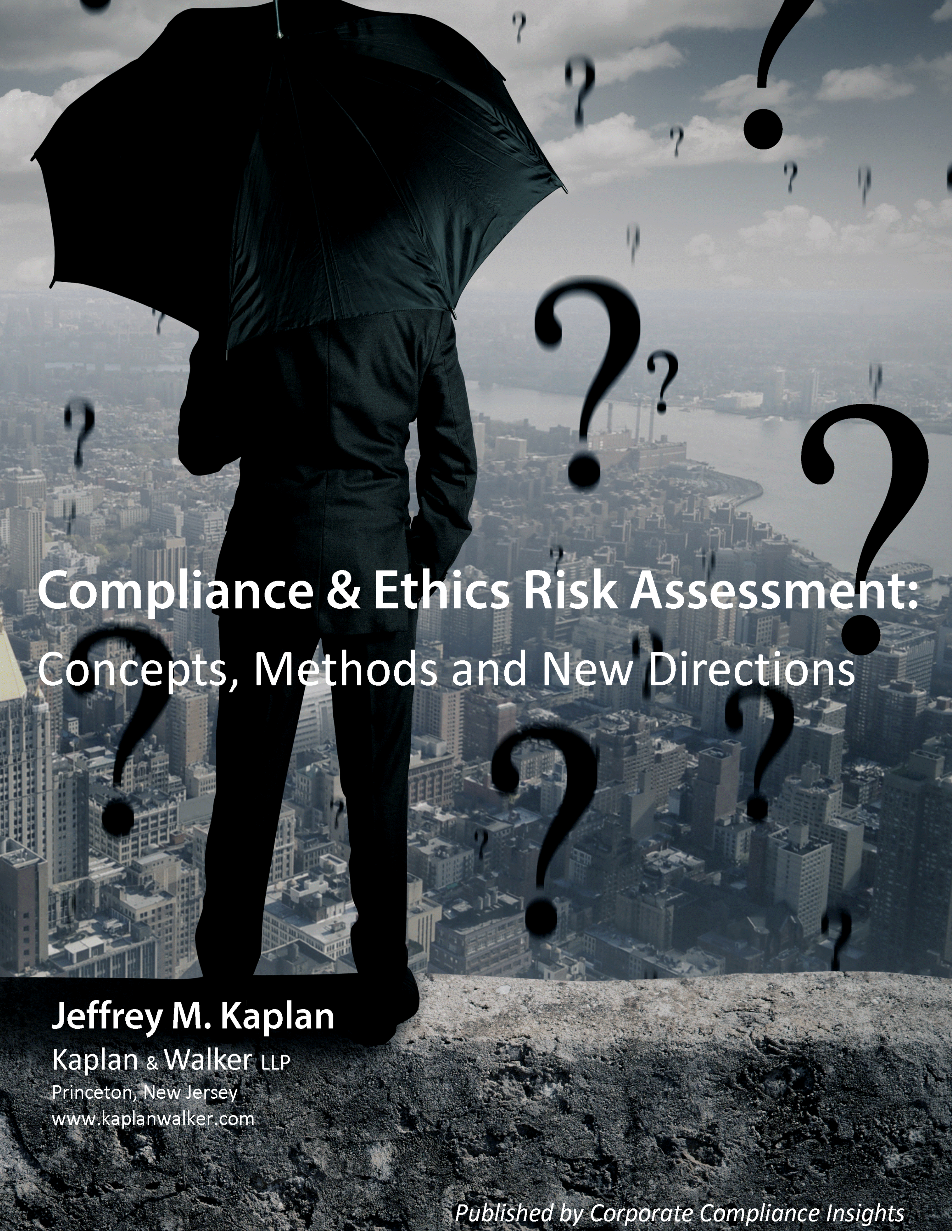

Compliance & Ethics Risk Assessment:
Concepts, Methods and New Directions

Jeffrey M. Kaplan
Kaplan & Walker LLP
Princeton, New Jersey
www.kaplanwalker.com

Published by Corporate Compliance Insights

Compliance & Ethics Risk Assessment: Concepts, Methods and New Directions

Jeffrey M. Kaplan
Kaplan & Walker LLP
Princeton, New Jersey
www.kaplanwalker.com

Copyright ©2013 Corporate Compliance Insights
Dallas, Texas

CONTENTS

Acknowledgements

I am grateful to Maurice Gilbert, Sarah Drost and the whole team at *Corporate Compliance Insights* for publishing my various columns on risk assessment in *CCI* and for their assistance in assembling this e-Book.

I am also grateful to my wife Deb Sugarman, son Ben, daughter Elizabeth and law firm partner Rebecca Walker for putting up with my tendency to see a risk around every corner.

-JMK

Introduction

This is an e-Book about compliance and ethics ("C&E") risk assessment, but it does not cover everything that every company or C&E professional needs to know about this vast, complex and important topic. Rather, it touches on an array of risk assessment ideas, methods, practices, tools and noteworthy items of C&E-related history that I think many organizations and practitioners need to know more about, and that have therefore been the focus of my columns in *Corporate Compliance Insights* for the past three years.

My interest in the topic goes back to the advent of the Federal Sentencing Guidelines for Organizations (the "Guidelines") in 1991 when I saw that there was a missing piece to their articulation of what was then called "an effective program to prevent and detect violations of law" (and what became, with the 2004 amendments to the Guidelines, an "effective compliance and ethics program"). That piece was risk assessment,[1] and so in 1993, when I co-edited a treatise on the Guidelines,[2] I drafted a chapter on risk assessment (called at the time a "liability inventory").[3] During the course of the 1990's wherever possible, I tried to include a component of risk assessment in my C&E advisory engagements.

Risk assessment was finally added to the Guidelines, in the 2004 amendments. It is now widely seen as the foundation of effective C&E programs.

Of course, largely independent of what was happening with the Guidelines (let alone my writings) the notion of broad-based risk assessment with compliance as one of several dimensions had been advanced through the COSO approach[4] to risk management with which C&E professionals are generally quite familiar. Nothing in this e-Book is meant to suggest that there are infirmities with this profoundly beneficial development.

Rather, the various columns here are intended to supplement and inform C&E risk assessments of all kinds, whether COSO-based or otherwise. That is, they are offered to help companies and their advisors enhance their current risk assessments practices by developing risk-related information in a way that can be most useful to maintaining all aspects of C&E programs in an effective manner.

---

[1] Of course, there were other missing pieces – but this one seemed to the most important to me.

[2] Kaplan & Murphy, *Compliance Programs and the Corporate Sentencing Guidelines: Preventing Criminal and Civil Liability* (Thomson Reuters 2013 ed.) (cited below as "Kaplan & Murphy"), Chapter Six.

[3] A decade later, that chapter was cited in a favorable way by an advisory group to the US Sentencing Commission, which recommended that risk assessment be added to the Guidelines – as indeed happened in the 2004 amendments. *Report of the Ad Hoc Advisory Group on the Organizational Sentencing Guidelines* October 7, 2003 available at http://www.ussc.gov/Guidelines/Organizational_Guidelines/advgrprpt/advgrprpt.htm at 91, n 280.

[4] Committee of Sponsoring Organizations of the Treadway Commission - http://www.coso.org/.

Risk Assessment Methodology and Scope

There is no one way to do a C&E risk assessment. However, from my experience with client organizations and what I know of the experience of others, the following general points seem worth noting.

First, assessing the likelihood of risks is vitally important to making decisions on how/where/when to deploy C&E program elements. Moreover, the process of assessing likelihood itself can be instructive to those involved, i.e., it can serve to raise awareness of C&E generally in a company.

Second, the utility of assessing the impact of C&E risks is often overrated, at least when done (as it often is) through a survey of employees - because those who are asked to assess impact may not have sufficient information to do so in a meaningful way. For example, if employees are asked in a survey to assess the potential impact of an antitrust/competition law violation and respond that such impact would likely be low, that is probably not a reliable piece of data, given that the heavy fines in this area are a matter of public record.[5]

Third, in addition to likelihood and impact, a C&E risk assessment should attempt to identify circumstances in which a violation is reasonably likely to occur. For instance, in the competition law field simply saying that a violation is likely and/or would probably be impactful does not get one very far in terms of designing effective (and targeted) mitigation. Rather, one would also want to know a) what type of violation (e.g., division of territories, price fixing, or abuse of a dominant position) should be of greatest concern; b) what products/services create the greatest competition law risks; c) what geographies are associated with the greatest risk of this sort of violation; and d) more about the circumstances in which a violation is reasonably likely to arise – (e.g., trade association meetings, teaming arrangements?) All of these sorts of factors I refer to collectively as the nature of the risk.

Of course, one would hope to ask similarly detailed questions about many other risk areas – such as corruption and confidential information. The point of all of these sorts of inquiries is to help the C&E officer develop "news you can use" – i.e., deploy program elements (such as training or monitoring) in the sort of risk-sensitive ways contemplated by the Guidelines and other C&E standards.

It is in this third dimension that I most often see risk assessments falling short of where they need to be. My hope is that some of the suggestions in this e-Book can help bridge the gap when it comes to understanding the nature (as well as likelihood and impact) of a C&E risk.

---

[5] Note, though, that in this situation, while not reliable, the response data may still be useful – to show the need to make managers more aware of the potential impact of an antitrust violation.

Fourth, while risk assessment can and should be a stand-alone process, there are also ways of building risk assessment into everyday business life, as discussed in one column in this first section. In my experience, many companies also have room for improvement on this front too.

Fifth, because it involves a self-critical exercise in areas that can hold considerable jeopardy for a company, C&E risk assessment is inherently difficult. One way of surmounting the reticence that employees often have to be candid about such areas as anti-corruption or competition law risks is by conducting the assessment under the organization's attorney-client privilege.

Finally, Justice Holmes famously noted that a page of history can be worth a volume of logic, and I think that is particularly true with risk assessment. So, I have tried to include a few pages of what I think are important C&E history – such as the Bankers Trust derivatives scandal and the Hoffman-LaRoche antitrust prosecution, both from the 1990's; or the TAP case, from 2001 – in this volume.

Does Your Risk Assessment Do This?

The U.S. Sentencing Commission is currently[6] considering making changes to the risk assessment provisions of the Corporate Sentencing Guidelines – and this offers a good occasion for companies to evaluate their own risk assessment practices.

While there are many standards for such an evaluation, to my mind the best is the simplest: does the process actually produce results that will help the company have effective C & E program elements? And in self-assessing against this standard, a company might ask whether its current process helps the company do the following:

- Determine whether additional C & E policies are needed for any given part of the company (e.g., business or geographical unit) on any given topic, or the extent to which such policies need to be revised.
- Develop company-specific examples or Q & A that can help make a code of conduct less abstract.
- Determine whether any additional C & E communications (training or other) should be targeted at any particular part of the company on any given topic.
- Develop/enhance C & E audit protocols, monitoring tools and other approaches to "checking" on both an enterprise-wide and local "level."
- Identify C & E risks for which additional controls are warranted, such as pre-approvals by management or staff for specified (high-risk) activities.
- Establish additional C & E oversight/reporting responsibilities for high-risk areas.
- Add C & E components to job descriptions, performance-evaluation criteria or business unit plans in a risk-based way.
- Determine whether incentives in any part of the Company pose an undue risk from a C & E perspective.
- Assess where and the extent to which aspects of a C & E program should apply to contractors, vendors and other third parties.
- Develop metrics for measuring the effectiveness of C & E efforts directed at individual areas of risk. (Note: for many companies metrics are still purely a matter of overall program process, e.g., number of calls to Concerns Line), and are not risk-area specific.
- Identify true ethics, as well as compliance, issues that the Program should address.
- Identify cultural C & E risks, such as lack of employee identification with the company or its mission, short-term thinking or other "moral hazard" related risks.
- Provide a stronger foundation for the Program oversight by the Board.
- Provide a basis for future/"evergreen" risk assessments.

In the columns that follow, I explore ways of using risk assessment for most of these and some other related purposes.

[6] As of early 2011. Ultimately, the Commission did not revise the risk assessment provision of the Guidelines at this time.

Third-Party Compliance and Ethics Risks: "Capacities" and "Reasons"

In the world of C&E risk assessment and mitigation third parties often present a special challenge, both because of the magnitude of the risks they pose and the difficulty of mitigating those risks.

This phenomenon is not new. In the 1980's, a number of significant defense industry procurement prosecutions arose from the actions of third-party business representatives. In the 1990's, many sales practices abuse cases in the life insurance industry centered around the actions of independent sales agents. More recently, various manufacturing companies suffered severe reputational harm from the labor practices of their suppliers. Most recently, corrupt practices by agents and distributors have been the basis for numerous FCPA prosecutions.

And, there is almost certainly more coming – probably a lot more. This is because of the seemingly inexorable trend in modern business to increasingly rely on third parties, for instance, through outsourcing or joint ventures.

How should companies try to stay ahead of the third-party risk curve? One way is to use a defined process for inventorying their third parties and analyzing the C&E risks for each.

Cataloging third parties – while potentially time consuming – is conceptually straightforward. But how can one begin to analyze the C&E risks associated with each of them?

The risk assessment concepts of capacities and reasons – meaning the capacities and reasons to engage in wrongdoing – offer a framework for such an analysis.

This is a complex subject, needless to say, but in brief, capacities tend to be specific to a given type of wrongdoing. For instance, the capacity to engage in certain types of competition law violations would include having pricing and/or bidding discretion; the capacity to violate privacy standards would depend largely on one's access to private data; and the capacity to commit fraud would turn in part on the ability to make or impact representations (express or implied) about an organization's products, services, financial condition, etc.

Reasons, by contrast, tend to be broader in nature, i.e., not specific to one type of offense. An obvious example is an incentive-based reason, such where an agent's compensation is based wholly on the amount of business she generates – a reason that can be particularly risk causing in a short-term relationship. Cultural reasons can also be significant, such as where the third party's values are generally questionable or where it fails to appreciate the importance of C&E standards in particular.

Depending on the results of this inventory and assessment, one should determine the appropriate mitigation measures for each type of third party with respect to each significant risk. The results of the analysis will be driven in part by the assessment of risk – not only quantitatively (i.e., how great is the risk?) but qualitatively, too (e.g., if the reason for the risk is that the third party fails to appreciate applicable C&E standards then training or other communications measures might be called for.) However, in conducting this analysis one must be mindful of the potential downsides of becoming too deeply involved in managing a third party's business, which can also be case specific.

Finally, for some companies creating this inventory will not be a minor undertaking. But the alternative is to be at the mercy of the unknown, which in the C&E realm is never a good thing.

"NANO COMPLIANCE"

In the great book of corporate compliance program failures, one of the most important stories is from the Bankers Trust derivatives marketing scandal of the mid-1990s. In that case, the bank – a major U.S. financial institution that was bought by Deutsche Bank shortly after the events in question here – was sued by both the government and various counterparties for deceptive practices in selling highly complex derivative instruments. (In some ways, the matter could be seen as a "prequel" to aspects of the financial meltdown of 2008.)

In connection with one of those cases, the government appointed an independent counsel to determine what the causes of the bank's compliance failure were, and interestingly he found that the bank did have policies and other compliance measures in place addressed to marketing derivatives appropriately. What the bank lacked was a key single piece for any compliance system: the designation of an individual to make sure those other measures were in fact being followed.

Given the horrific consequences to Bankers Trust of this lapse, the story calls to mind, "For want of a nail a shoe was lost," and so on up to the loss of a kingdom. It also suggests a need to "think small" – and to practice "nano compliance."

What is nano compliance? It is a local focus on the most risk-variable elements of a compliance and ethics program. By "risk-variable elements," I mean those addressed to setting standards, training and communications, auditing/monitoring and the various types of internal controls discussed in an earlier article. Other elements – e.g., investigations – can, but are less likely to, have a local dimension. And by "local," I mean not only using a geographic dimension but also analyzing risk by focusing on product and service lines or staff functions.

So, to illustrate, using the broad risk area of competition law, one would:

- Look at all of the above-listed dimensions – e.g., by geography, product line, etc. – to determine which have non-trivial competition risks. This can include examining the intersection of two or more dimensions (e.g., competition law risks of a product line in a given geography).
- Determine what existing mitigation is for each (meaning for each dimension or intersections of dimensions) using the five risk-variable elements, e.g., what competition law training or auditing there is for the high-risk dimensions or intersections.
- Identify what other mitigation (if any) is warranted for these dimensions or intersections.

This can be a significant undertaking, as can the process of monitoring the mitigation. But, at least for some complex organizations – particularly decentralized ones – it can help prevent the kingdom from being lost.

Refresher Risk Assessments

By now,[7] many companies have conducted foundational C&E risk assessments in response to the 2004 revisions to the Guidelines which established risk assessment as an overarching requirement of an effective C&E program. But risks obviously change over the course of time – both as a general matter, and by "mutating" in the face of newly constructed compliance-related obstacles. Companies developing C&E plans for 2013 may therefore wish to conduct a refresher risk assessment if they have not done so recently.

Indeed, the Guidelines speak of the need to assess risk periodically. But official C&E guidance documents are less clear on what a refresher risk assessment should entail, and so here are some considerations on this important but somewhat conceptually challenging topic.

First, one should review the foundational risk assessment and any subsequent refresher assessments to determine what circumstances have changed since those reports were prepared. Risk-related changes can, of course, be either internal (e.g., based on a new business line, a new geographical presence) or external (such as enhanced risk-causing pressures from customers or new scrutiny by enforcement agencies). Identifying which of the circumstances identified initially as relevant to risks have changed can be a good starting place for a risk assessment refresher.

Second, one should review how well identified risks in fact have been mitigated under the company's current approach. I stress this because the imperative of the Guidelines not only to assess risk but to use the results of the assessment in designing/improving all other parts of a C&E program is itself widely underappreciated. A refresher risk assessment can be a good opportunity to consider this unexciting but very important part of a compliance program.

Third, if you have not already done so, use the occasion to conduct a "deep-dive" assessment of substantive areas of high risk. Corruption is the most obvious such area for many companies. However, competition law is – at least for some organizations – also worth focusing on. Indeed, assessing pure ethics risks can be an important part of a refresher process – both to show that a company is serious about ethics, as well as compliance, and also to help identify compliance "risks around the corner."

Fourth, the assessment can be an occasion to develop in a comprehensive way a more granular understanding of risk, not only with respect to substantive areas of law (like corruption) but also the many parts of a company (including geographical and business units). This approach is discussed in more detail in an earlier column on "Nano Compliance."

Finally, and related to the immediately preceding point, the refresher assessment might include detailed review of how a company assesses C&E risks on its "frontier," meaning with respect to organizations that are not fully under the company's control but which can still create C&E risk for it. Two columns appearing later in this e-Book on assessing joint venture risks discuss part of what this sort of effort might entail, although

[7] As of 2012.

there is obviously much more that could be done in this regard.

Law Departments and Risk Assessment

Much has been written on the need for C&E functions to be independent of law departments but considerably less about the critically important roles of in-house counsel in assessing and mitigating C&E-related risk. For many companies, an ideal interplay of the two disciplines can be found in a model that, among other things, articulates assessment and mitigation responsibilities for both law and C&E departments in a risk-specific way.

For instance, under this approach, on a yearly basis the law department attorney with responsibility for antitrust would be required to provide the C&E officer with an analysis – using a defined set of parameters – of antitrust risks at the company (broken down, where useful to do so, by different geographies and business segments) and of the efficacy of C&E program elements in addressing such risks. He would also offer any suggested improvements to the latter in light of the former.

The C&E officer would then review this information with the attorney and suggest possible revisions. Together with similar information for other risk areas (e.g., corruption), she would present an analysis of her findings/plans in a detailed way to senior management (or some subset thereof) in the company and in a high-level way to the board committee tasked with C&E program oversight.

Such reports can help senior managers ensure the efficacy of a C&E program and board members exercise reasonable program oversight. They can also provide internal auditors with a basis for informed program-related auditing. And, the reports can help document the company's C&E progress for possible use in the event that it ever needs to "prove" its program to the government.

Finally, and most importantly, while preserving some independence between a law department and C&E personnel, the model can help a company draw – in a best-of-both-worlds way – on the substantive expertise of the former and the C&E program expertise (e.g., how to make training effective) of the latter. Indeed, particularly for companies with relatively high-risk profiles (whether due to the nature of their business, where they operate or other factors), both types of knowledge can be essential to C&E efficacy.

Risk Assessment: the "Demand Side" Analysis

Some C&E risk assessments are focused entirely on what might be called the "supply side," meaning on matters internal to a company giving rise to risk. But for most businesses, a full accounting of risk should also include the "demand side," meaning the risk creating impact of law enforcement priorities. Indeed, understanding the demand side may be critically important, at least in some organizations, to identifying "the risk around the corner."

At its most obvious, a demand side risk factor would be the government's perceived need to "make an example" of companies and/or individuals in a high priority area of law. The current focus on bringing FCPA prosecutions in the life sciences industry may be a reflection of this.

A less obvious but increasingly important demand side factor is that governments increasingly need money. And, in some instances, criminal prosecutions can be a non-trivial source of revenue for governments.

What does this mean from a C&E risk perspective? First, as a general matter, we are likely to continue to see "mega fines,"[8] which suggests in an across-the-board way the need for heightened attention to C&E.

Second, and more specifically, it could mean a greater focus on the types of criminal prosecutions or other proceedings that have the potential to result in large fines or other payments from companies. Chief among these is competition law/antitrust, and indeed we already seem to be in the midst of a significant expansion of competition law enforcement globally.

Competition law is also a good area for targeted risk assessment, because the risks here can vary dramatically by geography and product/service line. And – at least for some companies – it is a good area for additional mitigation such as training (particularly for senior executives), because understanding of competition law rules, and of the severity of penalties for violations, is far from universal.

What other risks might become more significant due to this demand side phenomenon? Presumably, tax-related ones will. Indeed, in recent years the US government has sharply increased its tax enforcement efforts in various ways, and it is hard to imagine that other countries (and other jurisdictions, such as state governments) will fail to do the same (because, as Willie Sutton said of his reason for robbing banks, "That's where the money is.")

Of course, few, if any, C&E officers have primary responsibility for tax compliance at their respective organizations. However, a fair – and for some companies, important – question for C&E officers to ask as part of a risk assessment is whether the organization's tax practices are consistent with its overall approach to doing business in an ethical manner.

[8] See list of ten largest corporate criminal fines in the US as of year-end 2012 at http://conflictofinterestblog.com/2013/01/a-record-year-for-corporate-criminal-fines.html. .

RISK, CULTURE AND "SOFT POWER"

Perhaps all C&E professionals know that a key element of risk assessment is determining culture-based risk, but not all companies use the cultural dimension of risk assessment to full advantage. This column will offer some practice pointers for doing so.

What risks? A list of cultural factors that could create or enhance risk includes the following:

- Short-term thinking
- Weak employee identification with the company, its customers, or its products/services
- Other indicia of "moral hazard" (misalignment of incentives and risks)
- Difficulty in asking questions/raising concerns (not just C&E ones)
- Marginalization of C&E issues or personnel
- A sense of unfairness or concern about lack of "organizational justice"
- Questionable managerial tone – not only at the top, but also in the "middle" and at the "edges"
- Unreasonable pressure to perform
- Rewarding bad conduct through promotions, compensation, etc.

.

What culture? At the most obvious level, an organization's own culture (or cultures) should be assessed. Perhaps equally obvious but less frequently done, relevant aspects of cultures in the geographies in which a company operates should be assessed for risk, too.

Finally, least obvious and quite infrequently the subject of assessment, a company should examine the risks arising from industry or professional cultures relevant to its business. This is particularly true of industries with a high degree of intercompany mobility.

Why culture? As noted above, C&E personnel universally understand the need to include a cultural dimension in risk assessment, but the importance of doing so may be less evident to others at a company. Being able to "sell" this internally may therefore be key to getting management support for the effort involved.

One way to do so is point out that a company with a strong culture C&E wise may actually need fewer of the restrictive aspects of a compliance program than a culturally imperiled organization. That is, just as the "soft power" (a phrase coined by Joseph Nye of Harvard) of diplomacy and other non-coercive sorts of influence can, in some instances, offer a more effective means to conduct foreign relations for a nation than armed intervention, so a healthy corporate culture can provide a type of soft power for C&E that may be more cost effective and otherwise desirable than the "harder" approach of having pervasive policies, procedures and monitoring.

Training Managers to be C&E "Risk Sentinels"

What does it mean for a manager to be ethical? At a minimum, of course, he or she must obey relevant laws and other standards of conduct herself, but in an age of maximum consequences for violations presumably the minimum in ethicality is only the starting point. Organizations seeking to minimize risks of this kind should also expect – and train – managers to have a heightened degree of ethical awareness, so that (among other reasons) they can be "sentinels" in spotting C&E risks.

Training managers to be effective risk sentinels has several aspects to it. One focuses on key C&E risk areas. By way of example, for confidential information one might:

- Begin the training with an attention getting hypothetical.
- Identify the principal categories of confidential information (by type and ownership).
- Describe the various legal and business imperatives for strong compliance efforts in this area.
- Review applicable company policies and procedures relating to confidential information.
- Identify pertinent "red flags."
- Examine some of the particular compliance challenges managers might face with respect to spotting confidential information issues.

A second aspect of this training is helping managers understand the general causes of risk, meaning risk causing factors that can lead to violations of all kinds. At an organizational level, these include pressures (both internal and external), compensation approaches, "organizational justice," workforce alignment with the company and its mission, openness of communication, and other cultural factors (including relevant regional and industry ones). However, the training should also address risk causing factors that disproportionately impact individuals in positions of power[9] or the fact that people in such positions seem to have an easier time lying than do others.[10] In other words, to be a true risk sentinel a manager needs to understand the risk "within."

Finally, the training should provide guidance on how managers can help address risks. This includes, of course, some things that they can do on their own, e.g., recognizing and encouraging ethical behavior by their subordinates. But often the role of a "sentinel" is to spot a threat – not to deal with the threat herself, and as C&E risk sentinels it is vital that that managers understand the need to follow the company's C&E escalation policy when issues arise.

---

[9] See sections on behavioral ethics later in this e-Book.

[10] See http://hbr.org/2010/05/defend-your-research-powerful-people-are-better-liars/ar for more information on this, and also on research tying power to risk taking.

Focusing on Managers' C&E Risks

A CEO – considerably wiser than most in these matters – once noted to me in the course of a risk assessment discussion that a compliance and ethics program should not "spread the peanut butter evenly" across the organization, meaning that a program's mitigation tools should be focused most on those who can create the most risk – the company's managers. Indeed, due to the 2010 amendments to the Guidelines concerning wrongdoing by high-level personnel, enhancing what might be called the managerial dimension of their C&E programs should be the concern of all companies. In this column I briefly examine three practical ways of doing this.

The first and most obvious of these is to provide manager-specific C&E training. Among other things, the training should address general C&E related responsibilities of managers – e.g., maintaining awareness of actions of subordinates, creating a work environment where it is relatively easy to raise ethical issues – including by responding appropriately to C&E concerns, leading by example and otherwise promoting a strong ethical culture. The training should also cover key individual areas of risk (e.g., conflicts of interest, confidential information/insider trading, use of company resources, financial reporting, corruption, competition law) to sensitize managers to their own risks of wrongdoing. One practice pointer: to get real buy in, consider presenting the training as a form of leadership development – i.e., a way of achieving a "heightened ethical awareness" that can be useful for career development, and possibly necessary for career survival.

A second, somewhat less common means is to ensure meaningful management oriented C&E components to key personnel decisions. This might include:

- C&E-based "behavioral interviewing" for management positions.
- C&E leadership-related questions and expectations in performance appraisals and performance management plans (e.g., does the manager provide feedback to others with regard to their compliance with company standards and procedures?)
- C&E department input into succession planning.

Third and most challenging, companies should consider requiring before-the-fact C&E consultations in connection with risk-sensitive decisions by managers. Such decisions might include developing new products or services, using new production or distribution means or moving into locations of relatively high C&E risk.

Note that each of these individual strategies should not be deployed in isolation from the others. For instance, the training should build on the leadership-related C&E performance criteria. And, the risk-based consultations can include an element of "just-in-time" training (which, behavioral economics research teaches, can be a particularly effective approach to risk mitigation.)

Finally, note that this is not remotely an exhaustive list. Among other things, it does not address management-focused approaches/issues relating to risk assessment, audits, investigations, discipline for violations, employee surveys and board C&E program oversight. Hopefully, however, the discussion will be helpful to some in optimizing distribution of the "peanut butter."

Conducting Risk Assessments Under the Attorney-Client Privilege

Should risk assessments be conducted under the attorney-client privilege? There is no one-size-fits-all answer to this question, but in every instance that a company is planning a risk assessment it should at least be considered.

I say this because without the protection afforded by the privilege some employees may resist providing the sort of candid critical information that may be necessary for a program to be effective. Indeed, I recall many years ago one executive of a financial services firm being asked to take part in a risk assessment interview and responding, "Are you crazy?" But when he was told that his comments would be treated as privileged and confidential he readily went ahead with the interview (and contributed valuable information to the process).

Of course, getting potentially damaging information is absolutely key to risk assessment efficacy for high-risk areas of law. Chief among these are the corruption and competition law areas, but for many companies there will be others (e.g., privacy for organizations that possess significant amounts of private customer information).

If choosing to proceed under privilege, one must be mindful of all the formal requirements of law in this area, starting with the documentation establishing the purpose of the assessment. Typically, I suggest that the engagement letter (if an outside firm is involved) state that the attorney is providing legal advice to help the company meet C&E-related expectations and otherwise reduce legal risk. (The latter part is to cover situations where legal standards are not clear or where the attorney is likely to recommend best practice C&E approaches that go beyond legal standards.) One must also treat the information obtained in the assessment as confidential.

Finally, the attorney must in fact give legal advice for the communications in question to be privileged. However, this should not be seen as a burden, as focusing on ensuring that the privilege is maintained can itself encourage a company to pay sufficient attention to C&E-related law, which, in turn, can be useful from the perspective of ensuring program efficacy.

Areas of Risk

The heart of any risk assessment is assessing substantive areas of risk. Each will, of course, have its own assessment methodologies, based on the nature of the prohibitions/restrictions involved.

For instance, in assessing insider trading risks for a given company one would look at the following factors, among others:

- Is the company's stock volatile?
- How much material inside information (beyond what is obvious) about itself does a company have?
- How many individuals (employees and others) generally have access to the company's inside information?
- To what extent does the company have material inside information about other business organizations?
- What is the state of the company's inside-information-related controls?

However, there are also various assessment-related commonalities among the different risk areas.

In this section of the e-Book, we look at two areas of legal risk - corruption and competition law, and one area that combines both ethics and legal risk - conflicts of interest. In a later section we look at how to assess and address true ethics risks.

Finally, for those considering which areas of legal risk to assess in their organizations, the Appendix at the back of this e-Book – a comprehensive list of legal risk areas, prepared by Joe Murphy – might be useful.

Competition Law

Based on the frequency of very large fines, no compliance risks are, as a general matter, greater than those in the area of competition/antitrust law. Yet many companies devote far too little effort to assessing and addressing such risks.

An important guidance document recently issued [11] by the European Commission – *Compliance matters: What companies can do better to respect EU competition rules* – should help to remedy that. The document is a helpful guide to the "why" and "what" of competition law compliance programs and offers the following framework for competition law risk assessment:

"A successful company's compliance strategy would be based on a comprehensive analysis of the areas in which it is most likely to run a risk of infringing EU competition rules. These areas will depend on factors such as:

- the sector of activity; for example a history of previous infringements in the sector indicates a need for particular attention.
- (frequency/level of) the company's interaction with competitors; for example in the course of industry meetings or within trade associations, but also in day-to-day commercial dealings.
- the characteristics of the market: position of the company and its competitors, barriers to entry… If a company holds a dominant position in a market, the preventive measures to be taken will differ from those where the risk factor is more in the nature of 'cartelisation'.

"But the exposure to that risk may vary greatly according to the position held by each member of staff. Employees whose specific areas of responsibility cause them to be particularly exposed (for example, employees who frequently interact with competitors as part of their job or through trade associations) would be made aware of what is at stake and of the basic principles to keep in mind."

Of course, this framework is pretty obvious (as well as quite general). But there are many things in the C&E world that are not only obvious but also important – and are still ignored. Coming from the European Commission, the imperative of conducting competition law risk assessments (and, of course, of using the results of those assessments to develop and maintain strong competition law compliance programs) will now be harder to ignore.

A final point: for global companies, a competition law risk assessment should not be limited to European- and U.S.-related risks. In recent years, a significant number of other countries have initiated harsher approaches to competition law enforcement, and given how fines in this area have proven to be a nontrivial source of revenue for some governments, there is reason to believe that that trend will continue.[12]

[11] Available at http://bookshop.europa.eu/is-bin/INTERSHOP.enfinity/WFS/EU-Bookshop-Site/en_GB/-/EUR/ViewPublication-Start?PublicationKey=KD3211985.

[12] See earlier column on the "demand side" of risk assessment.

CONFLICTS OF INTEREST

Recently, [13] the Securities and Exchange Commission identified a number of areas of potential conflicts of interest (COI) in the private equity field, in effect, strongly encouraging members of that industry to conduct COI risk assessments. But given the prevalence of COIs in the business world generally, this is a measure that other types of organizations should consider, too.

Additionally, the very nature of many COIs – in particular, those involving personal interests of powerful individuals within an organization – suggests that without a well-defined risk assessment process some conflict risks might go unaddressed. This article provides an overview of how to assess COI risks, either as a stand-alone effort or part of a more general assessment process.

First, one should be clear from the start about the purpose of the effort. It should be designed not merely to identify COI risks but also to develop the sort of information about them that can be used to design/improve all C&E program "tools." For instance, the information should be of use in drafting or revising a COI policy or FAQs on the organization's intranet; deciding whether to deploy COI certifications, and, if so, who should receive them and what their content should be; structuring/improving the COI disclosure and management approach; and making similar determinations regarding training/other communications, auditing/monitoring, board oversight and the use of technology (e.g., a COI data base).

[13] As of 2012.

Second – and in order to get the type of information that truly helps one tailor C&E program elements for optimum COI mitigation – one should use a methodology that, among other things, assesses the "reasons" for possible COIs.[14] Reasons, in turn, generally include "motivations" and "misunderstandings."

"Motivations" are reasons to engage in wrongdoing purposefully – most obviously, having a personal economic interest (e.g., ownership of or other revenue participation in an entity that does business with your organization). But less tangible personal interests can form the basis motivations, too – such as reputation enhancement, and one should also consider what the relevant risks are in that respect.

"Misunderstandings" refer, first, to COI-related expectations that may truly not be understood (such as, applicable third-party standards), and, second, to standards that are known but under-appreciated (as COI rules might be in certain cultures or even industries).

Third, the methodology should also include COI "capacities," most obviously encompassing individuals in management and procurement. But there are also many other, less obvious, functions that could have COI-risk creating capacities. For instance, in some companies "corporate opportunities" will present real COI risks with respect to some employees (or agents) but not others, depending on their exposure to such opportunities; determining who is in the

[14] See earlier article on reasons and capacities in risk assessment.

former group could be an important facet of COI risk assessment for such organizations.

Finally, as discussed in the Introduction, although broad-based efforts to analyze the "impact" are unnecessary with respect to many C&E risks (e.g., there is not much point in having executives vote on what they think the harm of an antitrust, bribery or employment law violation would be), with COIs an impact dimension can be important, because COI impacts tend to be less obvious than those arising from many other types of C&E risks. That is, they tend to be more business related in general and trust related in particular, and less a matter of legal penalties.

For this reason, identifying all the ways in which a COI can be harmful to trust could be useful in a number of ways, such as developing training and other communications, which tend to be more effective to the extent they are specific about harms from COIs.

CORRUPTION RISKS

At least conceptually, corruption-related risks should be relatively easy to assess because official expectations regarding such assessments are well articulated – most prominently in guidance documents published in 2012 by the U.S. Department of Justice and Securities and Exchange Commission, 2011 by the United Kingdom's Ministry of Justice and 2010 by the OECD. But putting those risk-assessment principles into practice can be can be daunting, particularly for large global organizations.

In undertaking anti-corruption risk assessments, it may be useful to start with what might be called general risk causing factors (i.e., factors that are relevant to not only corruption risks but other areas of C&E too). For some companies, that will include expansion of the business in developing countries, increased outsourcing and strategic partnerships and economic conditions that can lead to business pressures; of course, other companies will have their own general risk causing factors. So as not to reinvent the wheel, a practice pointer here is that those assessing a company's corruption risks should review the organization's most recent audit plan, as such a document will often have an analysis of precisely the factors in question which can be used for C&E purposes too.

Moreover, general (i.e., not corruption-specific) factors about a company can mitigate (as well as exacerbate) risk, and these should be part of an assessment as well. Among the key considerations here are the strength of a company's overall C&E culture (e.g., the extent to which C&E is seen by employees as a strategic advantage); the soundness of its overall controls; and the openness of communications in the organization. (On the other hand, culture probably mitigates corruption-related risks less than it does various other kinds, given how often bribery cases involve the "edges," rather than "top," of an organization.) Indeed, as described later in this e-Book, a risk assessment requires some degree of program assessment to accurately gauge what an organization's "net risk" is, and that is particularly true in the anti-corruption realm.

However, the gut of an anti-corruption risk assessment should be a risk-area specific analysis. Here, too, some of this aspect of assessment concerns the state of extant mitigation for the organization in question – particularly for such operationally demanding areas as controls with respect to providing things of value to "government officials" and engaging third parties; monitoring (both first and second lines of defense, as described later in this e-Book); and, perhaps less obviously, the realm of incentives. All of these, of course, go to the calculation of "net risk."

But the gross risk part of the equation is where the real challenge is for corruption, with the following being part of the focus of virtually any effort of this kind.

<u>Geographic risks</u>. The principal way in which geography is relevant to anti-corruption risk is through the degree to which a given country or other geographic unit is corrupt (e.g., the country's ratings on the Transparency International Corruption Perception Index). A key practice pointer is that other aspects of geography may also be relevant, such as having relatively isolated company facilities.

Product/service-related risk. There are many different risks of this kind, with the most obvious ones arising from dealings with the government as regulator (typically in manufacturing, transporting, storing or selling a certain type of product) or as customer. A key practice pointer here is that, at least in some instances, product-related risks should be examined granularly, e.g., by product line. (This can be seen as part of the "nano compliance" approach discussed earlier in this e-Book.) Another is that in looking at what constitutes "government business" one should not limit the inquiry to instances where one's direct customer is a government entity but also consider situations where the government is the end user of one's product, even if there are multiple market participants in between.

Third-party risks. This may be an area where some companies go too far (see the piece later in this e-Book on "Goldilocks compliance") but many more do not go far enough. The key, in my view, is to apply the "capacities" and "reasons" analytic approach to third parties that is described earlier (in a broader context than just anti-corruption compliance). However, this review needs to be informed by the extensive history of third-party-related violations that one finds in FCPA case law. For instance, a classic distributor takes title, and therefore under traditional legal analysis seems to have little capacity to create corruption liability for the company whose product it sells; but, experience teaches that there are many types of distributor relationships that can in fact give rise to corruption related liability. Here, too, there is - at least for many companies – no substitute for a granular approach when it comes to risk assessment.

Private-sector corruption. Corruption is, as a general matter, both more likely and impactful in the public sphere than in the private sector, but this can mislead companies into concluding that they need to do little with respect to the latter. Therefore, it is important to include private-sector corruption in C&E risk assessments, taking into account, among other things, the C&E standards of customers and other private-sector organizations with which one's company deals, relevant geographic culture, the organizational culture of the parties in question, the controls of such organizations and pertinent industry culture. A practice pointer here is to look for situations where a private sector entity (customer or other) is not subject to the type of market discipline that generally serves to enhance compliance, i.e., where the cost of corruption is on some level an "externality" (and arguably a "moral hazard").

Risks of the future. As described earlier in this e-Book, a "demand side" approach to risk assessment generally suggests that tax related prosecutions may become a key risk in the future. A logical extension of this analysis is that tax-related corruption risks should be on the radar screen of global companies, as suggested by an FCPA case brought in December 2013 involving bribes paid by ADM in the Ukraine in return for value added tax refunds.

MITIGATION APPROACHES

As already described,[15] a key – and often underappreciated – point about risk assessment is that the results of an assessment should be used to design, operate or improve the various aspects of a C&E program. Put simply, an assessment is only as good as the utility of its results in making a C&E program effective.

In this section, I explore various aspects of risk-assessment-based mitigation, including using assessment results: auditing and monitoring, internal controls, continuous improvement and annual risk-based plans.

[15] In the Introduction and "Does your risk assessment do this?"

Keys to Success When Mitigating Identified Compliance and Ethics Risks

Compliance and ethics risk assessment in the broad sense can be thought of as having three elements to it: risk identification, analysis and mitigation. The first two of these tend to be conceptually more challenging than the third, and perhaps for this reason generally receive more attention than it does (including in this column). Yet failure to mitigate risks that have been identified and analyzed can – and does – create no small amount of harm in companies.

One key to success in this area is having a defined and well-documented risk mitigation process. Among other things, this process should set forth in sufficient detail the nature and scope of the required mitigation; the parties responsible for taking the identified measures; the expected time and cost (so that neither becomes an excuse for failing to mitigate); start and end dates; and a list of any possible impediments to the mitigation and how these can be addressed. Formal signoffs by all key affected parties can also be a helpful step to ensuring sufficient cooperation with the mitigation.

Second, companies should consider having compliance personnel conduct periodic reviews of progress against the plan with the relevant risk owners. In many instances, a quarterly review will be sufficient, but for areas of relatively high risk greater frequency should be considered.

Third, the information generated as part of the process – both in the original plan and from the reviews – should be shared with others who (even if not directly impacted by) could benefit from it. This tends to be most relevant to large, complex organizations, but can be useful for small and mid-sized companies, too.

Fourth, audits should be considered for some or all of C&E mitigation efforts once they have been completed. In some instances, other forms of checking (e.g., self-assessments) should be deployed, too.

Finally, senior management should receive reports on mitigation of risks. This serves, of course, to ensure that these efforts are viewed as a priority. It also helps keep management knowledgeable about and involved in the program, another important area where many current companies' efforts fall short of where they should be.

ANNUAL COMPLIANCE & ETHICS RISK PLANS: FOUR PRACTICE POINTERS FOR SUCCESS

Does your organization apply a Sentencing Guidelines "seven-steps" approach to mitigating all significant areas of C&E risk? Many programs are built on the theory that they will do this, but far fewer actually do it to a meaningful degree.

A useful organizing tool for making an approach of this sort a reality is through the implementation of C&E risk plans, along the following lines.

First, the organization should appoint subject matter experts (SMEs) for all risk areas of significance (e.g., corruption, antitrust, IP).

While many companies do establish roles of this sort, the practice pointer here is to implement a written position description for SMEs and use this description for evaluation/compensation purposes.

Second, as part of their defined roles, SMEs should lead or participate in annual risk assessments for their respective areas. While also fairly common, the practice pointer here is here is to focus the SMEs less on estimating the likelihood and impact of a violation generally (both of which are often pretty obvious for given risks) and more on identifying specific points of vulnerability for use in enhancing mitigation measures (e.g., specific products for which collusion with competitors is relatively likely, regulatory offices in a given country where bribes are relatively likely to be extorted) – or what is referred to in this e-Book as the nature of the offense.

Third, the planning process should entail using the risk-related information to develop or enhance C&E program elements. The practice pointer here is that the actual "seven steps" framework actually is not optimal for these purposes since several of them (e.g., investigations, discipline) don't vary by risk area enough to merit inclusion for these purposes.

Instead, organizations should consider using this modified list of program elements/attributes for risk plans:

- standards and procedures (with the latter including internal controls);
- training and other communications;
- auditing, monitoring and self-assessment; and
- accountability and resources.

In addition to these "risk-variable" program elements, the annual risk plan template could also have an "other" category for those rare instances where tools beyond those listed above are needed for effective mitigation of a given area.

Finally, while the SMEs will typically have the principal role in this process, others – e.g., members of regional C&E committees – should have defined responsibilities in it, too. The practice pointer here is to articulate these duties in program governance documentation (e.g., committee charters) and to audit against them.

The Three Lines of Defense…and Two C&E "Fronts"

As the C&E program field matures, various forms of "checking" become increasingly important to ensuring program efficacy. The "three lines of defense" is a commonly used construct for identifying who does such checking (although the construct is not limited to C&E).

The first line of defense is business people monitoring their own operations. This responsibility – which, in my view, is not mandated in organizations nearly as often as it should be – serves not only as a device for checking, but also as a way of educating the business people on key risks. (A practice pointer: companies should consider reinforcing monitoring responsibilities of this sort by mentioning them in the "Managers' Duties" part of a code of conduct and perhaps including them – at least in a broad way – in managers' performance evaluations.)

The second line of defense is *non*-independent staff (e.g., finance, HR, EH&S or the C&E function) engaging in monitoring. This form of checking is important because in almost any large organization, the audit team cannot, as a practical matter, cover all pertinent areas of risk and so needs checking help from other experts from within a company. Moreover, the lack of true independence in this sort of checking tends, in my experience, to be more a theoretical than actual concern.

The third line of defense is true independent auditing or assessment, which is often performed by a company's internal auditors, but might also be performed by an external group – including accounting, law or consulting firms. Of course, this sort of checking tends to be the most impactful of the three types. But, as a matter of resources, there is only so much of it that any company can do. (Another practice pointer: among the areas to auditing this third line of defense is how well an organization is deploying the other two lines.)

In addition to the three lines of defense, it may also be useful to consider two C&E "fronts," meaning fields of activity for which companies should consider deploying any or all of the lines of defense.

One of these two fronts is risk-area checking. To take a somewhat obvious example, using the risk area of corruption:

- Business people monitor gift-giving/entertainment_and the use of third parties in the parts of the business for which they are responsible.
- C&E or finance also monitors such activity, but in a broader and more systematic way.
- Audit reviews various items – not just the operation of the above-described anti-corruption measures, but also various financial controls – and looks closely for possible violations in the locations/business operations of highest corruption risk.

Using a somewhat less obvious example for this "front," from the realm of competition law: business people monitor bidding activity in their unit; law (and possibly C&E) engages in some similar activity, as well as checking competition law processes (e.g., those requiring approvals before employees can engage in trade association activity); and, as with anti-corruption law, audit reviews locations/business operations of highest risk for compliance with relevant processes and for potential violations.

The second of the two "fronts" concerns what might be called generic (i.e., not risk-area-specific) program processes. To take the example of C&E training: supervisors are responsible for checking to make sure that employees in their work units have taken required training (both in-person and computer-based), C&E reviews training records to see that the required training is being delivered as planned (and also – if the information has been gathered – how employees are reacting to it) and audit conducts training related reviews (including perhaps interviewing some employees) to assess both the fact and efficacy of training.

Of course, no company can fully deploy the three lines of defense with respect to all risk areas and all program processes. Indeed, no one could come close to doing this.

However, a well-designed risk assessment process will help inform this effort and guide an organization in how to use its limited checking resources in an effective manner. And a risk assessment that is *not* helpful in this regard should be closely reviewed with respect to fitness for purpose.

RISK ASSESSMENT AND INTERNAL CONTROLS

Internal controls – meaning processes, structures or systematic measures to address risk – are an important but often overlooked expectation of C&E programs under the Sentencing Guidelines.

They are frequently overlooked because the mention of internal controls is more indirect than that of other program elements (such as training or auditing) in the Guidelines' seven items. That is, the Guidelines' item 1 does set forth general expectations concerning policies and procedures but it is only a Guidelines "commentary" which specifies that procedures include internal controls. Still, as a matter of C&E practice, controls can be utterly essential to effective risk mitigation.

One common type of compliance control is the requirement of pre-approval. Pre-approvals play an important role in FCPA compliance (required for retaining certain sorts of third parties or giving things of value to government officials); antitrust (mandated for attendance at trade shows or entering into business arrangements that could be considered unlawful vertical restraints); consumer protection (advertising must be pre-approved); and, perhaps most obviously, conflicts of interest (conflicts are forbidden unless disclosed and approved), including rules addressed to gifts, entertainment and travel issues beyond the FCPA realm.

Other types of controls – concerning division of responsibilities or levels of authority – play an important role in anti-fraud compliance measures.

Still another type relates to physical access to company resources. This latter sort of control can support both compliance for certain risk areas (e.g., limiting access to confidential or private information) and also the operation of a C&E program generally, such as by preventing employees from utilizing a company's information technology if they have not taken compliance training.

How do internal controls relate to risk assessment?

As described in an earlier column, a key function of risk assessment is developing information that can help a company determine which C&E tools it should deploy to address given areas of risk. And, while it may be difficult to generalize about the specific facets of risk that should trigger the use of controls (given how many types of controls there are), one can say that unless a company is actively considering internal controls for these purposes – the way it likely focuses on more commonly used program elements in conducting risk assessment – it may be missing important mitigation opportunities.

This is the case not only with respect to the traditional forms of controls described above but also possible use of newer technology-enhanced controls, for which – like nearly every choice relating to a C&E program – informed decision making should start with a meaningful understanding of a company's C&E risks.

Addressing the Risks of "Middle-Aged" C&E Programs

Oliver Wendell Holmes, Jr. – who served on the Supreme Court until he was ninety – once said: "From forty to fifty a man must move upward, or the natural falling off in the vigor of life will carry him rapidly downward." Do similar risks face C&E programs in their middle age?

On a most basic level, a middle-aged C&E program often lacks the vitality of its early days. The sense of urgency and purpose is often lost, and the program's standards and functions can begin to be seen as pointless bureaucracy, and be disregarded.

On a less obvious level, having lived with a program for several years can be lulling, and provide what an executive at a client recently described to me as an "it can't happen here" mentality, i.e., the program becomes a victim of its own success. Finally, a middle-aged program runs the dangers of establishing standards that the company fails to abide by, creating what could be in an enforcement setting a "worst of both worlds" scenario.

What are some ways for an organization to avoid these pitfalls?

First, a vibrant risk assessment process can show that significant C&E violations are indeed still possible at the company. C&E-related employee surveys are often useful for these purposes, too – especially ones directed to individual areas of risk, as is publicizing actual disciplinary cases (without "naming names").

Second, a strong approach to C&E-related incentives is perhaps the best way to signal to managers that a program is still mission critical to the organization's success. Training senior managers on their program-related responsibilities – to make clear the connection between individual C&E efficacy and leadership – can have the same effect.

Perhaps most useful, by documenting and explaining a program's strengths, an independent C&E program assessment can help doubters in a company understand how the program is in fact an important asset of the organization – one which is well worth preserving and indeed enhancing. And, by identifying potential weaknesses that a prosecutor would likely spot in an investigation, an assessment can demonstrate to the complacent the possibly grave dangers to the organization of the program becoming infirm as it grows older.

Risk Assessment and Program Assessment

There has long been some confusion regarding the relationship between risk assessment and program assessment, which should be not be a surprise – as there are natural overlaps between these two types of compliance assessments.

In this section of the e-Book we explore the relationship between risk and program assessment on several levels: generally, from a metrics-generation/use perspective, and in the context of post-offense review measures.

Points of Intersection Between Risk Assessment and Program Assessment

Since the 2004 amendments to the Guidelines moved risk assessments and program assessments from the realm of best practice to what can be seen as the territory of de facto requirements, there has been a fair bit of confusion regarding the distinctions between these two C&E program components.

In principle, a C&E risk assessment helps an organization understand not only what its risks are, but how to mitigate them. A program assessment, of course, tells the company how well the program is functioning. So, risk assessment can be seen as more design oriented, and a program assessment has more of an operational focus.

But in practice, the two overlap because one cannot assess risks without understanding how well a C&E program is mitigating them (i.e., the concept of "net risk") and one cannot measure program efficacy without meaningful reference to an organization's C&E risks. Moreover, some program measures will clearly serve both risk and program assessment purposes. For instance, C&E-related questions on employee surveys (e.g., whether the respondent agrees with the statement, "My manager acts with integrity") can be useful both for program assessment purposes (that is, assessing how well the program is impacting behavior) and also risk assessment ones (that is, variations in responses among business units and/or geographies can help an organization determine where its risks are, and hence where additional C&E measures – such as training or auditing – are warranted).

Further blurring these lines, some organizations conduct what are essentially stand-alone program assessments of discrete risk areas. While this would not be warranted for all risk areas of significance, it does make sense for anti-corruption compliance – at least for some organizations – and perhaps several other areas (competition law and trade compliance, among others).

A final part of this mix: a program assessment should always include review of the risk assessment function (and sometimes it works the other way, too). Among other things, this typically entails examining the following:

- The extent to which there is a defined C&E risk assessment process with a logical methodology.
- The breadth of C&E inputs (and note that in my view, a typical ERM survey of employees by itself is only a start in this direction).
- The depth of the C&E inputs (e.g., whether personnel who provide information on risks will, either by virtue of their day-to-day work or from preparation for the interviews, be sufficiently informed for the information to be meaningful to the risk assessment process).

Finally, a key question in this area – and for many companies, a major stumbling block – is whether the results of the risk assessments are used to a sufficient degree to design and enhance the various elements of the program (and not just the obvious ones, like training and auditing). In other words, to be effective, a risk assessment should provide "news you can use" in making other parts of your program effective.

A Risk Assessment Thought Experiment (About Metrics)

Risk assessment and program assessment are, of course, two different animals. They are referred to separately in the Guidelines – the former mentioned in section "(c)" of the definition of an effective compliance and ethics program and the latter in section "(b)(5)" of that definition.

They also serve largely different purposes. Risk assessment is mostly forward-looking – meaning an effort to understand enough about risks to implement all the other C&E program measures in an effective way. The latter is more backward-looking – meaning it is an assessment how well the measures deployed to date have fared.

But inside every risk assessment (or at least most of them) there is a program assessment struggling to be heard, and the converse is true of every program assessment. Making the most of these connections can be essential to optimizing both functions. There are several ways to do this, and in this column I want to focus on one that while (to my knowledge) is untested seems to hold a fair bit of promise.

By way of background, many risk assessments use the concept of gross and net risk, with the former representing unmitigated risk and the latter the level of risk when taking the organization's compliance measures into account. While gross and net risk can be measured both for risk likelihood and impact, the likelihood dimension is typically a more meaningful gauge of a compliance program's efficacy, since impact is more often a function of external factors (such as governmental enforcement policy or the expectations of other key third parties).

So, one way to connect risk assessment to program assessment is to measure the "spread" between gross and net risk likelihood findings over the course of time. By this I mean that if in year one for a given risk area (e.g., anti-corruption) the gross likelihood of a violation is 7 and the net likelihood is 5 and in year two the respective numbers are 7 and 4, then presumably that is some indication that the anti-corruption part of the program is working well, i.e., a factor that should be considered as part of one's program assessment. But, if instead the numbers go from 7/5 to 7/6, then that's a negative for the program assessment.

Note that there are a number of complications for this idea – including what "level" of the company is the focus of the inquiry. Moreover, one would want to make sure that using these numbers for program assessment purposes didn't prejudice the objectivity of those doing the risk assessment.

Finally, I've never seen this done and so I don't know how well it would work in practice. But at least in theory, it would seem to be a way of quantitatively assessing in a risk-area specific way the efficacy of a company's C&E program efforts – which, I imagine, would be of interest to a host of data-hungry constituencies within many companies.

And, one way for a company to gauge if it would work for them is to take historical risk assessment numbers and see whether calculating the spreads aligns with what is otherwise known about the functioning of their program *vis a vis* the risk area in question.

The Risks of Corporate Carelessness: Lessons from C&E History (and the Case for Post-Offense Assessments)

"To lose one parent … may be regarded as a misfortune; to lose both looks like carelessness," wrote Oscar Wilde, and something similar can be said for corporations that fail to learn from one compliance and ethics failure only to suffer a second such event.

Consider the case of Hoffman-LaRoche, which was prosecuted in the late 1990s for an antitrust violation and was fined $14 million dollars. According to press accounts, the company did not respond sufficiently to the offense, and, not too long after, it was prosecuted again. This time the fine was $500 million – then the largest criminal penalty in the history of U.S. law.

Interestingly, the record that Hoffman-LaRoche broke had been set in a case where the organization (Daiwa Bank) was also was penalized harshly in part because the government felt it had not responded appropriately to a prior violation.

Or, consider the even more striking case of Arthur Andersen, which was indicted for obstruction of justice in connection with the Enron investigation – a charge that literally put the firm out of business and threw its many thousands of employees out of work.

Why was the Justice Department willing to take this harsh and controversial step? One reason was that Arthur Andersen had not responded sufficiently, in the government's view, to an earlier act of wrongdoing.

More recently, in connection with a much-publicized case involving questionable investment activity by one of his lieutenants, Warren Buffett has been criticized for not having learned the lessons of an earlier scandal at a company in which he had invested – Salomon Brothers. In that earlier case, the firm's senior managers failed to respond adequately after discovering an act of serious wrongdoing by another employee – a lapse which caused considerable harm to shareholders, and which seems similar to what at least some press accounts suggest happen in the more recent matter.

To help companies be more careful in the wake of C&E failures, the Guidelines were amended in 2010 to provide (in a key commentary) that following detection of any offense an "organization should act appropriately to prevent further similar criminal conduct, including assessing the compliance and ethics program and making modifications necessary to ensure the program is effective."

Given the lessons of C&E history and the explicitness of this provision, not conducting a post-offense assessment runs a significant risk of being seen – and treated – as carelessness by the government.

Does such an assessment need to be conducted by an external party? The Guidelines are clear that this is an option, not a requirement: "[t]he steps … may include the use of an outside professional advisor to ensure adequate assessment and implementation of any modifications" (emphasis added).

Indeed, an external post-offense assessment will, in my view, most likely be warranted only a) in cases of significant wrongdoing; or b) where the analysis and/or recommendations involved in the assessment could be controversial within the organization, and hence independence is necessary for the process to be effective.

Post-offense C&E assessments have always been a sound idea. And, following the amendment to the Guidelines, they should now be considered part of the official definition of what it means to be a careful corporation.

The Ethics Dimension

In the 2004 amendments to the Guidelines, an ethics dimension was expressly added to the government's expectations regarding compliance programs. This dimension has steadily grown more important to the government. Indeed, as recently as October 2013, a high-ranking government official noted: "A strong ethical culture flows from good governance and requires leaders to promote integrity and ethical values in decision-making across the organization. This entails asking not just 'can we do this,' but 'should we do this?'" [16]

While the ethics dimension is often overlooked (or intentionally disregarded) in designing and implementing risk assessments, the next two columns argue that should be squarely in the focus of any business organization's attempt to assess its risks.

[16] http://www.sec.gov/News/Speech/Detail/Speech/1370539872783#.UpDVGcSkq8R.

BACK TO SCHOOL: ETHICAL REASONING AND RISK ASSESSMENT

Inspired both by the start of a new school year and Groucho Marx's timeless saying "Those are my principles, and if you don't like them… I have others," this column briefly considers how using the principal schools of ethical reasoning can help address C&E risks.

There are, of course, three predominant schools of thought in the business ethics field: utilitarianism (associated with Jeremy Bentham), which views the ethicality of actions by reference to their consequences; deontology (associated with Immanuel Kant), which is concerned more with the inherent nature of an action itself than its consequences; and virtue ethics (associated with Aristotle), which emphasizes moral character. Like Groucho, the C&E officer can be said to offer her organization a choice of different ethical reasoning approaches but – as an expert in the field (and presumably unlike Groucho) – she can also ensure that the selection is made in an informed way.

Part of what should inform that choice is risk assessment. That is, for some organizations the greatest potential ethics risks may come from failing to consider the interests of others (companies or individuals) in decisions of consequence, which suggests a need to emphasize utilitarianism. For other organizations greater risk is posed by failing to consider the rightness of possible actions, suggesting the benefit of emphasizing a deontological approach. (Of course, an organization or individual is not required to use one to the exclusion of the other – my point is purely one of emphasis.)

But perhaps of greater benefit to many C&E programs than these two schools of reasoning is deploying the third approach – one based on virtue ethics. Among other things, virtue ethics can be seen as being action oriented; stressing the importance of role modeling, responsibilities and excellence; and aiming to make ethical action a habit as much as a product of reflection.

Virtue ethics therefore has the potential to strike deeper than what is offered by the other schools. And in so doing, it may have a better chance of reaching the various forms of ethical decision making that are outside the realm of pure reason – such as those impacted by "overconfidence" (as discussed in one of the columns on behavioral ethics) and other sub-optimal forms of thought that in recent years have been identified by behavioral economists. Companies with significant ethics – as well as compliance – risks of this nature may be good candidates for virtue ethics.

ETHICS RISKS: ASSESSMENT AND MITIGATION

A recent court decision in a shareholder lawsuit against Goldman Sachs[17] is yet another reminder that when it comes to liability often there is no firebreak between the "merely" unethical and the clearly unlawful. (Among the many other examples of this phenomenon are various of the conflict-of-interest-based cases brought several years ago by the New York Attorney General against investment banks and the insurance brokers.)

For C&E professionals the takeaway from this history – which is unknown to many business people – should be that assessing and addressing ethics risks may be necessary to reducing legal exposure.

Ways to assess ethics risks include:

- Examining whether a company has any relationships (with customers or others) where the need for good faith and candor might not be sufficiently understood by employees or third parties acting on its behalf. Relationships such as these – which tend to involve a high degree of trust but not necessarily a formal fiduciary duty – may be rife with ethics risk potential.
- Seeking to learn whether there are business activities where the pursuit of admirable ends might lead to wrongful means.
- Asking employees in interviews, focus groups or otherwise: What types of conduct has occasioned criticisms that the company has acted unfairly? Do they have particular concerns that the company has acted wrongfully?

Indeed, the very process of gathering information of this sort will itself send a message that "ethics counts."

Other ways to address ethics risks include:

- Offering training on methods for ethical decision making.
- Deploying values-based communications.
- Providing, in training and communications, real-life examples of the company showing a willingness to walk away from business opportunities that, while lawful, were not ethical.
- Building ethics criteria into personnel evaluations.
- Training managers on how to recognize and encourage ethical actions by their subordinates and colleagues.

---

[17] Available at http://www.nylj.com/nylawyer/adgifs/decisions/062512crotty.pdf.

THE SOCIAL SCIENCE DIMENSION

In the past few years the ethics-related research of behavior economists has revolutionized our understanding of the causes of much wrongdoing. As well, the long standing notion of "moral hazard" has – by virtue of the financial crisis of 2008 – become a topic of far broader discussion than ever before.

Interestingly, despite its name, behavioral economics (from which the field of behavioral ethics emerged) is less about economics than psychology. And, despite its name, moral hazard is less about morality than economics.

In this section of the book we look at the relevance of behavioral ethics and moral hazard for C&E programs. More writings about both topics can be found in the *Conflict of Interest Blog*.[18]

[18] For more on moral hazard and C&E programs please go to http://conflictofinterestblog.com/interests/moral-hazard-bias/moral-hazard?menuid=submenu1&submenuid=submenu1.1 and for more on behavioral ethics and C&E programs please go to http://conflictofinterestblog.com/interests/moral-hazard-bias/bias?menuid=submenu1&submenuid=submenu1.1.

What Behavioral Ethics Means for C&E Programs

The spirit of liberty is the spirit which is not too sure that it is right," Judge Learned Hand once said, and the same may be true (at least in part) for the spirit of compliance and ethics (C&E). That is but one lesson that might be drawn from the emerging and important field of "behavioral ethics," which teaches that for many reasons we tend to overestimate our ability to do what is right.

In *Blind Spots: Why We Fail to Do What's Right and What to Do about It* (published by Princeton University Press), business school professors Max H. Bazerman of Harvard and Ann E. Tenbrunsel of Notre Dame provide an overview of behavioral ethics that is both concise but also brimming with intriguing and useful information. In my view, every C&E professional should read this book and strive to apply it's insights to their respective companies' C&E programs.

Behavioral ethics seeks to understand how "people actually behave when confronted with ethical dilemmas," and is part of a larger field of inquiry concerning imperfections in decision making of all kinds.

Drawing from research that both they and other behavioral ethicists have conducted in recent years, Bazerman and Tenbrunsel show how various psychological processes create a powerful phenomenon of "bounded ethicality" which leads even good people to engage in conduct that contradicts their own sincerely held ethical tenets.

This body of knowledge is far too vast to summarize here but the following will hopefully provide some sense of it:

- There is a strong tendency to make inaccurate predictions with respect to how one will respond to an ethical dilemma, with decisions actually being made much more by one's "want self" rather than one's "should self."
- Various processes of everyday life contribute to "ethical fading," in which ethical dimensions are eliminated from a decision.
- Post-decision recollection biases lead to moral disengagement.
- Outcome biases permit us to ignore bad decision making if it happens to lead to desirable results, which can encourage future bad decision making.
- Vested interests make it difficult to approach situations without bias, even for those who are honest.
- Overloaded (busy) minds tend to be highly vulnerable to ethical compromise.
- There is a powerful tendency to over-discount the future – which can have serious ethical implications when it forces others to pay for one's own mistakes.
- Slippery slopes not only lead to bounded ethicality with respect to one's own behavior but also in noticing the unethical behavior of others.
- "Motivated blindness" also contributes to our not noticing others' wrongdoing

Of course, experienced C&E professionals may be familiar with anecdotal evidence regarding some – and possibly many – of these phenomena. But there is a difference between knowing something and being able to prove it, and in the C&E field that gap has often been significant and harmful when it comes to the prevalence of ethics risks in companies.

Presented as hard scientific fact, as behavioral ethics does, these risks are harder to ignore. And that, in turn, should help to underscore the need for strong C&E initiatives in companies – because it shows that companies cannot be reasonably sure that their executives and other employees will, without help, do what is right.

I should note, however, that the authors also argue that what they call "compliance systems" can in fact contribute to ethical fading, by seeming to take ethics out of the picture of decision making and for a variety of other reasons they describe (such as making conduct more attractive by forbidding it). This may – but should not, in my view – give pause to some C&E professionals.

That is, I do not believe that there is a disconnect between the vision of behavioral ethicists and that of C&E professionals because the authors also suggest several approaches for organizations to adopt to address the challenges of bounded ethicality, which, in effect, are ideas for improving C&E programs, not abandoning them. Among these are focusing consideration in goal-setting on potential ethical downsides, including ethical assessments when making decisions concerning personnel, strategy and operations; setting zero-tolerance standards for unethical behavior; and inventorying a company's "informal systems" (i.e., its culture) to understand the pressures that could cause misconduct by employees.

Indeed, read broadly, *Blind Spots* provides a foundation for a host of C&E program reforms. In this sense C&E programs can be seen not as an impediment to deploying behavioral ethics knowledge within organizations but rather as a "delivery device" for doing so (although I should caution that those are my words and not something said in the book itself).

For instance, companies should incorporate into their formal C&E risk assessment frameworks behavioral ethics insights about the risks of employees being very busy or isolated, of business environments with a high degree of uncertainty and of situations potentially involving unseen victims and of indirect action – all of which contribute to C&E risk.

It is also important, I believe, to operationalize within C&E programs behavioral ethics learning regarding the benefits of group decision making – which can be relevant to both structures for dealing with ethical dilemmas and responding appropriately to ethical failures.

Additionally, the phenomenon of motivated blindness suggests the need for greater emphasis than one would currently find at most companies on disciplining managers for C&E-related supervisory lapses.

Still other insights are relevant to mitigation of conflicts of interest – particularly research showing that disclosure alone does little to minimize the harm from conflicts (and, according to one study, can actually exacerbate such harm).

Perhaps most importantly, senior managers should themselves be trained on the key lessons of behavioral ethics – and particularly on the dangers of being too sure of one's own ethical prowess. This should lead not only to better decision-making when managers face ethical dilemmas as individuals, but also, as noted above, to greater appreciation for and support of their companies' C&E programs.

Indeed, the further we get away from the "Big Bang" that led to the creation of most modern C&E programs in the U.S. – the combination of Enron, WorldCom and other prominent scandals occurring around the same time; the passage of the Sarbanes-Oxley Act in 2002; and the revisions to the Federal Sentencing Guidelines for Organizations in 2004 – the more essential such appreciation is likely to be to the success of the C&E field.

OVERCONFIDENCE, MORAL HAZARD, AND C&E RISK

In a recent[19] *NY Times* piece – "Often Wrong But Never in Doubt" – University of Chicago Business School Professor Richard Thaler describes a decision-making "flaw that has been documented in hundreds of studies: overconfidence." He also describes how business leaders may be particularly susceptible to this flaw. While the few studies summarized in Thaler's piece do not deal with C&E risks, concern with the general phenomenon of overconfidence should be heightened in this context due to the impact of "moral hazard" in much C&E-related decision making.

Moral hazard concerns the unhealthy impact on decision making when those who create risks do not sufficiently bear the impact of their decisions. Although – like overconfidence – it is largely addressed to other contexts (moral hazard was first used in the 19th century to describe how having insurance could create or exacerbate risk taking behavior by insureds), it is applicable to various types of C&E decisions, too. Illustrative of this is the following, now infamous, statement in an e-mail from a ratings agency employee concerning the unwarranted favorable treatment being given to certain investment instruments: "Let's hope we are all wealthy and retired by the time this house of cards falters."

The reason that moral hazard is particularly significant in the C&E context is due to the frequently great time lag between crime and punishment in the business world. In this connection, consider how many FCPA or fraud charges are not brought until many years after the misconduct at issue, often long after those who took the risks in question have moved on to other companies (or are "wealthy and retired"). Those who bear the costs are, of course, the shareholders, who were not involved in creating the risk.

The one-two punch of overconfidence and moral hazard can pose great peril for a company, i.e., those who are in the best position to mitigate risks either fail to recognize such risks or, even where the risks are understood, fail to sufficiently address them through strong C&E measures. This is among the principal reasons why conducting formal C&E risk assessments is so important.

While risk assessments cannot fully eliminate overconfidence and moral hazard, they do make it harder for managers to fail to recognize or respond to C&E risks. This is true not only as a general matter but particularly when boards of directors – who tend to bring a different time horizon to their decision making than managers do – are apprised of the results of the risk assessment.

[19] As of 2010.

Identifying and Addressing Behavioral Ethics Risks

The emerging field of "behavioral ethics" examines the effects of various social, cognitive and emotional factors on ethical decision making, and, in numerous experiments, has demonstrated the limited role that traditional notions of rationality play when we are faced with ethics-related choices. The implications of behavioral ethics– which is part of a larger school of "behavioral economics" - indeed extend across a whole spectrum of contexts, from the decisions made in our private lives to matters of public policy.

While a subject of great interest in academia, so far behavioral ethics is having less of an impact on compliance and ethics programs than it should. But, at least to me, it seem only a matter of time before this new understanding of human nature begins to shape the C&E realm and indeed in the cover story from the February 2013 issue of *CSj* – a leading corporate governance magazine in Hong Kong – I explore the possible ramifications of this field for such areas as managing conflicts of interest, training/communications and holding managers accountable for the wrongdoing of their subordinates. I also examine what can be learned about behavioral-ethics-based C&E risks, sections of which are reprinted below.[20]

"One [behaviorist] experiment showed that acting indirectly – that is through a third party – can blind individuals to ethically problematic behavior more than direct action does. This suggests that companies should recognize the limits of what could be called 'inner controls' – meaning personal moral restraints – in their dealings with third parties. So, as a matter of risk assessment, an organization may have to make up the difference with enhanced compliance measures (internal controls) in dealings with suppliers, agents, distributors, joint-venture partners and others.

"Another experiment showed that it is easier to disregard the interests of unknown individuals in making an ethical decision than those of known ones. This finding could help explain the relative ease with which so many individuals engage in offences where the victims are not identifiable, such as insider dealing, government contracting or tax fraud. Here, too, as a matter of risk assessment, an organization may have to make up the difference left by weak 'inner controls' with enhanced compliance measures.

"Of course, and as is true of a number of [behaviorist] findings, this insight is not a complete surprise. Indeed, Ben Franklin once said, 'There is no kind of dishonesty into which otherwise good people more easily and more frequently fall than that of defrauding the government'. Still, being able to prove with real data what is otherwise known just anecdotal or intuitively may be useful to compliance professionals in getting the company to devote extra attention to a risk area.

"The same can be said for a [behaviorist] experiment showing that individuals with depleted resources tend to have greater risks of engaging in unethical conduct. When faced

[20] The full article is available at http://conflictofinterestblog.com/wp-content/uploads/2013/02/CSj-article1.pdf.

with this knowledge it may be difficult for management or a board to ignore a recommendation to either reduce pressure or focus extra compliance and ethics mitigation efforts on parts of an organization where employees are subject to greater-than-ordinary stress.

"A more counterintuitive finding in this field concerns what might be called the risk of good intentions. Several [behaviorist] studies have shown that being cognizant of one's ethical failings actually increases the likelihood of subsequently doing good, and that the converse is true as well. Examples of this phenomenon are that acts promoting gender equality 'license' discriminatory ones, being reminded of one's humanitarian traits causes reductions in charitable donations, and purchasing 'green' products licenses ethically questionable behavior. While unsettling, these findings suggest a need for compliance programs to pay extra attention to risks that could arise from particularly virtuous-feeling activities."

Other Frontiers of Risk Assessment

Ethics, behavioral science and moral hazard - discussed in the two immediately preceding sections of this e-Book - can be seen as representing new frontiers in risk assessment, in the sense that for many organizations they will present new types of information and analysis to be used in such assessments. "Nano compliance" - also discussed earlier - will be another new risk assessment frontier for many companies, and the same can be said for the approach to using metrics outlined above in the "Thought Experiment" piece.

However there are also more traditional risk assessment frontiers for some (and perhaps many) organizations: the risks posed by C&E violations in affiliated entities, such as subsidiaries and joint ventures. Those frontiers are discussed in this section.

JOINT VENTURES AND COMPLIANCE RISKS: THE UNDER-DISCOVERED COUNTRY

In the lesson-rich history of compliance failures, one of the most important cases of all time is the prosecution in 2001 of a 50/50 joint venture (JV) between two pharmaceutical companies for violations of federal fraud and abuse laws (the "TAP case").

Evidently neither of the two companies paid much attention to the compliance and ethics program of the JV. And, although neither bore legal liability for the JV's wrongdoing, the cost to each this inattention – presumably half of the total penalties of about $875 million – was higher than almost any other prosecution's total cost up until that time.

In 2012 joint ventures seem to be more common than at any time before. This is due in part to many companies expanding operations into countries where as a matter of local law (or for other reasons) they need a local partner, and in part on "asset light" strategies being pursued by some corporations.

When a company's ownership of the JV is greater than 50%, it typically extends its C&E program to the JV's operations. But this is far less common in 50/50 situations or those involving minority ownership. Still, as the TAP case shows, even where an organization has no potential legal liability for the transgression of a JV in which it has invested, it can still face dire economic consequences.

Indeed, if costly enough, a corporate compliance failure in a JV could create the rare situation where individual directors could be liable for such a failure even though their company is not – since Caremark claims are predicated on economic harm to shareholders, not legal liability per se.

For these (and other) reasons, many companies should take a more hands-on approach to the C&E programs of their JVs, particularly those operating in emerging markets. Among the measures that should be considered here are:

Most obviously, screening the contemplated JV partner. This generally involves due diligence regarding both the organization and key individuals in it, including their respective histories and (where anti-corruption concerns are significant) relationships with the government.

- Structuring the JV agreement to promote compliance. There are a number of steps that can be taken here – concerning such areas as staffing, board operation, delegation of authority, requirements of super majorities for potentially sensitive transactions, audit rights and termination provisions.
- Once the JV is operational, working on an ongoing basis with key company personnel who serve as JV board members or seconded employees in senior positions to manage compliance. This could entail a) providing a turnkey compliance program framework (e.g., charter) to the board members/seconded employees and assisting them in

tailoring it to the JV's needs; b) having the JV board members/seconded employees, together with the company's C&E officer, conduct or commission periodic risk assessments and develop risk mitigations plans – which can form the basis for ongoing monitoring of the JV's compliance efforts; and c) periodically training the board members/seconded employees on key C&E issues.

-

Finally, I should stress that this column is not offered as a comprehensive discussion of JV compliance issues. (Among other things, there are many substantive compliance risk areas – such as IP protection, compliance with local laws and various supply chain issues – that may require particular focus in the JV context.) But hopefully it can help organizations coming to the challenging area of joint venture compliance for the first time know where to begin.

MORE ON JOINT VENTURE COMPLIANCE

A CCI column earlier this year briefly examined ways in which companies can analyze and mitigate C&E risks in joint ventures (meaning JVs that they do not control). Because there seems to be a lot of interest in the subject (but relatively little published about it) here are three additional thoughts, which should be read in conjunction with the earlier column.

First, assess risks on four levels. They are:

- Inherent/gross risks for the JV – based mostly on industry and geographic factors.
- Mitigated/net risks in the JV – taking into account its C&E measures and other control-related factors, e.g., trustworthy management.
- Gross risk to the investor in the JV – based largely on the amount of investment it has in the JV, but also on a) possible reputational effects; and b) if the JV has a strategic role for the investor, other business effects, such as disruptions to its supply or distribution chains.
- Net risks to the owner, based, in effect, the sum of all of the above, plus the mitigation measures the owner itself takes.

This is more complex than the typical risk assessment framework, but hopefully captures the full range of considerations a company should be mindful of in dealing with C&E risk of JVs.

Second, consider how far "down" to go. Here is a somewhat long-winded way of making the point (and is mostly an excuse for telling a great story)

As recounted in Steven Hawking's A Brief History of Time: "A well-known scientist (some say it was Bertrand Russell) once gave a public lecture on astronomy. He described how the earth orbits around the sun and how the sun, in turn, orbits around the center of a vast collection of stars called our galaxy. At the end of the lecture, a little old lady at the back of the room got up and said: 'What you have told us is rubbish. The world is really a flat plate supported on the back of a giant tortoise.' The scientist gave a superior smile before replying, 'What is the tortoise standing on?' 'You're very clever, young man, very clever,' said the old lady. 'But it's turtles all the way down!'"

The point of this story for those developing JV compliance approaches is that – at least for some risks, such as corruption related ones – effective C&E may mean requiring the JV to have its own due diligence measures for using third parties. Of course, it will be rare that one needs to truly go "all the way down" in this respect, but at least one extra level is advisable in some circumstances.

Third, pay particular attention to incentives in crafting JV C&E responsibilities. As noted in the first article, there are lots of measures that the management of the investing company can undertake to promote C&E in a JV. Responsibilities for such measures are typically given to the C&E officer; members of the law, finance, and audit functions; and/or business personnel.

Based on my experience, however, some companies do not do enough to ensure that those with such responsibilities have sufficient motivation to do what's expected of them. Put otherwise, given their many other duties, there is a danger that those with designated with C&E duties regarding JVs could view such responsibilities as "extra-curricular activities," which take a back seat to their "day jobs."

I have two suggestions for addressing this. First, companies should consider including JV compliance as part of how employees with defined duties in this area are evaluated/compensated. Second, JV C&E measures should – at least in companies with a high-risk profiles in this regard – be subject to regular audits, as this can also be pretty motivating.

OTHER WRITINGS IN *CORPORATE COMPLIANCE INSIGHTS*

While most of my columns in *Corporate Compliance Insights* have been about risk assessment, there have been several others - that I include here – touching on whether one can have too much C&E, what we have learned from more than two decades of C&E programs, and the risks of individual liability with which C&E personnel should be concerned.

IN SEARCH OF "GOLDILOCKS COMPLIANCE"

"It's not complicated – more is better," concludes a wonderful AT&T commercial. But for many C&E officers, it's not that simple.

In the wake of Enron/S-Ox/the Sentencing Guidelines revisions a great many companies seemingly had bottomless appetites for implementing compliance measures. That's no longer the case. With the exception of those employed by companies that are under investigation, playing catch-up with FCPA compliance expectations or in highly regulated industries, C&E officers seem increasingly under pressure to be not only effective but also highly efficient in their work, and to steer clear of "compliance overkill."

Note that this focus on efficiency should not be misinterpreted to mean that the need for effective C&E programs is any less powerful now than it was during the formative age of compliance. Indeed, the costs of non-compliance have, I believe, gone up since then – as reflected in (among other things) the fact that of the ten all-time highest corporate criminal fines in the U.S. five were imposed in 2012 alone. But perhaps precisely because harsh penalties have become the new normal, C&E programs in many companies seem to command a smaller portion of senior management mindshare than they did just a few years ago – and hence the growing imperative to avoid what are seen as unnecessary efforts in this area and to achieve "Goldilocks compliance."

There are various settings in which C&E officers should be attentive to the possibility of going overboard, including but by no means limited to the following.

- Training. While many companies do too little in this regard, some actually do too much – subjecting employees to training that is unwarranted from a risk perspective. (E.g., there are not many businesses where every single employee truly needs antitrust training.) Painting with an overly broad brush here can waste not only considerable amounts time and money; it can also reflect poorly on the C&E program as a whole.
- Background checking of third parties. As with training, on the whole more companies need to do more – rather than less – with this essential compliance tool, but some have instituted background checking regimes that seem unmoored from any meaningful risk calculus. And – as with training – overkill here can trigger negative feelings toward C&E generally in a company.
- Technology. This is a particularly tricky area about which to speak generally, given the diversity of technology-related products and services now being developed in the C&E space, both by vendors and in-house resources. Similar to the case with training and background checks, on the whole, I think that there needs to be more done here, not less. But the devil is really in the details with this emerging part of the C&E world, and companies need to remember that

cool does not necessarily mean necessary.

Note that C&E overkill is not only about doing too much – it can also be about saying too much. For instance, C&E officers need to be careful in discussing the relevance of C&E provisions in settlement agreements to their own companies. To use a medical analogy, what's essential for a patient who has had a heart attack is not necessarily indicated for those who merely have somewhat elevated cholesterol levels.

So how do you know when you're going from enough to too much? In some instances it is like the famous saying about obscenity, you know it when you see it. But that won't do in all cases, and for many reasons the better approach is to base determinations of this sort on your risk assessment.

Indeed, by identifying in a risk assessment anything that's not needed, a program can gain greater credibility among key decision makers in a company. This, in turn, can help the program focus on what is essential – and implement C&E measures that are "just right."

TWENTY YEARS OF COMPLIANCE PROGRAMS

Nov. 1[21] will mark the 20th anniversary of the Federal Sentencing Guidelines for Organizations, and of the expectations that they created concerning compliance and ethics programs.

It is worth recalling, as Sentencing Commission Chair William W. Wilkins Jr. noted shortly after the guidelines became effective, that the approach they pioneered of offering companies a "shield against potential liability with well-designed and rigorously implemented compliance systems" was at the time nothing more than an "exploratory invitation."[22]

Indeed, the encouragement of compliance programs was hardly inevitable – as early drafts of the guidelines were predicated instead "on the optimal penalties theory developed in the economics literature." (For more information about early compliance history – including this alternative "Chicago School" approach.[23])

The approach ultimately adopted was based on the notion that the best way to promote law abidance in companies was through what a top federal prosecutor called at the time a "practical partnership" between business and government, in which government provides business with both the guidance and incentives to develop compliance and ethics programs.

Twenty years later this experiment should – on many levels – be judged a resounding success. The Guidelines approach has been adopted by other federal agencies; local enforcement officials (such as the New York County District Attorney in a policy published in 2010); and other nations' governments (such as Spain, also in 2010). Indeed, with the recent U.K. Bribery Act, it may be fair to say the U.S. is no longer the leader in providing compliance program incentives and guidance to businesses. One of the legacies of the Guidelines is that compliance has "gone global."

Also noteworthy, but not yet sufficiently appreciated, is that in recent years social scientists working in the area of behavioral ethics have demonstrated just how imperfect human ethical decision making often is, which, in turn, has powerful implications for the compliance field. In essence, this research has showed that individuals often need help to do the right thing, which is what the sentencing commission understood was the case in providing for compliance program guidance and incentives. In other words, behavioral ethics should help establish that compliance programs work as a matter not only of practice but also theory. (See earlier column on "What Behavioral Ethics Means for Compliance and Ethics Programs" for more information about behavioral ethics.)

Finally, and most importantly, the Guidelines' approach has been instrumental in causing companies of all kind to establish rigorous compliance programs. Of course, part of that

21 Of 2011.
22 This is in the Introduction to the Kaplan & Murphy book on the Guidelines.
23 In chapter two of Kaplan & Murphy.

approach is the prospect of devastating liability for companies that refuse to accept the government's offer of a compliance-related "practical partnership," and we have indeed seen fines that twenty years ago would have been largely unimaginable become so common as to be barely noticeable. Additionally, the prospect of these "mega fines" has, in turn, focused the attention of boards of directors – who now face the possibility of personal liability that would also have been unthinkable pre-guidelines – on the need for strong compliance programs.

Yet any fair reckoning of the results to date of the guidelines experiment should note the presence of compliance "stragglers," meaning companies that – while paying lip service to the guidelines' expectations – have not in fact developed or maintained "well-designed and rigorously implemented compliance systems." Some of these companies lack sufficient management and board-level support. Others have devoted insufficient resources to their programs. Still others have not conducted meaningful compliance risk assessments. Of course, most stragglers suffer from multiple program infirmities.

If pressed, many of these companies would doubtless say that they just haven't found the time to develop strong compliance programs. But with the guidelines expectations now nearly twenty years old, one can readily imagine how persuasive the explanation would be for any company that, in an investigation, had to beg the government for leniency.

Risks to C&E Professionals – Lessons from Two Near Misses

While I generally think that compliance and ethics personnel worry too much about the risks of individual liability arising from their work, two client experiences from my days as a criminal defense attorney may be worth briefly recounting on this issue.

Neither resulted in charges against my clients (nor were charges, in my view, remotely warranted in either) and so I can write only in a general way about each. Still, knowing the theories of the prosecutors in these investigations may be of use for C&E professionals in steering clear of the zone of personal danger.

<u>Matter No. 1</u>

Prosecutors were investigating several consumer products companies (including one that I represented in the inquiry) for various types of possible wrongdoing and formulated a theory that as a matter of course the companies' regular inside and outside counsel had engaged in a fraud on regulators/courts and obstruction of justice by trying to claim attorney-client privilege for communications that in fact did not involve legal advice.

What makes this relevant to C&E is the real possibility that communication regarding training, audits, investigations, risk assessments and program assessments will be marked privileged where legal advice could be – but is not actually – involved, or without sufficient documentation of such involvement.

<u>Matter No. 2</u>

Prosecutors were investigating a health care company for fraud and formulated a theory that an internal investigation conducted by the organization's regular outside counsel (whom I represented) was not a good faith inquiry but rather a sham designed to "paper the files," meaning to make it look like the company was engaging in real self-policing when such was not the case. Here, too, no charges were brought against my clients, but I can certainly imagine circumstances involving a truly phony internal inquiry where the result could be different.

A final point: the more prosecutors rely on internal investigations to make enforcement decisions involving companies, the greater the likelihood that at some point charges will be brought under either or both of the above theories. Not a happy thought, but forewarned is forearmed.

Appendix: A Checklist of Common C&E Risks[24]

Antitrust/Competition Law
Clayton section 8
Monopolization/Abuse of a Dominant Position
Premerger Notification
Robinson-Patman
Collusion/anticompetitive agreements
Unfair Practices
Vertical Restraints

Compliance program requirements (mandatory programs)
Court orders, consent agreements, CIA's, etc.
State laws on harassment training
State laws requiring compliance programs, e.g., California for pharmaceutical companies
Industry specific requirements, e.g., banking, mutual funds, government contractors
Sarbanes-Oxley Act
NYSE and other listing requirements

Conflicts of Interest/Commercial Bribery
Charitable Contributions
Corporate opportunities
Employment
Entertainment
Gifts
Ownership interests
Travel
Vendor stock options, warrants and IPO preferences

Consumer Protection/Advertising
Accommodations for those with disabilities
Advertising accuracy and substantiation
Consumer credit/bankruptcy fraud
Customer discrimination
Customer safety
Pricing accuracy
Selling to children
Telemarketing/mail order selling
Warranty notice/disclosure
Weights and measures

Document Retention

EEO/Labor
ADA
Accommodations for religious practices/beliefs
Affirmative Action
Bullying
Discrimination
ERISA
FMLA
GINA
Immigration
Harassment--Age, Race, Other Protected Categories
Labor relations/union organizing/labor corruption
Military service/reserve leave
Sexual Harassment
Substance abuse
WARN

Environmental
Clean Air
Clean Water

---

[24] This list was principally prepared by Joseph E. Murphy and appears in Jeffrey M. Kaplan and Joseph E. Murphy, *Compliance Programs and the Corporate Sentencing Guidelines*, App. 6A (2013-2014 edition). Reprinted with permission (Thomson Reuters). Further reproduction is prohibited. This publication can be purchased at http://legalsolutions.thomsonreuters.com/law-products/Treatises/Compliance-Programs-and-the-Corporate-Sentencing-Guidelines-2013-2014-ed/p/100204247.

Endangered species/wildlife protection
Local Right to Know
RCRA
TSCA/asbestos

Escheat (abandoned property) laws

Government Contracting
Anti-Kickback Act
Bid Rigging
Fraud
Gifts and entertainment
Hiring Government Employees
Mandatory compliance program elements
Mandatory disclosure of violations
OFCCP

Government Investigations/Contacts
Preserving Records
Responding Truthfully

Intellectual Property
Competitive Intelligence Gathering
Infringement
Misuse of Trade Secrets
Trade and Service Marks
Trade Dress infringement

International
Anti-Boycott Act
Country-of-origin marking
Customs
FCPA/UK Bribery Act/other anti-corruption laws
ITAR & Export Control
U.S. Boycotts/Trade Restrictions

Money Laundering

Political Contributions/Bribery/Lobbying
PAC's

Privacy
Customers
Employees
European Union Laws
Reporting data security breaches

Product Safety
CPSC
Product recalls

Purchasing
Kickbacks
Suppliers' practices (foreign workers' treatment)

Securities Law
Earnings Management/Accounting Fraud
Insider Trading
Options timing
Reg FD Disclosure Requirements
Retaliation against whistleblowers
Sarbanes-Oxley Act
Section 16

Social media
Access by employer
Labor law rights of employees/limits on employers
Use for work
Use outside work

Specialized Industry Areas
Banking
Creditors--FTC Red Flags Rule
FAA
FCC
FDA
Healthcare
Nuclear Safety
FERC/State Energy Utility Regulation
Securities industry/broker-dealers/investment advisors

Transportation Safety

Taxes
Employee Withholding
Income

Sales/Use
Tax shelters

Terrorism
USA Patriot Act

Wages and hours
Child labor
Hours of work
Minimum wage
Overtime

Workplace Safety
OSHA
State Law

Workplace violence
Negligent hiring/background checks
Weapons in the workplace

About the Author

Jeff Kaplan is a partner in Kaplan & Walker LLP, a law firm in Princeton, New Jersey, and Santa Monica, California. He specializes in all aspects of assisting companies in developing, implementing and reviewing corporate compliance/ethics programs, including conducting risk analyses; writing/editing codes of conduct and other policy documents; counseling companies in matters regarding training; developing compliance audit protocols and reporting systems; establishing compliance/ethics offices; and assisting boards of directors in meeting their fiduciary duties under the *Caremark* case. Jeff's compliance/ethics program practice has included work for clients in the health care, medical devices, pharmaceuticals, government contracting, insurance, manufacturing, energy, retail, paper, publishing, professional services, telecommunications, technology, securities, private investments, food and chemical fields, as well as non-profit organizations.

Jeff has served as a compliance monitor in a criminal tax case for the New York County District Attorney, has reviewed and reported to the Department of Justice and SEC on a company's compliance/ethics program in connection with the settlement of an FCPA investigation and has reviewed and reported to a state attorney general on another company's compliance/ethics program in connection with a settlement of another matter. He also conducts internal investigations on behalf of boards and companies into allegations of wrongdoing brought by whistleblowers and others. He received his B.A. (magna cum laude, Phi Beta Kappa) from Carleton College in 1976 and his J.D. (cum laude) from Harvard University in 1980. He is a former partner of Chadbourne & Parke, where he served in the Special Litigation Group, and also a former partner of Arkin Kaplan & Cohen LLP and of Stier Anderson, LLC.

For many years Jeff was Counsel to the Ethics Officer Association (now the ECOA), a professional association of more than 1200 compliance/ethics officers. He now serves as the Program Director of the ECOA's "U.S. law school" for compliance/ethics officers and will also serve as Program Director of the global version of the "law school" being launched by the ECOA in early 2014. In 2011 he conducted a C&E program benchmarking survey of ECOA members. He has, as well, served as Program Director for the Conference Board's annual Business Ethics conference and of its Council on Corporate Compliance, and has co-authored two research reports for that organization. *Ethics Programs – The Role of the Board: A Global Study* and *Ethics and Compliance Enforcement Decisions – the Information Gap* (both with Ronald Berenbeim).

Jeff is, together with Joe Murphy and Win Swenson, co-editor of *Compliance Programs and the Corporate Sentencing Guidelines: Preventing Criminal and Civil Liability* (West 1993), a leading legal treatise on designing and implementing compliance/ethics programs which he updates annually. He is co-author of *The Prevention and Prosecution of Computer and High Technology Crime* (Matthew Bender 1989). He was for many years co-publisher/executive editor of *ethikos*, a bimonthly magazine for compliance/ethics professionals. He is author and co-author of numerous articles about business crime and compliance/ethics programs in periodicals such as *The California Management Review, The Journal of Securities and Commodities Regulation, The Prevention of Corporate Liability: Current Report, The Preventive Law Reporter, Directorship, Director's Monthly, American Banker, Business Crime Commentary, the New York Law Journal* and *the National Law Journal*, and also various book chapters on these topics.

Jeff co-chairs the annual Practicing Law Institute's annual Advanced Compliance & Ethics Workshop and chairs the annual Continuing Legal Education program in corporate compliance sponsored by the Association of the Bar of the City of New York. He is the Featured Risk Assessment Columnist for *the Corporate Compliance Insights* web site; is editor of the *Conflict of Interest Blog*; and writes a bi-monthly column on compliance programs and the law for *Compliance and Ethics Professional*.

Jeff is Adjunct Professor of Business Ethics at the Stern School of Business, New York University, and is a Researcher on the Ethical Systems project being run by a professor there. He is a member of the New York and New Jersey bars. In 2009 he was a recipient of a Compliance and Ethics Award from the Society for Corporate Compliance and Ethics, which that organization bestows annually on "Compliance and Ethics Champions."

About *Corporate Compliance Insights* and Conselium

Launched in December of 2008 and sponsored by Conselium, Corporate Compliance Insights is a knowledge-sharing forum designed to educate and encourage informed interaction within the corporate compliance, governance and risk community.

Corporate Compliance Insights combines featured articles written by some of the most experienced compliance and ethics professionals in the world with regular updates of important news events in the world of governance, risk, and compliance. Additionally CCI offers an events calendar, professional company directory, leadership library and compliance jobs board.

Founded in 2001, Conselium is a global executive search firm focusing exclusively on governance, risk and compliance. Conselium helps Fortune 500 companies around the world manage risk by placing top talent in key positions. Contact founder Maurice Gilbert for more information about Conselium or Corporate Compliance Insights.

Index

In preparing this index I have tried to be reasonably comprehensive, but have omitted references to topics that appear very frequently in the text - e.g., the Sentencing Guidelines; C&E officer; and, of course, risk assessment itself. I also do not include in the index the various references to areas of law in the appendix or topics where the sole references can be found in the relevant column's title.
