Board Assessment of a Compliance Function

One of the features of the OSFI Corporate Governance Guideline that goes fully into effect on January 31, 2014, is an expectation that the Board of Directors will regularly assess the effectiveness of the firm's oversight functions and processes. The Guideline goes on to state that, occasionally, as part of the assessment, the Board should conduct a benchmarking analysis with the assistance of an external adviser. However, as benchmarking is to be only an occasional part of the assessment, the clear implication is that the Board assessment will entail more than just benchmarking.

The Guideline provides some further helpful context to the Board in designing an assessment. First, the Guideline notes that oversight functions exist to assist a Board to fulfill its role of stewardship and oversight. The Guideline notes that the functions do this by validating for the Board whether the controls within the business units are effective and whether the firm's operations, results and risk exposures are reliably reported to the Board. To be considered to be effective, an oversight function is to provide the Board with objective assessments.

The balance of this article will focus on a Board assessment of the effectiveness of a compliance oversight function. This article is intended to assist directors by providing some suggestions for an effective assessment.

DOES THE COMPLIANCE FUNCTION HAVE AN APPROPRIATE ROLE?

Since the financial crisis of 2008, there has been a significant evolution in the role of a compliance function within a firm. Prior to 2008, while the compliance function may have been independent from local management in a business unit, in practice, the role of the function was often to assist the business units to meet their compliance obligations. It did this by taking responsibility for keeping the business informed of the applicable regulatory requirements and assisting with the design of appropriate controls. Therefore, while the compliance function and the business function were separate, compliance was not in an oversight role. What has been made much clearer by the Guideline is that independence is more than just a separation of functions. For example, the Guideline speaks to the oversight functions providing "objective assessments" of the controls within the business units. Clearly, a function cannot provide an objective assessment of a control that it has designed and implemented.

To be effective from the perspective of the Guideline, the compliance function must truly be acting as a oversight function. Evidence that the function has the right role could be obtained by reviewing the compliance framework adopted by the firm. Is management clearly the first line of defense with direct accountability for compliance and developing and maintaining effective compliance controls? Is it the role of the compliance function to monitor the activities of management and to form an independent objective view of the adequacy of the controls established

by management. Unless this distinction is clearly established and enforced, the function cannot effectively fulfill its role as set out in the Guideline.

Question 1: Is compliance an oversight function?

ASSESS THE AUTHORITY

The Guideline provides that oversight functions must have the appropriate standing, authority and independence within the firm. In order to assess the strength of controls and the commitment to remedy compliance issues, the compliance function must have full access to information and to management and staff of the business units. The head of compliance and the function must have the ability to obtain the cooperation of leaders of the firm's business units. If business management fails to support compliance efforts, issues could remain hidden. While it is important for the Board to be satisfied that the head of the function has the appropriate organizational title, having the appropriate standing and authority requires more than a title. It is the firm's overall attitude to compliance is critical.

In order to assess true standing and authority, the Board should watch for evidence that management is watering down compliance issues or failing to take prompt corrective action. The Board itself could take steps to support the standing of the function. For example, the Board should ensure that sufficient time is allocated to the compliance report and, if appropriate, hold regular in camera sessions with the head of the compliance function. More importantly, the Board should reinforce the accountability of the leaders of the business units by receiving reports directly from them about the status of compliance efforts in their business units.

Question 2: Is the head of the compliance function a respected member of senior management?

Question 3: Do the business leaders report on compliance issues related to their business units?

Question 4: Are compliance issues reported by the compliance function being remedied in a timely manner?

DOES THE HEAD OF THE FUNCTION HAVE THE NECESSARY SKILLS

Increasingly, compliance risk management is becoming a recognized profession. Regulators, therefore, expect that the individuals that head the compliance function will have the training and experience required for the role.

The experienced required for the head of the compliance function will depend to some extent on the circumstances of the firm. The qualifications necessary for the leader of the function may also vary depending upon the number and quality of the supporting staff in the function.

Obviously, direct prior experience in a compliance role is helpful. However, other experience closely related to the compliance function, such as internal audit or legal, can be useful. Previous

experience with a line of business may also be beneficial as it builds credibility and relationships with business leaders. Of course, if the head of the function previously held a significant position in a line of business, issues of independence will also need to be considered.

Another important consideration is whether the individual has the right personality to head a compliance function. Again, the answer to this question may depend upon the circumstances of the firm. While it is important that the directors are confident that the head of the function will speak up when necessary, the ability to work with management in a collaborative manner is just as important as the ability to be critical.

Question 5: Does the head of the function have the necessary training, expertise and personality for the job?

ONGOING TRAINING

Neither the regulatory environment nor the business environment is static. The head of the compliance function and function staff must be equally knowledgeable about developing compliance techniques and processes and about developments in the business. An effective compliance function seeks out training opportunities to ensure that the skills and knowledge of the head and the key staff of the function are keeping pace with changes in the environment. The compliance budget should allocate sufficient funds to these activities.

Question 6: Does compliance function staff receive ongoing training in the regulatory, compliance and business environments?

RISK ASSESSMENTS

Regulators expect that directors will understand the regulatory risks particular to the firm. One of the key responsibilities of the compliance function is to perform a regulatory risk assessment identifying the business activities and regulations that give rise to the greatest risk and integrating these assessments into its oversight activities. This ensures that the areas of greatest risk are receiving appropriate attention.

Because the environment is not static, risk assessments cannot be static. At very least, risk assessments must be updated at regular intervals in light of known changes in regulations or business activities.

The Board should understand the risk assessment program used by the compliance function and how areas of material risk were identified. If, however, the firm is consistently being caught off guard by the findings of its regulators, it could be an indication that the areas of greatest risk are not being identified and that the risk assessment program needs improvement. Of course, if regulators feel that management and the Board are being consistently caught off guard by its findings, it

erodes their confidence and reflects negatively on the Board's ability to provide the expected oversight.

Question 7: Is the Board provided a description of the risk assessment process and the areas of greatest risk for the firm?

Question 8: Are the company's regulators consistently identifying issues in areas that were not identified as high risk by the compliance function?

MONITORING

Under the Guideline, an oversight function assists the Board by validating whether the controls in the business units are effective and that the risk exposures (in this case, the risk of a compliance breach) are reliably reported. The compliance function does this by establishing an oversight or monitoring program.

A Board should understand how the compliance function reaches its conclusions. To do so, the Board must have an understanding of the monitoring techniques that are used. Is the program risk based using the function's risk assessments? If areas of higher risk are subject to a testing program, what is the testing schedule?

While compliance monitoring is useful in identifying current compliance issues, monitoring results should also be analyzed to identify trends and findings should be shared across the business units so that the same problems do not repeat elsewhere. Does the compliance function conduct this analysis?

Question 9: Has the compliance function established a monitoring program?

Question 10: Are monitoring results being clearly communicated to the board and senior management?

Question 11: Does the compliance function attempt to identify trends from compliance monitoring results?

CHANGE MANAGEMENT

Because a firm's products, systems and services do not remain static, a compliance function should have a means of monitoring and assessing material changes to these products, systems or services. The compliance function should meet regularly with the business units to stay abreast of new developments. The compliance function must be brought into the planning process from the beginning -- not just before implementation. In addition, when significant, unresolved compliance issues are identified, the compliance function must have the authority to delay implementation until any concerns are addressed.

Question 12: Is the compliance function part of the new business planning process?

Question 13: Does the compliance function have the authority to delay implementation of new or materially changed products, systems or services?

COMMUNICATION

The Board needs to be sure that the compliance function is properly escalating issues it identifies throughout the organization. After all, in addition to identifying concerns for the Board, the real goal of the function is to ensure that issues are being appropriately remedied. The Board should be provided information about the escalation process and the basis upon which issues are reported to the Board and to management. When issues are reported to the Board, information should also be provided about the remediation plans and how progress against these plans is being monitored.

Compliance reports must also be useful for the directors and management. Reports must be presented in a user-friendly, easy-to-read format. Reports that provided too much information are as ineffective as those that provided too little. The compliance function must describe regulatory risks in clear, comprehensible terms. The Board should critically assess the quality of the information that it receives, whether it is actionable and linked to the associated risk.

Question 14: Has the compliance function established an escalation policy?

Question 15: Are board reports easy to read and understand?

RESOURCES

Obviously, a compliance function cannot be effective unless it has the necessary resources. The Guideline requires that the Board approve the resources and budget for all of the oversight functions. The compliance function should assist the Board by maintaining a human resources assessment program to assess whether there are enough people with the right skills to meet the function's needs. Where appropriate, the compliance function should enlist the support of the human resources function to assist with this assessment.

In some cases, technology has enhanced compliance-monitoring capabilities and provided opportunities for efficiencies. In other cases, the function simply could not operate or meet regulatory expectations without the use of technology. The compliance-resourcing plan should include an analysis of the current and potential future use of technology.

This resource assessment and plan should be provided to the Board so that the directors can understand the compliance function leader's assessment of the adequacy of the function's resources and the bases for that assessment.

Question 16: Does the compliance function provide the directors with an explanation of the function's resourcing assessment?

INTERNAL AUDIT

As the head of internal audit is an expert in control assessment, one potential source of information about the quality of the compliance function and, in particular, its monitoring program is internal audit's assessment of the function. However, as internal audit may not have the same level of experience with regulation and the expectations of the regulators, in assessing the compliance function, a Board would be unwise to rely solely on the views of internal audit.

Updated November 2013

Please contact us for more information

John Jason, President

(416) 726-2355

john.jason@CanadianComplianceGroup.com

APPENDEX

THE QUESTIONS

Question 1: Is compliance an oversight function?

Question 2: Is the head of the compliance function a respected member of senior management?

Question 3: Does the head of the compliance function meet regularly with the Board, CEO and other business leaders?

Question 4: Are compliance issues reported by the compliance function remedied in a timely manner?

Question 5: Does the head of the function have the necessary training and expertise?

Question 6: Does compliance function staff receive ongoing training in the regulatory, compliance and business environments?

Question 7: Is the Board provided a description of the risk assessment process and the areas of greatest risk?

Question 8: Are the company's regulators consistently identifying issues in areas that were not identified as high risk by the compliance function?

Question 9: Has the compliance function established a monitoring program?

Question 10: Are monitoring results being clearly communicated to the board and senior management?

Question 11: Does the compliance function attempt to identify trends from compliance monitoring results?

Question 12: Is the compliance function part of the new business planning process?

Question 13: Does the compliance function have the authority to delay implementation of new or materially changed products, systems or services?

Question 14: Has the compliance function established an escalation policy?

Question 15: Are board reports easy to read and understand?

Question 16: Does the compliance function provide the directors with an explanation of the function's resourcing assessment?