Real Guidance (Finally) On the Compliance Oversight Role of Boards

Carrie Penman and Mary Bennett | Jun 23rd, 2015

New guidance for boards of directors on what it means to have "reasonable oversight" for the implementation and effectiveness of corporate compliance programs could signal the beginning of a global trend towards more—and more specific—board accountability.

According to the Federal Sentencing Guidelines, an organization's governing body is responsible to "*exercise reasonable oversight with respect to the implementation and effectiveness"* of the compliance and ethics program. This expectation has been around as long as compliance programs. But practical guidance on what boards of directors should do to meet the standard has been incomplete at best—until recently.

In April, the Department of Health and Human Services, Office of Inspector General (OIG) released a new, more comprehensive set of guidelines, **"Practical Guidance for Health Care Governing Boards on Compliance Oversight"** to help healthcare boards successfully execute oversight of their compliance programs.

This is a landmark document that draws from the Federal Sentencing Guidelines, the OIG's compliance program guidance documents, and OIG Corporate Integrity Agreements. The guidance addresses five key areas that should be reviewed and addressed by all healthcare compliance officers and their boards of directors.

While directed to healthcare boards, we believe the OIG guidance offered is helpful to boards in any industry and in any jurisdiction. In fact, **similar guidance has been released recently by the Bank of England Prudential Regulation Authority**, which contains some of the same elements found in the new OIG guidance and could signal the beginning of a global trend.

Top Three Takeaways For All Ethics and Compliance Officers and Boards of Directors

We have learned three important things from the new OIG guidance:

- First, boards need to take very specific and proactive roles relative to their compliance oversight duties.
- Second, boards can gain a good understanding of the adequacy and effectiveness of the organization's compliance program by setting the right expectations and by knowing and asking the right questions.

- And third, most of the direction provided by the OIG for healthcare boards is broadly applicable to any industry and country.

To help make these takeaways and the OIG guidance more practical for ethics and compliance officers and boards, we have developed a list of questions for each of the five key areas in the guidance. E&C officers can provide this to their boards, and work with them as needed to answer these questions. We hope this worksheet will help board members of any organization reconsider their roles and responsibilities related to compliance programs—and help healthcare board members in particular ensure they are meeting OIG expectations.

An Ethics and Compliance Oversight Assessment Checklist for Boards of Directors and Compliance Officers: Key Questions to Ask and Answer

As noted, this guidance was created for healthcare boards, but can easily be adapted to boards of directors at any organization.

Guidance Section 1: "Expectations for Board Oversight of Compliance Program Functions"

In order to execute their duty of oversight, board members need to review and understand their organization's compliance program. If there is one supreme compliance oversight guideline for board members, it is this: *"A critical element of effective oversight is the process of asking [the compliance officer] the right questions" to determine the adequacy and effectiveness of the organization's compliance program*. These questions could include:

- ***What standards form the foundation for the compliance program?*** Healthcare boards should expect to hear that the program is structured on the U.S. "Federal Sentencing Guidelines" (or possibly OECD Standards for non-U.S. based organizations), "OIG voluntary compliance program documents" specific to the type of entity, and "OIG Corporate Integrity Agreements (CIAs)."
- ***Is there a confidential reporting system in place to take reports of misconduct and legal violations, and is it adequate and appropriately resourced?*** For example, is it easily accessible? Are employees aware of the system and comfortable using it? Is case intake, handling and investigation conducted in a timely way by qualified staff? Is it offered in appropriate languages? Is timely follow-up given to the reporting party?
- ***What assurance does the board have regarding timely escalation of appropriate matters?*** This is often in the form of an escalation policy included in the charters of the board committee, the compliance program, and/or the chief compliance officer. Such a policy mitigates any business or political pressure to delay or suppress prompt reporting of serious matters to the board.

- ***What compliance education is expected of the board?*** The full board should expect to participate in formal internal and/or external education at least annually on: organizational and industry risks; the risks they bring as directors (e.g. conflicts of interest, insider trading); current and evolving regulatory requirements; and the structure and operation of an effective compliance program.
- ***How do you [the compliance officer] know that the compliance program is effective?*** The board should expect to see the results of periodic internal program reviews plus periodic externally conducted program assessments. There should be a formal compliance work plan that includes board regulatory updates. Such reviews help plan adequate "funding and resource allocation." The board should also ask specific questions regarding effectiveness, such as:

  - Do you have the resources you need to do your job appropriately?
  - Do you feel you have access to the CEO and board whenever you need it?
  - Do you have visibility to business unit compliance, including Sales and Marketing (or other potentially high risk function)?
  - Do leaders set the right tone? How are they perceived by employees?
  - How likely is it that an employee will take an issue to an outside agency before reporting a concern through internal channels?
  - How do we address concerns about retaliation?

To better focus on the right questions, the guidance also comments that "…a Board can raise its level of substantive expertise with respect to regulatory and compliance matters by adding to the Board, or periodically consulting with, an experienced regulatory, compliance, or legal professional."

Guidance Section 2: "Roles and Relationships"

As the guidance underscores, while compliance may be the name of a function within the organization, compliance is actually the responsibility of everyone who works there. Per the guidance, the major functions that shape the program and play a key role in its operation are compliance, audit, legal, human resources and management. According to the guidance, the board should ask questions to understand and oversee the effectiveness of these roles and relationships with respect to their compliance-related activities.

- ***What is the role of the audit, compliance, legal, human resources and other relevant functions in the compliance program?*** Well-documented definition of compliance roles and responsibilities should be in place with articulation of their boundaries, plus board-approved expectations for cross-functional "cooperation and collaboration" on relevant compliance matters.

- ***Is the compliance function reporting relationship sufficiently independent?*** The guidance requires independence in the compliance reporting relationship, which means legal and compliance should be separate functions *without* a reporting relationship.

- ***Do audit, compliance, legal, human resources and other related functions have access to appropriate and relevant compliance information and resources?*** Functions with compliance responsibilities should have appropriate access to both information and resources necessary to execute their duties that is defined in written charters, job descriptions or other documentation.

- ***Do managers understand their compliance related responsibilities?*** Management *at all levels*should be familiar with the requirements of the foundational program standards and what is expected of them personally.

Guidance Section 3: "Reporting to the Board"

The guidance states the oversight responsibility of the board is to set and enforce expectations for receiving specific types of compliance information. For example per the guidance, the ongoing expectations of the board should include *"regular reports regarding the organization's risk mitigation and compliance efforts… from a variety of key players."* The following questions can help set these expectations:

- ***Are the reports we receive providing appropriate metrics, context, and analysis of our E&C program to inform our oversight and decision-making?*** According to the guidance, this information should include; *"internal and external investigations, serious issues raised in… audits, hotline call activity… allegations of material fraud or senior management misconduct, and all management exceptions to the … code of conduct and/or expense payment policy."* In addition, boards should expect to see and review results of risk assessments; E&C program assessments; training, policy and audit/monitoring activities; implementation and status of appropriate work plans, and any other information that will assist them with their responsibilities.

- ***How do we know that management is fulfilling their E&C responsibilities?*** Reports should be provided on management actions to address, at a minimum, *"regulatory changes and enforcement events relevant to the organization's business."* Ideally, measures of other management actions are included, such as: survey results of management as role models, performance in handling E&C issues, departmental completion of training requirements, and documentation of formal communications delivered to staff.

- ***Do we provide regularly-scheduled and confidential access to compliance personnel?*** Holding "executive sessions with leadership from" relevant "functions to encourage more open communication" is an important practice. Such sessions are often held before or after every board meeting. In addition, as a best practice board members should reach out to compliance and audit personnel between meetings and often provide direct contact information in case key personnel need to speak with them directly.

Note that provision of data alone is not enough for the board to draw conclusions regarding program effectiveness. The board should expect trending and analysis by the compliance officer that is based on benchmarking and the CCO's experiences, observations and best judgment.

Guidance Section 4: "Identifying and Auditing Potential Risk Areas"

The guidance makes clear that the board is responsible for ensuring that risks are identified and appropriately managed. While it is the job of management to do the work of risk management, the board must conduct proper oversight by asking questions of the CCO and/or other risk-responsible management about the adequacy and effectiveness of the organization's risk management efforts, such as:

- ***Do we conduct a formal and regular process to identify ethics, compliance and reputational risks?*** A solid risk assessment process should inform the design, resourcing, and implementation of all ethics and compliance activities.
- ***How are we managing our highest industry risks?*** Healthcare boards will be especially interested in the organization's management of its major industry risks—*"referral relationships and arrangements, billing problems… privacy breaches and quality-relate events."* These are areas of intense government scrutiny and enforcement actions.
- ***What "industry trends" inform our latest/upcoming risk assessment?*** Emerging risks and new management methods should be considered in every risk assessment. These can vary by industry. Also, compliance failures in peer organizations should be considered in formulating your organization's risk list.
- ***What trends in issue types/business units/company locations are you seeing?*** This is a good question to ask between risk assessments to make sure any emergence or changes in localized risk is promptly identified and addressed.
- ***Are we "monitoring and auditing to detect criminal conduct"?*** The answer should be a resounding "yes"—through management, a host of internal reporting resources including a confidential reporting mechanism and risk-specific monitoring and auditing activities. Most organizations go further to require detection of misconduct related to violations of the code of conduct, organizational policies and applicable regulatory standards.
- ***Does "management consistently review and audit risk areas" and "implement and monitor corrective action plans"?*** Risk management is an ongoing operational responsibility that includes monitoring and auditing by functional management. The findings of these reviews combined with those of internal audit should be organized into action plans that include corrective measures and timelines. The status of these actions plans is periodically reported to the board.
- ***What information do you receive to give you comfort that ethics and compliance risks are covered?*** Enterprise risk management functions typically assess financial

and operational risks. Sometimes they will include regulatory risks in their assessments. True E&C risks include compliance with laws and regulations but go further to encompass ethics, third party relationships, and reputational risk areas. If these are not covered through ERM processes, the E&C function should conduct its own risk assessment to determine if all E&C risks are properly addressed.

- ***Are there any risks that aren't being addressed as they should be?*** Because the answer to this question may implicate specific managers, it may be best to discuss in executive session with the CCO to increase openness about potentially sensitive matters.

- ***Is there anything else we should know? What keeps you [the compliance officer] up at night?*** This is also a good question for executive session although the hope is that the compliance officer is appropriately supported by management that any concerns can be raised with management present.

Guidance Section 5: "Encouraging Accountability and Compliance"

The Sentencing Guidelines say the program should be *"promoted and enforced consistently throughout the organization through appropriate incentives to perform in accordance with the compliance and ethics program."* The OIG guidance suggests several such incentives that should be overseen by the board:

- ***How is employee performance tied to "promoting and adhering" to ethics and compliance standards?*** The board should assess the organizational processes to hold employees at all levels accountable for compliance, such as performance appraisals, and the outcomes of these processes for the "individual, department, and facility", plus how the results are linked to financial rewards. This may include "claw-back/recoupment provisions if compliance metrics are not met" to "mirror government trends."

- ***How are issues of self-disclosure handled?*** Healthcare boards are incentivized *"to build compliance programs that encourage self-identification"* of *"failures to the government"* within a specific time period (e.g. the 60-day rule). Therefore, the management policies and processes related to self-disclosure should be thoroughly understood and approved by the board.

- ***How does management respond to violations of policy or law?*** This goes beyond issues reported to the hotline to address how rank and file managers handle misconduct of which they are aware. This is an area where managers often lack the skills or knowledge to do the right thing and an area that suffers for lack of training.

- ***How consistent are we with discipline? Are top performers and high level people held accountable to the code of conduct in the same way as other employees?*** Boards should inquire about these important measures of accountability and ask for data to back up the answers.

Additional Area of Focus for Boards: Culture

While it is not part of the OIG guidance, experience has shown time and again that the tone at the top sets the tone for the culture, and the state of the culture is the best evidence of compliance program effectiveness. The 2004 amendments to the FSG recognize the importance of a culture that promotes compliance and ethics. Boards can gain insight into the tone of their organization's culture by asking the compliance officer these questions:

- ***Do we have a culture of open communication? Is candor rewarded or punished?*** All organizations dealing in a complex business environment will face problems and challenges. The most successful organizations consider diverse viewpoints carefully and encourage respectful discussion of risks in decision making. Employees need to know and be confident that they can raise issues or concerns and not believe that "the first whale to the surface gets the harpoon." The only way to know how employees feel about this is to ask them directly, either through focus groups or surveys.
- ***Do employees feel they can raise issues without fear of retaliation?*** Virtually all codes of conduct and company policies feature an anti-retaliation policy, but what is the level of fear in the workforce, despite the policy? This question is best answered through employee data gathering tools such as surveys, focus groups, exit interviews and investigation notes. Boards should ask for specific data on reports of retaliation and monitor outcomes and any actions taken.
- ***To what extent do we (the board) and management fulfill our responsibilities to build and sustain a commitment to ethics and compliance? How can we improve?*** We know that employees look to their leaders as role models. That is the power of tone at the top. That said, board members and management should have their own objective scorecards for their behavior inside and outside the organization and for fulfilling their E&C responsibilities, such as:

  - Avoiding behavior that contradicts the code of conduct (e.g. conflicts of interest, favoritism, unintended influence, insider trading, misuse of confidential information, gifts and gratuities, and accountability).
  - Communicating the importance of the E&C program verbally and by inclusion of the function in appropriate discussions.
  - Fulfilling E&C requirements promptly and in the right spirit, such as training, certifications, etc.
  - Becoming knowledgeable about the E&C program elements and foundations and their related role.
  - Actively engaging in oversight and discussion of E&C matters and metrics. (e.g. emerging risks, consistency of discipline, culture surveys, etc.)
  - Asking questions to determine adequacy and effectiveness of the E&C program.
  - Cooperating with investigations.

- Collaborating with E&C to understand regulatory changes.

- ***Are ethics, compliance, or even legal requirements—or the people responsible for them in our organization—marginalized?*** When E&C staff gets on the elevator, does everyone stop talking? Is E&C included in strategic planning discussions? Is the E&C function seen as a real partner to the business? The answers to these questions indicate whether E&C is truly embedded in the culture and recognized as a key piece of the organization.

- ***Do performance goals and incentives put unreasonable pressure on employees to act contrary to our ethics and compliance standards?*** One of the most important and impactful actions that a board can take in its oversight responsibilities is to consider this when reviewing and approving the organization's financial and growth targets. Boards are often the primary drivers of aggressive growth plans to support shareholders. And while stretch goals and targets are necessary and often healthy, boards should be mindful of the pressure they themselves may be putting on the organization and evaluate whether they are inadvertently leading employees to engage in risky behavior in order to meet targets. Stretch goals tied to employee financials that are practically unattainable without bending or stepping over the rules and values of the organization create a perverse incentive.

Conclusion

The OIG guidance may be only the first in a series for different industries and/or countries—or it may start a trend towards the creation of one "uber" set of guidance that is industry neutral and globally applicable. Furthermore, we may also start seeing a movement to holding compliance programs—and boards—to more standardized and comprehensive standards in future government investigations.

Regardless of what direction this trend might take us, all ethics and compliance officers and boards can and should use this latest OIG guidance to direct appropriate action now.

Accessed: April 17, 2018: https://www.navexglobal.com/blog/real-guidance-finally-compliance-oversight-role-boards