

COMPLIANCE WEEK

The leading resource on corporate compliance and governance for U.S. public companies.

Building Ethics, Compliance Risks Into ERM

By Andrea Bonime-Blanc, *Compliance Week Guest Columnist* — October 31, 2006

In today's world of daily and instantaneously communicated risks, crises and scandals related to ethics and compliance—or what we call “E&C” risks—it is no longer simply desirable for companies to have an E&C risk-management program: It is a business necessity. Indeed, it is increasingly crucial to have an E&C risk-management system that is integrated with a company's enterprise risk-management system.

At Bertelsmann AG, the €17.9 billion global media company, we have engaged in such a holistic risk assessment and management process for a variety of sound business and legal reasons. Indeed, we began to conduct E&C risk management in the United States years ago even before the 2004 revisions to the U.S. Federal Sentencing Guidelines, which made it a legal requirement for companies in the United States to conduct periodic E&C risk assessments.

Thus, in addition to legal requirements, there are even stronger business reasons for companies to develop an integrated and holistic approach to corporate risk management, including ethics, compliance, governance, and corporate-responsibility risks. If companies do not pursue such a holistic integration strategy, they risk missing serious issues that could affect the bottom line financially, as well as the company's reputation.

Such a holistic approach is critical especially in a complex global organization such as Bertelsmann. Comprised of six global divisions—including Random House and Luxembourg-based RTL Group—we operate dozens of television and radio stations, more than 100 publishing houses, nearly two dozen music publishing labels and magazines, and a multitude of manufacturing, printing, and other high-technology businesses around the globe. With almost 100,000 employees operating in almost 60 very diverse countries—from Slovakia to Uruguay—it only made sense for us to unify our approach to all types of global risks.

By having a fully integrated ERM system, a company creates an invaluable business tool—a form of a reputational early warning system—that can save the company from serious embarrassment and financial loss. It also can provide the company with an improved reputation as a solid and reliable corporate citizen.

An E&C risk-management program that is integrated into an ERM system can provide a sharp new tool for operations, financial, and risk managers. It can help them to identify, ascertain, prevent and mitigate a spectrum of potentially “big ticket” risks that may not be on their radar screens either because such topics were previously unknown to them or considered irrelevant, soft or unquantifiable.

An integrated E&C risk-management system is also a powerful tool for the E&C office, as it elevates key issues to greater visibility at the upper echelons of an organization—including the corporate suite and the boardroom. Moreover, an integrated E&C risk-management system also can provide a powerful awareness

tool as it requires executives and managers to think about E&C issues not only from a risk-management standpoint but also from an operational and educational standpoint.

Major E&C Risks

A mere scan of the headlines over the past few years—or even the past few months or weeks—yields a wide array of E&C and related governance and corporate-responsibility risks and scandals. What follows is a quick list of some (but certainly not all) of the E&C risks that should be considered as part of an integrated E&C risk-management system:

- **Bribery & Corruption**. Risk of national or international criminal investigation, indictment and/or conviction and fines (of both company and employees involved) for paying bribes or engaging in other corruption with foreign officials to get business, retain business, or receive some other undue advantage.
- **Antitrust & Unfair Competition**. Risk of violation of national and/or international civil and/or criminal laws concerning business collusion, conspiracy, unfair competition, or another violation of competition laws.
- **Privacy & Data Security**. Risk of non-compliance with data-privacy laws of the country where the business is located, as well as the data-privacy transfer protocols between countries.
- **Harassment & Discrimination**. Risk of violation of applicable national laws and company policies concerning the protection of certain personal categories (gender, race, religion, ethnicity, age, sexual orientation, etc.) with regard to workplace conduct and applicable personnel decisions.
- **Human Rights**. Risk of violation of basic human rights concerning employees and others—especially in developing country manufacturing and factory settings—including the use of child labor, slave labor, and other unfair labor practices.
- **Conflicts of Interest**. Risk that upper- and mid-level management do not follow applicable conflicts of interest rules with a potential adverse reputation or financial impact on the company.
- **Environment, Health & Safety**. Risk of violation of applicable environmental, health, and safety laws and policies with an adverse impact on people and/or property.
- **Whistleblower Protection**. Risk that an employee who in good faith raises concerns or allegations about another employee, manager, executive, vendor, or customer is retaliated against for raising such concerns.
- **Political Lobbying**. Risk that an improper individual or corporate political lobbying activity or contribution is made in violation of applicable local, national, or international laws.

Integrating E&C Risks Into ERM

The single most important step the E&C function can take to get the integration process moving forward is to get a senior-level advocate to champion the cause of E&C risk-management integration into the company's ERM system. And the more senior the executive the better—preferably, the chief executive, operating, or financial officer or a board member becomes the internal champion.

Once started, the dialogue between E&C and ERM will yield a systematic identification of risks. Those E&C risks then will be incorporated into the inventory of ERM risks, and processes and tools can be leveraged for the tracking and mitigation of risks.

For example, here is how such a system might be organized, and how the E&C element would be integrated:

- **Risk Identification.** The most important and potentially significant E&C risks confronting an organization must be identified through programmatic review, systematic documentation, organized brainstorming, or other similar exercises that are appropriate for your organization and its culture. The risks identified should include common “generic” ones—such as those identified above—as well as industry or business specific risks. At our decentralized global company, for example, each major business unit has its own risk manager who engages in a yearly risk-identification-and-documentation exercise. Such risks are then inventoried and reported up the corporate chain to produce information that is useful to senior management and the board.
- **Risk Performance Indicators.** Next, for each identified risk, specific performance indicators need to be ascertained. For example, if the risk is bribery and corruption, possible performance indicators for such a risk might include potential financial liability, possible jail terms, adverse publicity, and a sustained reputation hit.
- **Risk Reporting Tools & Processes.** A systematic method for periodically assessing and reporting risks needs to be devised. The results of the reporting need to be organized and packaged from both a quantitative and qualitative standpoint, whichever is applicable. Tools could include financial and other reporting by which one could gauge whether activities or actions are taking place that might heighten the possibility of a risk taking place.
- **Risk Handling & Mitigation.** Through this exercise, key elements of a preventative and mitigating strategy would be enumerated, for example, the creation of a policy, reporting system, training program, monitoring system, or other processes that might lessen or prevent a risk from occurring.

The critical link for the successful integration of E&C risk management into a more holistic ERM system is senior management and/or board support. By getting the blessing and support of the upper echelons of an organization, the work of the E&C and ERM teams not only will be easier but will yield a better and more reliable product; namely, a fully integrated and comprehensive risk-management system that not only lives up to legal requirements but, more practically, becomes a useful tool for achieving operational improvement, liability reduction, and reputation enhancement.

About The Guest Columnist

Andrea Bonime-Blanc is senior vice president and chief ethics and compliance officer at Bertelsmann AG where she oversees global business ethics and compliance for the \$22 billion German-based global media company and works closely with all divisions on the creation and implementation of business- conduct programs. In 2005 and 2006, Bonime-Blanc and the Bertelsmann ethics team received several prestigious communications awards for the originally developed Bertelsmann Family Feud Ethics Game Code of Conduct employee-training program and the Bertelsmann's Ethics & Compliance Intranet and E-Communications Program. Bonime-Blanc previously served as General Counsel and Chief Compliance Officer of the global power division of PSEG, a leading U.S. energy company. Prior to that, she practiced international transactional law at Cleary, Gottlieb, Steen & Hamilton and King & Spalding. She serves on the Board of Directors of the Ethics and Compliance Officer Association and is the chair of its External and Governmental Relations Committee and a member of its Executive Committee. She is also a member of The Conference Board's Global Council on Business Conduct, the Council on Foreign Relations, and the Board of Directors of the American Association for the International Commission of Jurists.



Disclaimer

This Compliance Week guest column solely reflects the views of its author, and should not be regarded as legal advice. It is for general information and discussion only, and is not a full analysis of the matters presented.