Responding To The Evolving Roles And Responsibilities Of Boards Of Directors And Audit Committees: The Importance Of A Compliance Risk Assessment – Part II

Robert E. Bostrom

WINSTON & STRAWN LLP

The following checklist suggests some, but certainly not all, of the kinds of questions that Boards of Directors and, in particular, Audit Committees should be asking management:

• Do compliance risk managers or a risk management committee have the authority and backing of the Board?

• Has the CEO made compliance and risk management a strategic priority?

• Has a senior level position been established with firm-wide risk and compliance oversight responsibilities?

• Has a compliance structure been established? Is there a senior, full-time compliance officer? Are there appropriate compliance policies and procedures in place?

• Is there a direct reporting line between the senior risk officer and compliance officer to the Audit Committee and the Board?

• Have the responsibilities of the company's executive management and organizational leadership for compliance been specified?

• Are there adequate resources and authority for individuals within the company with the responsibility for the implementation of the compliance and risk management programs?

• Is the Board fully apprised of all risks faced by the company including not only business and financial but also legal, regulatory, compliance, operating, treasury, vendor, customer, product, political, international, supply, reputational, human resources, technology, insurance and audit?

• Has the Board made an independent determination that management has implemented and maintains an effective enterprise risk management and compliance process, including policies and procedures?

• Is there an effective training program and process for the dissemination of training materials and information?

• Is there periodic evaluation of the effectiveness of the program and a requirement for monitoring and auditing systems?

• Are ongoing risk and compliance assessments conducted?

• Has executive management demonstrated and communicated an effective "tone at the top" and created a culture of compliance?

• Has the Audit Committee allotted enough time and attention to discussions of internal control and compliance with management, the internal auditor and the external auditor?

• Has the Audit Committee obtained written representations based on an appropriate and effective assessment from management on the effectiveness of internal control over financial reporting?

• Do the above mentioned written representations cover prevention and detection of fraud?

• Has the Audit Committee established specific expectations with management and the internal and external auditors about their information needs related to internal control, with particular attention to the control environment and controls in high risk areas?

• Is the Audit Committee aware of the existence and adequacy of a compliance system including policies, procedures, training and certification?

• Has the Audit Committee discussed the company's risk assessment and risk management policies?

***Robert E. Bostrom** is Head of the Financial Services Practice Group and a Partner in the Corporate Department of Winston & Strawn LLP in New York City.*

The Importance Of A Legal And Compliance Risk Assessment

As more fully discussed in Part I of this article, the revised Sentencing Guidelines require organizations to conduct periodic evalutions of the effectiveness of their compliance programs.

In responding to these new responsibilities, the first step is for the Audit Committee and management to review applicable laws and regulations that the company is subject to and assess the company's system for ensuring compliance with laws, regulations and ethical business practices. Based on such a review and assessment, an analysis of the company's compliance and risk management process should be followed by recommendations to enhance the compliance system to ensure that it meets the requirements of: (1) the U.S. Sentencing Guidelines, (2) Section 404 of Sarbanes-Oxley, (3) the relevant provisions of the NYSE listing standards, (4) the COSO Framework, (5) PCAOB Audit Standard No. 2, and (6) the evolving jurisprudence following *Caremark* regarding the duties of the Board of Directors. It is important to note that this is not a static process – it is an ongoing process that must continue to evolve on a regular basis.

The following sets forth a summary of a three-phase approach to conduct a review and assessment and make recommendations for an international company in the following areas: (1) the structure of the risk management and compliance structure in the U.S. and between the U.S. and foreign operations; (2) the nature and the scope of required risk management and compliance monitoring and reviews; and, (3) the legal, regulatory, corporate and tax structure of all operations and activities in the U.S. and abroad.

Phase I – Review And Assessment

1. ***Review principal business activities and business unit policies.***

Obtain an understanding of the business structure, management organization, and principal activities in the U.S. and abroad. This will provide essential information about what the business units perceive as key issues and how those issues are addressed and provide a basis for recommendations. This will include interviews with relevant personnel and review of all policies and procedures.

2. ***Review corporate structure.***

Obtain an understanding of the legal, regulatory, compliance, tax and corporate structure of all domestic and foreign operations.

3. ***Review recent risk management and compliance reports and certifications, self-assessments, audit and regulatory reports (and all responses thereto) for the domestic and foreign operations submitted to senior management and to the Audit Committee and appropriate regulatory filings submitted to the regulators.***

Determine the assessment of risk management and compliance activities, and identify unusual or recurring issues that have arisen during the conduct of recent business operations. This will include meetings with officers in the U.S. and abroad with responsibility for all regulatory and compliance matters.

4. ***Review any regulatory or supervisory enforcement actions.***

Review any regulatory enforcement actions to determine existing problems or issues that need to be addressed or are being addressed as part of an action plan in response to any enforcement activities.

5. ***Review compliance policies and structure.***

Determine the organizational structure of the risk management and compliance functions, including reporting lines within the risk management and compliance function and relative to the audit and legal functions and the Board of Directors. Assess the process of risk management and compliance, including the key objectives and the manner in which those objectives are expected to be achieved.

6. ***Interview all officers and staff with risk management, compliance and audit responsibilities.***

Obtain internal viewpoints on the strengths and opportunities for improvement regarding regulatory management in the existing risk management and compliance system, understand how the businesses operate and any particular issues presented by the businesses, and collect information on experience with risk management and compliance systems in other organizations.

7. ***Review the risk management and compliance training programs.***

Determine how information on key laws, regulations and business policies and risk management and compliance policies and procedures are evaluated and imparted to business management and staff.

8. ***Identify the scope of issues that need to be addressed and set forth the broad outlines of recommended changes in (a) the structure, organization, objectives and operation of the risk management and compliance function, (b) the management of regulatory relationships, and (c) the legal, regulatory, corporate and tax structure for domestic and foreign businesses and operations.***

9. ***Prepare recommendations based on industry best practices on key risk management and compliance topics and the COSO Enterprise Risk Management Framework.***

10. ***Prepare a description of the regulatory expectations regarding key risk management and compliance and operational subjects applicable to domestic and foreign operations and management of regulatory relationships.***

11. ***Provide a description of and rationale for the management and structuring of regulatory relationships and a consolidated risk management and compliance structure and a legal, regulatory, corporate and tax structure.***

Phase II – Preparation Of Recommendations Regarding A Risk Management And Compliance Structure, Management Of Domestic And Foreign Regulatory Relationships, And The Legal, Regulatory Corporate And Tax Structure For Domestic And Foreign Operations

Based on the review and assessment, an independent recommendation should be made with appropriate revisions to be implemented regarding the (a) management of regulatory relationships, (b) the risk management and compliance structure and (c) the legal, regulatory, corporate and tax structure of domestic and foreign operations and business. There are several key memoranda or discussion papers that will serve as the basis for completing the design of the compliance structure.

1. ***Design a structure of risk management and compliance function.***

Provide detailed recommendations for the overall structure of the risk management and compliance function elaborating on the general recommendations developed in Phase I, including structure, objectives, responsibilities, organization, staffing, reporting lines, and their relationship to the legal and audit functions and to the business units in the U.S. and between the U.S. and foreign operations based on best practices and regulatory requirements.

2. ***Design risk management and a compliance monitoring and self-assessment system.***

Prepare a monitoring program that risk management and compliance staff would use to review and assess compliance by the business units with applicable laws and regulations and key business policies.

3. ***Develop a compliance reporting and review process.***

Recommend a risk management and compliance reporting and review process that would encompass six levels of reporting and review: (i) within the risk management and compliance function, (ii) between the risk management and compliance function and business unit managers, (iii) from the risk management and compliance function to senior management, (iv) from the risk management and compliance function to the Audit Committee of the Board of Directors, (v) between U.S. and foreign operations and (vi) reports to persons outside of the company, e.g., regulators and the Board of Directors.

4. ***Design a compliance training program.***

Prepare a risk management and compliance training program for business staff, including, for each significant business unit or activity, the subjects to be covered, the length and scope of training sessions, the various media to be used to deliver training, and the training methodology.

5. ***Recommend enhanced policies and procedures to support risk management and compliance function.***

Recommend specific material to be included in risk management and compliance policies and procedures throughout the business units.

6. ***Develop mechanisms for responding to risk management and compliance issues.***

Recommend a process for identifying and addressing potential risk management and compliance problems, including interaction of the risk management and compliance function with the individual business units, the legal, audit and risk management functions and senior management.

7. ***Develop risk management and internal controls assessment methodology for risk management and compliance function.***

Develop methods for identifying at any point in time the greatest sources of compliance risk for purposes of efficiently allocating compliance resources. This methodology also would consider how to identify activities that require internal controls, where such controls should be located, and what types of controls should be used.

8. ***Recommend an audit program for central and business unit risk management and compliance functions***

Recommendations for the scope, content and frequency of internal audits of the activities and effectiveness of the risk management and compliance function.

9. ***Recommend management structuring of domestic and foreign regulatory relationships and addressing regulatory issues.***

Phase III – Implementation

The principal areas in the implementation phase include.

1. Introduction of new compliance structure and process to business unit managers.

2. Assist in training compliance staff on compliance reporting system and compliance training program.

3. Establish an appropriate division of responsibilities between the compliance, legal and audit functions and the business units.

4. Develop a compliance monitoring and self-assessment function.

5. Develop compliance policies and procedures and other related documentation.

6. Assist in creating an audit program to review the compliance function.

7. Develop ongoing assessment and audit programs of the compliance function.

Conclusion

Before an appropriate risk management and compliance process can be implemented, it is imperative that a thorough assessment be undertaken of the compliance risks that a corporation faces. Once this first step has been undertaken, the next step is to analyze and implement a risk management and compliance process that is appropriate for the risks that the corporation faces.

Please email the author at rbostrom@winston.com with questions about this article.