Reprinted from THE CORPORATE BOARD

Overseeing Legal Risk: First Make It Visible

By David A. Collins

Oversight of company risk jumped to the top the board agenda with the economic meltdown of 2008, and now the new SEC governance rules effectively mandate a board role in monitoring risks. Directors are learning that one of the biggest risk exposures—legal and compliance—is one of the hardest to pin down. However, a well-planned compliance program will give the board a good dashboard for both monitoring and reducing legal risks.

The SEC's new proxy disclosure rules require that publicly traded companies describe the board's role in "risk oversight." Because the portfolio of a company's risks includes not just financial and operating risks, but also the risk of violating legal requirements, this rule has implications for the way directors oversee legal and regulatory compliance. Risk oversight is a forward looking function, so the SEC rule will prod boards to focus on their companies' efforts to prevent legal and regulatory violations.

It is virtually impossible for a board effectively to oversee the risk of legal violations without an effective compliance program. It makes risk visible at the board level.

Companies cannot tell a convincing story about risk oversight if directors limit their oversight of legal risks to the reactive function of reviewing compliance "spills"—violations that boards have watched over since at least the *Caremark* decision. The strongest proxy statement, and the one companies will want to make, is that the board oversees the risk of legal violations through an organized compliance program designed both to *prevent* and *detect* violations. As I argue below, it is virtually impossible for a board effectively to oversee the risk of legal violations *without* an effective compliance program. Legal risks become visible at the board level only with the help of such a program.

There were compelling reasons even before this SEC action for boards to view their compliance oversight duty expansively, covering not just spills but also the company's preventive efforts. Oversight limited to the remedial aspects of compliance—identifying, correcting, and drawing lessons from compliance spills—can have the effect of closing the barn door only after the horses have escaped.

True, this is better than not closing the barn at all. Yet it is cold comfort to shareholders when a company implements strong corrective measure in response to a violation that has already damaged the company's reputation and balance sheet. As a legal matter, enforcement agencies view a board's oversight of compliance as incomplete unless it includes attention to preventive efforts.

To illustrate that point, consider the several regulatory compliance protocols that require both preventive and detective efforts. The most comprehensive of these (and the gold standard for compliance programs) are the United States Sentencing Commission's "Organizational Sentencing Guidelines." This set of guidance defines an "effective" compliance program as one that "exercises due diligence to prevent and detect" violations. It requires, among other provisions, the regular review of the program "not less than annually" (for large companies) by the organization's "governing body."

With compliance defined as including preventive efforts, board oversight will look incomplete if it is limited to the company's compliance spills. By requiring discussion of the board's role in risk oversight, the new SEC rule adds to the pressure boards already face to watch over compliance comprehensively.

What does comprehensive legal compliance oversight mean for a board? What specific steps should a board take to meet these higher expectations? Following are four steps a board should take to oversee legal compliance comprehensively. These measures will strengthen compliance by improving the odds that the company effectively prevents and detects legal violations. They demonstrate diligent oversight.

Stressed executives may trust that good compliance flows inevitably from the personal integrity of employees. Compliance can then fall victim to neglect.

☐ *Step one: Accept ownership at the board level.* Managers understand that meeting legal obligations is not

David A. Collins *is an attorney with Dykema Gossett PLLC in Detroit, Michigan. [www.dykema.com]*

optional, but they do not see it as a core business function. Particularly when times are hard, compliance issues may drift to the periphery of their radar screens. Stressed executives may trust that good compliance will flow inevitably from the personal integrity of the company's people. They feel confident that the lawyers and specialists know what they are doing, and shift their focus to other business imperatives. Compliance can then fall victim to neglect.

Directors can prevent that by assuring that compliance does not get short shrift. As long as compliance stays on the directors' agenda, managers will keep it on theirs. The natural home for this oversight function is usually the audit committee, which for most listed companies is already charged with helping the full board oversee "compliance with legal and regulatory requirements." Moreover, corporate compliance programs serve as a form of internal control, oversight of which is familiar terrain for audit committees.

☐ *Step two: Secure a clear line of sight on compliance.*

Tough questions lie at the heart of effective oversight, so ask them when monitoring compliance. A particularly useful question about compliance is, "How do you know this company does a good job meeting its legal obligations?" Or, in the context of the SEC's proxy disclosure rule, "How do you know what the company's biggest legal risks are? And how do you know that those risks are being properly managed?"

Those simple questions hit squarely at a subject central to the board's duties. They are virtually unanswerable unless the company has implemented a comprehensive compliance program.

The object of oversight must be discernible to the overseer; a board cannot oversee what is invisible to it. Yet legal risks in a complex organization lurk in all sorts of places that can be hard for the board to see. The structures companies create to cope with their legal duties are elaborate and do not lend themselves to easy transparency.

Companies face dauntingly vast portfolios of legal and regulatory requirements. These include: workplace discrimination, wages and benefits, privacy, anti-bribery, antitrust, tax, export compliance, insider trading, consumer protection, anti-money laundering, real estate, workplace safety, financial reporting, real estate, lobbying, environmental protection, and on and on.

Some (perhaps most) of the risk-specific compliance activities do their jobs well enough to meet legal standards, but others probably fall short.

Each category confronts the company with many legal duties, which is to say many risks of violating the law. To cope, the company implements multiple compliance activities, each focused specifically on a category of legal duty.

However, there are real-world obstacles to board oversight of this realm. Some of the risk-specific compliance activities are managed centrally, others regionally or by business units. Still others are out-sourced to third-party contractors. Some are directed by the legal department, others by other staffs (such as HR or the controller), and others by business functions. These scattered compliance activities typically do not interact with one another, and they report through different chains of command, converging only at the very top of the company. Some (perhaps most) of the risk-specific compliance activities do their jobs well enough to meet legal standards, but others probably fall short.

The risk of a legal violation exists to a greater or lesser degree in each of them. The trick, then, is to create for the board a line of sight into this unwieldy realm. Directors need information about what goes on in all these disconnected functions.

What kind of information do directors need? Since compliance means preventing and detecting violations, the board should expect data about both these categories of the compliance function. On *prevention,* for example, the board might want to know whether management (presumably the chief legal officer) has identified all the legal requirements that apply to the business. This is a first-order legal risk assessment.

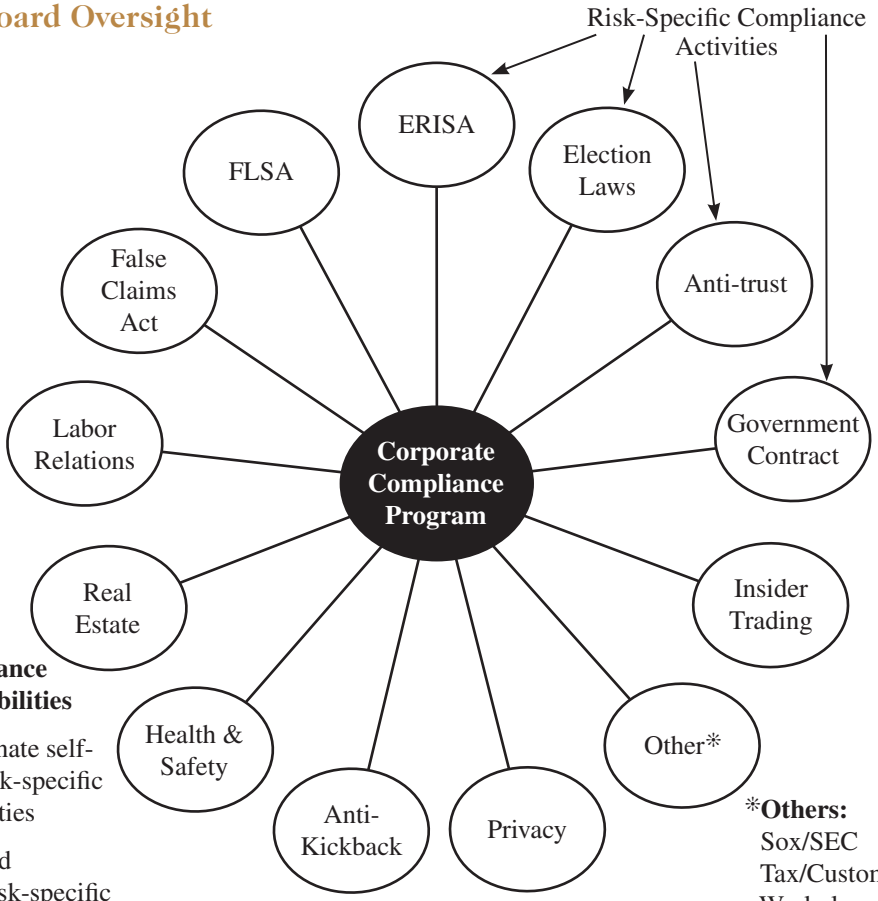
Then, are there policies and procedures that translate the legal requirements into "dos and don'ts" for the company's personnel? Is accountability for compliance clearly assigned? Do employees receive training about the various legal requirements relevant to their jobs? Are the resources necessary for compliance provided? Are the risks associated with each category of legal requirement periodically reassessed?

On *detection,* we might look for assurance that employees are encouraged to report potential violations, that they are protected from retaliation when they do, and that reported violations are acted upon. Auditors should monitor essential compliance processes. The time it takes to close out internal investigations should be tracked. Assurance should be provided that discipline is meted out consistently.

Without such information, the board lacks a sufficient foundation for performing its oversight responsibilities. For that matter, so does management. That is where a *corporate compliance program* comes in. It opens a window to the company's scattered compliance activities. It does so by gathering information sufficient to evaluate the effectiveness of each, and then reporting about that assessment directly to the board. This makes legal risk visible by shining light on the quality of the company's efforts.

Legal Risk Made Visible

A Model For Board Oversight



Corporate Compliance Program Responsibilities

- ☐ Assess (or coordinate self-assessment of) risk-specific compliance activities
- ☐ Catalyze improved effectiveness in risk-specific compliance activities
- ☐ Provide information about compliance effectiveness to senior leadership → **Executive Compliance Committee** Senior executives oversee the program and ensure its effectiveness
- ☐ Provide information about compliance effectiveness to the board of directors → **Audit Committee** At NYSE-listed companies, the audit committee assists the board in overseeing "compliance with legal and regulatory requirements."
- ☐ Lead or coordinate with investigative function
- ☐ Code of conduct
- ☐ Corporate policy

***Others:**
Sox/SEC
Tax/Customs
Workplace discrimination
Environmental
Advertising
Etc.

☐ *Step three: Keep your eye on the real prize.*

The most compelling reasons to install a good compliance program are to strengthen the company's performance of its legal duties and to generate data about legal risk to support oversight by the board. There are also less compelling reasons. Regrettably, these lesser reasons dominate lawyerly discussion. They are basically defeatist, and they distract from the fundamental point that an effective compliance program can pay big dividends operationally. A focus on them may lead a company to decide instead that a compliance program is not worth the trouble of implementing it.

The secondary reasons assume that the payoff for having a compliance program comes after the company commits a major violation. This is the very outcome a compliance

program should prevent. So, for example, we hear compliance programs defended as a way for the company to earn a sentence downgrade after it is criminally convicted in federal court. Or we are told that a prosecutor investigating the company's alleged misconduct will temper her charging decision if the company shows it had a good compliance program.

A good compliance program can indeed deliver post-calamity enforcement benefits, but only infrequently and unpredictably.

A good compliance program can indeed deliver these post-calamity benefits, but only infrequently and unpredictably. The first, a sentence downgrade, is written into the federal sentencing guidelines. Federal judges are indeed encouraged to lighten the sentence for a convicted company if it shows it had a compliance program meeting federal standards. In theory this is a big inducement, potentially amounting to many millions of dollars in reduced criminal fines.

In the real world, however, sentence downgrades almost never happen. So seldom have convicted companies won a reduced sentence on the strength of their compliance programs that one scholar describes the purported incentive as "a carrot that virtually no one ever really gets to eat." This mostly hypothetical benefit does not by itself justify the implementation of a corporate compliance program.

The second commonly cited payoff, prosecutorial forbearance, is more likely to actually happen—although exactly how much more likely is hard to know, since data are unavailable. What we do know is that a good compliance program is one factor that federal prosecutors are instructed to take into account when deciding how severely to charge a corporate defendant.

However, there are other factors in the Department of Justice's instructions, so this benefit is not entirely predictable. More importantly, like sentence downgrades, it presupposes failure. It justifies a compliance program for the cushion it (maybe) provides after a violation upends the company.

The real value of a compliance program is to make the company better at performing its legal duties, and to help the board provide oversight.

Imagine defending other fields of endeavor in this defeatist way. Question: "General Eisenhower, why did you prepare so painstakingly for the Normandy invasion?" Answer: "So that I wouldn't be court-martialed after Hitler beat us." Serious people mount their efforts not for forgiveness after they fail, but to succeed.

The real value of a compliance program (the prize to keep eyeing) is that it makes the company better at performing its legal duties and helps the board perform its oversight responsibilities. The idea is to stay away from prosecutors and sentencing judges, and a compliance program can help do just that.

☐ *Step four: Adopt the U.S. Organizational Sentencing Guidelines as the model for the design of your compliance program.*

As we have seen, several models for compliance programs exist in current law. All require preventive steps (policies/procedure, employee training, risk assessment) as well as steps for detecting and correcting violations. The most comprehensive and widely respected of these is Section 8B2.1 of the U.S. Sentencing Guidelines. Its guidance is applicable to all companies in all industries, and it encompasses the broadest array of legal requirements. It requires active involvement in the program by both senior management and the board, and is the only protocol specifically identified by the Department of Justice's charging manual as a model for designing corporate compliance programs. In short, it is the gold standard.

For purposes of supporting the board's oversight, Section 8B2.1 offers the advantage of requiring that the board receive periodic reports directly from the person with day-to-day operating responsibility for the company's compliance program. That direct access to the person actually running compliance affords the board a clear view of the workings and effectiveness of the company's compliance activities, and face-to-face contact with the person managing the risk of legal violation.

Boards should install the best window onto a company's legal risks, and on the company's efforts to manage those risks. They are well advised to make sure that the company's approach to compliance conforms to this protocol.

Directors must pay attention not only to compliance spills after they happen, but also to the company's preventive efforts. Attention to the preventive element of compliance has been made even more important by the SEC's requirement that proxy statements include a discussion of the board's role in "risk oversight," including the risk of violating legal requirements. ■