Association of Corporate Counsel

By in-house counsel, for in-house counsel.®

InfoPAK℠

Framework for Conducting Effective Compliance and Ethics Risk Assessments

Sponsored by:

corpedia
ETHICS. ELEVATED.

Association of Corporate Counsel
1025 Connecticut Avenue, NW, Suite 200
Washington, DC 20036
tel 202.293.4103, **fax** 202.293.4701
www.acc.com

Framework for Conducting Effective Compliance and Ethics Risk Assessments

August 2008

Provided by the Association of Corporate Counsel
1025 Connecticut Avenue, NW, Suite 200
Washington, DC 20036
Tel 202.293.4103
Fax 202.293.4701
www.acc.com

This InfoPAK[SM] is designed to provide corporate counsel with a general overview of the concept of risk assessment and to suggest useful practices for the handling of such in the corporate setting. It is based upon examination of more than a dozen leading organizations' risk assessment methodologies and was authored/compiled by Corpedia, Inc., the leading provider of ethics and compliance program solutions.

The information in this InfoPAK should not be construed as legal advice or legal opinion on specific facts, and should not be considered representative of the views of Corpedia, Inc. or of ACC or any of its lawyers, unless so stated. Further, this InfoPAK is not intended as a definitive statement on the subject and should not be construed as legal advice. Rather, this InfoPAK is intended to serve as a tool for readers, providing practical information to the in-house practitioner.

This material was compiled by **Corpedia, Inc.**

For more information about Corpedia, please visit their website at www.corpedia.com or see the "About the Author" section of this document.

Contents

TABLE OF FIGURES

I. Glossary

Below are summary definitions of some of the terms used in this InfoPAK[SM].

A. Enterprise Impact

A product of risk severity and likelihood of occurrence, Enterprise Impact is the significance or effect (either positive or negative) that a unique risk or risks can have on an organization.

B. External Aggravating Factors

The factors (political, legal, environmental, socioeconomic, etc.) outside of the actual organization, which play a role in subjecting the organization to heightened risk.

C. Internal Aggravating Factors

The factors specific to an organization's unique circumstances or operation. Such factors can be identified through a number of methods, including, but not limited to, interviews, assessments/surveys, examination of available policies and procedures, financial reporting, etc.

D. Internal Mitigating Factors

These pertain to specific elements unique to the organization that can provide a reduction effect to identified risk areas relevant to the organization.

E. Occurrence Likelihood

The reasonable likelihood of a risk event occurring for a typical or average company in a given industry.

F. Risk Severity

The maximum potential economic outcome of violation or misconduct for a typical company in a given industry, measured in terms of total enterprise impact.

G. Risk Area Weighting

Practice of assigning unique values or ratings to areas of risk, where the specific weights are quantified by both impact and likelihood of occurrence.

H. Risk Assessment Team

Collection of individuals or employees of an organization tasked with the re-

sponsibility of researching and evaluating the overall environment of risk in the organization, as well as recommending future action to manage identified risk areas.

I. Risk Universe

This term pertains to a catalog or inventory of identified risk areas relevant to the subject organization.

J. Sarbanes-Oxley § 404

Pertains to the information detailed in Section 404 of the Sarbanes-Oxley Act of 2002 ("SOX 404"). This section outlines the requirements for a publicly traded organization to present a Management Assessment of Internal Controls when issuing an annual report.

K. PCAOB Auditing Standard #5

Pertains to AS#5 that recently replaced AS#2. Approved by the SEC in July 2007, AS#2 is aimed at improving the accuracy of financial reports while reducing unnecessary costs, especially for smaller companies. The standard allows management to rely on assessment of internal controls by other independent managers when certifying to the effectiveness of internal controls to meet SOX 404 requirements.

II. Introduction and Overview

In this era of heightened expectations for proactive corporate governance and compliance with the Federal Sentencing Guidelines for Organizations (FSG) and the Sarbanes-Oxley Act, more institutions are looking to develop effective risk assessment procedures to help: (1) meet Federal Sentencing Guidelines; (2) prioritize compliance program initiatives and spending; (3) provide a roadmap for improving compliance programs to reduce the likelihood of any material violations of federal, state, and foreign jurisdiction laws and regulations; and (4) demonstrate good-faith compliance efforts in the event of civil or criminal proceedings.

While the reasons for conducting a risk assessment are apparent, the overall process and methodology for developing and implementing such an endeavor are less clear. Some of the questions commonly posed by ethics and compliance professionals include:

- How often should risk assessments be performed?
- Should the process be managed by an external third party or can it be performed internally?
- How should risk areas be prioritized, weighted, or ranked?
- Which internal stakeholders should be involved?
- What type of report should be generated and for which audience?
- How should a risk assessment be conducted to provide a strong legal defense in criminal or civil proceedings?
- What type of risk assessment will meet Federal Sentencing Guidelines criteria?

This InfoPAK, based upon examination of more than a dozen leading organizations' risk assessment methodologies, will help address the above questions.

III. What is a Risk Assessment and Why is it Important?

Risk is defined as an uncertain event or condition that, if it occurs, has a positive or negative effect on the entity to which it is tied. The key word is "uncertainty," and as such, it is incumbent upon organizations to proactively and responsibly engage in a process where risks are identified and analyzed, and where strategy is developed to manage or mitigate those risks. The process is commonly known as "risk assessment." It is important to note that other disciplines consider risk assessment and its related activities as an element of a larger enterprise risk management program. Such a claim is valid, but for the purposes

of this paper, we will focus on the specific role and associated tactics and processes of risk assessment as they apply to completing an ethics and legal compliance risk assessment.

Parsing the actual components of a risk assessment, we have the following[1]:

- *Risk Identification* – determining which risks are relevant to the organization and documenting their characteristics.
- *Qualitative Analysis* – prioritizing risks for subsequent further analysis or action by assessing and combining their probability of occurrence and impact.
- *Quantitative Analysis* – numerically analyzing the overall effect of risks on the organization.
- *Defining Risk Appetite* – To properly prioritize risks for setting compliance priorities, management must define its risk appetite (whether financial, legal, operational or reputational).
- *Risk Mitigation* – developing options and actions to enhance opportunities and/or reduce threats to the organization.

A. Goals of Risk Assessment

For organizations intent on completing an ethical and legal compliance risk assessment, the primary goals are as follows:

- To evaluate, quantify, and prioritize legal/ethics misconduct and compliance risks specific to current organizational operations;
- To provide rationale for planned compliance and ethics programs, including ethics and compliance training;
- To develop risk mitigation plans, including corporate policies and controls
- To align an organizational compliance program with the Federal Sentencing Guidelines for Organizations
- To develop a benchmark for ongoing risk assessment and measurement of the program's effectiveness.

B. Legal Defense and Federal Sentencing Guidelines

The concept of assessing risk is a critical underpinning to any corporate compliance program. In fact, the Federal Sentencing Guidelines for Organizations explicitly state:

> In implementing subsection (b), the organization shall periodically assess the risk of criminal conduct and shall take appropriate steps to design, implement or modify each requirement set forth in subsection (b) to reduce the risk of criminal conduct identified through this process.[2]

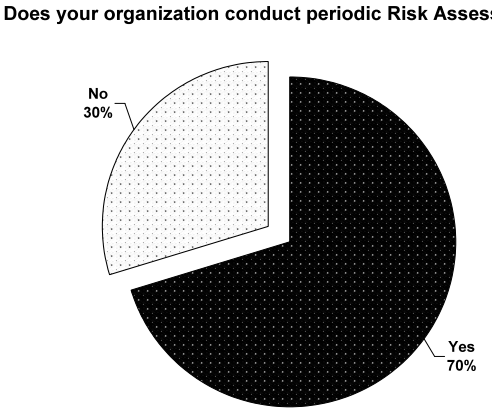
C. Benefits

The associated benefits of conducting an effective risk assessment include:

- Helping organizations prioritize compliance budget spending by identifying those areas most in need.
- Enabling the organization to modify and improve compliance program components to reduce risk and increase the likelihood of preventing criminal conduct.
- Providing an affirmative defense to allegations of deficiencies in the design and administration of a compliance program.

Given these benefits, more organizations are conducting periodic risk assessments. As illustrated in Figure 1, in 2007, 70 percent of all surveyed U.S.-based organizations conducted periodic risk assessments.

Figure 1: Percentage of Organizations that Conducted Periodic Risk Assessments



Source: ACC-Corpedia 2007 Compliance Program Benchmarking Survey

IV. Leading Practices

Many organizations are confused as to the scope, frequency and structure of an effective risk assessment. However, as more and more organizations have embarked on compliance risk assessments and started to develop their methodologies, leading practices are emerging, which are outlined below.

A. Examine All Major Areas of Potential Misconduct

An effective risk assessment examines all major areas of potential misconduct. A common mistake made by organizations when conducting a risk assessment is to limit the potential risk universe to a preconceived short list of likely high impact risks. However, a proper risk assessment includes the full realm of potential risks, both systemic to the average organization, as well as those that are unique to the industry within which the organization operates. A good risk assessment would seek to catalogue and examine risks of non-compliance with every applicable federal, state, and local law or regulation, as well as other ethics-related areas which may have an adverse impact on organization's image and reputation.

B. Examine Risk Contextually

To be most effective, a risk assessment must examine risk within the context of the ability of the organization to plan for, prevent, or mitigate each risk area. This means including an examination of the controls, processes and procedures designed to prevent compliance failure. It may also entail assessing the capabilities of the individuals in positions of substantial authority from the standpoint of their effectiveness in recognizing and preventing a compliance breakdown.

C. Address Current and Potential Risks

An effective risk assessment should address both current and potential risks. It should not only address risks that exist today, but also address those risks which may not yet be deemed illegal but could reasonably be called into question in the future. Moreover, acceptable industry practices today could be called into question tomorrow.

D. Industry Information and Historical Incidence Reports

Risk assessments should include an examination of industry information as well as historical incidence reports. Document review should not be limited to internal corporate documents, but should also look externally. To be adequately predictive, an effective risk assessment should not only include "compliance breakdowns and failures," but "near misses," as well. This is particularly important when it comes to modifying the compliance program as outlined under FSG.

E. Participants From All Levels of the Organization

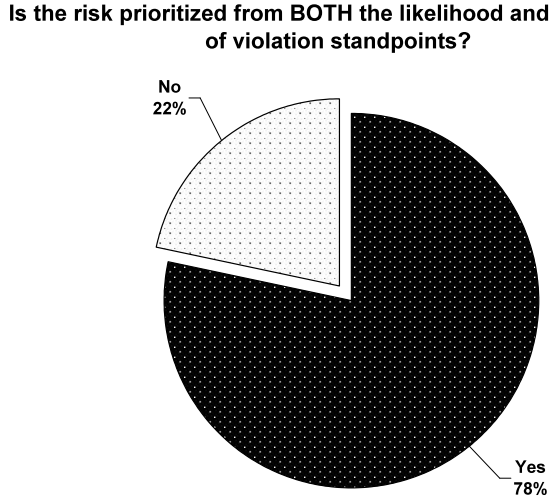
Risk assessments should involve participants from all levels of the organization. The leader of the risk assessment process should solicit the involvement of both functional (e.g., sales, marketing, finance) and line (e.g., division heads, executive team) leadership in collecting and assessing potential risk areas. This is

commonly done through workshops, focus groups, surveys, and interviews.

F. Impact and Likelihood of Occurrence

Risk areas should be weighted to account for impact and likelihood of occurrence. When conducting the risk assessment, the organization should assign quantifiable "likelihood" and "severity" weights or ratings to each relevant risk area. Utilizing this type of analysis helps organizations rank relevant risk areas (from minor to severe impact and low to high chance of occurrence). Performing such an activity is becoming a more common trend among organizations. As Figure 2 illustrates, nearly 80 percent of all surveyed U.S.-based companies now analyze risk for both likelihood of occurrence and severity basis.

Figure 2: Percentage of Organizations that Examine Risk by both Likelihood and Severity in Risk Assessments



Source: ACC-Corpedia 2007 Benchmarking Survey

G. Document the Outcome

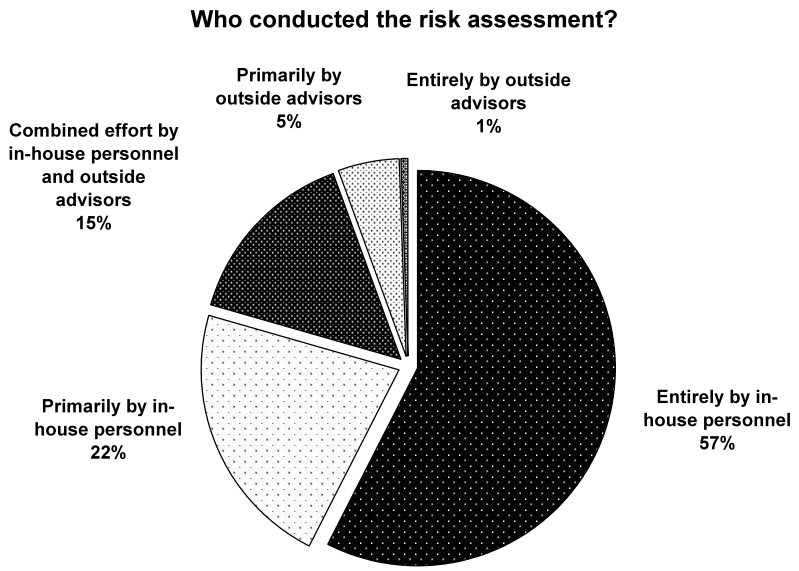
The organization should document the outcome of the risk assessment into a defensible action plan. Good documentation may be introduced as an affirmative defense, supporting the existence of an effective compliance and ethics program in the event of misconduct. Such documentation should not only include the risk assessment process followed; more importantly, it should also specify what actions were taken to design and implement a new compliance program or modify the existing one.

H. Be Defensibly Objective

The process methodology behind the risk assessment must be defensibly objec-

tive. This includes fairly assessing the full universe of potential risks, including existing acceptable industry practices. An organization needs to resist any temptation to ignore or de-emphasize risks simply because they may be costly to address (either from a financial or internal political vantage point). To help ensure objectivity, an increasing number of companies are involving domain-expert outside advisors in the assessment. As shown in Figure 3, 43 percent of all surveyed organizations currently involve independent outside parties in conducting risk assessments.

Figure 3: Level of Involvement of Independent Parties in Compliance Risk Assessment

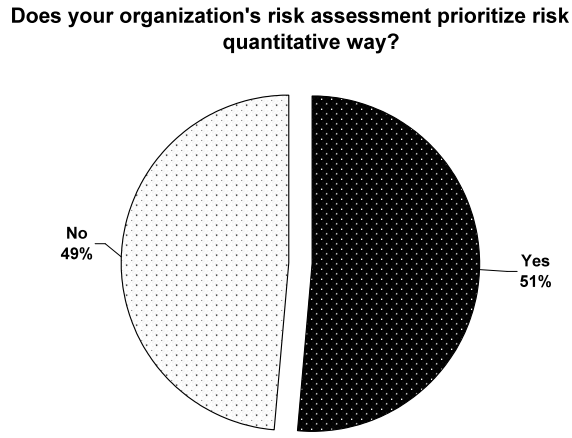


Source: ACC-Corpedia 2007 Benchmarking Survey

I. "Quantification" of Each Risk Area

The process in which the risk assessment is conducted should allow for specific "quantification" of each risk area. A risk assessment that goes beyond examining mere "likelihood" and "severity" can be more useful in prioritizing compliance budget spending and activities, as well as justify any incremental controls, policies, processes or costs that need to be implemented. Furthermore, if executed correctly, such quantification can be used to measure program effectiveness (another FSG criterion for effective compliance and ethics programs). For example, of the 78 percent of organizations that rank risk by likelihood and severity of impact, 51 percent of these companies also quantify each risk area.

Figure 4: Percentage of Organizations that Quantify Risk as Part of Risk Assessment Process Outcome



Source: ACC-Corpedia 2007 Benchmarking Survey

J. Be Sufficiently Periodic

The risk assessment should be sufficiently periodic. Risk assessments should not be a one-time activity. The frequency at which an organization chooses to conduct risk assessments and schedule follow-up risk reviews may depend on the nature of the organization's industry. However, if the methodology and process for the risk assessment is adequately defined, a risk assessment can be conducted on an annual basis. Operating environments, regulations and government enforcement priorities routinely change. As such, it is inadvisable to conduct risk assessments less frequently than every two years. Furthermore, infrequent risk assessments are of less value when they are used to measure the effectiveness of a compliance program.

K. Measure of Employee Knowledge

The risk assessment should include measurement of employee knowledge and awareness of the compliance program and supporting controls. Most companies include employee knowledge and awareness as a measurement factor in their risk assessments.[3] Doing so can help pinpoint where communications and training programs need to be improved. One of the most common ways of accomplishing this is through online employee surveys, either as part of a COSO-aligned self-assessment, or run independently.

L. Benchmarking

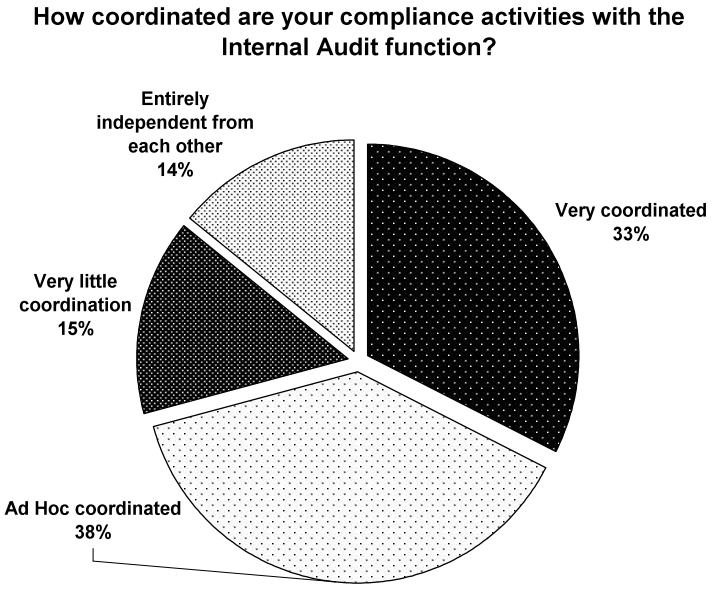
The risk assessment should benchmark against peer organizations. If it is feasible and such information is accessible, companies should compare their risk

areas and compliance program activities with others within their industry or with other companies that may have a similar size and operational profile. This is of particular importance as it ensures that the organization meets "accepted or applicable industry practice" as outlined in the application notes to the U.S. Federal Sentencing Guidelines Manual[4] Although a company may reach out directly to a competitor to conduct a benchmarking survey, this is not advised due to antitrust concerns. Another 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.[5]

M. Coordinating with Internal Audits

It is common and often useful to coordinate the risk assessment with internal audits. More and more companies these days are taking steps to increase coordination between the internal audit and ethics and legal compliance risk assessment. After all, a risk assessment is used to identify, measure, and rank risk areas. Completing one produces the following results for the internal audit: (1) aligns company focus and resources to address areas of greatest significance to the organization; and (2) allows the auditor to design a program that tests the most important internal controls. According to the 2007 ACC/Corpedia Benchmarking Survey, approximately one-third of respondents said that their risk assessment process was very coordinated with internal audit (see Figure 5). Moreover, a significantly higher percentage of publicly-traded companies (82 percent) reported that some form of coordination on risk assessment with internal audit existed, either in a formal or ad hoc basis, compared to private organizations.[6]

Figure 5: Percentage of Organizations that Coordinate Compliance Activities with Internal Audit



Source: ACC-Corpedia 2007 Benchmarking Survey

Using information from one in the preparation for the other is acceptable and recommended. However, the organization must never confuse the primary purpose of either, and the associated analysis must be kept separate and distinct. Remember, an internal audit focuses primarily on internal controls and financial risks, whereas an effective risk assessment will look at a much broader universe of compliance and ethics risks (such as employment law, antitrust, environment, safety, health, trade compliance, privacy, etc.).

V. Major Universal Components of an Effective Risk Assessment

Before commencing your risk assessment, it is important to understand some of the key components that comprise the design of any effective risk assessment. These components help ensure that a risk assessment will capture and measure all risk, both apparent and unforeseen, and they provide a framework for a repeatable process that can be used effectively for planning and improving any compliance program.

Below are the five fundamental components that a risk assesment plan should include:

☑	Sufficiently Flexible to Add Unforeseen Risks Introduced During Assessment Execution
☑	Measures and Ranks Risk in Accordance with Enterprise Impact
☑	Has a Standardized and Documented Approach that is Defensible and Repeatable
☑	Enterprise–Wide to Accommodate Global Risks
☑	Distinct from Sarbanes-Oxley 404 Assessments

A. Sufficiently Flexible to Add Unforeseen Risks Introduced During Assessment Execution

Naturally, organizations attempt to catalogue a portfolio of potential risk areas when embarking on a risk assessment. This risk portfolio may be independently derived, or alternatively, the organization may leverage an external resource (for example, a risk database that bears information on common risk areas). Regardless of how comprehensive a "risk universe catalog" may appear to be, a good risk assessment process is flexible enough to allow for the addition of new or unforeseen risks. New risk areas may be identified by the risk assessment team, advisory councils, business leadership, or employee surveys, but there may also be an "alternative interpretation" of a catalogued risk that needs to be addressed. For example, it is not unusual for established commonly-accepted business practices in any industry to come under new scrutiny given increased awareness and sensitivity to compliance and corporate governance.

B. Measures and Ranks Risk in Accordance with Enterprise Impact

Not all compliance failures that could result in violations of the law are equal. While one "material violation of law" may result in a fine or penalty as well as substantial legal defense costs, a different "material violation of law" can have a far greater impact on an organization's operations through substantial customer and contract losses, reputation damage or even necessitated changes to the business model. The varied impact of various compliance failures by area or category of risk are not the same for all organizations, but may depend on such factors as the industry in which an organization operates, any historical incidence of compliance failures, and judicial enforcement trends. OMB Auditing Standard 133 translates the internal control deficiencies defined in SAS 112 into compliance terms (e.g., defines substantial deficiency and material weakness to possible compliance risks), and these are useful for standardizing and comparing compliance risks. The compliance risk assessment should also define standard "risk appetites" across risk areas (financial, operational, legal, and reputational),

so that different risks may be objectively compared.

C. Has a Standardized and Documented Approach that is Defensible and Repeatable

A common failing of risk assessment efforts is when they are treated as a one-time event and lack sufficient process and documentation. Federal Sentencing Guidelines criteria for an "effective compliance and ethics program" set forth expectations that risk assessments are a recurring activity within an organization's overall compliance program. A well-designed risk assessment has a systematic methodology and well-documented process, and therefore is more likely to be deemed objective. Organizations should be concerned about objectivity because imputed subjective bias on the part of those conducting the risk assessment (particularly if conducted by internal personnel) can undermine the credibility of the final outcome.

Documented and standardized processes allow for more cost-effective repetition of the risk assessment processes as the inevitable endemic change occurs both within the organization, as well as the business environment in which it operates (e.g., new laws or interpretations of existing laws come into existence; compliance and legal departments experience personnel turnover; organizations divest operations or enter into new business activities or markets). Additionally, with a standardized and documented process towards assessing and prioritizing risk, a risk assessment may be sufficiently defensible as to be able to "measure effectiveness" of an organization's compliance and ethics program through comparing outcomes over a series of sequential risk assessments.

D. Enterprise Wide to Accommodate Global Risks

When examined through the lens of an "effective compliance and ethics program," limiting a risk assessment to an organizational "silo," such as specific geographic regions or unique functional areas, can leave the organization open to exposed risks. For example, in recent years, some of the most costly compliance failures (in terms of out-of-pocket and reputational damage) for U.S. organizations have occurred overseas. While it is tempting to focus an assessment on those areas with which the legal department is most familiar, doing so would undermine the defensibility of the analysis outcome.

E. Distinct from Sarbanes-Oxley § 404 Assessments

While there are certainly correlations between work performed by the internal audit function of any organization and a risk assessment undertaken by the compliance, ethics or legal department, analyses must still be kept separate and distinct. Sarbanes-Oxley § 404 requires management to document and assess the effectiveness of their internal controls over financial reporting. With the advent of new guidance from the SEC in the form of the May 25, 2005 Bulletin,

organizations may use a risk prioritization approach to conducting their § 404 work in the future. While such risk prioritizations may interlay with risk assessment, the fundamental elements being examined under § 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 an assessment of risk areas from a weighted, occurrence likelihood and deterrence element, which are essential to any effective risk assessment.

In short, the type of "risk" from the internal audit viewpoint is fundamentally different from the type of "risk" that should be applied by the legal compliance function. Using information from one analysis or assessment in the preparation of the other is acceptable and recommended. However, allowing the two to become interchangeable is a mistake as these are not identical types of "risk." While internal audit may participate in, or possibly even lead a legal compliance risk assessment, a legal compliance risk assessment must be sufficiently distinct and independent from the material disclosure work done for Sarbanes-Oxley § 404. However, the assessment of internal controls conducted in the course of a § 404 audit can be effectively used as a part of the risk assessment, and vice versa. Many companies successfully use COSO methodology for conducting internal control surveys, including surveys of compliance internal controls to the extent that they may potentially impact on financial statements. Compliance risk assessment can be aligned with internal audit by using COSO methodology to conduct broader compliance risk analysis, which requires an assessment of internal controls. Under PCAOB AS #5, management can use our independent assessment of compliance internal controls to support their annual certifications. Conducted properly, compliance risk assessments can, in part, serve this dual purpose.

VI. What to Examine in a Risk Assessment

So what exactly does an organization examine in a risk assessment? When conducting the risk assessment, the organization should assign quantifiable "likelihood" and "severity" weights or ratings to each identified risk area. There are numerous resources, both internal and external, that are extremely useful in helping to determine likelihood and severity of any given risk. When looking at severity of risk, a good approach is to compute maximum potential severity, or the worst that could happen to the organization should a particular type of misconduct occur. The factors that drive the severity are almost too numerous to be listed. However, we list here the most obvious ones that should be considered.

- Civil and criminal penalties potentially resulting from violations

- Legal defense costs
- Litigation settlements
- Impact on a company's revenue, earnings, and bottom line
- Impact on a company's stock value
- Impact on credit rating and cost of capital
- Employee turnover
- Customer loss
- Change in business model and operations, such as shutdown of various business operations or product or service lines
- Debarment from participation in government contract or grant programs
- Change in market share
- Reputation damage
- Negative media coverage
- NGO/advocacy group pressure
- Increased future costs of compliance
- Current and anticipated regulatory initiatives and enforcement/prosecution priorities.

We recognize that most organizations lack internal data or internal experience from prior incidences to accurately determine severity of risk areas under examination. However, industry experience, as well as broader corporate experience, can provide adequate information for reasonably accurate analysis of risk severity. There are a number of studies available that seek to statistically measure severity of various risk areas for major industries. It is important to note that while it is very important to have an accurate understanding of risk severity, in reality there is little an organization can do to reduce the risk severity. What the organization can do, however, is to reduce the likelihood of risk. Therefore, an accurate assessment of the likelihood and a good understanding of the underlying factors are key elements of any good risk assessment methodology.

The risk likelihood is a combination of internal factors which determine the probability that a particular type of misconduct will occur. The following major factors affect—indeed, create—the risk probability:

- Organization's business activities;
- Organization's policies, processes, and controls;
- Organizational culture and ethics;
- Employee knowledge, awareness and intent.

Below is a sample of some of the key tools and activities an organization can utilize to aid the risk assessment process:

- Executive interviews and focus groups
- Organizational health survey

- Employee awareness/knowledge assessment
- Examination of corporate policies, processes and controls per risk area
- Examination of the anonymous reporting system statistics
- Review of other historical incidence
- Evaluation of existing training inventory and courseware
- Interviews with training "owners"
- Examination of prior audits, surveys and reports
- Review corporate publications (Code of Business Conduct, Employee Guides, New Hire Kits, etc.)
- Examination of organizational charts and reporting relationships
- Review of Audit Committee Charter and Corporate Governance Principles
- Assessment of employee disclosure and acknowledgement forms
- Analyst reports.

VII. The 10-Step Risk Assessment Process

The following is a discussion on the ten key steps in an effective risk assessment process. This process represents an amalgamation of best practices and methodologies employed by leading organizations that Corpedia has either observed or worked with via prior engagements. Depending on resources and facility with risk analysis, some companies may eliminate or combine certain steps. Others may wish to add incremental steps, such as peer analysis and benchmarking.

Step	Description
1.	Definition of Objectives, Criteria, and Documentation
2.	Planning the Process
3.	Profile the Organization
4.	Catalogue Risk Area Universe
5.	Rate Risk Areas for Severity
6.	Conduct Interviews, Surveys, and Assessments
7.	Catalogue and Measure Mitigating & Aggravating Factors
8.	Determine Risk Event Probability or Likelihood
9.	Determine Aggregate Risk Scores (Enterprise Impact) and Final Ranking
10.	Finalize Risk Assessment Report and Create Mitigation Action Plan

Although your organization may deviate from these steps, the fundamental sequential principles are the same in any effective risk assessment. These principles include: plan, profile, assess, rank, and report.

Figure 6: Risk Assessment Process Grid

A. Step 1: Definition of Objectives, Criteria, Process, and Documentation

The first step in commencing a risk assessment is to define the process. The proposed methodology needs to be specified as to the desired outcomes and supporting processes for communication and handling documentation. The critical questions that you will need to address are:

- What is the desired outcome?
- Who is the target audience for the final report?
- How will this report be used?
- How will your organization manage the documents to be created?
- How will the issue of "privilege" be addressed?

1. Desired Outcome

For most, the practical role of a risk assessment is to meet the criteria of an "effective compliance and ethics program" set forth in the Federal Sentencing Guidelines. However, taking it one step further, your risk assessment should reaffirm the priorities of and the emphasis on an existing compliance program, or

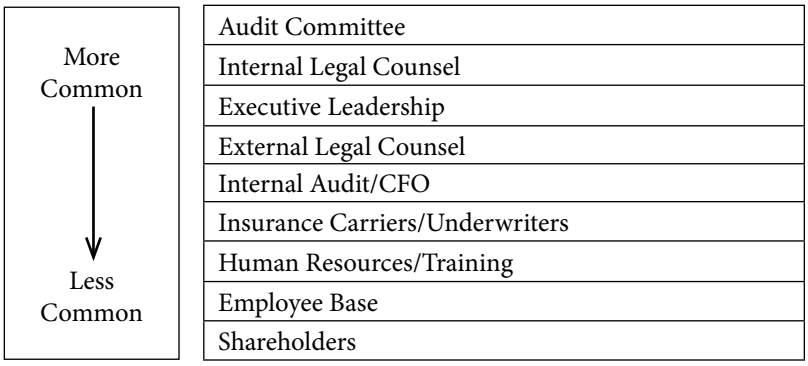
it can serve as a guidepost for the creation of a new program where none exists. Knowing the parameters of the outcome may sound simple, but in reality the answer to the above questions will determine the scope, depth and breadth of your risk assessment. For example, if you are reaffirming priorities of an established program, then the risk assessment might be built around a focus on the risk categories and areas already contained and set forth in your organization's Code of Conduct. On the other hand, in the absence of a mature compliance program, in order to use the risk assessment for purposes of budgeting and building a new or reestablished compliance program, it is preferable to:

- Examine a far greater range of risk areas;
- Research what peers of similar size or industry are doing; and
- Broaden the scope of the risk assessment team to include key functional areas and business leaders.

2. Target Audience

It is quite possible to have several target audiences. Knowing your target audience will better prepare you for the type of data that needs to be collected in the risk assessment itself. In our experience and review of leading organizations' risk assessment reports, some common target audiences include those featured below:

Figure 7: Target Audiences for the Risk Assessment



3. Use of Report

This report can be and is used to address/support such things as:

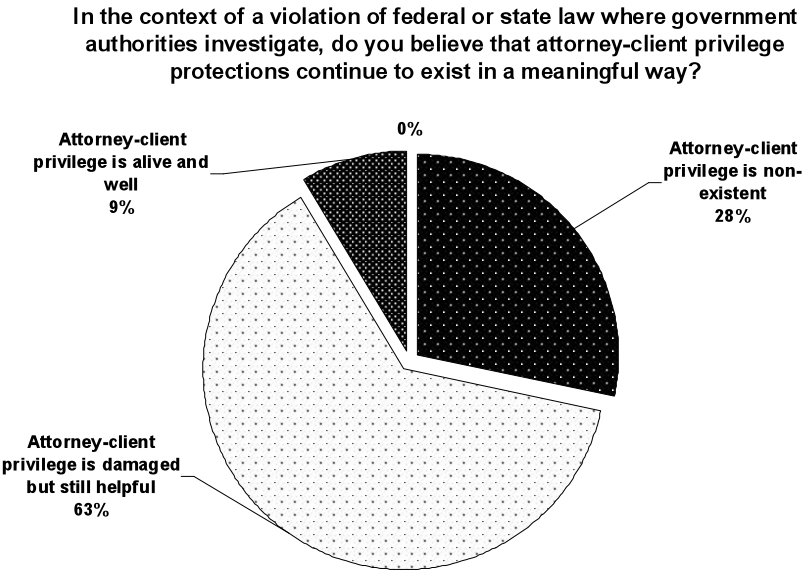
- Policy and process creation
- Training initiatives
- Sarbanes-Oxley § 404 work prioritization
- Purchase of incremental insurance
- Divestment of product lines, customers or markets, etc.

4. The Issue of Document Creation and Privilege

While completing a risk assessment can be very beneficial, organizations should be aware that, if poorly executed, the sensitive information collected as part of the risk assessment can potentially subject the organization to harm. One of the most vexing issues facing any legal department today when it comes to conducting a risk assessment is making sure that the form, content, and tone of any document created by the risk assessment team does not subject the organization to any unintended harm. Assuming that all created documents are protected by attorney-client or work product privilege is a flawed and dangerous assumption, as many documents may fall outside of the established privilege parameters in how they are generated or shared.

Privilege is very hard to maintain in today's legal environment, and the veil of privilege is commonly pierced through waiver in regulatory and judicial investigations. In light of these issues, many corporate counsels embrace an operating assumption that privilege is of limited use or thereby should not be relied upon. As illustrated in Figure 8, twenty-eight percent of organizations feel that attorney-client privilege within the context of a government investigation no longer exists in a meaningful form.

Figure 8: Percentage of Organizations that Believe Attorney-Client Privilege Protections Still Exist and Are Meaningful



Source: ACC-Corpedia 2007 Benchmarking Survey

Any risk assessment will contain lists, descriptions, and theoretical suggestions about current or possible future compliance problems. For example, envisioning

"what could go wrong" is a useful exercise in helping to prevent such an occurrence. At the same time, should such an envisioned compliance problem later occur, a written document from such an exercise could be taken out of context as "evidence" of preexisting knowledge of a compliance problem or deficiency that an organization failed to address.

An additional complication is that an effective risk assessment commonly includes a diverse team of individuals, including employees and non-company personnel. It is likely that the majority of these individuals will not be attorneys, and many of them may not be knowledgeable about the concept of privilege and the associated dangers of document and content creation. Furthermore, some of these individuals, bearing an intention of wishing to grandstand their participation or simply being misguided, can lend themselves to dramatic verbiage and pronouncements about potential risk areas in their documentation creation. As a result, at this stage in the risk assessment process, guidelines and protocols for document creation should be established for the risk assessment team and any other key contributors. At a minimum, documentation guidelines should include the following:

- **Detailed Guidelines on Document Creation**

Guidelines should focus on counseling participants to be clear in their writing and to use neutral language that avoids hyperboles and exaggeration. Participants should also understand that any document might be taken out of context. Furthermore, participants need to understand that these guidelines also apply to shorthand, margin and handwritten comments and notes.

- **Limitations on Document Distribution**

Naturally, the more broadly that drafts and documents are copied and distributed, the greater the risks of losing control over what exists. There should be clear parameters for where documents are submitted and stored after creation.

- **Provide Guideline Templates**

Should participants be part of ranking risks and creating hypotheticals, it is best to provide a description template with which they should work.

B. Step 2: Planning of the Process

Once the organization has clearly defined the purpose, process, and desired outcomes of the risk assessment, it is important to map out a plan for how the organization plans to execute the process.

1. Appoint a Risk Assessment Leader

Important to any new endeavor, a leader must be selected to oversee the risk assessment process. Depending on the organization, this individual could be drawn from any number of roles including general counsel, chief compliance

officer, ethics officer, head of risk management, or possibly the director of human resources. It is also possible that this individual could be appointed by any of the individuals listed above. Regardless of the level, the leader of the risk assessment process must be empowered to control the process from inception through final implementation.

2. Identify and Select Team Members

No leader can succeed without effective team members. As such, it is important to identify key individuals in the organization who will serve as members of the risk assessment team.

Some of the more common ones include:
- General Counsel and/or Chief Compliance Officer
- Legal and/or Compliance Subject Matter Experts
- Business Unit or Functional Heads
- Outside attorneys or consultants (as necessary).

When selecting team members, it is important "to ensure participants are familiar with the purpose, scope and elements of a risk assessment process and possess relevant functional and/or business unit background information and experience.[7]

3. Decide Which Steps to Include/Perform

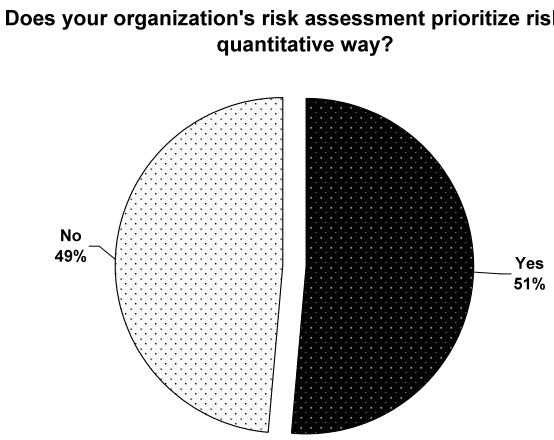
Each organization is unique and therefore is likely to be at a different stage or maturity level in terms of conducting risk assessments. Novice organizations that are implementing or planning to implement a risk assessment for the first time would be advised to complete each step, while other more experienced entities that have completed multiple risk assessments may decide to limit the process.

4. Will You Quantify Risk or Just Write a Qualitative Report?

Another decision to be made by the organization is whether or not the portfolio of risks will be quantified or assigned a value based on impact to the organization as well as likelihood of occurrence. The value in conducting a risk assessment is the ability to measure the degree to which a specific risk can impact the organization, either positively or negatively. Positive risks present opportunities for the organization while negative risks naturally serve as potential threats. Depending on the type of organization and its associated industry, the number of potential risk areas for the organization can vary. As such, the quantification of risk areas provides a mechanism to allow for the ranking of risk areas.

Incidentally, based on recent research, many companies still decline to quantify their risk areas and instead rely on a more subjective, qualitative analysis where they base their risk assessment and corresponding mitigating strategies on opinions and feedback from personnel in their organization. As illustrated in Figure 9, a little over half (51 percent) of all organizations actually quantify risk in their risk assessments.[8]

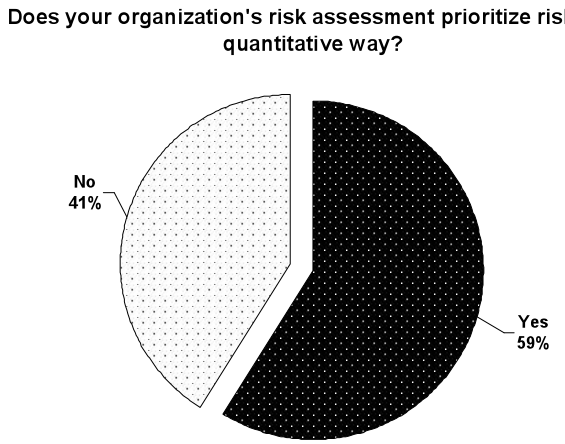
Figure 9: Percentage of Organizations that Prioritize Risk in a Quantitative Manner



Source: ACC-Corpedia 2007 Benchmarking Survey

Moreover, as shown in Figure 10, publicly-traded companies in the United States are 59 percent more likely to quantify risk versus foreign or private organizations.

Figure 10: Percentage of Publicly-Traded Companies in the U.S. that Prioritize Risk in a Quantitative Manner



Source: ACC-Corpedia 2007 Benchmarking Survey

5. Will You Be Conducting Workshops?

Some organizations choose to conduct group meetings or workshops to identify, evaluate and prioritize risk areas. These meetings are managed by the risk assessment leader with the aid of the risk assessment team. All of the relevant risks to the organization are examined, and a severity and likelihood score is assigned to each risk. Whether or not workshops will be a productive activity really depends on the organization. In order for them to work, it is important for the risk assessment leader to fully manage the process. This includes selecting the right participants, defining both guidelines and expectations for these participants, providing sufficient background material and guidance and creating an effective schedule and agenda for the meeting.

6. Will You Be Conducting an Employee Survey?

In the past, when conducting risk assessments, some firms have chosen to exclude the broad employee base and focused their risk assessment queries on key functional area and business leaders of the organization. In fact, recent research conducted by Corpedia and the Association of Corporate Counsel found that less than 24 percent of organizations actually use workforce surveys as part of the risk assessment process.[9] Taking the time to perform an employee survey can help protect the organization from premature dismissal or a failure to recognize certain risk areas. It is not uncommon, especially in highly decentralized organizations, for gaps in information and communication failures to exist. As such, including an employee survey as part of the overall risk assessment will

lessen the chance of omitting a key risk area.

7. Estimate Resources

When planning the scope of the risk assessment, decisions will need to be made on what resources are needed, estimates on how much time is required of those resources, and verification of availability of those resources. It is important for all participants of the risk assessment to make an honest and effective contribution to the process. Given the importance of the risk assessment to the organization, any weakened participation can lead to holes in the overall risk assessment effort. As part of the resource identification and planning, another important decision will be whether to conduct the risk assessment entirely in-house or in association with an external party or advisor (law firm, audit firm, etc.). A more in-depth discussion of the associated costs/benefits is available below in Section VIII, In-house vs. Outsourcing the Risk Assessment.

8. Set Milestones

An effective risk assessment involves a significant number of interrelated tasks necessitating the active involvement of many individuals. Moreover, depending on the actual number of risk areas assessed, the process can become a very complicated activity. As such, it is important for the overall leader of the risk assessment to set specific measurable goals and checkpoints throughout the process. The use of milestones will help guide individual contribution as well as place structure around a process with multiple diverse inputs.

C. Step 3: Profile the Organization

Once the planning stage has been completed, the next step is to develop an accurate profile of the organization. This step is not to be underestimated as it effectively drives the rest of the risk assessment process. Moreover, diligence and care should be taken when performing this step of the process. A company's profile dictates the types of risk areas, relevant to the organization. A weakened organizational profile will only lead to an ineffective risk assessment.

Some of the typical elements addressed in a company profile include specifications of the organization in the following areas:

- Industry Type
- Company Size
- Classification (public versus private)
- Key aspects of business operations (e.g., consumer products, government contracting, union environment, etc.)
- International operations

Profiling the organization includes a comprehensive review of business activities, strategy and priorities, industry and geography of operations, workforce

composition, and other operational circumstances that generate exposure to particular risk areas.

D. Step 4: Catalogue Risk Area Universe

Completion of the organizational profile enables the development of a complete catalog of risks also commonly known as a *risk universe*. There are many risks that an organization is exposed to on a daily basis. Many individuals associate risk to the organization with business risks or those risks that affect the delivery of a product or service by affecting the critical constraints of schedule, budget and quality. Our analysis here focuses specifically on ethics and legal compliance risks–that is, those risks related to the potential for business misconduct and/or violations of federal, state and/or local laws and regulations. A robust risk assessment process would attempt to map out every business process, the associated ethics, and the associated compliance risks for an organization. This process would be updated annually and used for conducting risk assessment.

1. Tips

When developing the risk universe, it is necessary to take a comprehensive view. The organization must strive to first identify and scrutinize risks to pinpoint the root cause and then widen the examination to account for systemic risks (common to the average organization), industry-specific risks, and finally, organization-specific risks. It is also useful to rely on the experience of peer groups and review historical incidence.

Figure 11: Risk Universe

Moreover, it is useful to display the entire set of risks in an Excel grid format. Doing so enables risk assessment leaders or team members to capture, sort and rank the risk areas later in the process, once they have been rated for severity and likelihood of occurrence. An example of this type of grid is available in Section XI, Sample Forms.

E. Step 5: Rate Risk Areas for Severity

Once the risk area universe is fully developed and you are confident that all relevant risk areas to the organization have been addressed, the next step in the process is to rate those risk areas for severity. Industry severity can be described as the maximum potential outcome of violation or misconduct for a typical or average company in a given industry, measured in terms of total enterprise impact.

Risk event severity is a product of many factors including:
- Civil/criminal penalties, such as SEC/DOJ settlements, lawsuits, etc.;
- Impact on stock price and bottom line;
- Employee turnover and loss of intellectual property;
- Loss of customers and market reputation;
- Systemic business model impact;
- Increased future cost of compliance;
- Current and anticipated future enforcement trends and priorities.

1. Rating System

Risk areas can be rated for severity both subjectively and statistically. The former will typically scale the level of a risk from minor to moderate to severe impact while the latter will rely on a numeric rating or weight assigned to the risk. The scale can vary but often appears in a range of either 1-5 or 1-10 where the level of severity is ranked in ascending order. Furthermore, once the risk likelihood is calculated later in the process, organizations often process both data sets and visually map them on a probability-impact matrix. An example of this matrix is available later in this document.

2. Leverage Peer Data

When evaluating the complete portfolio of risk areas for impact to the organization, one may find it helpful to research available benchmark information on how their industry peers rate or have rated specific risk areas to their organizations. Obviously, when benchmarking, it is important to choose one or more peer organizations that closely match the subject organization in terms of size, industry type, etc. Organizations commonly rely on Corpedia's ECERA™ database for such a benchmarking activity, as it contains specific critical risk severity metric data for over fifty unique industries, collected as a result of in-depth research of over 1,000 U.S. and international corporations.

Another alternative is to actually design a customized industry peer survey and distribute it among a selection of peer organizations in order to obtain common

severity metrics. However, this process may be lengthy and requires effective planning and design by the host organization. Some companies opt to develop an internal database of news items from multiple media sources, which identify potential or actual risks relevant to those companies so they will be "remembered" at the time of periodic risk assessment.

F. Step 6: Conduct Interviews, Surveys, and Assessments

Once the risk universe has been fully developed, the next step in the process is conducting interviews and/or assessments with senior and mid-level managers and key functional area leaders (finance, sales, etc.) of the organization, as well as a sample of the workforce. The prime goal of such interviews and assessments is to collect information that will enable you to determine the likelihood of misconduct with sufficient accuracy. The secondary goal is to verify the integrity of the risk-area universe constructed earlier, and to see whether there are any material risk-areas that may be missing from it. Sometimes, interviews and assessments uncover totally unforeseen yet *material* risks.

1. Interviews

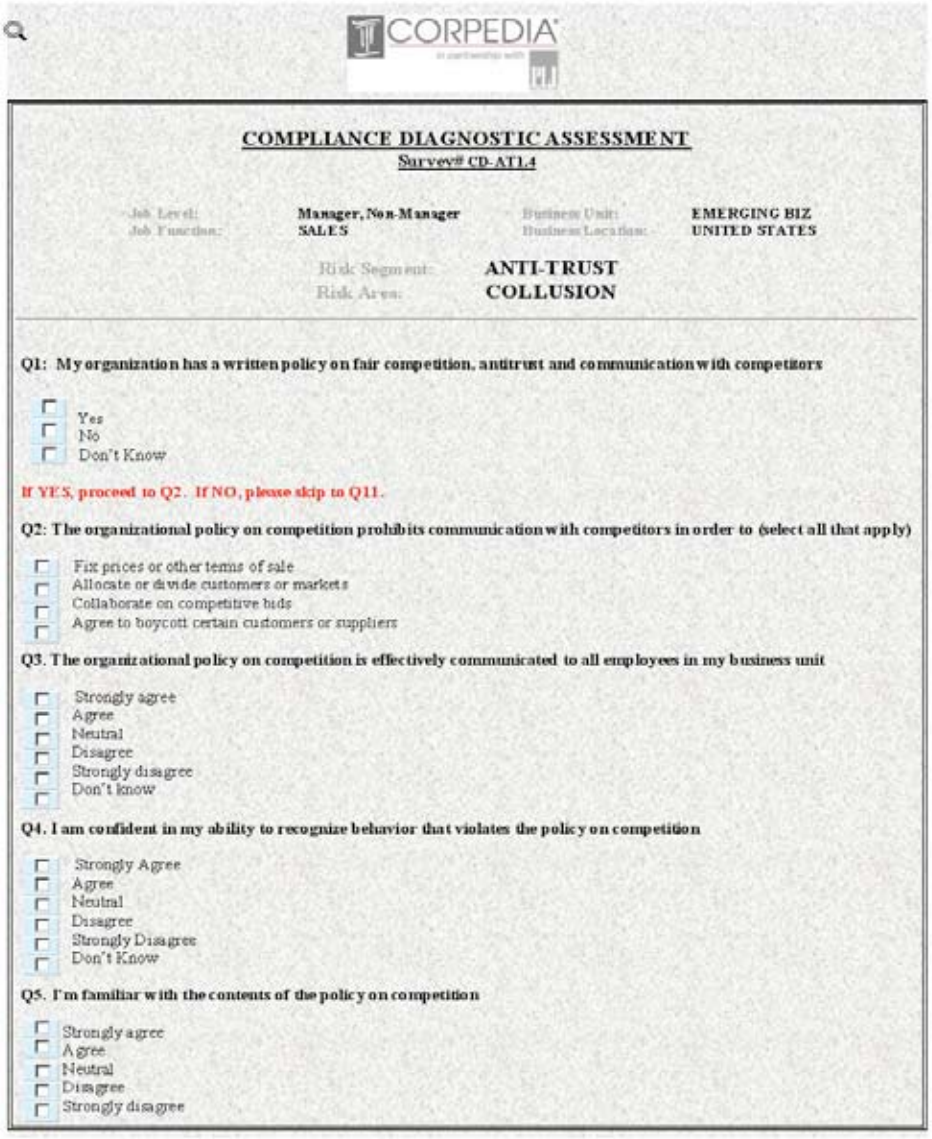
For organizations that do conduct employee interviews as part of the risk assessment process, the three most common groups to be interviewed (based on the survey results) are: 1) Executive Team (81%); 2)HQ Functional Department Management (73%); and 3) Operational Field Management (66%). However, there is a significant drop-off before involving additional lower-level employees in the risk assessment process, with only 37% of organizations interviewing any line employees.

2. Assessments

Two general types of assessments can be utilized: *Compliance Diagnostic Assessments* and *Employee Surveys/Assessments.*

- **Compliance Diagnostic Assessments** evaluate such things as organizational policies, processes, procedures and controls, cases of historical incidence, the quality and extent of existing compliance efforts, existing ethics/compliance training programs, current compliance issues, corporate culture (as viewed by senior management), business priorities, an evaluation of the overall compliance and ethics environment, and the commitment to ethics and compliance. While some components of the Compliance Diagnostic are examined through comprehensive analysis of existing data—like training curriculum, code of conduct, management communications, written policies, internal audits, reporting hotline statistics, prior surveys, etc.—a significant portion of data is collected through targeted surveys, questionnaires, and interviews. (See Figure 12 for a snapshot of a typical compliance diagnostic assessment.)

Figure 1 corpedia ETHICS. ELEVATED. stic Assessment



CORPEDIA

COMPLIANCE DIAGNOSTIC ASSESSMENT

Survey# CD-AT1.4

Job Level: **Manager, Non-Manager**
Job Function: **SALES**
Business Unit: **EMERGING BIZ**
Business Location: **UNITED STATES**

Risk Segment: **ANTI-TRUST**
Risk Area: **COLLUSION**

Q1: My organization has a written policy on fair competition, antitrust and communication with competitors

- Yes
- No
- Don't Know

If YES, proceed to Q2. If NO, please skip to Q11.

Q2: The organizational policy on competition prohibits communication with competitors in order to (select all that apply)

- Fix prices or other terms of sale
- Allocate or divide customers or markets
- Collaborate on competitive bids
- Agree to boycott certain customers or suppliers

Q3. The organizational policy on competition is effectively communicated to all employees in my business unit

- Strongly agree
- Agree
- Neutral
- Disagree
- Strongly disagree
- Don't know

Q4. I am confident in my ability to recognize behavior that violates the policy on competition

- Strongly Agree
- Agree
- Neutral
- Disagree
- Strongly Disagree
- Don't Know

Q5. I'm familiar with the contents of the policy on competition

- Strongly agree
- Agree
- Neutral
- Disagree
- Strongly disagree

- **Employee Surveys/Assessments**, on the other hand, consist of both organizational health and knowledge assessments. The former seek broad impressions of the organization in regards to the ethics and compliance environment, culture, and overall ethical health, while the latter seek to determine employee comprehension of compliance issues with respect to their specific functional area.

G. Step 7: Catalog and Measure Mitigating/Aggravating (M&A) Factors

The next step of the process involves identifying those specific factors relevant to the organization that can serve to either reduce or increase the level of risk for the organization. Recall that this information is derived from the internal and external factors originally examined in earlier stages of the risk assessment.

H. Step 8: Determine Risk-Event Probability or Likelihood

Information gathered during interviews, surveys, and assessments helps to accurately determine the "risk-likelihood." Risk-likelihood is defined as a reasonable likelihood of a risk-event occurring for a typical company in a given industry. "Risk event likelihood" is a product of mainly internal organizational factors, including:

- Organizational culture and ethics;
- Compliance initiatives;
- Organizational policies;
- Internal controls;
- Workforce awareness and knowledge; and
- Employee intent.

In terms of an actual scale for rating the likelihood of a risk event, it is common to use a scale of 1-5, as shown in Figure 13 below:

Figure 13: Risk Likelihood Scale Example

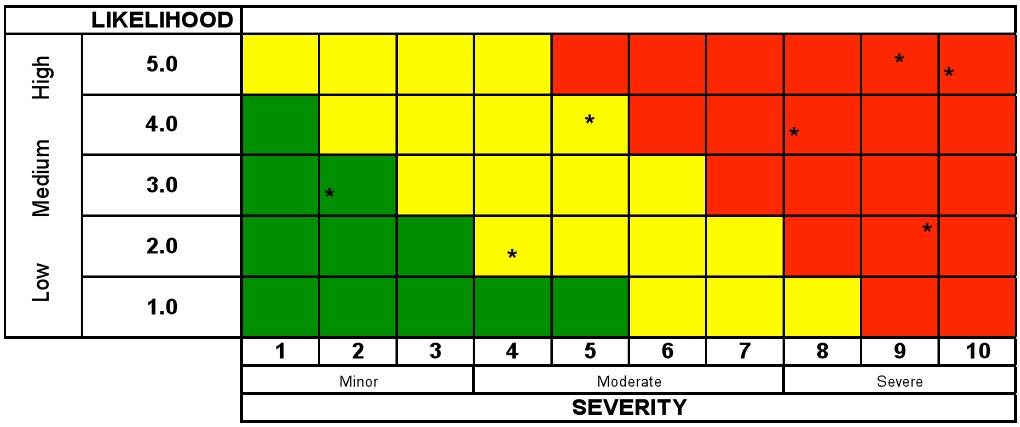
Rating	Scale	Description
1	Rare	Highly unlikely, but it may occur in unique circumstances
2	Unlikely	Not expected but there's a slight possibility it may occur
3	Possible	Event may occur at some point – typically there is history to support it
4	Likely	Strong possibility that an event will occur and there is sufficient historical incidence to support it
5	Almost Certain	Highly likely, this event is expected to occur

I. Step 9: Determine Aggregate Risk Scores and Final Ranking

Once risk severity and likelihood is known, an aggregate risk score (Enterprise Impact Score) can be developed. This risk score is essentially the product of risk area severity and likelihood of occurrence. It reflects the significance of a par-

ticular risk area to the organization. It is important to note here that this aggregate risk score is only used to facilitate the ranking of the risk areas. This score is *not* a measure of compliance effectiveness of the organization, nor is it intended to compare, rate, or grade the organization's compliance efforts, controls and programs against peers, the market as a whole, or industry best-practices. In practice, it is also common to map these risk scores visually, often in a grid format, like the one featured in Figure 14 below. Mapping the scores will enable the organization to quickly view the most critical risk areas (highlighted in red) and will enable the risk management team to deploy a phased approach to risk mitigation.

Figure 14: Risk Likelihood-Severity Matrix



- **Level Green:** Risks at this level should be monitored but do not necessarily pose any serious threat to the organization at the present time.
- **Level Yellow:** Organization should proactively take steps to actively monitor and further evaluate these risk areas and likely engage mitigation strategies.
- **Level Red:** Immediate action is required to address these risk areas as the potential for violations or damage to the organization is significant.

J. Step 10: Finalize Risk Assessment Report and Create Mitigation Action Plan

The last phase of the process is the development of a formal written risk assessment report and the creation of the risk mitigation action plan.

1. Report

A risk assessment report should be a comprehensive yet easy to understand document that should reflect a completed compliance risk assessment process which reasonably meets or exceeds Federal Sentencing Guidelines' risk assessment criteria under the definition of an "effective compliance and ethics pro-

gram." The report and supporting documentation must be created, maintained, and delivered in a methodology that decreases the likelihood of information, as well as surrounding collection of data inputs, being misconstrued or used out of context. This is particularly important for "discovery" reasons, in the event the organization must later serve as a party, a witness, or a principal in litigation or a government investigation.

Some of the key elements of an effective risk assessment report may include:

- **Top Risk Areas.** The report should highlight a specified number of key risk areas.
- **Quantification and Ranking of Risk.** Each risk area should be weighted for severity and likelihood, and ranked according to significance of risk to the organization.
- **Supporting Documentation for Risk Quantification.** Each risk area and its relative weighting are supported by critical information that factors into the final report, including existing key risk aggravating and mitigating factors, such as employee knowledge measurement, existence or lack of a specific policy or control, etc.
- **Specific Risk-Reducing Steps and Recommendations.** Each of the top risk areas is accompanied by specific actions that the organization can take to reduce its contribution to the quantified risk score and "manage" its risks on an ongoing basis.
- **Year-Over-Year Effectiveness Measurement.** As the organization begins to conduct multiple annual risk assessments, the report includes measurements of effectiveness by analyzing and tracking the quantification of each major risk area on a year-over-year basis.
- **Compliance Program Benchmark.** A benchmark of the organization's compliance program and activities versus its industry peers.

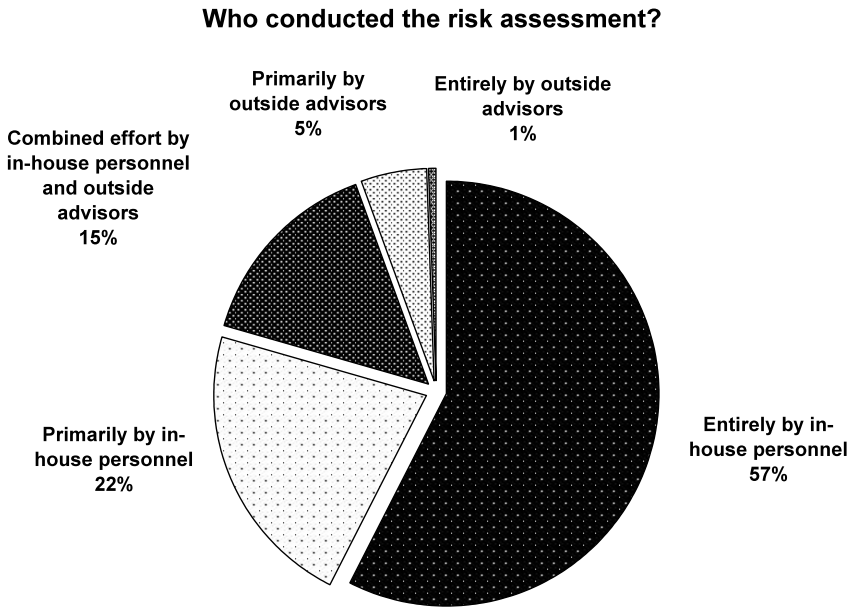
2. Mitigation Action Plan

Once developed, the formal risk assessment report serves as the guide for the creation of an Action Plan to mitigate the top risk areas to the organization. This action plan will enable the risk assessment leader to assign specific risk owners who will lead the process in managing each critical risk area. For each risk, milestones should be developed and tracking of these milestones will help ensure that the process is successfully completed. The action plan itself can take many forms, depending on the desired investment of the subject organization. Types of tools that have been used by organizations range from simple documents and Excel-based workbooks to more advanced risk management software packages and/or web-based applications.

VIII. In-house vs. Outsourcing the Risk Assessment

A decision any organization faces when planning for and implementing an organizational risk assessment is whether the activity should be conducted entirely in-house or if the organization would be better served by hiring external expertise. This decision should not be taken lightly and there are positives and negatives to both approaches. In a recent survey (conducted by ACC and Corpedia), results showed that over half (57 percent) of all organizations conduct their risk assessments entirely in-house, while the remainder (43 percent) use an outside advisor in the process.

Figure 15: Percentage of Organizations that Conducted Risk Assessments In-House vs. Using External Advisors or a Combination of Both



Source: ACC-Corpedia 2007 Benchmarking Survey

A. In-House

Organizations may choose to conduct a risk assessment purely in-house. There are various reasons why an organization may choose to follow this path including:

- Size of the organization

- Budgetary constraints
- Concerns over confidentiality

However, there are also limitations when opting to conduct risk assessments internally.

1. Inadequate Process Knowledge

One of those concerns is whether or not there exists adequate process knowledge of conducting an effective risk assessment within the organization. As demonstrated in this paper, conducting a risk assessment is a methodical engagement with numerous phases requiring the coordination and participation of various individuals across the organization.

2. Ineffective Survey Knowledge and/or Interviewing Skills

A significant part of any risk assessment process is the ability to extract the most relevant information from individuals in the organization who have domain expertise in their functional area. To do this, individuals on the risk assessment team must be equipped to ask the right types of questions in order to obtain the critical information needed to examine. Without this, certain risk areas must actually be understated and the organization may be exposing itself to future harm.

3. Weak Data Analysis and Interpretation

A good risk assessment process generates a vast amount of data, a large amount of which is qualitative. The inability to accurately quantify all collected data and/or properly analyze and interpret it can significantly undermine the quality of the results.

4. Biased Judgment

Objectivity of the risk assessment includes fairly assessing the full universe of potential risks. An organization needs to resist any temptation to ignore or de-emphasize risks simply because they may be costly to address (either from a financial or internal political vantage point). To help ensure objectivity, an increasing number of companies are involving domain-expert external advisors in the assessment.

B. Hire Outside Advisors

Organizations may also choose to hire the expertise of outside advisors or experts to help them conduct the organizational risk assessment.

1. Who Are They?

When deciding among outside advisors, depending on the level of knowledge or expertise required, an organization can seek to hire the resources of:

- Outside lawyers or law firm
- Audit firms
- Other compliance experts, consultants, etc.

2. Why is it a Good Idea?

There are several reasons, not always readily apparent, why utilizing the advice, counsel, or services of an external advisor is a good idea. A few of those are detailed below.

a. Document/Information Security

One of the benefits of using an outside advisor is the ability to keep sensitive or potentially damaging information off of company premises. By utilizing an independent third party, much of the information that is generated can be stored, maintained, or held by the third party. This is important because the various documents that are created may detail potential compliance problems of varying levels of severity. By keeping the information with a third party, the organization can better protect itself from private litigants and/or regulatory bodies obtaining this information and using it as evidence of pre-existing knowledge of compliance failures.

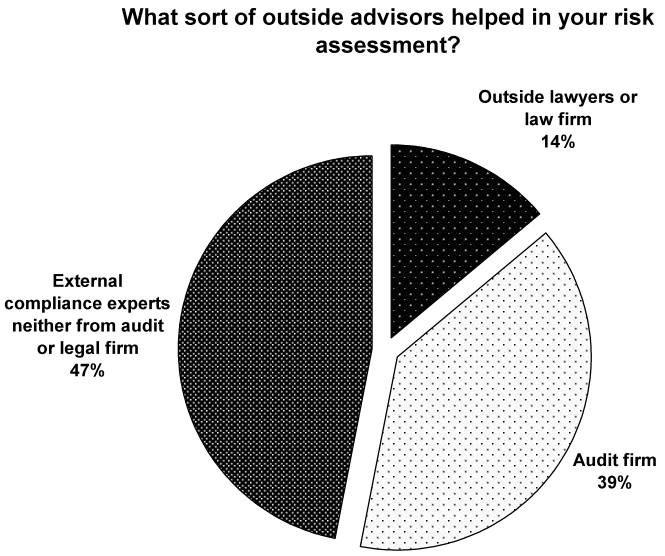
b. Analytical and/or Statistical Expertise

There is a high level of analytical and statistical expertise required for an effective risk assessment. Although some organizations may be more adept and experienced when conducting risk assessments, often, a wise choice may be to rely on the available skills and experience of outside consultants, who have current knowledge of the intricacies and frequent changes in the risk management field.

c. Non-Biased

When conducting a risk assessment internally, a natural bias will always exist. Individuals who are too close to the business operations have a tendency to misinterpret information and might overestimate or underestimate the degree of potential risk to the organization. This can introduce questions regarding the credibility of the risk assessment itself. As such, hiring an independent outside observer to help manage part or all of the risk assessment will help prevent the disillusioned effects of organizational bias.

Figure 16: Types of Outside Advisors Hired to Help Conduct Risk Assessments



Source: ACC-Corpedia 2005 Benchmarking Survey

IX. About the Author

Corpedia Corporation was founded in 1998 and its co-founders, Alexander Brigham and Jay Wiggins, continue to serve as President/Chief Executive Officer and Chief Technical Officer, respectively.

Corpedia designs, develops, and delivers award-winning custom and off-the-shelf, web- and computer-based ethics and legal compliance training programs to over 500 organizations across the globe. Our compliance library addresses more than 400 key topics and is developed in partnership with several prominent law firms—including Akin Gump, Sherman & Howard, Morrison & Foerster, Winston & Strawn, and O'Melveny & Meyers—and several nationally recognized think tanks and organizations, including The Conference Board.

Corpedia prides itself in being a total solution provider in the ethics and legal compliance arena. As one of the pioneers in our industry, we have seen the industry mature over the past ten years. In the past three years alone, the industry has changed significantly and, as such, our clients demand more from us in order to ensure that their program effectively complies with the Revised Federal Sentencing Guidelines and best practices.

To respond, Corpedia created the Total Corporate Ethics & Compliance Solution Set, a comprehensive suite of ethics and compliance-related products and services including: compliance program consulting; code of business conduct evaluation, creation, design and training; risk assessment, organizational health, and culture evaluation; risk-based training plan and curriculum development; ethics and compliance program design, review, benchmarking and audit; FCPA services; executive and board of director training; professional development, and more.

Corpedia has a dedicated team of internal consultants and attorneys with global expertise that help clients address the arduous task of building and managing an effective ethics and compliance program. Corpedia consultants include a highly qualified staff of former federal prosecutors, corporate ethics and compliance officers, lawyers, risk analysts, culture and communications experts, and more. Corpedia knows what it takes to guide clients through potentially confusing areas and is the only organization to bring such a qualified staff to the table.

X. Additional Resources

Alexander F. Brigham and Robert Leffel, "Benchmarking Compliance, Risk and Anticorruption Efforts–How Does Your Company Compare," ACC Presentation Transcript (Jan. 16, 2000) *available at* http://www.acc.com/resource/index.php?key=9537.

"2007 Compliance Program and Risk Assessment Benchmarking Survey," ACC Survey (2007), *available at* http://www.acc.com/resource/v8530.

John Beccia III ET AL., "Challenges Faced When Establishing an Enterprise-Wide Compliance Risk Management Program," ACC 2007 Annual Meeting, Session 208, *available at* http://www.acc.com/resource/v9046.

"Strategic Issues in Intellectual Property Risk Management," Briefing Material, ACC CLO Think Tank Series (2007), *available at* http://www.acc.com/resource/v8713.

XI. Sample Forms

A. Risk Universe Chart

Risk Areas	Industry Severity (1-10)	Industry Likelihood (1-5)	Organization Likelihood (1-5)	Organization Impact Score	Rank
Risk Area	7.4	2.8	2.7	100.9	1
Risk Area	8.4	2.9	2.3	95.3	2
Risk Area	6.3	2.1	2.9	90.5	3
Risk Area	6.1	2.2	2.9	89.5	4
Risk Area	7.5	2.0	2.4	88.1	5
Risk Area	5.6	2.3	3.1	86.5	6
Risk Area	5.2	2.6	3.2	81.7	7
Risk Area	6.0	2.5	2.7	80.6	8
Risk Area	5.9	2.7	2.7	78.4	9
Risk Area	4.4	3.4	3.3	73.4	10
Risk Area	5.0	2.8	2.9	71.7	11
Risk Area	6.2	2.9	2.3	71.1	12
Risk Area	5.9	2.8	2.3	67.0	13
Risk Area	5.7	2.7	2.3	66.3	14
Risk Area	4.5	2.0	2.5	56.3	15
Risk Area	8.5	1.9	1.3	54.6	16
Risk Area	4.0	3.7	2.6	51.0	17
Risk Area	5.8	1.8	1.7	48.2	18
Risk Area	5.0	2.1	1.9	47.8	19
Risk Area	4.9	2.1	1.9	47.5	20
Risk Area	5.0	2.4	1.8	46.2	21
Risk Area	5.6	1.6	1.5	43.0	22
Risk Area	4.0	2.2	1.9	38.0	23
Risk Area	4.5	1.6	1.6	35.8	24
Risk Area	6.9	1.6	1.0	34.9	25
Risk Area	4.4	2.3	1.6	34.8	26
Risk Area	3.0	2.1	2.3	34.5	27
Risk Area	4.0	1.9	1.7	31.0	28
Risk Area	4.8	1.4	1.3	30.9	29
Risk Area	5.2	1.7	1.2	30.0	30
Risk Area	3.0	2.0	1.9	28.5	31
Risk Area	3.6	1.9	1.4	25.3	32
Risk Area	4.4	2.0	1.1	23.3	33
Risk Area	2.0	3.2	1.9	19.5	34
Risk Area	1.0	2.9	3.6	18.0	35
Risk Area	3.2	1.3	1.0	16.4	36
Risk Area	1.9	1.6	1.5	15.0	37
Risk Area	2.1	2.5	1.5	15.0	38
Risk Area	2.0	1.6	1.3	12.8	39
Risk Area	2.0	2.2	1.1	11.0	40
Risk Area	1.1	1.0	1.6	8.0	41

B. Risk Severity Scale – Example

Score	1	2	3	4	5
Descriptive					
Reputation	*No reputation damage*	*Extremely minor reputation damage*	*Very minor negative impact; easily recoverable*	*Minor but noticeable localized negative impact; generally recoverable*	*Moderate reputation damage on a regional level; negative national media coverage (minor); generally recoverable over time*
Loss of stock value (%)	*~0*	*<1*	*1-2*	*2-5*	*5-10*
Damages, fines, settlements & legal costs (% of revenues)	*~0*	*<1*	*1-2*	*2-3*	*3-4*
Operations	*No operational impact or loss of business*	*Extremely minor operational impact or loss of business*	*Very minor impact on operations; easily recoverable*	*Limited impact on operations; minor loss of business; generally recoverable*	*Moderate impact on operations; minor to moderate loss of business; moderate changes in business model may be required; requires serious attention at the senior level*

Score	6	7	8	9	10
Descriptive					
Reputation	*Moderate to serious reputation damage; nationwide negative media coverage*	*Serious reputation damage; nationwide negative media coverage (serious); serious regulatory harm; partially recoverable over time with considerable effort*	*Severe reputation damage; negative national media coverage (severe); severe regulatory harm; low chance of recovery*	*Extremely severe damage to reputation; sustained and extremely negative national and international media coverage (front page); very low chance of recovery*	*Irreversible damage to reputation. Sustained and extremely negative national and international media coverage*
Loss of stock value (%)	*10-20*	*20-40*	*40-60%*	*60-90%*	*>90*
Damages, fines, settlements & legal costs (% of revenues)	*4-5%*	*5-7%*	*7-10%*	*10-15%*	*>15%*
Operations	*Moderate to serious impact on operations; moderate loss of business*	*Significant impact on operations; serious loss of business; possible elimination of business lines*	*Severe impact on business; significant loss of competitive positions; exit from significant market segments*	*Very severe impact on business with massive loss of revenue; exit from key market segments*	*Catastrophic impact on business with near total loss of revenue; recovery impossible*

XII. Endnotes

[1] *See generally* Project Management Institute, A Guide to the Project Management Body of Knowledge (PMBOK® Guide) (3d ed. 2004).

[2] U.S. Federal Sentencing Guidelines Manual § 8B2.1(c) (2005).

[3] "2007 Compliance Program and Risk Assessment Benchmarking Survey," ACC Survey (2007), *available at* http://www.acc.com/resource/v8530.

[4] U.S. Federal Sentencing Guidelines Manual § 8B2.1, app. n. 6 (2007).

[5] For more information on ECERA™, see Corpedia, Inc., *available at* http://www.corpedia.com.

[6] "2005 Compliance Program and Risk Assessment Benchmarking Survey," ACC Survey (2005), *available at* http://www.acc.com/resource/v6454.

[7] General Counsel Roundtable: "Performing a Legal and Compliance Risk Assessment," 1-5.

[8] "2007 Compliance Program and Risk Assessment Benchmarking Survey," ACC Survey (2007), *available at* http://www.acc.com/resource/v8530.

[9] "2005 Compliance Program and Risk Assessment Benchmarking Survey," ACC Survey (2005), *available at* http://www.acc.com/resource/v6454.