operations internationally. ✳

Greg Dickinson *(dickinson@hiperos.com) is CEO of Hiperos in Somerville, NJ.* ***D'Anne Hurd*** *(dhurdbourne@gmail.com) is an active independent board member for a number of companies, including Hiperos. She also serves as a faculty member of the National Association of Corporate Directors' Board Advisory Services Practice.* ***William Wise*** *(william.wise@hklaw.com) is Senior Counsel at Holland & Knight in Boston. His practice focuses on assisting chief legal officers, general counsels, and companies with review and implementation of compliance and ethics programs, code of conduct training, and evaluation of a company's risk assessment process.*