ALM
LAW JOURNAL NEWSLETTERS

The Corporate Counselor®

Volume 22, Number 9 • February 2008

What Is a 'Risk Assessment' and How Do You Perform One?

By Christopher A. Myers and Gregory A. Baldwin

Government attention to corporate compliance, ethics and governance has vastly increased over the last few years. Massive corporate scandals such as Enron, MCI and others, combined with ongoing fraud and abuse enforcement in the health care and government contracts industries, have created a "perfect storm" of civil and criminal enforcement. The result has been an alphabet soup of acronyms, programs and initiatives suggesting, encouraging, cajoling and, in many cases requiring formal, written codes of ethics and business conduct. Extensive compliance programs, internal control systems, training, auditing and other activities have, in some instances, been imposed on already heavily regulated industries.

This article endeavors to make sense of these standards and provide some practical advice on to best protect your company by focusing on the one common thread found in virtually all of the new statutory, regulatory and enforcement guidance: "Risk Assessments."

Christopher A. Myers (chris.myers@hklaw.com) is a partner in Holland & Knight's McLean, VA, office. He is the co-chair of the firm's Global Compliance and Governance National Practice Team and a member of the firm's White Collar Defense Team. **Gregory A. Baldwin** (gregory.baldwin@hklaw.com) is a partner in Holland and Knight's Miami office and practices in the areas of complex commercial litigation and white-collar criminal defense. He specializes in the Foreign Corrupt Practices Act, U.S.A. Patriot Act, the Bank Secrecy Act, the Money Laundering Control Act, and OFAC regulations, as well as anti-money laundering and OFAC compliance program development and implementation.

What *Is* a Risk Assessment?

A Risk Assessment is the process of identifying all the areas of statutory and regulatory compliance your company faces, assessing the likelihood of one or more of your employees violating one of those compliance standards, and then prioritizing and tailoring your compliance controls and procedures to ensure that they focus your compliance efforts according to the degree of risk you've identified in each area. The end product is a written document, chart, or both that identifies categories of risk and assesses risk in each.

There are five key points to keep in mind about a Risk Assessment. *First*, it requires senior management support and involvement, because senior management is ultimately responsible for supporting your company's compliance efforts. *Second*, the completed risk assessment is not a secret. If it is to achieve its purpose, it has to be communicated within the company to key personnel and the board. So, while it must be comprehensive, it also has to be concise and understandable. *Third*, it is a *process*. Even though it's a written document, it has to be continuously updated to keep pace with the changes in your business (*e.g.*, in products, services, customer base, geographic areas of operation, etc.) and changes in applicable laws and regulations. Even if there are no changes in those areas, it should be reviewed and revised periodically (that is, about annually). *Fourth,* a Risk Assessment is not a "scoring" exercise designed to come up with one overall "compliance risk score" for your company. Risk Assessments don't work that way. A Risk Assessment is not designed to determine an institution's *overall* risk level for compliance violations, it's designed to enable the business to *identify specific areas of risk within your areas of operations* so that appropriate controls and procedures can be designed and applied by the organization to mitigate the risk in those areas. *Fifth*, and most importantly, a "Risk Assessment" is not an end in itself. It is a only a *tool*, albeit an essential one, for you to use in assessing your current compliance program's effectiveness, in identifying its weak spots, and in focusing your compliance controls and procedures on different areas according to the risk assessed in that particular area. Think of it as a tool for prioritizing your scarce compliance resources.

Why Should You Conduct A Risk Assessment?

Two reasons. First, your senior management can get sued if you don't do your compliance program right, and part of your job is to protect them. Second, to put it bluntly, because the government expects your company to, whether you like it or not, and the other part of your job is to protect your company.

Reason number one: Companies must promote an organizational culture that encourages "ethical" conduct. Senior managers have overall responsibility for a compliance program, and they, along with the Board of Directors, can be held accountable for compliance and ethics failures. In a case commonly referred to as the *Caremark* decision, shareholders filed a lawsuit alleging that Caremark directors bore *personal* responsibility for their failure to supervise company activity. A Delaware Chancery Judge suggested that "by establishing and maintaining an effective compliance program, board members can protect themselves from personal liability suits." *In re Caremark International Inc. Derivative Litigation,* 698 A.2d 959 (Del. Ch. 1996); *see also, Stone v. Ritter*, 2006 LEXIS 597, *30-31 (Del. November 6, 2006). Failure to have

such a program, on the other hand, may "render a director liable for losses caused by non-compliance."

Reason number two: From the SEC to the Public Company Accounting Oversight Board to the Department of Justice to the Bank Secrecy Act Anti-Money Laundering Examination Manual to the Health and Human Services Department's Office of Inspector General to the United States Sentencing Commission (Sentencing Commission), government agencies either strongly recommend or flat out require the companies they regulate to implement "risk-based" compliance and ethics procedures. It is increasingly the case that regulatory agencies are also taking into account companies' compliance and ethics programs in determining whether to bring administrative enforcement or civil money penalty actions against corporations and other organizations. The DOJ has adopted a formal policy *requiring* all federal prosecutors to consider a company's compliance and ethics program when making decisions about whether to bring criminal charges against a company. Prosecutors are trained to use the Sentencing Commission's Guidelines for Organizations (the Sentencing Guidelines) as the standard for these evaluations. The underpinning of an effective Guidelines program is a well constructed, thorough, written Risk Assessment (United States Sentencing Commission, *Guidelines Manual*, § 8B2.1).

Sentencing Commission Guidance on Risk-Based Compliance Programs

The Sentencing Commission's Guidelines have incorporated all of the risk-based compliance concepts of most other agencies, so that makes them probably the best place to focus most of our attention. After a two-year study of compliance programs, in 2004 the Sentencing Commission issued its "Amended Guidelines" to clarify and expand its earlier compliance standards. These contain detailed guidance on the elements of an "effective" compliance and ethics program.

While the Amended Guidelines specifically address "criminal conduct," it is common — and, in the minds of most commentators who take the *Caremark* decision into account, mandatory — practice to expand the scope of the assessment (and the compliance and ethics program) beyond only criminal conduct to include any regulatory compliance or ethical violations. Identifying risk includes matters that could lead not just to criminal enforcement, but to civil or administrative enforcement as well as private law suits and even damage to reputation. (*Note, because the Sentencing Guidelines are specifically focused on the criminal sentencing process, the U.S. Sentencing Commission [the "Commission"] felt it was beyond its mandate to issue rules for evaluating compliance programs in a non-criminal context. However, the Commission has also made clear in commentary that civil law standards and other non-criminal legal and regulatory risks should be addressed in a truly effective compliance and ethics program. "Best practices" for compliance programs would dictate that all legal and regulatory risks be evaluated and addressed.*)

What Do the Amended Guidelines Require?

The Amended Guidelines state what compliance practitioners have long known: The appropriate starting point for the design, implementation, or modification of a compliance and ethics program *is* a Risk Assessment. They say that periodically, and no less than annually, the company should assess the risk of compliance violations within the company and design, implement or modify the compliance and ethics program to reduce or mitigate the risk of wrongdoing. There are other elements of an effective compliance program, of course, but none of them can really be accomplished unless the company first identifies and assesses its risk areas. Thus, it's fair to say that the Risk Assessment is — or should be — the cornerstone of your compliance program.

The Critical Elements of a Risk Assessment

There are a number of elements that are critical to the "Risk Assessment." These are:

- Identification of all of the legal and regulatory regimes that impact the company's business;
- Identification of the policies, procedures and controls the company already has in place to ensure compliance with legal and regulatory requirements;
- Identification of the areas in which the company's policies, procedures, controls and compliance program elements are not sufficient to ensure compliance with legal and regulatory requirements;
- Evaluation of the likelihood that legal and regulatory violations will occur;
- Evaluation of the seriousness of potential violations and the harm to the company that may be caused by the potential legal and regulatory violations identified;
- Identification of the reasonable steps that can be taken to prevent, deter and detect the identified improper conduct;
- Evaluation of the prior history of the company and other similarly situated companies (appropriate consideration should be given to prior criminal, civil and regulatory enforcement actions);
- Prioritization of the identified compliance risks in order to focus the compliance and ethics program on preventing, detecting and deterring the violations most likely to occur and to cause the most harm to the company; and
- Identification of compliance and ethics program elements most likely to achieve the goal of preventing, detecting and deterring the violations identified as the top priorities of the compliance and ethics program for the coming year.

Documenting

If it's not in writing, it wasn't done. This is the frequent mantra from regulators, enforcement agencies and the DOJ. Thus, to make the risk assessment process effective, and to get credit for it from the government and the courts, your Risk Assessment must be in writing, and you should document *each step of the assessment process*.

How much documentation? The answer depends on the company. For large, multinational corporations involved in heavily regulated business activities, the "Risk Assessment" should be comprehensive and involve personnel from each business unit and department. They will need to evaluate a broad and complex range of risk exposures, including things like the bribery of foreign officials, financial reporting fraud, insider trading, import and export law requirements, specific industry regulations and many others. For small, purely domestic companies that are not in heavily regulated industries, the process can be much simpler. Many companies find the process easier to monitor and to communicate to both management and the board of directors through the use of tables, or "matrixes" that chart the risks and assign some kind of scoring to enable a numerical prioritization of the risks to be addressed.

How Do You Conduct The Risk Assessment?

The first time a company conducts a risk assessment, it should seriously consider doing it with the assistance of an "expert" and the oversight of a lawyer, in-house or outside. Also, document that the process is

being undertaken in order to provide legal advice to the company, because a first-time "Risk Assessment" can uncover serious legal problems that you may want to cloak with the attorney-client privilege. After the first "Risk Assessment" has been done, the ongoing changes and updates to it can be done through your compliance department or risk management office.

In conducting a first-time "Risk Assessment," we typically envision a three-step process.

Step One: Information Gathering: The first step consists of "information gathering" designed to achieve a thorough understanding of the company's operations and its legal regulatory environment and identify all risk areas. This step itself involves three separate but overlapping parts: first, an initial, detailed consultation; second, the collection and review of appropriate company documents and data; and third, interviews and/or surveys of appropriate personnel.

(a) Consultation: Start with a consultation between the expert and a designated individual or group at the company. The designated company person(s) should have, or should be able to arrange for consultations with the persons who have, a thorough knowledge of the company's: organization; methods of operation; financial controls; identity of key personnel; the various types of data and documents the company has; and its current compliance procedures.

One cost-saving point: Since your written Risk Assessment will be continuously updated and revised, your compliance and/or risk management person(s) should work closely with the "expert" the first time around to learn the process so that they can do later updates themselves. Retain an "expert" who is willing to teach your people how to do it themselves.

(b) Data and Document Collection: The second part of this process involves collecting appropriate documents and data. Get supporting materials for your identification and assessment of risk areas. Some of these documents (such as the current compliance program materials) can be readily identified. Other materials will require discussion in the consultation process to identify (and collect). You, as in-house counsel, will already know the statutory and regulatory regimes you have to address, but you may not know the actual business as well as you think.

(c) Interviews/Surveys: Based on the initial consultation activities, the third part of the data gathering process involves interviewing and/or surveying appropriate personnel who represent the critical areas of the company's structure and operations. These interviews or surveys are conducted to ensure a complete understanding of the company and its operations, and also to learn which compliance procedures work, which ones do *not* work and *why*, and to identify as many loopholes and risk areas within the procedures as we can. Quite often, the persons most intimately involved with the actual day-to-day operations of an institution will be the persons who can most readily identify the loopholes and some previously unidentified problem areas. In order to collect information consistently, a standard interview form can be developed for use during all interviews. For larger companies, consider doing an employee survey to supplement interviews.

Step Two: Evaluation of Risk Categories and Level of Risk: The second step starts with breaking down the risk categories identified into specific components or sub-categories (types of risk) Next, each sub-category should be evaluated to actually assess the risk level associated with it. The risk levels should include an evaluation of the likelihood of a violation in each area and an assessment of the level and type of damage a violation could cause. This step should also include an evaluation of the sufficiency of existing compliance or control procedures. It is usually helpful to prepare tables, or matrixes listing the categories of risk and tracking the steps in the analysis. Standard scoring systems can be established using designations such as "high," "moderate" or "low," or a numerical designation, such as 1 to 5. The degree of analysis will, of course, vary, depending on the information collected and the risk categories identified.

Step Three: Analysis, Document- ation and Setting of Priorities: The third step in the process will be to prepare a written risk assessment based on steps one and two. This will include two things. First, it will include an analysis of identified risks, presented in a concise manner so as to provide clear guidance to the company in identifying various risk profiles and in tailoring and prioritizing its compliance activities accordingly. Second, it will include a chart of risk areas together with their level of risk and a brief explanation. The aim will be to present the Risk Assessment as clearly as possible so that it can be easily used and efficiently referred to by the compliance officer, senior management, the board and appropriate supervisory personnel.

Finally, based on the final product, the team involved in the process should make recommendations on the priorities in addressing risks during the coming period of time. For example, the team might list five risk priorities it recommends to be the focus of compliance efforts for the coming quarter, or year. The process of analysis and the recommended priorities would then be documented in a report to management and the board. As a best practice, the recommendations should be ratified or approved by either management, the board, or both. The reason for this is two-fold. First, it keeps these bodies informed of key issues affecting the company and their oversight responsibilities; and second, having the risks outlined in black and white can have a salutory effect on obtaining the resources necessary to appropriately mitigate the risks.