

Risk Assessment, Program Assessment and Corporate Culture

Jeff Kaplan

Stier Anderson, LLC/Midi, Inc.

Greater Houston Business Ethics
Roundtable, May 18, 2005

Overview of Presentation

- **Compliance Risk Assessments**
- **Overall Program Assessments**
- **Assessing Corporate Culture**

What is a compliance risk assessment?

- **At its core, it is not...**
 - **An *operational* or *financial* risk assessment.**
 - **An *investigation* or *audit*.**
 - **An assessment of where the company can be a *victim* of a crime or unethical act.**
 - **Fraud assessments are different.**
- **But the above processes are sometimes combined with compliance risk assessments.**

What is a compliance risk assessment?

- **Rather, it is an effort:**
 - **To obtain information concerning an organization's risks of:**
 - **Direct legal liability.**
 - **Indirect legal liability.**
 - **C&E-type reputational harm.**
 - **For use in designing, implementing and improving a C&E program.**

An example

- **The Revised Sentencing Guidelines mandate that companies train independent agents “as appropriate.”**
- **A risk analysis would tell you:**
 - Which agents need to be trained.
 - On what subjects.
 - How frequently.

Short legal history of risk assessments

- **Need was inferable from the 1991 Sentencing Guidelines and from other government (e.g., DOJ) standards, as well as some industry specific compliance mandates.**
- **But scandals of 2002-present have created a greater understanding of their importance.**

History (continue)

- **E.g., In 2003 SEC enforcement chief calls for COI risk assessments for financial service firms.**

Risk Assessments under the New Sentencing Guidelines

- **The 2004 Guidelines establish that risk assessments are a foundational element for other aspects of a C&E program:**

In implementing [the various other C&E program elements] the organization shall periodically assess the risk of criminal conduct and shall take appropriate steps to design, implement or modify [each element] to reduce the risk of criminal conduct identified through this process.

Our discussion of risk assessment

- **Explore risk assessment process by reviewing/commenting upon the results of a survey that I conducted among EOA members in July-August last year.**
- **Overview of the survey:**
 - **85 members responded.**
 - **From most major industry groups.**

Companies *are* doing risk assessments

- **Has your company conducted an RA in the last 12 months?
Yes – 68%, no 32%.**
- **More than half of those answering yes report having conducted more than one risk assessment.**

What they are looking for?

- **Risks of:**
 - **Criminal law violations – 57%.**
 - **Non-criminal law violations – 61%.**
 - **Ethical or reputational harms – 52%.**
- **Comment: this accords with necessarily broad (but often under-appreciated) reach of C&E programs (and recognition of often fuzzy lines between criminal/civil/ethical violations.)**

Sources of risk

- **Have you sought risk-related information about:**
 - **Performance pressure – 31%.**
 - **Incentives to engage in wrongdoing – 31%.**
 - **Organizational pressure issues – 33%.**
 - **Internal controls - 62%.**
 - **Lack of appreciation of applicable legal/ethical standards – 45%,**

Sources of risk (continued)

- **Third-party-related risks – 41%.**
- **Other factors – 18%.**
- **Comment – Some companies may not be seeking information in a wide or rigorous enough way – because all of the above could be useful or even essential in designing, implementing or improving C&E program elements.**

Who conducted your risk assessment?

- **Entirely in-house – 74%**
- **In-house/non-company personnel – 26%.**

Comment – makes sense not to completely outsource it for a variety of reasons. (But, value of outsider – a set of fresh eyes, so that you won't have blinders of industry practice, in the words of SEC chief of enforcement.)

Done under attorney-client privilege%

- **40% - yes, 60% - no.**

Comment – it probably depends on how litigation intense one's industry is.

What methods did you use?

- **Conduct interviews – 53%.**
- **Surveys/other written instruments – 41%.**
- **Focus groups – 24%.**
- **Review company documents – 53%.**
- **Review external (e.g., industry) information – 34%.**

A comment on methods

- **They are obviously not mutually exclusive.**
- **In my experience, often confidential interviews reveal richer risk data than do surveys/focus groups because:**
 - **1. Responding individuals may not have enough information to make the latter type of sources useful.**
 - **E.g., consider all the “why” categories – misunderstandings of law - described above**

Benefits of interviews

- **Also, respondents may need to have certain risks explained to them before they can evaluate the likelihood, possible impact or foreseeable causes of such risks.**
- **Second, individuals may be reluctant to respond to sensitive matters without appropriate assurances of confidentiality, etc.**

Benefits of interviews

- **This is true with:**
 - **The presence of risks. (It may be difficult for managers to admit that they have previously been allowed to exist without being addressed).**
 - **The presence of risk enhancers (e.g., performance pressure, customer-based risks, weak internal controls).**

If you conducted interviews, with whom did you speak?

- **Operations personnel – 49%.**
- **Functional staff – 52%.**
- **Senior management – 48%.**
- **Board of directors – 7%.**
- **Independent agents – 7%.**
- **Outside lawyers/consultants – 12%.**

Comment, with the possible exception of the board, I would try to do *all* of these in all risk assessments.

What I ask about in risk assessment interviews

- **Actual violations.**
- **Near misses.**
- **Violations and near misses among others in the industry.**
- **Laws/rules/industry standards.**
- ***And, what would the devil do in this part of the business to create liability/reputational harm?***

The “devil” question

- **Allows respondents to provide information without admitting to prior compliance failures.**
- **Encourages free thinking that can be key to a successful risk analysis.**

What is also useful in such interviews

- **Talking through everything that goes on in a business unit – and conducting risk “thought experiments” based on:**
 - **What *reasons* exist for risk creation (e.g., pressure, incentives, misunderstandings).**
 - **What *capacities* exist for risk creation (e.g., discretion, internal control weakness.)**
- **This can give you the vital “why” information for a risk assessment.**

7 questions for the interviews

- ***Where do you get ideas for products/services?***
- ***How do you sell/market?***
- ***How do you create/deliver products/services***
- ***Where do you operate?***
- ***Who works for you?***

7 Questions continued

- ***Who are your customers?***
- ***How are you paid?***

List not exclusive.

Each question has many sub-questions.

Did you prioritize risk in a quantitative way?

- **Yes – 70%.**
- **No – 30%.**

Comment – I would be careful here. Prioritization is necessary under the Guidelines, but quantification is not.

Who received information about the risk assessment?

- **Senior management – 53%.**
- **The board – 27%.**

Comment – as new Guidelines go into effect, both groups should receive such information as a matter of course. (Indeed, for the board, it can be essential as a means to *reasonably* oversee the C&E program.)

Were results used to develop/modify:

- **Written policies – 55%.**
- **Training/other forms of communication – 54%.**
- **Compliance auditing/monitoring – 51%.**
- **Assignment of responsibility – 33%.**
- **Reporting relationships – 13%.**

Final thoughts on risk assessment

- **Document your process.**
- **Create a regular cycle.**
- **Build risk assessment into other aspects of the C & E program.**
- **Try to get the additional benefit of risk assessment interviews - as a means of high-level communication about the program itself.**

Overall Program Assessments

- **Sentencing Guidelines create a clear mandate –**
 - ***The organization shall take reasonable steps ...to evaluate periodically the effectiveness of the organization's compliance and ethics program.***

Assessments and the Law

- **Additionally, assessments are advisable under new leadership responsibilities**
- **Board’s duty to oversee the “implementation and *effectiveness*” of the program.**
- **Top management’s duty to “ensure that the organization has an *effective* compliance an ethics program.”**

Assessments and the law

- **As a general legal matter, officers and directors can meet due diligence/oversight duties (in part, least) by reliance on experts.**

Assessments and the law

- **Another dimension to assessments relates to the fact that if a company gets in trouble its program will be “assessed” in a hostile setting.**
- **Companies may wish to consider how their program (including program documentation) would fare when scrutinized by an adversary.**

Three levels of assessment

- **General program review**
 - Legal efficacy of program elements against applicable standards.
 - Guidelines.
 - Other general standards.
 - **Best practices**
 - Because law is not that specific.
 - Because as a practical matter, these are suggested by legal analysis.

Basis of the assessment

- Organizational culture.
- Deep dives into selected risk areas.

General Program Assessment

- **Legal review:**
 - **On one level, the most straightforward aspect of the assessment.**
 - E.g., does the code of conduct meet applicable standards?
 - **But even on this level things get missed.**
 - E.g., Discipline for supervisory lapses.

General Program Review

- **It becomes more complex when combine:**
 - **Revised Guidelines elements, with**
 - **Risk- and culture- based assessment, and**
 - **Review through a best practices lens.**

General Program Assessment

Selected topics

- **Assessing the risk assessment.**
 - Using some of the criteria previously described.
- **The role of the board.**
 - Are they getting the right information?
 - Are they sufficiently engaged?

General Program Assessment

- **High-level personnel**
 - What is done to *ensure* program's effectiveness?
 - See handout.
 - How knowledgeable are HLP's about Program?
 - How are they perceived by employees?
 - Use of focus groups.

General Program Assessment – selected topics

- Day-to-day person
 - Authority/Access.
 - Resources.
- Line managers
 - How are they perceived?
 - Use of focus groups.

General Program Assessment – selected topics

- How well do incentives align with company's professed C & E values?
- Does the training really reach the employees? What message do employees draw from it?

General Program Assessment – selected topics

- **Do employees feel comfortable calling the HelpLine? How much concern is there about retaliation?**
 - **Focus groups/surveys are key.**
- **Is discipline fair and even-handed? Is there a perception of favoritism?**

General Program Assessment – Selected topics

- **Ethics, as well as compliance:**
 - **Is there a framework for discussion (both in terms of substance and process)?**
- **Application to third parties.**
 - **Has this been analyzed to a meaningful degree?**
 - **Where do joint ventures fit in?**

General Program Assessment – Selected topics

- **Documentation**
 - **How is it organized?**
 - **Is there a retention program for the E & C office's own records?**

Culture Assessment

- Two levels of inquiry:
 - Culture and ethical/law abiding behavior.
 - Culture and the C & E program.

Culture and ethical behavior

- *Identification with the company*
 - Lack of respect for employees is a contributor to unethical behavior.
- *Identification with customers*
 - The insurance industry example.
 - The specialty pipe example.
- *Sense of business mission*
 - Belief in value of company's products/services makes crime less likely.

Culture and ethical behavior

- *Pressure*
 - Contrasting the (presumably legitimate) pressure management thinks is there with what employees may feel.

Culture and the C & E Program

- Another inquiry: How well does the Program use/address cultural factors to minimize illegal and unethical conduct?
 - E.g., do training, discipline, etc., deal with pressure?
 - Are cultural strengths used to best C & E advantage?
 - E.g., emphasizing pride in products and services makes short cutting less likely.

Culture and the Program

- Another issue: How does culture bear on the operation of “program elements.”
 - Does culture make it easy or hard to report violations/express concerns?
 - Are compliance functions (including Law Dept.) marginalized? (The WorldCom finding.)

Deep Dives

- Third-level of assessment.
- Based on recognition of *context-specific* nature of violations.
- Typically in high-risk areas (e.g., FCPA., antitrust).

Deep Dives

- Use of standards applicable to the areas in question. E.g.,
 - Do you do antitrust auditing, as indicated by key DOJ speech?
 - Do you monitor agent activities, as suggested by FCPA cases?

Deep Dives

- Also use a Revised Guidelines lens:
 - How do you assess risks in a given area?
 - Is there sufficient ownership of that area?
 - Is there a need for high-level involvement?
 - What are resources?
 - How effective is the training?
 - Do you do auditing (both kinds)?
 - What is third-party reach?
 - How do you assess performance?

Summing up

- Revisions to USSG (Guidelines 2.0) have raised the bar in many ways.
- Risk assessment is needed to ensure that your plan for meeting new standards is adequate.
- Program assessment helps you determine if you're meeting your plan.