The New Board Role In Compliance Oversight

by Richard Sibery and Paco Garcia

With companies today facing huge potential losses for everything from foreign bribery, to cyber crime, to risk failures, to financial fraud, where is your board when it comes to monitoring compliance? Before your company can prevent such risk and regulatory disasters, your board needs the knowledge and motivation to assure that an effective compliance control system is in place.

Should a board of directors change its approach to regulatory compliance? Every board should consider the question, but for many the answer is yes. In 2009, the Securities and Exchange Commission approved certain amendments to enhance proxy disclosures, including a new requirement for disclosing the board's role in the company's risk management process. A little over six years and several disclosures later, the focus by boards on risk management is continuing to increase, and the expectations of investors and government regulators continue to rise.

A company's management is responsible for its day-to-day risk management operations. However, the board is ultimately responsible for the company's risk management program. In the 2016 business climate, what should a board expect from its management team and how can it fulfill its own compliance and risk management obligations? There is little doubt that compliance in general is a high priority for boards, and there are many ways to consider change.

A common two-step approach is to first, gain an in-depth understanding of the current state of compliance at the company, and then assess how it fits future needs. The analysis of the current state includes understanding the current compliance program at the company as well as more generally (competitors or industry norms). The analysis will typically include thinking through critical questions that challenge the current risks, assumptions, and methods. The result will be potential ways to improve the effectiveness and efficiency of the compliance program.

Regulators today are using fines, deferred prosecution agreements—and even the threat of imprisonment—to enforce compliance.

Forming a solid baseline that will allow for thoughtful changes to a compliance program requires a strong understanding of the company's current regulatory environment, as well as its internal compliance structure. The objective of understanding the current regulatory environment is straight forward, but international risks are often not considered on par with domestic risks. Understanding the compliance environment internally is more nuanced, and requires both more circumspect thinking and challenging preconceived notions.

☐ ***Understanding the current environment.*** Regulators have taken their role as "watchdog" to protect customers, employees, investors, and the general public very seriously. They have used a wide variety of tools—including fines, deferred prosecution agreements, and even the threat of imprisonment—to enforce compliance. It is an uncommon day when various compliance problems are not in the day's leading stories.

The U.S. continues to be a leader in enforcement, particularly in global corruption matters, and the efforts of U.S. regulators are easy to see and consistently referenced in the media reports of investigations, settlements, and litigation.

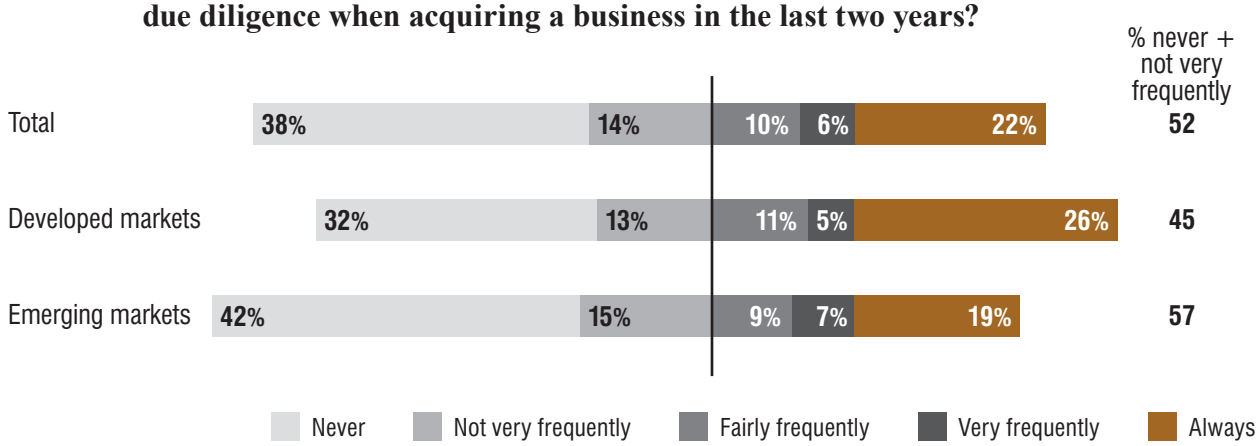
Last September, Deputy Attorney General Sally Yates issued a memorandum to U.S. prosecutors that focused on strengthening the U.S. Department

Richard Sibery *is America's leader for Fraud and Investigations and* **Paco Garcia** *a senior manager with audit and consulting firm EY. [www.ey.com]*

Un-Due Diligence

Why Companies Are Still Surprised By Corruption

Question: **How frequently has your company conducted forensic or anti-corruption due diligence when acquiring a business in the last two years?**



Source: EY 13th Global Fraud Survey, June 2014.

of Justice's pursuit of individual accountability for corporate wrongdoing. While any impact of the "Yates Memo" is not yet determined, companies will be required to provide relevant facts about responsible individuals in order to qualify for any cooperation credit with the DOJ. Also, prosecutors will not be allowed to resolve a matter with a corporation without a plan to resolve the cases related to responsible individuals. The guidance in the Yates memo applies to matters pending as of its release date, which includes approximately 80 ongoing and unresolved FCPA cases as of December 2015.

U.S. regulators also continue to offer substantial incentives to individuals to blow the whistle on corporate wrongdoing. The SEC's Dodd-Frank whistleblower program has awarded more than $54 million to 22 whistleblowers since 2011, including over $37 million in 2015.

The UK's Serious Fraud Office (SFO) secured its first conviction at the end of 2014 against a corporation for the bribery of foreign officials, which included a fine of £2.2 million. In November 2015, the SFO entered into its first Deferred Prosecution Agreement with a company for failing to prevent bribery of foreign officials, which included a $33 million fine.

Other countries have taken notice of the enforcement actions and ramped up their own efforts. Germany's BaFin continues to steadily increase its corporate and individual investigations, including 696 new investigations in 2014. China's Central Commission for Discipline Inspection has implicated over 100 "tigers" and "flies" (powerful leaders and lowly bureaucrats) for bribery and abuses of power since 2012. Brazil enacted the Clean Company Act in 2014 to hold companies responsible for corrupt acts and is very active, including arresting over 100 people over a two-year period.

A company's industry environment is also relevant. While no board will make choices based solely on what competitors are doing, understanding of their peer's approach to compliance must be considered. Being an outlier in this analysis is typically unwise and inefficient. Further, if competitors are under investigation in areas such as corruption or competition law, then boards would be wise to make sure that their company is also aware of their risk for being involved in similar schemes.

☐ ***Understanding the company environment.*** A relatively new phenomenon is referred to as "compli-

ance fatigue." This refers to a continuous struggle and financial drain stemming from efforts to identify, implement, monitor, investigate and remediate an increasing number of fraud and compliance risks. This is compounded by activities related to expanding into new markets, acquiring new companies, and establishing new business partners and agents.

Ten percent of C-suite respondents have been asked to pay a bribe (including one in five CEOs), yet only 38 percent of these executives have attended anti-corruption training.

In addition to these challenges, new risks such as cyber-security are regularly popping up. For example, a company may make significant efforts to improve compliance with the Foreign Corrupt Practices Act (FCPA), only to be faced at the end with increased export control risks or cyber risks that may require similar efforts. In short, the compliance demands are constant, changing, emerging and demanding of management attention.

Most boards do not have a false sense of security when approaching compliance risks, but significant work remains to be done. For example, the 2014 EY Global Fraud Survey found that ten percent of C-suite respondents have been asked to pay a bribe (including one in five CEOs), and yet only 38 percent of C-suite executives have attended anti-corruption training.

When looking at the broader organization, less than 50 percent of respondents have attended anti-corruption training and about one-fifth of respondents indicated that their company does not have an anti-corruption policy or do not know if there is a policy. Senior executives are as likely to justify misstating financial performance as other colleagues, and CEOs specifically are more likely to justify such activities.

The board's sources for compliance oversight most often include risk assessments, internal audit, and compliance reports. Traditional risk assessments focus on a company's inherent risks and their mitigating controls to identify residual risks to address. Executives present to the board their understanding of the company's risks and their plan to address them.

Similarly, boards rely on the internal audit function for a sanity check on whether the company's internal controls are in place and operating effectively. Compliance executives also provide key performance statistics, report on issues identified to date, and provide updates on implementation of compliance activities.

Is the company optimizing its financial and non-financial compliance resources? How do I as a director really know that the program is operating effectively?

In our experience talking to directors, we find that many say they have a good general understanding of the company's compliance environment. Still, what has been done to understand or identify what is not known or has not been adequately considered? What questions are directors not asking? Is our focus on risks misaligned? Are compliance objectives inclusive enough? Is the company optimizing its financial and non-financial resources? Why so few whistleblower complaints? How do I as a director really know that the program is operating effectively?

Specific questions we have recently heard from directors include:

- Is there a disproportionate amount of time and effort focused on travel and expense reimbursement?
- Are cyber or privacy risks properly included in our compliance objective?
- Does the cost/benefit of employing a large compliance or investigative team make sense? Would outsourcing or co-sourcing around the globe be more beneficial?
- Why are there no whistleblower complaints concerning the FCPA?
- Do we have the right plan to monitor our largest risks?
- Does the company have enough resources to prevent and detect the key risks on a timely basis?

The objective is to push beyond previous thinking and approach the question of company compliance environment from new perspectives.

Directors provide guidance on the company's ac-

tivities to protect shareholder interests. While this objective includes strategic and longer term focus, pressing current responsibilities and decisions may demand significant time. For example, assessing the operational effectiveness of compliance procedures sometimes takes priority over understanding and addressing the design effectiveness.

A board may commonly receive positive reports on the thoroughness and effectiveness of controls—but frauds usually involve circumventing these controls. Finding fraud requires that the holes in the controls must also be found. The board is uniquely empowered to ask management to detail their process for appropriately monitoring and addressing day-to-day risks.

Simple questions may provoke compelling results. Why are there not more internal audit or compliance findings? What was not considered? Is the internal audit department staffed with specialists to perform anti-corruption audits versus more traditional internal audit testing? How is the materiality different between traditional audit functions and compliance assessment or fraud investigation? Only by understanding the answers to these questions, and thus the business and its processes, can compliance activities be prioritized.

☐ ***Board compliance objectives.*** Reassessing and defining a company's compliance objectives can be a good first step for a board rethinking its role in compliance. Not only thinking about the risks themselves, but also what the directors want to achieve. Our experiences show that as the board's engagement in compliance increases, compliance across the company increases. The board is responsible for setting the tone at the top by developing a focused, challenging compliance plan, and actively holding senior management accountable for the results.

Managing compliance often comes down to money and resources, and it is not a revenue generating activity. However, it can be an income-saving process that generates value for the company. A well-functioning compliance program works hand in hand with the business to build growth that is controlled and compliant—thereby avoiding substantial penalties and fines.

The board can help focus compliance activities into the highest risk areas. Cyber fraud has been a recent hot topic given some of the high-profile attacks. Boards are now engaged with management in addressing this risk. Was cyber fraud a consideration one year ago? Three years ago? Did management consider this a risk before it became headline news?

Similarly, what other emerging risks should the board consider? The expansion to emerging markets opens a company to significant and possibly less known risks. Even new or refreshed products can present new risks for the company. Many directors understand these risks, but feel ill-equipped to handle them.

☐ ***Compliance structure.*** Boards trust their management teams. They are confident in them, and usually rightly so. That said, the structure of the compliance team can often be muddled with disagreements over headcount, budget, and perceived power or influence in an organization. Oftentimes, the result is ineffectiveness, inefficiency, and higher risk.

The board's fiduciary duty to shareholders compels the board to be an active participant in driving compliance activities across the company.

For example, consider the following areas:

- Who is responsible for compliance and if multiple people have responsibility, how do they interact?
- Is there a direct line from those with compliance program responsibility to the board? Or is it through the general counsel or other executive?
- How much time should the board spend focused on compliance? How often?
- How does the company deal with managing international compliance?
- If there is regular reporting to the board, does it contain relevant information? Is it in the right form and level of detail? How much is data driven vs. anecdotal? When management reports on compliance, how do you answer the question "How do you know that the compliance program is operating effectively?"

The structure of the compliance system, its makeup, budget, and reporting lines are all areas where more board involvement would be beneficial. The board should build relationships throughout the company, including a collaborative environment across compliance teams.

☐ ***Compliance operations.*** How does the board define its expectations of the company's management team for carrying out the day-to-day compliance plan? The board's fiduciary duty to shareholders compels the board to be an active participant in driving compliance activities across the company.

The board should appropriately challenge management's understanding and decisions. For example, the board should "pull" information from management regarding new risks like cybercrimes, or traditional risks like revenue recognition fraud, and not passively wait for information to be provided.

Consider training. All companies have some type of training, but it is often ineffective and does not reach the right audience. Participation should be monitored and accountability should be enforced. The training should also be tailored to levels of seniority, job functions, and language through a mix of live and online training courses.

The use of data analytics is another common area of debate. How can the board use forensic data analytics to improve compliance? While forensic data analytics is an area of great interest, the cost and ultimate use should be considered. Understanding the underlying source data and assumptions that go into those results is a critical step in challenging the information presented.

Finally, potential "red flags" identified by analytics must be considered and looked into. The board's role in resolving problems is often very significant and clearly defined escalation procedures, whether to respond to a whistleblower allegation or a cybercrime, should be documented.

☐ ***Charting the path forward.*** The board's focus on the compliance program should be in proportion to the company's risks. Taking that one step further, the compliance program budget should also be in proportion to the company's risks. We have seen many companies with understaffed and underqualified compliance operations attempting to address highly complex risks.

In one instance, an internal auditor who focused on tax compliance efforts was also charged with completing a company's anti-corruption internal audit. In another instance, two auditors crammed two weeks of fieldwork into four days due to "budget constraints." Better upfront planning of compliance objectives and the structure to achieve those ends can prevent this most of the time.

The board's evolving responsibility for risk assessment and compliance is straightforward, and these activities support the company in driving ethical growth. Changing employee's perspectives on compliance activities is not an overnight process. A board's support helping management respond to constantly changing and complex risks is an advantage. Boards need information that is decision-ready in order to address known and emerging risks. Generating the information, however, requires a strong working relationship between the board and executives.

A typical complaint from board members is that they are inundated with information because compliance executives are not clear on what the board wants to hear. The board must be clear on what information it wants, and ensure that responsible executives understand the objectives and information required. ■