Board Perspectives: Risk Oversight

Positioning Compliance for Effectiveness

Issue 65

Positioning the compliance function for effectiveness is a matter of first defining the roles executive management and the board want the function to play. An understanding of these roles provides a powerful context for evaluating how to position the compliance function within the organization.

We often receive questions regarding the proper positioning of compliance in an organization. The debate often centers on addressing to whom compliance reports. Unfortunately, this line of inquiry does not focus on the fundamental issue of roles and responsibilities. One reason there is disparity among organizations in positioning compliance is that there are different views regarding the responsibilities expected of the function. Below, we explore these views and their implications to positioning.

Key Considerations

Regulatory settlements addressing egregious non-compliance issues sometimes stipulate a different line of reporting for a company's compliance officer. For example, it is not unusual for settlement deals to stipulate that the chief compliance officer (CCO) not be subordinate to the chief legal officer or chief financial officer and that he or she should report directly to the chief executive officer (CEO) and the board. But the question remains: What is the CCO expected to do?[1]

Generally, a company's compliance function is responsible for overseeing or coordinating compliance efforts, ensuring that the company and its employees understand and are complying with applicable laws and regulations and internal policies. Some functions

Two Roles of the Chief Compliance Officer (CCO)

The "Champion" CCO

- Framework Advancer/Enabler
- Coordinator/Integrator (Ensures Consistency)
- Educator (Provider of Insights)
- Facilitator
- Consultant
- Communicator
- Reporter

The "Line of Defense" CCO

- Evaluator
- Initiator
- Approver
- "Escalator"
- Vetoer
- Arbitrator

[1] "More Compliance Chiefs Get Direct Line to Boss," by Gregory J. Millman and Ben DiPietro, *The Wall Street Journal*, January 15, 2014: www.wsj.com/articles/SB10001424052702303330204579250723925965180.

may deal with all compliance matters. Depending on the organization's industry, other functions may focus on specific compliance domains, such as environmental, health and safety, contracting, product quality, employment and labor, and anti-corruption. Ethical and responsible business behavior may also fall within the scope of a compliance function's responsibilities.

A compliance function may be led by someone designated as the compliance officer or an equivalent title. If responsible for overall compliance, that person may be the CCO, which we use here to refer to the function's leader.

We see two distinct CCO roles in practice, as well as variants of each. An understanding of the two roles provides context for framing the positioning conversation:

- **The "Champion"** CCO advances the framework for identifying the applicable compliance requirements (as defined by laws, regulations, contracts and internal policies), aligning policies and processes with those requirements, assessing risk of noncompliance and closing gaps to ensure ongoing compliance. The frontline operating units and process owners are responsible for applying the compliance framework. They retain primary ownership of the risks created by their respective units and processes. The Champion CCO:
  - Enables application of the framework by providing tools, guidance and other resource materials to support its application.
  - Educates primary risk owners on the proper use of the framework, provides them with appropriate insights and offers consultation upon request.
  - Coordinates and integrates cross-unit and cross-functional application of the framework to ensure sharing of effective practices to address enterprise compliance matters and common risks.
  - Facilitates risk assessments and formalization of risk mitigation plans and supports executive management in communicating relevant compliance messages.
  - Prepares reports on the state of compliance, typically on an annual basis, and either presents that information to the board of directors or assists a senior executive who presents it to the board.
  - Reports compliance activities with periodic summaries to appropriate executives and the board, including an assessment of risks and the potential impact of noncompliance against the estimated costs to achieve compliance, along with recommended compliance funding priorities and initiation of appropriate corrective actions.
- The **"Line of Defense"** CCO undertakes the activities of the Champion CCO and, in addition, is authorized to do a combination of the following:
  - Evaluate the (1) state of compliance; (2) quality of compliance risk assessments; (3) design and implementation of risk mitigation plans; and (4) operating effectiveness of those plans, all in coordination with internal audit and other evaluators.
  - Establish standards and implement procedures to ensure the organization's compliance programs are cost-effective in preventing, deterring and detecting noncompliance with applicable laws and regulations, contracts and internal policies, and making necessary corrections through enhancement of existing policies and improvement of compliance infrastructure.
  - Approve policies and compliance risk mitigation plan designs to address identified risks.
  - Coordinate internal compliance reviews of lines of business and functions and monitoring activities to ascertain whether compliance programs are working.
  - Escalate issues to executive management, including the CEO and, through appropriate channels, the board of directors.
  - Veto activities affecting compliance with the organization's mission-critical policies.
  - Arbitrate disagreements between operating and functional units affecting compliance.

The Line of Defense CCO may not be authorized to do all of the above, but the position clearly extends beyond that of the advocate because it has the teeth of escalatory and/or veto authority.

The above role descriptions are not necessarily exhaustive, but they clearly differentiate. We can use them as a context for articulating several principles relating to the positioning of compliance within organizations:

- The Line of Defense CCO must have sufficient stature with business-line leaders and across the organization to serve in the role effectively. Stature comes from the authority, compensation and direct reporting lines that command respect. The authorities of the Line of Defense CCO, enumerated above, should convey to the organization, as a whole, that this executive is a player. To illustrate, this positioning is accentuated if the Line of Defense CCO:
  - Reports to someone who has strong influence in the organization, such as the CEO or executive committee (perhaps with administrative reporting to another C-level executive) or the chief risk officer (CRO); in any case, the reporting line should establish the CCO's independence from core business activities;
  - Is vested with the authority to escalate issues to a senior executive who has access to and influence with the board and, in appropriate circumstances as determined by the board of directors, has direct access to a standing committee of the board;
  - Engages in mandatory and regularly scheduled executive sessions with the board or a standing committee of the board;
  - Has influence on compensation practices incenting the desired compliance behaviors; and
  - Is sufficiently resourced with a support staff commensurate with his or her responsibilities.

  In addition to the above positioning, some believe that the authority to hire and fire the Line of Defense CCO should be vested in the board. We are not convinced this is necessary, although there may be circumstances where a board may conclude that it is.
- A Line of Defense CCO also:
  - Needs an escalation process that is formalized, meaning written procedures and agreements requiring escalation of any significant issues raised by the compliance function that are being challenged by business-line executives.
  - Should be a centralized role; this means all personnel with compliance responsibilities report through the CCO's line rather than through their respective lines of business.
- If the CCO or equivalent executive plays the role of the Champion, that person may report to a C-level executive (e.g., chief administrative officer, chief operating officer, chief legal officer, general counsel) or to a direct report of a C-level executive, and operate with adequate support staff commensurate with his or her designated responsibilities. While independence may be desirable, the Champion CCO doesn't necessarily need to be independent. In fact, depending on the nature of the designated responsibilities, over time, the Champion CCO may not even be a full-time job. In practice, the Champion CCO typically reports to the board of directors or a standing committee of the board only by invitation. A prime issue with the Champion CCO is clarifying how the compliance function interfaces with the lines of business.
- In heavily regulated industries, the Line of Defense CCO model is likely the preferred option. In other industries in those situations where management expects the CCO to focus primarily on understanding and coordinating an organization's fragmented compliance efforts and reporting on the state of compliance, the Champion model might be appropriate.

When applying the above principles, the key question is what do the board and the CEO expect from compliance? Effective compliance management starts at the top. If a viable line of defense is intended, the Champion CCO will not be able to deliver.

Questions for Boards

Following are some suggested questions that boards of directors may consider, based on the risks inherent in the entity's operations:

- If the organization has a compliance function, is the board satisfied (a) with the scope of the function's roles and responsibilities and (b) that it is getting the insights it needs from the function?
- If there isn't a compliance function, is the board satisfied a cost-effective plan is in place to monitor the top compliance risks and oversee implementation of the organization's compliance program?
- If the organization has implemented the Champion CCO model, is the board confident that compliance programs are updated periodically in light of changes in the company's needs and in applicable laws, regulations and contractual requirements?

How Protiviti Can Help

Protiviti assists directors and executive management in public and private companies in developing, implementing and maintaining effective regulatory and internal compliance programs that maximize the benefits of their investment and protect their reputations. We help companies identify, assess and manage risks related to compliance by taking a holistic view of the organization when creating compliance solutions.

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, and has served more than 40 percent of FORTUNE 1000® and FORTUNE Global 500® companies. Protiviti and its independently owned Member Firms serve clients through a network of more than 70 locations in over 20 countries. The firm also works 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.nacdonline.org/Magazine/author.cfm?ItemNumber=9721. 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.**

© 2015 Protiviti Inc. An Equal Opportunity Employer M/F/Disability/Vet. PRO-0215
Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services.

protiviti®
Risk & Business Consulting.
Internal Audit.