Compliance Readiness – Legal Service Providers

Gaps In Your Compliance Posture? Consider A Legal Compliance Risk Assessment

The Editor interviews ***Alex Brigham****, President and Chief Executive Officer, Corpedia Corporation d/b/a Corpedia.*

Editor: Tell us about Corpedia and its involvement in risk assessment.

Brigham: Corpedia (www.corpedia. com) offers a wide variety of programs to help organizations address legal compliance and ethics issues. Our solutions familiarize employees with all facets of regulations affecting their companies and offer measurable outcomes for their compliance and ethics initiatives. We develop our programs in exclusive partnership with the Practising Law Institute (PLI). It has over 400 customers in more than 60 countries, including Radio Shack, EMC, Xerox and PepsiCo for its training programs.

Through combining the extensive content expertise of PLI with Corpedia's technological and risk assessment capabilities, Corpedia is able to provide risk assessment services of the highest quality.

Editor: Why is it critical for companies to have legal compliance risk assessment programs?

Brigham: Legal compliance risk assessments are an important component of a company's overall strategy because they help it: (1) meet Federal Sentencing Guidelines' stipulations; (2) identify potential risks that need to be addressed thus providing an early warning of problems; and (3) develop an effective strategy for the company's compliance program.

The Federal Sentencing Guidelines provide that an organization shall periodically assess the risk of criminal conduct and shall take appropriate steps to reduce the risk of criminal conduct identified through this process. A risk assessment program that meets this definition not only can mitigate criminal penalties, but will be helpful in the event of future investigations or plaintiffs' suits.

A major component of this assessment is an evaluation of company practices to determine whether there is a potential for criminal misconduct or legal liability. This includes potential problems with IP, theft, loss, employment law, product liability, antitrust, bribery and other inappropriate practices. Companies become overwhelmed with this process when they look for hypothetical risks without first examining their actual business practices in relation to the legal requirements applicable to those practices. Those conducting the assessment must be or become familiar with each of the company's lines of business.

Legal risk assessment programs are distinct from Sarbanes-Oxley Section 404 assessments. There are certainly correlations between work performed by the Internal Audit function of any organization and a risk assessment conducted by the compliance, ethics or legal functions. However, the fundamental elements being examined under Section 404 (effectiveness of internal controls, which may include processes and procedures to detect material violations of law that could affect financial statements) are very different from a legal assessment of risk that includes weighting, occurrence likelihood and deterrence elements.

Editor: How does a risk assessment program serve as an early warning system?

Alex Brigham

Brigham: Once the program is in place, it is a great way to uncover potential problems. By looking for compliance risks that might open the door to potential criminal conduct or other compliance failures, you may find gray areas indicative of compliance issues. You can then proactively address these situations and stop them before they blossom out of control.

A company should recognize that if it does identify a potential problem but does not follow through and address it, it may have created a bigger problem for itself. Knowingly ignoring a problem will play into the hands of government investigators or plaintiffs' counsel. This could trigger greater penalties or punitive damages.

We have been involved in a number of risk assessments which uncovered inappropriate conduct that was stopped before it could become a problem. Companies tend to be reactive in addressing situations as they are raised by either whistleblower hotlines or field reports. By waiting for these triggers, it may be too late to address a problem. A risk assessment may uncover a problem that may never be reported by an employee.

Given these benefits, the 2006 Corpedia Benchmarking Survey ('Survey") found that 65% of all organizations conducted periodic risk assessments.

Editor: How frequently should a risk assessment be conducted and should it have a global reach?

Brigham: Risk assessments should not be a one-time activity. If the methodology and process for risk assessment are adequately defined, a risk assessment can be conducted on an annual basis. Operating environments, regulations and government enforcement priorities routinely change, and the effectiveness of a compliance program can decline. Therefore, it is ill-advised to conduct risk assessments less frequently than every two years.

The backdating scandals also illustrate how important issues can be overlooked where organizational "silos" are created that prevent the internal audit and legal functions from becoming aware of abuses. For example, in recent years some of the most costly and publicly embarrassing compliance failures for U.S. corporations have occurred overseas. While it is tempting to focus a risk assessment program on those areas with which the legal department is most familiar, such a narrow focus can significantly undermine the utility and credibility of the program.

Editor: How can a risk assessment program focus a company's compliance programs on issues that need to be addressed?

Brigham: A periodic risk assessment allows a company to pinpoint potential problems and to adjust its compliance efforts to prevent such problems from arising in the future. Thus, a company may revise its code of conduct or make it more accessible. It may modify its training programs or target them to particular audiences depending on the risks uncovered in the assessment. Reporting relationships may be altered to assure improved supervision. Corporate counsel and other staff services provided to particular areas may be enhanced.

The targeted approach to remedying compliance issues based on a risk assessment is far more effective than a blanket approach attempting to address hypothetical risks. It also prevents unnecessary waste of resources. Surveys of corporate counsel confirm the importance to them of risk assessment programs in discharging their responsibilities.

Editor: Should a risk assessment include quantitative measures of risk? How important is exchange of information with the organization's peers pertaining to risk areas and compliance program activities?

Brigham: When conducting a risk assessment, the organization should assign quantifiable "likelihood" and "severity" weights or ratings to each relevant risk area. Nearly 80% of companies rank risk for likelihood and severity – of which 44% quantify risk in each relevant risk area.

If it is feasible and such information is accessible, companies should benchmark their risk assessment results by comparing their risk areas and compliance program activities with those of their peers – those organizations that may be similar in size and operational profile. This is of particular importance since it ensures that the corporation meets "accepted or industry practice" as outlined in the application notes to the Sentencing Guidelines. Although a company may reach out directly to a competitor to conduct benchmarking, there may be some reluctance to do this because of antitrust considerations. A resource that is commonly used by organizations for benchmarking data is Corpedia's ECERA™ (Enterprise Compliance and Ethics Risk Assessment) database on hundreds of organizations' compliance programs. It contains specific critical risk severity metric data for over 50 unique industries that was collected as a result of in-depth research of 700 U.S. and international business organizations.

Editor: How can a risk assessment program prevent problems such as the backdating of stock options that are often discovered after the fact?

Brigham: The importance of a periodic risk assessment program is highlighted by the stock option backdating issue. If companies had such a program in place at the time the backdating took place, the backdating would have probably been uncovered, properly accounted for and disclosed. Backdating may also have been indicative of a corporate culture in which people were afraid to question management's decisions. One of the things we measure when doing a risk assessment is the company's culture. We look at whether there is a culture of discourse and transparency where people can raise issues without fear of retribution or a culture where employees fear that they will be treated unfairly if they raise an issue. Such a culture of fear can exist even though a company has a non-retaliation clause in its code of conduct and legal protection is accorded to whistleblowers under Sarbanes-Oxley and many state laws.

Editor: What steps are necessary for a risk assessment program to work effectively?

Brigham: There are four important factors for properly implementing a compliance program: (1) you need to differentiate the compliance risk assessment from enterprise risk management; (2) you need to make sure that the process does not come across as an internal investigation of inappropriate conduct; (3) you need to develop a process for collecting documents and information; and (4) you need to be prepared to address what you find. If you do not have a good handle on these four issues, you should not do a risk assessment because you will create more problems for yourself than you had to begin with.

Editor: What is the difference between compliance risk assessment and enterprise risk management?

Brigham: Enterprise risk management (ERM) requires you to look well beyond legal liability and compliance issues. For example, an ERM program will look at the impact a war or economic downturn will have on your assets. These types of situations are out of the legal department's control and should not be included in a compliance risk assessment.

Editor: Should the planning and implementation of a risk assessment program be conducted entirely in-house or include outside expertise?

Brigham: The Survey revealed that nearly half (45%) of all organizations conduct their risk assessments entirely in-house, while the remainder (55%) use an outside adviser. There are several advantages to retaining an outside adviser. Sensitive or damaging information can be better protected, including from private litigants and prosecutors and regulators. A high level of analytical and statistical expertise is required for an effective risk assessment. Outside consultants are current in the intricacies and frequent changes in the risk management field. Individuals too close to the business operation may have a natural bias that may cause them to potentially over or underestimate the degree of potential risk. An outside advisor with experience doing risk assessments for other companies may be perceived to have a better perspective on the actual severity of a risk and, thus, lend greater credibility to the assessment.