The Metropolitan
Corporate Counsel®

www.metrocorpcounsel.com

Volume 14, No. 10 October 2006

Compliance Readiness – Legal Service Providers

A General Counsel And His Experts Tackle Risk Assessments

By John M. Spinnato, Debra Sabatini Hennelly and Steven A. Lauer

The corporate ethics and compliance practice and the compliance profession arose after two noteworty events. First, scandals involving activity in the electrical industry in the 1950s and '60s that violated the antitrust laws led to prison terms for some corporate executives. Later, the scandals that centered on the bribery of foreign government officials in the 1970s led to the enactment of the Foreign Corrupt Practices Act. The United States Sentencing Commission ("Commission") issued Sentencing Guidelines for Organizational Defendants (the "Guidelines") in 1991, which articulated the concept of a corporate compliance program as a means of qualifying for a reduced sentence in the (unlikely) event that a business suffers conviction for a federal crime. The following year, twelve corporate ethics officers formed the Ethics Officer Association (now called the Ethics & Compliance Officer Association) to "[b]e … the leading provider of ethics, compliance, and corporate governance resources to ethics and compliance professionals worldwide." (See www.theecoa.org/AboutECOA.asp#mv v.) ECOA's membership now numbers over 1,000 and other associations have grown up over the last few years, all evidence of the growing acceptance and maturation of the ethics and compliance practice.

The profession has matured to a greater degree than has the practice itself. To some extent, there is less consensus on what constitutes "best," "leading edge" or "best existing" practices in corporate compliance than on the attributes of a chief compliance officer position or that of an ethics officer. ECOA has published a list of those attributes that reflects recent changes to the Guidelines. See www.theecoa.org/ Whatis.asp. (Whether those two roles – ethics officer and compliance officer – ought to constitute distinct positions or represent simultaneous roles of one corporate officer constitutes an issue beyond the scope of this article.) We have achieved, however, broad agreement that an effective compliance program is a comprehensive system of policies and procedures designed to prevent – or, if they occur, to detect and correct – violations of law or company policy.

The changes to the Guidelines adopted by the Commission that became effective as of November 1, 2004, introduced a new element to the constellation of compliance practices. Among other things, the Commission enunciated a requirement that companies develop their compliance and ethics programs after conducting risk assessments and that they use such tools periodically to assess the effectiveness of those programs. A risk assessment thus now occupies a central and strategic position in the compliance universe.

Despite introducing the risk assessment into the calculus of compliance program design and the management of such a program, the Commission offered little guidance as to how an organization might conduct one. It listed in its commentary to the Guidelines the following criteria that such assessments should take into account, but it did not advise companies how to do so:

1. The nature and seriousness of possible criminal conduct that might occur in the business;
2. The likelihood that criminal conduct might occur in the course of the business operation, and
3. The prior history of the organiza-

***John M. Spinnato** is vice president-general counsel, pharmaceutical operations, at sanofi-aventis in New Jersey. **Debra Sabatini Hennelly** is founder and president of Compliance & Ethics Solutions LLC, a consulting team bringing decades of in-house and outside experience to helping companies manage legal and reputational risk, building sustainable compliance programs and cultures of integrity. Information about the team is available at www.callces. com. **Steven A. Lauer**, who previously worked as in-house counsel, is director of Integrity Research, a division of Integrity Interactive Corporation of Waltham, MA, a provider of Web-based corporate ethics and compliance services to Global 2000 companies.*

Please email Steven A. Lauer at slauer@i2c.com with questions about this article.

tion in respect of past criminal conduct.

How might or should a company conduct a risk assessment as described by the Commission? Would a risk assessment for purposes of designing a compliance program differ from a risk assessment conducted to evaluate a program's ongoing effectiveness? If so, how would they differ? These issues are the focus of ongoing discussion in the profession.

An assessment, whether conducted prior to organizing a compliance regimen or as part of the periodic evaluation and improvement of an existing one, should serve the same ultimate purpose: determining whether the business operations violate, or present a substantial risk of violating, external or internal requirements or standards. (Though an organization needs to worry only about external standards that define criminality for purposes of the Guidelines, an understanding of other behavioral expectations, such as civil statutes and other standards, may be important enough to qualify for consideration in this regard.) To the extent that the assessment uncovers such violations or risk of violations, it should proceed to specify the type of violation or quantify the potential impact and likelihood of risk so represented. Having established these parameters, the organization may more effectively correct violations and mitigate potential risks.

You should plan your risk assessment with the following goals in mind:

• To enhance the organization's ethics and compliance program to meet expectations and "best practices;"

• To coordinate methodology and scheduling, as appropriate, with the organization's existing enterprise risk assessment procedures;

• To identify and prioritize significant legal and ethical (or reputational) risks;

• To identify means by which to mitigate the most significant risks so identified by means of new or existing compliance program elements, and

• To establish a basis for continual improvement to the organization's risk management, synchronized with the organization's budgetary cycle.

Those goals will provide touchstones by which to measure your progress in conducting the risk assessment and, later, designing and implementing or improving an ethics and compliance program that will serve the organization's interests well. Those goals also lead you to a means by which that program will support the company's business goals and assist to establish support for the program (a "business case") that transcends its "compliance" nature.

Conducting A Risk Assessment

The Guidelines provide that a corporate compliance and ethics program "shall be reasonably designed, implemented, and enforced so that the program is generally effective in preventing and detecting criminal conduct." The group that the Commission had charged with reviewing the first ten years of the Guidelines' operation had expressed the view that "risk assessments need to be made at all stages of the development, testing, and implementation of a compliance program to ensure that compliance efforts are properly focused and effective." Report of the Ad Hoc Advisory Group on the Organizational Sentencing Guidelines (October 7, 2003), p. 87. The Guidelines as adopted by the Commission, however, "are clear about the role of risk assessment in compliance, [but] they are conspicuously thin on *how* one goes about doing a risk assessment." McGreal, "Legal Risk Assessment After the Amended Sentencing Guidelines: The Challenge for Small Organizations" *Corporate Counsel Review* (January 19, 2005), pp. 101, 115.

Before even beginning the formal risk assessment, one must gain a thorough understanding of the company's self assessment of its risk tolerance. This is the most daunting challenge and must start with an analysis of the firm's compliance and litigation history. Have there been numerous investigations, either by governmental agencies or internal auditors due to violations of law or policy? Is the business in an area that is highly regulated or under intense public scrutiny? Has the company been involved in litigation that could have been avoided by better internal controls? Is the organization under some sort of consent decree? Given that many compliance standards are not necessarily crystal clear, it is critical for the organization to evaluate how strictly it is willing or comfortable it is to operate within a "gray zone." The strictness of the application of compliance standards when so much is gray will depend on the responses to the questions raised above.

Having achieved an understanding of itself and its tolerance for risk, how does a company conduct a risk assessment with the goals listed above in mind? Begin with a clear action plan. Treat the effort to develop and implement a risk assessment as a project and apply project-management tools. You should begin with a "toolkit" – a methodology, task list, timeline – and a cast of players with clear ownership of various responsibilities before, during and in response to the risk assessment.

The toolkit need not have a lot of "bells and whistles" to be effective in identifying current or potential violations or risks of violations. In fact, it might only include:

• a methodology for identifying the external and internal requirements that apply to the organization (including an understanding of the various jurisdictions in which the organization operates);

• a methodology for identifying whether and how the organization's activities could violate those requirements;

• a methodology for addressing the findings of actual or potential violations (prioritizing, developing and implementing mitigating activities) (a risk assessment conducted to meet the Guidelines' standards may not necessarily qualify as "attorney work product" or even come within the attorney/client privilege, so consider carefully the privilege issues attendant to such an exercise; this issue is beyond the scope of this article), and

• a system for documenting the assessment's activities and their owners, the assessment findings, and then for tracking the mitigating activities that result (tasks, owners, timelines, etc.).

Numerous firms offer software and other tools for risk assessment, but be a cautious consumer. Most such software has been developed to serve the "enterprise risk management" requirements in the financial accounting field, particularly after enactment of the Sarbanes-Oxley Act, and may not be helpful in –

or easily adapted to address – the non-financial, more intangible issues that arise in other regulatory areas or in the ethics arena. It may be more cost-effective to invest some time in reviewing the principles of the widely-regarded standard for enterprise risk management outlined in *Internal Control – Integrated Framework* developed by the Committee of Sponsoring Organizations of the Treadway Commission, as it contains much that can be extrapolated into the compliance and ethics risk assessment methodology. (See www.coso.org/.)

Outside experts, law firms and consultants can help in establishing risk assessment methodologies or managing this project, but the long-term sustainability of meeting the goals articulated above (as with the compliance program as a whole) relies on the assimilation of compliance and ethics risk mitigation into the day-to-day operations of the business. Accordingly, that might be achieved most effectively when the assessment is "home-grown," rather than having the look-and-feel of an outside audit. If required to choose between committing resources for acquiring sophisticated software or tools or freeing up internal personnel to contribute to the assessment, the latter may be the better choice.

Critical factors in assessing the organization's risk profile will be the participants and their roles. Regardless of the tools employed, an effective assessment will always require a broad understanding of the company's operations and a clear understanding of the regulatory schemes that apply across those operations and across the organization's locations. (For this purpose, you may need to involve several internal business people, counsel and subject matter experts.) The involvement of internal business people, subject matter experts and in-house counsel may yield some considerable tangible and intangible benefits, such as:

- gaining "buy-in" for the goals of the risk assessment and ownership among the business leaders for the related mitigation activities;
- educating business people about potential risks in their operations and activities;
- positioning in-house counsel and subject matter experts as the "go-to" resources for addressing the risks that are identified, and
- building traction for incorporating the mitigating behaviors and tasks into the day-to-day operations.

Having prepared your toolkit and identified your team, make sure that your methodology includes at least three basic steps. The first step entails an analysis of the business operations against applicable laws and requirements. A review of how the business operation meshes against the behavioral expectations of various external and internal audiences requires a detailed look at the activities of employees and agents of the business and how they interact with others, such as competitors, government officials, customers and suppliers.

You must understand whether and, if so, the extent to which the business operates in one or more regulated industries. While activities of all business entities must comply with certain government mandates, such as anti-discrimination requirements in the employment law arena and requirements for the proper disposal of hazardous substances, some industries are wholly or mostly regulated by the government. The development, manufacture, sale and marketing of pharmaceuticals, for example, must satisfy a host of regulations adopted by the federal Food and Drug Administration. Radio and television broadcasters must comply with those of the Federal Communications Commission.

In addition to the government's mandates, you should review other behavioral or operational standards that do or might apply to the business operations. A company whose stock is publicly traded on the New York Stock Exchange or through the channels of Nasdaq must satisfy the listing standards of the NYSE or Nasdaq, respectively. Industry standards, usually voluntary, may also be incorporated into market expectations or customer specifications such that their violation could affect the company's reputation. Many consumer products companies apply the product standards identified by the "UL" label or the "Energy Star" rating. Many global companies try to satisfy the United Nation's Declaration of Human Rights.

The company's own, expressed policies, procedures and external commitments can provide fodder for the company's critics and, for that reason, probably should also animate the analysis of possible risk. Those policies and procedures reflect a company's risk tolerance profile as they embody its own understanding and application of laws and regulations. The development of policies is the initial task that will most reflect the corporate commitment to compliance and its own understanding of the risks associated with its business. Benchmarking of industry standards in various industries almost always shows a wide variety of interpretations of the laws or regulations that give rise to the policy need. These differences reflect the varying cultures and histories of different organizations, though they may not reflect each organization's commitment to compliance or high ethical standards.

The Commission determined in 2004 that the Guidelines should cover actions that constitute criminal activity only, rather than "'violations of any law, whether criminal or noncriminal, (including a regulation), for which the organization is, or would be, liable...'" Such a broader scope had been recommended by the group to which the Commission delegated the task of reviewing the then-existing Guidelines and recommending any possible changes in light of then-extant experience. Those extra-legal standards of behavior often represent or influence the opinions and decisions of creditors, insurers, potential board members, current or future employees, jurors, investors and others whose judgments can impact the reputations or fortunes of businesses. Thus, they might merit attention in the assessment process.

With these considerations in mind, your risk assessment should examine current (and planned) operations against the external and internal standards you've identified in all of the jurisdictions in which you do, or expect to do, business. (A particularly problematic subject is that of a joint venture by two companies. Should the venture adopt the two companies' compliance and ethics policies or adopt its own, distinct ones? These questions are beyond the scope of this article, but worthy of consideration.) Document your approach and findings

so that you can maintain a record of your activities and also drive improvements in how the organization addresses its compliance obligations and ethical commitments.

The expression, "you can't boil the ocean," bears some consideration in the context of risk assessment. The Guidelines provide that a corporate compliance and ethics program "shall be ***reasonably*** designed, implemented, and enforced so that the program is ***generally effective*** in preventing and detecting criminal conduct." (Emphasis added.) It would be unreasonable to expect a risk assessment to address all potential risk areas across all operations in all jurisdictions during its first run-through. Only a rare organization could sustain such activities while still attending to its regular business.

For this reason, the second step should include prioritizing the identified risks so that the company can address the most significant risks first. To do otherwise might squander scarce resources by allowing for limited employee focus on minor risks (those with very low potential impacts or those only remotely likely to occur). Such "low-hanging fruit" might seem easy to address and tick off the list – or might be in the bailiwick of an enthusiastic subject matter expert who proactively addresses that risk area – but focusing resources and attention on these activities could distract the company from identifying and mitigating more significant risks. During each cycle through the risk assessment, the organization can measure its progress in mitigating those more significant risks and then move down the risk inventory toward the lower-priority risks in order of lessening priority.

The third step involves systematically developing mitigating activities or tasks to address the prioritized risks previously identified. Each task must have an owner and a commitment for a timeframe for its completion. The prioritization approach of the second step, if addressed in a timely manner by this third step, can deliver important early successes, which will not only reduce the company's risk profile cost-effectively, but also help secure "buy-in" from the business people who are asked to own parts of the exercise. This step should also include procedures for reporting violations internally and, as required, externally, instituting internal investigations as necessary, and then tracking progress of correcting violations or mitigating potential risks.

Finally, an effective compliance and ethics program includes a commitment to continual improvement. With regard to the risk assessment, this means committing to on-going tracking of the implementation of the mitigating activities and a periodic (annual?) renewal of the risk assessment process, being sure to include new or revised requirements (external or internal) as well as reflecting any changes in the organization's operations or footprint locally or globally. Risk assessment is arguably the most difficult task in the development of an effective compliance and ethics program, given that it is necessarily subjective and requires not only a thorough understanding of the laws and regulations that affect the industry in question, but an understanding of the corporate culture by the compliance officer as well as the company itself. If well done, though, a risk assessment can lead to reduced risk and even operational improvements.