

**CONDUCTING CAMPUS RISK ASSESSMENT AND SETTING  
COMPLIANCE PRIORITIES**

November 11–13, 2009

**Andrea Bonime-Blanc**

Daylight Forensic & Advisory LLC  
New York, NY

**Marcia Isaacson**

State University of New York  
New York, NY

**Stephen Sencer**

Emory University  
Atlanta, GA

**Craig Stewart**

Arnold & Porter LLP  
New York, NY



THE  
ETHICS  
AND  
COMPLIANCE  
HANDBOOK

A Practical Guide From Leading Organizations

Ethics and Compliance Officer  
Association Foundation



---

# TABLE OF CONTENTS

---

PREFACE & ACKNOWLEDGMENTS	7
INTRODUCTION	9
CHAPTER 1 Risk Assessments	13
CHAPTER 2 Creating an Ethics and Compliance Office	29
CHAPTER 3 Oversight by the Board and Senior Management	43
CHAPTER 4 Codes of Conduct	59
CHAPTER 5 Providing Ethical Advice and Receiving Allegations	77
CHAPTER 6 Internal Investigations	95
CHAPTER 7 Rewards and Discipline	111
CHAPTER 8 Communications and Training	125
CHAPTER 9 Employee Screening	141
CHAPTER 10 Program Assessment and Evaluation	155
CONCLUSION Looking Forward: Where Are Ethics and Compliance Heading?	163
BIBLIOGRAPHY	175
ABOUT THE ECOA, THE ECOA FOUNDATION, AND THIS BOOK	180
INDEX	181

# RISK

# ASSESSMENTS

---

# CHAPTER 1

---

## INTRODUCTION

A comprehensive risk assessment is one of the building blocks for an effective ethics and compliance program. By understanding the nature of risks it faces, an organization can better design and manage a program that serves its ethics and compliance needs. An ethics and compliance risk assessment can provide both a broad perspective on risk in general, as well as an in-depth analysis of risks that should be of particular concern. The results are typically used to assess the effectiveness of the current controls and develop new controls to mitigate risks. It is crucial that an ethics and compliance risk assessment extends beyond an assessment of the organization's potential exposure to criminal conduct. It should incorporate a broad review of the risks that impact the organization's reputation for ethical and legal conduct. It should also assess the likelihood that an adverse event will occur, the significance of the impact it would have on the organization, and the effectiveness of the measures the organization currently takes to minimize these risks.

Armed with this knowledge, an organization can implement ethics and compliance systems tailored to the realities it confronts. Every major element of an ethics and compliance program should relate back to the risk assessment. Risk assessments must not be one-time efforts, but should be conducted periodically and often in conjunction with broader, enterprise-wide risk assessments. This will allow the organization to ensure that it is addressing not only well-established risks but emerging ones as well.

## U.S. SENTENCING GUIDELINES

The U.S. Sentencing Guidelines provide that, in order to have an effective ethics and compliance program, an organization should “periodically assess the risk of criminal conduct and . . . take appropriate steps to design, implement, or modify” its program “to reduce the risk of criminal conduct identified through this process.”<sup>1</sup> Although the guidelines describe risk assessment as a vehicle to detect and prevent *criminal* conduct, most organizations take the prudent view that *all* ethics and compliance risks must be examined, including those that affect criminal liability, civil liability, regulatory exposure, business ethics or conduct, and the organization’s reputation.

The Sentencing Guidelines further state that the risk assessment should take into account the nature and seriousness of criminal conduct, the likelihood that such conduct might occur, and the organization’s history. They also note that an organization should prioritize the steps it will take to prevent and detect criminal conduct and modify its ethics and compliance program to reduce these risks.

## GUIDING PRINCIPLES

- Ethics and compliance (E&C) risk assessments should help an organization evaluate how well current ethics and compliance programs are actually operating.
- E&C risk assessments should result in an action plan to mitigate identified high-priority risks.
- E&C risk assessments should be conducted regularly, to accommodate changes in the legal, regulatory, and business environment, as well as adjustments to the organization’s activities.
- Organizations should examine not only the potential for criminal conduct but also the likelihood that unethical or other problematic decisions might be made.
- E&C risk assessments can, but need not always, be conducted as part of larger, enterprise-wide risk assessments.

<sup>1</sup> According to the U.S. Sentencing Guidelines:

The organization shall periodically assess the risk of criminal conduct . . . including assessing the following:

- (i) The nature and seriousness of such criminal conduct.
- (ii) The likelihood that certain criminal conduct may occur because of the nature of the organization’s business.
- (iii) The prior history of the organization. The prior history . . . may indicate types of criminal conduct that it shall take actions to prevent and detect.

An organization shall . . . prioritize periodically, as appropriate, the actions taken pursuant to any requirement set forth in subsection (b) [regarding an effective ethics and compliance program], in order to focus on preventing and detecting the criminal conduct . . . as most serious, and most likely, to occur.

An organization shall . . . modify, as appropriate, the actions taken pursuant to any requirement set forth in subsection (b) to reduce the risk of criminal conduct . . . as most serious, and most likely, to occur.

*U.S. Sentencing Guidelines Manual* § 8B2.1(c) and cmt.n.6.

- E&C risk assessments should prioritize risks according to the likelihood of occurrence, the seriousness of the impact on the organization, and the factors that contribute to the risk.
- E&C risk assessments should include evaluation of why those risks occur and what can be done to reduce those risks.

## DEFINITIONS

***E&C Risk.*** An uncertain event or condition that, if it occurs, has the potential to affect the achievement of an organization's strategies and objectives. It is a product of two things: the severity of a potential negative event and the likelihood of its occurrence.

***E&C Risk Assessment.*** A systematic process for identifying, evaluating, analyzing, and prioritizing the ethics and compliance risks an organization faces.

***E&C Risk Management.*** A comprehensive and continuous process for: (i) identifying the most significant risk exposures facing an organization (i.e., risk assessment); (ii) evaluating the extent and adequacy of existing controls; (iii) modifying controls to address gaps, areas for improvement, or even areas of "over-control"; and (iv) monitoring controls to ensure they are functioning effectively.

***Enterprise Risk Management (ERM).*** A comprehensive risk assessment and management process that evaluates the universe of overall business risks, including ethics and compliance risks. For example, every organization faces a broad array of risks, from financial and operational to political and reputational. An ERM system provides a holistic and inclusive approach to all of these risks.

## IMPLEMENTATION

### ***Determine how the ethics and compliance risk assessment fits in a broader enterprise-wide risk assessment.***

Ethics and compliance risks can arise in a variety of contexts throughout an organization. An ethics and compliance risk assessment must therefore be broad-based, covering topics such as legal or regulatory compliance; organizational policies; financial directives; information technology; products/services developed, manufactured, or distributed by the organization; and environmental, health, and safety concerns.

Because it touches so many areas of the enterprise, the ethics and compliance risk assessment is often integrated into a broader risk framework. This approach—commonly called enterprise risk management or ERM—results in ethics and compliance risks being assessed as part of broad risk categories, such as strategic risks, operational risks, reporting risks, financial risks, legal risks, and regulatory risks.

There are at least two advantages to enterprise risk management. First, because existing risk assessments may overlap with some of the issues that would be covered

by an ethics and compliance-focused effort, integration may well be more efficient. Second, it can help foster the perception that ethics and compliance is central to all of the organization's activities, rather than functioning as a stand-alone or "niche" activity outside of mainstream organizational concerns.

There are, of course, some disadvantages to blending the ethics and compliance risk assessment into a broader enterprise-wide effort. For instance, ethics and compliance risks may not be as obvious as business risks and therefore may receive less attention from those performing the assessment. In addition, an enterprise-wide assessment will necessarily require more time and resources to complete.

Whichever approach is adopted, the key is to develop a systematic approach to the identification, classification, and prioritization of ethics and compliance risks. In some organizations, leaders may believe that a formal risk assessment is not necessary because their own, deep knowledge of the organization ensures they will identify the relevant risks themselves. Although this approach may produce adequate results in small organizations, it is almost certainly insufficient to identify the key risks facing medium and larger ones. For these entities, no single individual will be familiar enough with the organization's operations to understand all of its relevant risks. Therefore, a more formalized risk assessment is prudent.

***Designate a working group to lead the risk-assessment process.***

Successful risk assessments require the involvement of many individuals with a variety of areas of expertise. Their divergent business experiences, both inside and outside of the organization, add richness to the data collection and analysis, and ensure that the risk assessment is not the exclusive product of a single department or mind-set. An organization should therefore designate a dedicated team to lead the ethics and compliance risk assessment. Such a group typically includes representatives from the internal audit, legal, finance, and ethics and compliance departments, as well as some business or operational functions.

In some organizations, the legal department is the designated "home" of the ethics and compliance risk-assessment function, as well as its leadership team. This occurs because litigation exposure and history are central parts of any risk-assessment. In other organizations, the risk-assessment function resides in the internal audit department, due to that department's deeper knowledge of the organization's control systems. Still others have a freestanding ethics unit or a risk department with its own chief risk officer. Whatever department "owns" risk-assessment, senior management must ensure that it has adequate resources (e.g., time and organizational support) to complete its work.

## IN PRACTICE

There is active debate whether risk assessments—and specifically those examining ethics, compliance, and reputational issues—should be closely held within the organization. The data and analysis are designed to identify gaps to be filled and problems to be resolved; honest risk assessments rarely conclude that everything is under control. Some organizations fear that they might be held legally liable for risks they identify but fail to mitigate or address expeditiously. Where an organization is concerned about public disclosure of its risks and weaknesses, it may choose to restrict access to the risk analysis. This can be achieved through careful document classification and control. Alternatively, risk assessment materials—or portions thereof—might be structured so as to be protected by the attorney-client or work-product privileges.

### ***Anticipate and address barriers to a risk assessment.***

In organizations that do not have a tradition of talking openly about risk, there are a number of barriers to performing comprehensive risk assessments. First and foremost, there is certain to be apprehension about any process that promises to identify organizational weaknesses. Second, there may be some concern that by undertaking a risk assessment the organization is tacitly promising to “fix” all the risks it identifies—an impossible task. Third, senior leaders may believe that their knowledge of the organization is so deep and thorough that an ethics and compliance risk assessment has nothing to teach them. And fourth, a worthwhile risk assessment requires an organization to budget adequate human and financial resources for its completion.

There is no simple way to overcome all these concerns. Those involved in the risk assessment may need to have multiple conversations with many organizational and departmental leaders in order to address their reservations about the process. Another helpful tool is benchmarking. The fact that a competitor has recently conducted a risk assessment may serve as a call to action for those concerned about the organization’s place in the industry.

### ***Identify the types of risks the organization is likely to face.***

The first step in conducting a risk assessment is to identify the universe of potential risks faced by an organization. This list can be drawn from a number of sources, such as the organization’s litigation or claims history, a catalogue of the most-frequent

allegations made to the ethics and compliance office, an inventory of the most common concerns in the industry, and recent public examples of organizational misconduct.<sup>2</sup> In compiling such a list, an organization should be particularly attuned to “gray zone” issues—that is, practices that may be common in the industry but are not yet clearly defined as legal/ethical or illegal/unethical. In this manner, an organization can proactively address emerging risks.

## IN PRACTICE

The inventory of risks should be a very thorough accounting of risks embodied in laws and regulations; organizational and divisional policies and practices; prior and current litigation involving the business; helpline investigations; complaints received from customers, contractors, employees, and others; and any other source of information affecting ethics and compliance. Following are some of the ethics and compliance risks that might be considered:<sup>2</sup>

- ***Bribery and Corruption.*** Risk of national or international criminal investigation, indictment, and/or conviction and fines (of both the organization 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 and Unfair Competition.*** Risk of violation of national or international civil or criminal laws concerning business collusion, conspiracy, and unfair competition.
- ***Privacy and Data Security.*** Risk of noncompliance with data privacy laws of a country in which the business operates, as well as the data privacy transfer protocols between countries.
- ***Harassment and Discrimination.*** Risk of violation of laws and organizational policies concerning workplace conduct pertaining to certain personal categories (gender, race, religion, ethnicity, age, sexual orientation, etc.).
- ***Human Rights.*** Risk of violation of basic human rights concerning employees and others (especially in developing nations) including the use of child labor, slave labor, and other unfair labor practices.

<sup>2</sup> List from: Andrea Bonime-Blanc, “Integrating Ethics & Compliance Risks into Enterprise Risk Management.” *Compliance Week*, October 30, 2006.

- ***Conflicts of Interest.*** Risk that personnel—particularly upper and mid-level management—do not follow applicable conflict-of-interest rules, especially where there is potential adverse impact on the organization’s reputation or finances.
- ***Environment, Health, and Safety.*** Risk of violation of environmental or health and safety laws and policies with an adverse impact on people and/or property.
- ***Whistleblower Protection.*** Risk that an employee who raises good-faith concerns about another employee, vendor, or customer faces retaliation for making such allegations.
- ***Political Lobbying.*** Risk that an improper contribution or political lobbying activity is undertaken on behalf of the organization or an individual employee in violation of law.
- ***Theft, Embezzlement, and Other Financial Misconduct.*** Risk that one or more employees or agents engage in dishonest or criminal financial misconduct including theft, misappropriation of property, or other financial misdeeds.
- ***Fraud and Earnings Management.*** Risk that management engages in the illegal or unethical manipulation or distortion of accounting, financial, or other records regarding the performance and results of the organization.
- ***Money Laundering.*** Risk that the organization knowingly or unknowingly engages in illegal transactions with third parties engaged in laundering funds from illicit activities.

Many of the risks faced by an organization are unique. The particular risk issues for a given organization are influenced by many factors, including:

- Size of the organization
- Nature of the industry or sector
- Organizational structure
- Leadership and governance
- Workforce composition
- External legal, regulatory, and political environment
- Physical environment

- Geographical dispersion of employees
- Vulnerability to catastrophic events, including terrorism
- History of claims, litigation, and external inquiries
- How allegations or violations are handled once brought to light

## IN PRACTICE

Because the array of risks faced by every organization is unique, so, too, is the risk assessment—both its precise methodology and its outcome. There can be no “cookie cutter” or “one size fits all” set of conclusions. For instance, a retail sales organization may determine that employee theft ranks among its most significant risks. A mining operation may determine that environmental impact, health issues, and worker safety rank among its most significant risks. A pharmaceutical corporation, employing sales personnel who have flexibility to set prices, may conclude that price-fixing and other health care fraud concerns rank among its most significant risks. A commercial banking operation may decide that insider trading and market manipulation are among its most significant risks.

### ***Gather both qualitative and quantitative data about these potential risks.***

Ethics and compliance risk assessments should be based on a collection of data from a variety of sources. Risk itself is not easily described or measured. Therefore, it must be inferred from a wide range of data from both inside and outside the organization . Three broad categories of data are generally incorporated into a risk assessment:

- Information about the external legal, regulatory, business, and political environment in which the organization operates.
- Internal perceptions and opinions about frequency and severity of ethics and compliance risks, as well as future or emerging risk areas.
- Historical risk data, as reflected in the organization’s claims and litigation history as well as its internal audit findings.

This data should be both “hard” (typically quantitative measures of claims, audit results, and the external environmental factors) as well as “soft” (typically qualitative descriptions of key individuals’ perceptions about risk, severity, priorities, and potential impact).

“Hard” data may include the following:

- Legal claims history (both at the organizational and operating unit levels) of the organization and its competitors.

- Internal and external audit findings and recommendations.
- Data from the ethics and compliance reporting and advisory functions.
- Stated reserves.

“Soft” data can be more challenging to collect and interpret. Typically, organizations use the most current tools of social science—such as focus groups, interviews, and opinion surveys—to obtain information about how risk is perceived and addressed by a wide variety of individuals, different business units, or organizational functions. Many organizations use a neutral, independent, and confidential researcher—perhaps an outside consultant or academician—to lead the effort to gather qualitative data.

The composition of focus groups and the types of individuals interviewed can vary. Some organizations limit these efforts to upper-level managers, most often from departments such as human resources, legal, ethics and compliance, finance, and audit. It is preferable, however, to include a broad cross-section of individuals to ensure that the opinions and perceptions about risk are as diverse and comprehensive as possible. In either case, it is crucial that the perceptions and opinions about risk be offered freely and without attribution.

## IN PRACTICE

Participants in focus groups and individual interviews should be asked a similar set of open-ended questions. Here is a sampling of questions that might be used:

- What is the single most compelling risk facing our organization today?
- What factors helped you identify this risk?
- Name other compelling risks that face our organization and your operations.
- What factors helped you identify these risks?
- What might help reduce the damage that these risks might cause?
- How effective is our organization (and your business unit) in reducing the damage that these risks might cause?
- Are there any risks facing the organization that “keep you up at night”?
- What kinds of risks could emerge in the next two years that could harm our organization?

Many organizations augment the data from interviews and focus groups by administering surveys. Surveys can reach a broader population and be designed to elicit a wide range of perceptions about risks and their mitigation. Using a numeric scale, survey-takers provide their opinions about the likelihood of each risk and the level of impact.

***Analyze the data gathered and conduct a gap analysis.***

One effective method to analyze data results is to convene a high-level group of organizational leaders and ask them to review the data and offer observations about its meaning and implications for the organization. Depending on the volume of data and availability of key individuals, this type of review can be conducted in the course of a one-day meeting or spread over multiple sessions. When all the risk data is evaluated, themes and trends should emerge that shed light on the nature of the organization's work, significant risk areas, the effectiveness of current risk-mitigation efforts, and gaps in organizational policies and other control systems.

If an organization chooses to evaluate data in this way, it should also consider incorporating employees from outside the risk assessment working group. Eliciting multiple viewpoints will help limit “groupthink” about ethics and compliance issues. In addition, by involving a broad group of individuals, an organization can increase the likelihood that the results of the assessment will be “owned” by leaders and managers throughout the organization rather than being viewed as an exercise that impacts only selected functions.

***Prioritize risks and recommend mitigation strategies.***

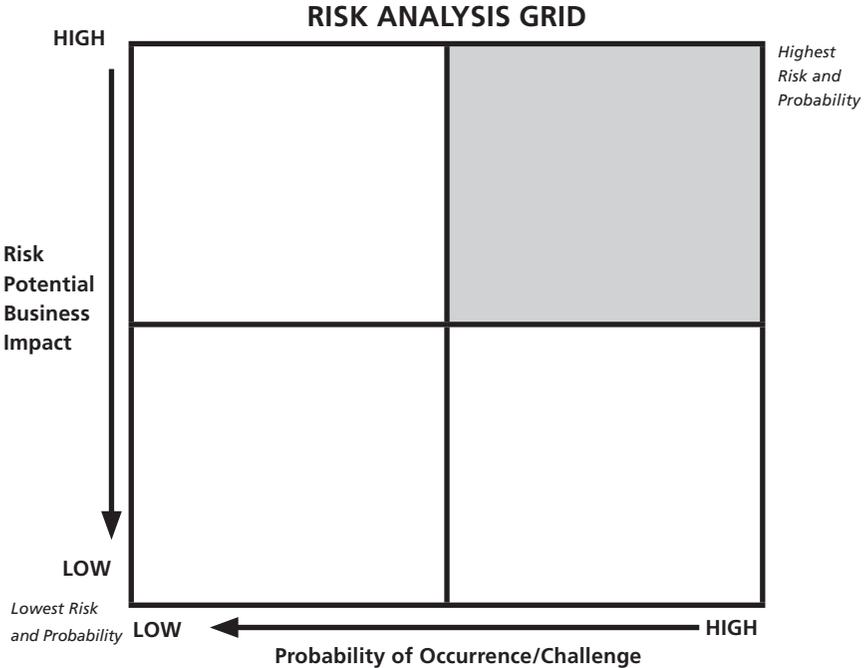
Based on the data-gathering and interpretation sessions, the working group should be prepared to prioritize ethics and compliance risks and recommend how to mitigate them.

By prioritizing risks, the organization can focus its resources on those risks that occur most frequently and/or are likely to have the greatest impact on the organization. Each organization has a different “appetite” or tolerance for risk. That appetite may impact how risk areas are prioritized. When prioritizing risks, an organization should focus on three metrics:

- *Likelihood of occurrence:* By reviewing prior claims and polling knowledgeable employees, an organization can gather data about how frequently a specific risk has arisen in the past. This is critical to understanding the significance of any single risk area. As with many types of human endeavor, past problems are a good predictor of future issues and risks.
- *Severity of the consequences:* An organization should consider the impact

an adverse event would have if it were to occur. The seriousness of the consequences can be measured in many ways, including estimated economic loss, civil or criminal claim exposure, loss of customer or shareholder confidence, breach of employee loyalty, adverse publicity, and overall impact on the organization's ethical culture.

- *Controls already in place:* An organization should account for the controls it already has implemented.



After considering these factors (see Risk Analysis Grid above), the organization should create a list of risk categories that pose the most serious threat to the organization and where adequate controls are not already in place. Of course, other risks should not be ignored, but they may not receive the immediate attention that more serious risks do.

Once risks are prioritized, mitigation strategies and controls should be developed to reduce the likelihood of adverse events, i.e., contain the impact should they occur and improve the ability of the organization to detect problems early. Mitigation steps can include activities such as education and training, new policies and procedures, increased audit activity, new equipment and materials, organizational change efforts, enhanced oversight, or changes in management and reporting structures.

Mitigation may also require discontinuing a product line or ceasing to do business in a particular jurisdiction.

***Present results of the risk-assessment process to those with a need to know.***

The final product of the ethics and compliance risk-assessment exercise should summarize the risk profile of the organization, identify gaps and opportunities for improvement, set the ethics and compliance strategy for a specified period of time (e.g., 3–5 years), and shape the direction of the ethics and compliance program and related operations. This document should record how the assessment was conducted and, to the extent possible, include an action plan for addressing specific risks.

In some organizations, senior management formally adopts the findings and recommendations of the risk-assessment group, thereby making the results of the assessment official and binding. In other organizations, approval by senior management is presumed, particularly if the organization has convened a high-level group to review data and identify trends.

## IN PRACTICE

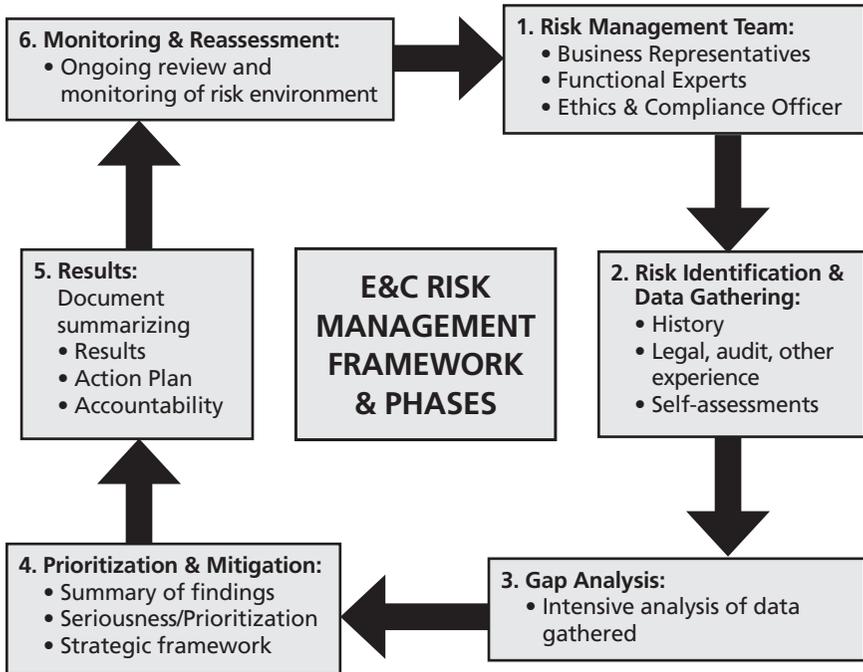
If the potential for bribery of a foreign government official is identified as a high-priority risk, the action plan might include steps such as:

- Revise and reissue policies on the U.S. Foreign Corrupt Practices Act.
- Design targeted training and certifications of compliance for sales personnel involved in sales to government customers.
- Prepare briefings for the board of directors and executive officers.
- Issue guidance on how to retain foreign agents and representatives.
- Require an approval process before a sale to a foreign government is consummated.
- Preapproval for gifts, entertainment, or any expenditure on a foreign government official.
- Review related policies on gifts and entertainment.
- Monitor gift and entertainment reports.

The ethics and compliance office may be tasked with ensuring that the actions and mitigation strategies are communicated to those responsible for implementation. Senior management may also request regular updates on progress toward implementing the plan. Finally, the board of directors should be briefed on the risk-assessment process and its results.

***Commit to updating and revising the risk-assessment process on a regular basis.***

Risk assessments should not be static. The business environment and operating models of organizations change regularly, as does the external legal and regulatory environment. The risk assessment should be updated regularly so that assumptions and perceptions about risk can be charted and tracked over time. (See E&C Risk Management Framework & Phases chart below.) A periodic assessment provides an opportunity to step back and assess how well the mitigation strategies have worked and identify new or emerging risks that were not previously considered.



While the Sentencing Guidelines state that risk assessments should occur “periodically,” they do not define the term. Many organizations update their risk-assessment exercises every three to five years. Depending on the particular organization, however, the assessment may be conducted more frequently. The goal should be to determine a schedule that allows the organization to detect and prevent the unique array of ethics and compliance risks it faces.



# Learning to Harmonize

To manage for potential threats, Emory University worked from the most basic operational level upward to fine-tune a strategy that's now part of its overall planning process.

By Shulamith Klein, Michael Mandl, and Stephen Sencer

Over the past two years, Emory University, Atlanta, has built an enterprise risk management system tailored to the higher education environment. The process, which involved more than 100 staff and faculty, was a useful and productive experience for Emory, and the resulting ERM system is now integrated into our planning and evaluation of administrative issues. It is not perfect, it does not rely on outside consultants, and it does not use three-dimensional cubes. But, it does constitute a significant step forward in Emory's ability to manage its risk, prepare for adverse occurrences, and ensure that senior management is communicating with those in the field about key issues facing the university.

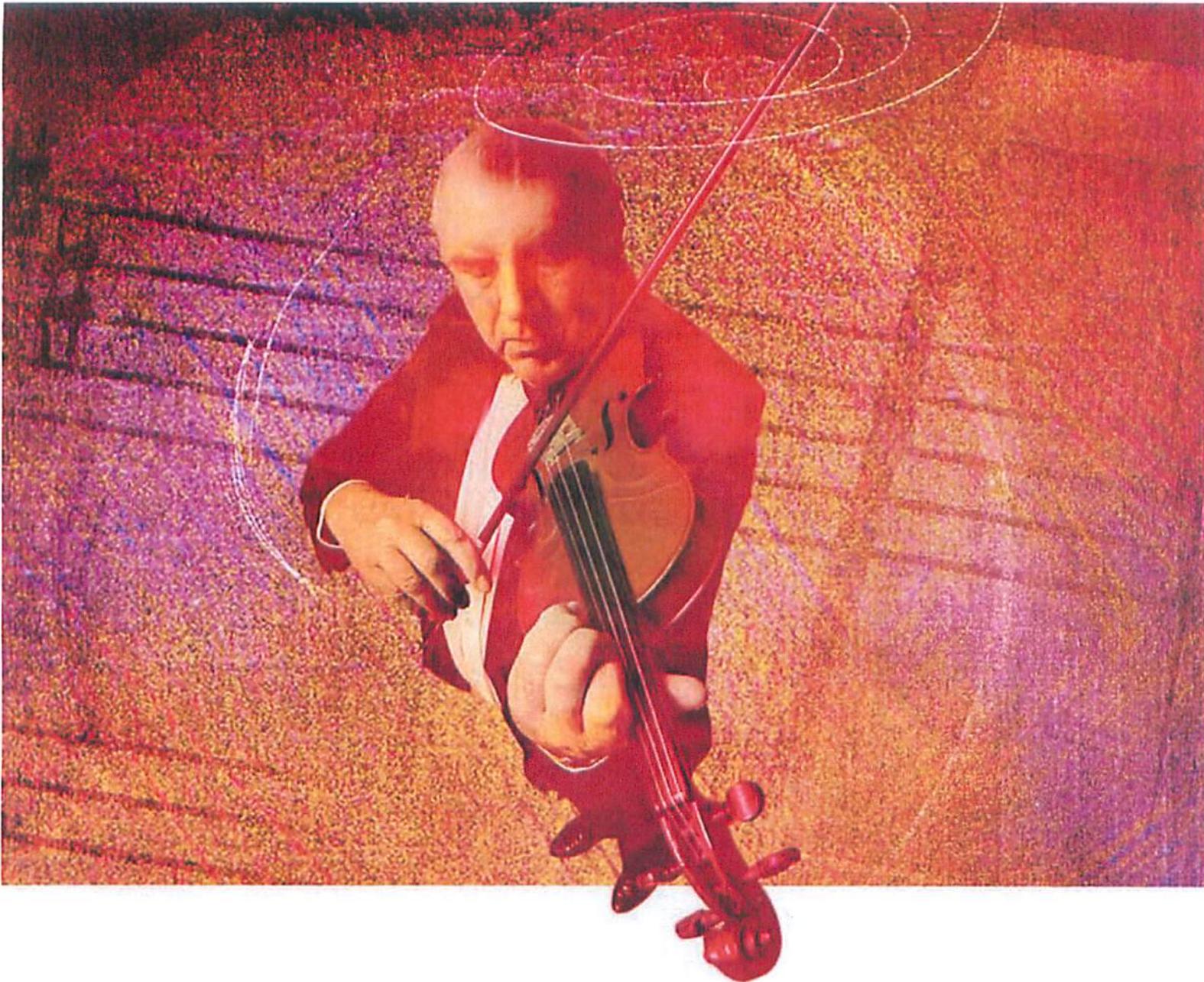
## ERM's Emergence

The ERM process began at Emory when a number of developments, some national in scope and others unique to our campus, focused attention on corporate governance. On the national level, notorious corporate governance failures such as Enron and WorldCom had heightened scrutiny of all large corporations, including nonprofits. In addition, several higher education institutions had been publicly criticized for failing to handle adverse events effectively, with the allegedly inadequate response gaining as much or more attention as the underlying event.

At Emory, a new executive team—the president, provost, and executive vice president for finance and administra-

tion arrived within the same year—was developing a comprehensive strategic plan and launching a capital campaign. Senior leadership wanted donors and other stakeholders to be confident that Emory was a worthy investment. Furthermore, Emory's leaders wanted a set of principles and practices in place to ensure adequate financial controls and to guide the university's response to adverse events.

As it happened, the chair of Emory's audit and compliance committee, a bank executive, was familiar with ERM's merits. His portrayal of ERM appealed to Emory's president, an engineer by training who was attracted to ERM's systematic approach to a historically intuitive exercise, and to Emory's executive vice president for



finance and administration, who focused on unanticipated events that could hurt the university's effectiveness. Both believed that ERM would provide immediate and tangible value to Emory, and they asked a team of administrative leaders to create a process.

Because ERM is relatively new to higher education administration, we couldn't find an off-the-shelf product to incorporate into Emory's practices. (For more about ERM, see "Ensemble Performance" on page 14.) A literature review—including Committee of Sponsoring Organizations of the Treadway Commission (COSO) materials, white papers, and material available on the Internet about other higher education ERM practices—revealed that

many models exist for ERM. None of these sources, however, nor the several consultants eager to ply their trade, provided an existing protocol that Emory felt would result in a practical yet substantive ERM process conducive to widespread involvement and organizational ownership.

We did, however, have a clear idea of what we wanted ERM to accomplish, which we captured in a set of five objectives. First, the ERM process should identify the risks, particularly those that could significantly interfere with Emory's mission. Second, it should assess the major risks, identify vulnerabilities, and help management decide either to accept the existing risk level or invest additional resources to mitigate it. Third, it should

detail a plan for operational and communication responses to potential adverse events. Fourth, it should build processes to implement these plans. Finally, ERM should help eliminate surprises.

### **Building an ERM Team**

A university environment does not generally lend itself to top-down instructions, and an ERM process that dictated, rather than persuaded, could have been a waste of time. Moreover, if the initial goals were too abstract, ERM would fail to garner the broad support needed to have a significant impact. In an effort to engage as many people as possible in a productive manner, we created an ERM organizational structure with each group having distinct and

clearly defined roles and deliverables:

- An ERM executive committee, chaired by the president and consisting of senior executives, including the CEO of Emory Healthcare, which sets the general direction and reviews the entire range of risks facing Emory.
- An ERM steering committee, consisting of operational vice presidents and other senior administrators, which is the central coordinating body for the ERM process.
- Eight ERM subcommittees, each consisting of a handful of administrators organized around subject matter areas—academic and student affairs, campus safety and physical plant, finance and investment, governance and corporate affairs, health care, human resources, information technology, and research—whose members identify, analyze, and communicate about risks in their respective areas.

The steering committee, whose members have broad exposure to the range of risks facing the institution, was the core working group that led the development of the ERM process. Relying on a group of senior administrators rather than one individual or office was an effective decision, so that ERM did not become the “turf” of a single department. Shared ownership and accountability motivated the entire committee to produce.

### Getting to Guiding Principles

Setting the right tone about Emory’s tolerance for risk was critically important. With the teams in place, the first step was to agree on a set of guiding principles. After several iterations, the principles emerged, beginning with a general statement about risk:

Risk, in one form or another, is present in virtually all worthwhile endeavors. We recognize that not all risk is bad and our goal is not to eliminate all risk, for by doing so we would cease all productive activity. Rather, our goal is to assume risk judiciously, mitigate it when possible, and prepare ourselves to respond effectively and efficiently when necessary.

This attitude was liberating. Many administrators assumed that executive leadership wanted to eliminate risk, an assumption that raised unneeded bureaucratic obstacles. By starting the process with a declaration that not all risk is bad, the guiding principles changed the tone of risk discussions.

In addition, the principles contain several operational commands, the most important of which address how Emory deals with adverse events. Again, this required balancing various pressures. Among the key principles:

- All individuals are empowered to report problems and concerns early on, without fear of retribution.
- Investigations of adverse occurrences, complaints, and concerns are conducted with integrity and continue until the fact-finding process is concluded.
- Communication with the campus community and the public at large is proactive, honest, and respectful of individual privacy.

### Assessing the Risks

Next, we conducted a risk assessment. The search for an existing generic list of risks facing higher education institutions was fruitless. (In hindsight, this may be attributable to Emory’s initial focus on operational risks.) Our philosophy was to start with the university functions and work up toward strategic analysis. ERM literature often takes the opposite approach, encouraging an initial engagement at the strategic level. Concerned that such an approach would be too abstract, Emory decided to stay with the bottom-up approach.

Each of the ERM subcommittees was then asked to brainstorm and develop a list of every risk within its domain, ranked as to likelihood of the adverse occurrence and severity of the harm should the event occur. Groups were instructed not to worry about overlapping risks and to think expansively with the knowledge that others—the ERM steering committee—would weed out duplications. With that instruction, the subcommittees identified some 555 risks, each of which was rated on a four-point scale for both severity and likelihood.

Initially, that number was daunting, but close examination revealed duplications as well as efforts to draw unnecessary distinctions. “Breach of confidentiality” in its many forms is a good example of what came to be known as the “taxonomy” challenge. The risks on a university campus do not fall neatly into buckets; our subcommittees identified several “species” of confidentiality breaches. At the “genus” level, so to speak, a breach of confidentiality might be described as any unauthorized release of confidential information and could occur in many environments (such as health care, research, or student records). At the “species” level, however, an administrator charged with managing a potential breach of confidentiality knows that the seriousness and consequences may be very different depending on the cause and context.

Understanding the need to balance these taxonomic challenges, the steering committee culled through the list, eliminating duplicates and editing descriptions for consistency, reducing the list to 141. The committee then reassessed the frequency and severity of each risk. Doing so, we found that giving equal weight to both likelihood and severity inaccurately skewed the rankings, as it overrated risks that are certain to occur yet have a moderate impact to the university, and underrated risks that are unlikely to occur yet would have a catastrophic impact.

For example, petty theft happens frequently and is a problem we would like to eliminate, but its impact on the university will never be crippling. Conversely, an influenza pandemic is unlikely but would be catastrophic. Because the latter is more critical for ERM purposes, a multiplier was applied to the severity factor.

A list of 141 risks, however, was considered too cumbersome, so we shared only the top 50 risks (as ranked through the frequency and severity analysis) with executive leadership, who fortunately found little to change. Had there been glaring omissions or perceived overinflation of risks, the process itself would have become suspect and ERM as a tool would have lost credibility.

## A Detailed Analysis Plan

Once we had the list of key risks, the difficult part began. For the process to work, we needed a written analysis of each risk; without a written document, it would be too easy to avoid difficult issues. But, the steering committee was hypersensitive about asking administrators to engage in internal memo-writing without solid justification. Instead, we developed a process that combines a written analysis with a face-to-face dialogue between the authors of the analyses and the ERM executive committee.

First, we identify a risk management process owner for each risk. The RMPO (an acronym that entered the Emory lexicon) is defined as the person on campus "sufficiently familiar with the risk and best positioned to execute a comprehensive risk management plan." Notably, an RMPO is *not* necessarily the "owner" of the risk, in that often the RMPO may not have operational responsibility with respect to the risk.

Second, we instruct each RMPO to prepare a risk management plan of no more than two pages. The plans follow a template that describes (1) the risk, its components, and examples; (2) the steps being taken to manage the risk at an acceptable level; (3) the operational response to an adverse occurrence; and (4) the communication response to an adverse occurrence. We decided to limit plans to a rigid format, recognizing that if left open-ended, some were likely to be lengthy yet still fail to answer the key questions.

Effectively selling the ERM concept to the RMPOs and asking them to prepare risk management plans was crucial; without buy-in from the RMPOs, the process would flounder. Our president became our chief advocate. He conducted the first meeting, introduced the ERM concept and details, and demonstrated that he understood and valued the process. His grasp of the small details convinced the RMPOs that the process had his support and, perhaps more to the point, that their failure to fulfill obligations would come to his attention.

Third, face-to-face dialogue occurs with presentations to the ERM executive committee—effectively, the president's cabinet—at least once a year. Groups of similar risks are presented at the same time in quarterly "risk hearings," each about three hours in length. Each risk is allotted one PowerPoint slide and five minutes of presentation, followed by five minutes of questions and answers. Rigorous enforcement of that rule allows 12 to 15 risks to be presented at each sitting and allows all 50 risks to be covered in four quarterly sessions.

**The risk hearings are the most effective part of the entire process. For executive leadership, it is an opportunity to learn about a range of risks.**

The first risk hearing was devoted to the subject area of campus safety and physical plant. We selected this topic because the Virginia Tech tragedy was still a fresh memory, and, as expected, there was frank discussion about Emory's preparedness and our processes for preventing such an event. Student mental health and related possible violent acts are a prime example of the need for ERM.

Preventing a tragedy from occurring requires groups from across the enterprise—the institution—to collaborate. At Emory, the ERM process generated a threat assessment team, with representatives from law enforcement, student affairs, public relations, general counsel, student mental health, and others, who meet regularly for confidential review of potentially threatening circumstances. That sort of collaboration has traditionally been a challenge for the decentralized university, and ERM facilitates a mechanism for crossing departmental "silos."

The risk hearings are the most effective part of the entire process. For executive leadership, it is an opportunity to learn about a range of risks, assess them in rela-

tion to each other, and probe weaknesses or strengths unmediated by intervening managers. For the RMPOs, it is a chance to have the ear of the president and his senior advisers on an issue that the RMPO knows best and typically deals with on a daily basis.

Fourth, at the conclusion of each risk hearing, the executive committee identifies any gaps between Emory's risk tolerance and our current status with respect to specific risks. From this information, RMPOs are directed to prepare an action plan for closing the gaps that they will present to the committee at the next meeting.

Finally, we periodically re-evaluate the list of risks. Inherent in the ERM framework is the recognition that priorities change over time; therefore, the risks are expected to shift in response to changes in the operating environment.

## A Process for Sharing Knowledge

Emory's ERM process development has been a learning experience. The lessons we have learned likely have value to any higher education institution attempting a similar process.

■ We found it necessary to repeatedly explain ERM. Administrators make decisions that involve risk every day, so incorporating risk in the analysis is not a new concept, and it can be insulting to suggest to an experienced administrator that considering risk in an institution's decision making is a novel idea. Our approach was to implement a process that had immediate benefits and that involved specific inputs from various individuals. We set reasonable expectations, and people were involved in ways that made sense to them. ➤

## Emory's ERM process primarily focuses on operational risks and does not attempt to replace the valuable strategic planning processes that Emory engages in regularly.

■ The ERM literature has its share of "consultant-speak." We made a significant effort to translate ERM to an audience with limited time and energy to devote to an enterprisewide initiative. Clear instructions, requests for specific deliverables, and the use of templates were helpful. Even if people did not grasp the concept initially, they understood their personal obligations.

■ Because we were asking for a significant commitment from many across the institution, the president's active involvement

was critical. Everyone knew that the president was enthusiastic about ERM and was expecting results.

Emory's ERM process primarily focuses on operational risks and does not attempt to replace the valuable strategic planning processes that Emory, like most other higher education institutions, engages in regularly. Indeed, campus leaders can overemphasize strategic planning at the expense of the critical day-to-day operations. Failure to attend to the latter—and

to manage the risks inherent in those operations—can disrupt in an instant the most carefully constructed strategic plan. ERM at Emory plays an important role in sharing knowledge about specific operational risks and collectively developing and communicating an appropriate risk tolerance.



**SHULAMITH KLEIN** is senior director, Office of Risk and Insurance Services, Emory Healthcare and Emory University, Atlanta. **MICHAEL MANDL** is executive vice president and **STEPHEN SENCER** is deputy general counsel at Emory University.  
[shulamith.klein@emoryhealthcare.org](mailto:shulamith.klein@emoryhealthcare.org)  
[michael.mandl@emory.edu](mailto:michael.mandl@emory.edu)  
[steve.sencer@emory.edu](mailto:steve.sencer@emory.edu)



## Building an Enterprise Risk Management Program for A Small to Medium Size Company: Essential First Steps

Contributed by: Andrea Bonime-Blanc, Esq. Daylight Forensic & Advisory LLC

### *Introduction*

We have all heard about ERM or Enterprise Risk Management especially in the past few years. ERM is the practice of building a company-wide risk management program to identify, manage, mitigate and eliminate a wide diversity of risks – from financial and operational risks to political and compliance risks. Whether they have formally put ERM into place or not, most large, international companies have some type of program in place developed organically over time. As these companies have encountered risks, they have developed mitigation strategies and tactics to manage such risks. Most of these larger, established businesses know that they need policies and protocols to keep up with the increasingly complex, unpredictable and risky business world.

Just because a company is relatively small or medium in size does not mean that it does not have a similar set of risks to confront in a business environment that is equally (or even more) complicated for smaller to medium size players (“SMC”).<sup>1</sup> Indeed, in the absence of some form of ERM, the impact of an unidentified, unmanaged risk can be far more devastating to a SMC. A risk that blows up into an uncontrollable reputational or financial conundrum may be much harder for a SMC to tackle successfully and overcome because of the very size and resources available to a SMC. Thus an unattended risk can have an even greater impact on a SMC, threatening not only the viability of its current business cycle but also potentially its long term survival.

Larger, more established companies have had the relative luxury of time, resources, experience or regulatory pressure to develop strategies and programs to address risks. The same cannot be said for most SMCs. A SMC may not have been around for very long and has not become aware of the need for an ERM program. Or a SMC may not have the internal experience or resources necessary to create a formal ERM program. It is also possible that because a SMC does not have (or does not think it has) the same regulatory and legal pressures that a larger company has, building an ERM program does not appear on its radar screen. Or a SMC may have been lucky not to encounter a “life-threatening” risk yet and thus continues to do business as usual.

The bottom line is that SMC need an ERM program as much as larger more established companies do. We may be witnessing the beginnings of the next major micro-trend in global business as SMCs seem to be proliferating as a new, more nimble form of business in the 21<sup>st</sup> century. The advent and development of the Internet, social networking and other virtual tools has made it much easier to be a smaller player in a global business world. For these reasons and more, SMCs should attend to their risk profiles, understand how to address and mitigate their risks and build some form of customized ERM program into their strategy and corporate DNA. This article identifies six critical steps for SMCs to develop such a customized, useful and un-bureaucratic form of ERM.

### *Step I: Setting up a Risk Management Committee*

The best way to set up a risk management committee is for two to three key leaders in a SMC – the chief financial officer, the general counsel, the controller, a business head, an operational manager or the chief operating officer — to get together to brainstorm who within the SMC would be best to include in a risk management committee (“RMC”). Depending on the expertise available within the company, the key business lines, the geographical spread and the extent of regulatory and legal risk, it should become clear fairly quickly who should form part of the RMC. The RMC should not have more than three to five members and should be a nimble body that avoids clutter, bureaucracy and inaction. The RMC can draw on additional internal (and external) subject matter experts from time to time who should be brought into meetings and projects for specific advice and analysis. It may also be useful to have a high level administrative person or junior business person become the “secretary” to the RMC to take notes, prepare reports and manage action items from meeting to meeting. Finally, the real work of the RMC will be done through a network of company contacts who will be the local or subject matter experts who will help to fill in the specifics of risk at the grass roots level of the company on an initial basis through an initial risk assessment (“IRA”) as discussed below and on an annual or periodic basis thereafter.

### *Step II: The RMC Mission & Charter*

Once the RMC team has been identified, the first order of business is to develop a draft mission statement and “charter” for the RMC and present this proposal to the chief executive officer and even the board or governing body of the SMC for approval and blessing. A simple yet effective mission statement might state something along the following lines:

“The mission of the RMC is to identify, inventory and analyze the most important risks facing the SMC and develop an overall strategy and specific tactics to prevent and mitigate such risks on an ongoing and periodic basis.”

The charter of the RMC can be a simple list of the following key elements:

- A.) Who forms part of the RMC
- B.) Who is chair and secretary of the RMC and how that role is assigned, rotated or otherwise filled
- C.) How often the RMC meets and makes decisions
- D.) The principal tasks and activities of the RMC
- E.) Who the RMC answers to – the CEO, COO and/or board
- F.) How often and to whom the RMC provides official ERM reports – whether interim, monthly, quarterly or annual

*Step III: Embracing the Initial Risk Assessment*

The next step the RMC must take is to identify a core group of qualified individuals in each business line or geographical area to be brought into the IRA process. They may be members of the operations team, controllers at each business or regional location, members of the legal team or other business functions. The key to success is to recruit responsible individuals who will work with the RMC on the IRA in a timely and responsible manner.

There are different ways in which the IRA can be conducted, but by way of an example, the following pieces should be included:

- A.) IRA Project Manager. Appoint a project manager to conduct IRA. This can be a member of the RMC or someone else who is well organized and senior enough to command respect from the rest of the company.
- B.) Q&A Document. Prepare IRA question and answer document providing the why's and what's of the IRA.
- C.) ERM Framework. Have a document outlining the major categories of risk described in Step IV below, identifying some that the RMC has already singled out and asking questions to elicit further inputs from the business lines and administrative functions.
- D.) Information Network. Create a network of competent information providers within the company. This group should be small but diverse enough to be able to tackle the wide variety of issues that may be identified as risks.

- E.) Risk Brainstorming Sessions. Have brainstorming sessions at the business lines and/or geographical areas. These can be conducted ideally in person but also virtually through webcasts and other social networking tools.

*Step IV: The ERM Framework: Identifying the Universe of Risks*

Once the RMC has been put into place, the most important substantive exercise the team must tackle is identifying the SMC's universe of risks. Once the larger risk categories are identified, the more painstaking exercise of identifying specific risks can take place.

Each company has a different risk profile based on its business focus, geographical area of activity, whether it is publicly listed or not, highly regulated or not. and type of business. However, for most businesses the larger categories of risk will not differ substantially although there will always be a need to customize to the specific business. Table 1 provides an overview of one way to categorize overall business risks:

<b>Table 1: The ERM Framework: Identifying the Universe of Risk</b>
• Financial and Operational Risk
• Political Risk
• Governance Risk
• Compliance & Ethical Risk
• Third Party Risk
• Business Continuity & Crisis Management Risk

- A.) Financial and Operational Risk. These kinds of risks lie at the core of the business. They would include the specific business cycle, contractual, inventory, supply and demand, credit, insurance and other financial and operational risks particular to the business. The inputs of leading business and financial people within a company including that of the chief financial officer, head of insurance, controller and specific business heads is critical for this exercise to be complete and properly focused.
- B.) Political Risk. Depending on where a company does business, it will have to get its arms around what is called "political or regulatory" risk. Within this larger category of risk it is possible to identify several nuances:
- i. The Government as Client. The risk of doing business with a government or one or more of its agencies (whether fully or quasi-governmental) with the attendant issues of corruption, bribery, procurement fraud.
  - ii. Political Stability. The risk of political regime stability in the regions or countries

it does business in.

- iii. Violence. The risk of violence or other forms of bodily or property risk not only if doing business physically in that location but also if importing or exporting goods or services to that location.
- iv. Regulatory and Judicial Transparency. The risk of regulatory and judicial transparency and predictability. In other words, is the institutional political framework within a country able to provide the SMC with a predictable and transparent set of rules or is a business at risk that if it has a contractual dispute with a local entity, for example, that it will receive independent and appropriate judicial treatment?

C.) Governance Risk. All companies have some form of governance – whether they are privately held, publicly traded, partnerships, limited liability companies, quasi-governmental entities, academic institutions or non-profits. All governance bodies need to act in a predictable and transparent manner through periodic meetings, the keeping of minutes, the passing of appropriately vetted resolutions and the proper vetting of conflicts of interest. The governance mishaps of many major corporations over the past decade have amply demonstrated that when governance is weak, a company can suffer seriously negative consequences.

D.) Compliance and Ethical Risk. There is a category of risk many businesses fail to identify in their ERM and which if left unidentified and unmanaged can create serious problems for a business up to and including dissolution. Table 2 outlines only some of the many ethical and compliance risk that should form part of any company's inventory of risk:

<b>Table 2</b>
<b>Examples of Regulatory, Compliance &amp; Ethical Risks to include in an ERM</b>
• Antitrust and unfair competition
• Anti-bribery and corruption
• Anti-money Laundering & OFAC compliance
• Conflicts of interest vigilance
• Environment, health and safety
• Government and regulatory relations
• Harassment and discrimination
• Privacy compliance and data security
• Political lobbying. parameters

- |   |
|---|
| • Human rights and corporate responsibility |
| • Whistleblower mechanisms and protection   |

- E.) Business Continuity & Crisis Management Risk. All companies have employees. All businesses – even the smallest, most virtual ones — have property, offices or other assets. Thus, all businesses need to have some form of contingency planning – for a physical location emergency (such as a natural disaster where employees live), a business emergency (when company records are destroyed by a computer crash), or a personal emergency (an employee has an accident while traveling on business). To avoid the risk of harm to employees and loss or destruction of company property, as well as to be able to restore business operations as quickly as possible in an emergency, all companies, including SMCs, must have some form of crisis management and business continuity plan in place.
- F.) Third Party Risk. Third party risk is a category of risk that many companies don't think about until it is too late. There are several subcategories of third party risk that all companies should focus on:
- i. Employees and Subcontractors. Employees and subcontractors must be vetted in advance to minimize or eliminate the risk of hiring people with criminal or other questionable backgrounds or having reputationally challenged individuals representing the business.
  - ii. Vendors and Suppliers. This is the risk of hiring suppliers or service providers who produce shoddy products (that can lead to product liability, e.g.), provide substandard services (that can lead to design failures, e.g.), or engage in illegal activities affecting the company (that can lead to accusations of bribery and corruption, e.g.).
  - iii. Clients and Customers. The primary risks involving clients include: (i) non-payment or late payment for products or services; (ii) insufficient, deficient or non-existent contractual rights when things go wrong; and (iii) client reputational damage that somehow becomes associated with the company.
  - iv. Business Partners. The risk with business partners is clear – if they do not conduct business with integrity, or they have credit issues, or there are significant lawsuits or liens against them, entering into business with them can not only taint a company but may also drag it into the partner's mess.

Most businesses will find these larger categories to be useful in building an ERM framework. However, depending on the business, there may be additional categories. A consumer products business would have a category for product liability risk. A pharmaceutical or health business would target the risk of not obtaining regulatory approval for new

medicines. For a business in the extractive or natural resources area, geological risk will be critical. And so on.

*Step V: Translating Your Risk Universe into an Action Plan*

Once the RMC and project manager for the IRA have gathered all possible information through the work described in the foregoing steps, it is time to pull it all together into a manageable, readable document that allows the risks to be clearly described and perhaps even measured or quantified. There are many and different ways to do this and it is not the purview of this article to review and describe all of these possibilities. Suffice it to say, that the key objectives of this part of the IRA exercise are to ensure:

- i. That all relevant business lines, geographical areas and key functional parts of the business have had an opportunity to participate in the IRA
- ii. That sufficient discussion has taken place at the executive level of the organization requiring input from the heads of the business lines and administrative functions
- iii. That a carefully prepared and thought through IRA report has been put together outlining the major categories of risk and identifying and analyzing each major risk
- iv. That all identified risks have been prioritized from most to least risky with a rationale as to why such a characteristic has been assigned to each risk
- v. That for each risk identified there is a suggested solution or action item to mitigate or eliminate such a risk

*Step VI: Embedding the Process and Answering to a 'Higher Authority'*

The final and absolutely critical link in the chain of a successful ERM – no matter how big or small the company – is to tie the findings of the IRA back to senior management and the governing body of the company – its shareholders or owners, and board of managers or directors. Both at the beginning of the process – when a company decides to undertake an ERM, create a RMC and conduct an IRA – and at such time as the IRA has been completed to the satisfaction of the RMC, the governing body of the organization needs to be informed and their consent or blessing provided to secure the success of such an important undertaking. Communications with the governing entity should be formal and made part of the official agenda of their quarterly or annual meeting, especially when the IRA report is produced at the end of the initial risk management exercise for the SMC. However, an IRA is only the beginning of a successful ERM – after all it is the “initial risk assessment”. Going forward, the RMC must continue to manage its risks proactively and periodically. It should undertake a new risk assessment – depending on the organization perhaps annually – that builds on the findings of the previous risk assessment and allows for the identification and management of new risks that have not been previously identified.

<b>Table 3: The Five Essential Steps to Create a SMC ERM</b>
• Set up a Risk Management Committee
• Create a RMC Mission & Charter
• Embrace the Initial Risk Assessment
• Identify the Universe of Risks and set up ERM Framework
• Translate Your Risk Universe into an Action Plan
• Embed the ERM Process and Report to Senior Management & Board

Thus, an SMC can have an ERM that is customized to its needs, isn't bigger or more complicated than it needs to be and isn't expensive to run as it makes use largely of internal resources. A successful ERM may also have a more subtle but nevertheless dramatic impact on the very existence and viability of an SMC: it can improve the bottom line by identifying risks before they blossom, it may avert the unraveling of an unattended risk that could threaten the very existence of the SMC and it can bolster the reputation of a business as a solid, ethical and reliable partner, supplier or service provider with a host of key stakeholders such as clients, regulators and employees.

*Andrea Bonime-Blanc, Esq. is General Counsel, Chief Compliance Officer & Corporate Secretary of Daylight Forensic & Advisory LLC, an international regulatory and advisory firm. Ms. Bonime-Blanc is a member of the Board of the Ethics & Compliance Officer Association and recently co-authored/edited The Ethics & Compliance Handbook: A Practical Guide from Leading Organizations, published by the ECOA Foundation in 2008.*

---

<sup>1</sup> In this article, SMCs are defined as companies with one or more of the following characteristics: (1) under 2000 employees; (2) under \$100M in revenues; (3) privately or closely held; and (4) not highly regulated.

# 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.