Compliance & Ethics Professional®

June 2017

A PUBLICATION OF THE SOCIETY OF CORPORATE COMPLIANCE AND ETHICS

www.corporatecompliance.org

Meet Sheryl Vacca

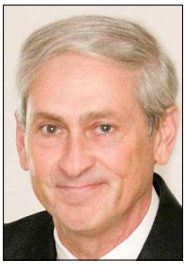
Senior Vice President/Chief Risk Officer
Providence St. Joseph Health
Irvine, CA

See page **16**

by Jeffrey M. Kaplan

Risk assessment for smaller companies

Based on both various legal standards and common managerial sense, effective risk assessment should be at the foundation of compliance programs. There is indeed no shortage of conceptually elaborate and operationally challenging risk assessment models available. For some organizations—particularly large companies or those in heavily regulated businesses—going down this sort of path may be warranted. But for "the rest of us" (to quote the immortal Seinfeld episode about "Festivus") doing so may be neither necessary nor desirable.



Kaplan

So, what might a basic "short form" risk assessment look like?

The initial step is for the chief ethics and compliance officer (CECO) to develop a list of risks to be assessed. The table of contents of a company's code of conduct is often a good starting place, but its list of risks should be modified in two ways.

First, some areas in the code may already have been the subject of a targeted risk assessment, such as environmental, health, and safety; data privacy; and fraud. For such risk areas, there is generally no need to "reinvent the wheel."

Second, for some areas there may be a need for more granularity than what appears in the code's table of contents. Examples here include corruption and misuse of confidential information; for each, the assessment should be of both scenarios where the company is the victim of the wrongdoing and where it is the beneficiary. A granular approach to competition law risk assessment is also generally a good idea.

Next, the CECO should distribute the revised risk list to assessment participants. Who should be involved in the process will, of course, vary by company. However, at least in my experience, staff (Law, Audit, Finance, HR, and Procurement) tend to do better with providing risk assessment information and ideas than do business people.

Along with the risk list, the CECO should provide a set of easy-to-follow instructions which asks the participants not only to rank the risk by likelihood and impact, but also to identify:

- reasonably foreseeable scenarios of violations; and
- desirable mitigation enhancements for each area—particularly involving standards of conduct, training and communications, process controls, accountability, and auditing/other checking.

They should also be asked for identification of any risks that are not, but should be, on the CECO's list.

Finally, the results of this process should be "rolled up" to the CECO, who generates a report that includes an analysis of risks and recommended mitigation for each risk area on both an enterprise-wide and more granular (e.g., by geography or business unit) basis. The report—which should be approved by senior management—might also describe what steps can be taken for refresher assessments in the future. ✳

Jeffrey M. Kaplan *(jkaplan@kaplanwalker.com) is a Partner with Kaplan & Walker LLP in Princeton, NJ.*