Compliance and Ethics Risk Assessments

By José A. Tabuena, MA, JD, CFE, CHC[1]

Background on Risk Assessments

Regularly conducting a comprehensive *risk assessment* is now recognized as one of the key "elements" of an effective compliance and ethics program. Even more broadly as regulators have emphasized the importance of effective risk management[2], boards and management teams have increased their focus on the concept of "risk" and have observed a measurable shift on this focus at their organizations[3]. By understanding the nature and the impact of the risks being faced, it is expected that an organization can better design programs and develop controls to mitigate those risks.

Performance of risk assessments falls under the discipline of *risk management* where evolving and enhanced frameworks and techniques have emerged. Risk management comprises the identification, assessment, and prioritization of risks followed by the coordinated and efficient use of resources to monitor, minimize, and otherwise control the probability and/or impact of the risks occurring. Risks arise in many forms and can range from uncertainty in financial markets, operational failures, and natural disasters, to legal liabilities and reputational harms.

To proactively identify and reduce major risks, the compliance and ethics program first looks to trailing indicators such as recent claims, lawsuits, regulatory encounters, and nature of calls to the whistleblower helpline. More forward-looking is the use of leading indicators to anticipate risks that may occur. Risk assessment is one method to help anticipate and forestall incidents that have not yet occurred, but can be readily preventable.

For the compliance and ethics professional, the risk assessment is the foundation upon which the program is built. At a basic level, an organization cannot design an effective compliance and ethics program without first thoroughly identifying the laws with which it must comply. Moreover, the risk assessment enables the organization to establish priorities that permits the most efficient use of program resources. Benefits of a risk assessment include:

---

[1] **José Tabuena** is Senior Vice President of Governance and Compliance with PhyServe Physician Services, Inc.

[2] The Securities and Exchange Commission (SEC) in September 2009 created the Division of Risk, Strategy, and Financial Innovation which will highlight the use of risk and economic analysis. The SEC also issued rules that would require disclosure of the board's role in risk oversight. SEC Release No. 33-9089 (December 16, 2009).

[3] Deloitte Dbriefs Web cast, "Risk Intelligence Governance: The Finance Executive's Role in Supporting the Board," October 7, 2009, 1,570 participants.

- providing an early warning process for detecting compliance and ethics threats
- allowing companies to correct identified problem areas before they are discovered by regulators, investors, potential acquirers, buyers, the media or potential plaintiffs
- allowing for prioritizing of compliance and ethical risks with concomitant strengthening of existing controls or the development of new controls for those risks
- enabling a company to revise the ethics and compliance policies, training, auditing, and initiatives that require attention
- improving decision-making by providing managers with critical information on compliance risks and mitigation strategies
- demonstrating to regulators a proactive approach to compliance and thereby meet a due diligence element of an effective compliance and ethics program.

As legal, compliance, and ethical risks are a major subset of the overall risk universe faced by an organization, it is worthwhile to be aware of risk management techniques, particularly those used in your industry sector. Risk management components and the role of risk managers vary by industry, the size and structure of the organization, as well as the risk financing strategies it employs. Similar to the field of compliance and ethics, the risk management profession has evolved along functional needs and growing regulatory mandates[4].

The Role of Risk Assessment in Compliance and Ethics Programs

The Organizational Sentencing Guidelines, when amended in 2004, explicitly included risk assessment within the definition of an effective compliance program[5]. Although commentators believed that the importance of performing a risk assessment was already implicit in the original definition of an effective program, the Advisory Group appointed by the U.S. Sentencing Commission intended to make clear that:

> … risk assessments need to be made at all stages of the development, testing, and implementation of a compliance program to ensure that compliance efforts are properly focused and effective[6].

---

[4] Examples of risk management professional organizations include the Professional Risk Managers' International Association, the Risk Management Association for the financial services industry, the Risk and Insurance Management Society and the American Society for Healthcare Risk Management. Some associations offer professional certifications in risk management.

[5] U.S. Sentencing Guidelines Manual § 8B2.1(c) (2004).

[6] Ad Hoc Advisory Group on the Organizational Sentencing Guidelines Report at 87 (2003).

Thus to obtain the benefit or credit for an effective compliance program (and the reduction in the organization's culpability score) the revised Sentencing Guidelines mandate the performance of periodic risk assessments. Specifically the amended Guidelines provide that:

> The organization shall periodically assess the risk of criminal conduct and shall take appropriate steps to design, implement, or modify each (of the components of an effective compliance and ethics program) to reduce the risk of criminal conduct identified through this process[7].

Additionally the Sentencing Guidelines comment that organizations must:

> Prioritize periodically the elements of the program in order to focus on preventing and detecting the criminal conduct identified in the risk assessment process as most likely to occur[8].

These provisions in the Guidelines provide the foundational perspective for the performance of the risk assessment. It becomes apparent that the risk assessment should precede all other steps in the establishment of the compliance and ethics program in order for program efforts to be properly focused. How would you know what policies, training, auditing, etc., is needed without an assessment of the compliance risks? Further, while a risk assessment is a good starting point, it clearly is not a one-time event and must be conducted periodically in order for the program to adapt to changing business and regulatory conditions. And in order for the program to remain effective, the risk assessment must then be integrated into the organization's overall compliance program and company processes on an ongoing basis.

The Scope of the "Compliance and Ethics" Risk Assessment

A strict reading of the Sentencing Guidelines would appear to limit the focus of the risk assessment to possible "criminal" conduct. The commentary to the amended Guidelines state that the organization should identify the *criminal* conduct that might occur considering "the nature of the organization's business[9]." The organization is to further consider the prior history of the organization[10]" and the legal violations highlighted by government regulations[11].

---

[7] U.S. Sentencing Guidelines Manual § 8B2.1(c) (2004).

[8] U.S. Sentencing Guidelines Manual, comment 6(B)-(C) (2004).

[9] U.S. Sentencing Guidelines Manual 8B2.1, Application Note 6(A)(ii) (2004). The commentary provide an example of an organization where sales personnel who have the flexibility to set prices who should have policies and procedures designed to prevent and detect price fixing.

[10] U.S. Sentencing Guidelines Manual 8B2.1, Application Note 6(A)(iii) (2004).

[11] U.S. Sentencing Guidelines Manual 8B2.1, Application Note 2(B) (2004).

Although the Guidelines focuses on criminal conduct, most organizations take the prudent view that a broader range of compliance and ethics risks must be examined, including those that affect civil liability, regulatory exposure, business ethics or conduct, and the organization's reputation[12]. Essentially a key step in conducting the risk assessment will be establishing a definition and shared understanding in the organization of what constitutes a "compliance and ethics" risk.

Extending the risk assessment beyond exposure to criminal conduct is essential, as legal mandates can be ambiguous and cumbersome especially in highly regulated industries. When employees understand how the company's ethical values apply in gray areas, they are more likely to align their behavior in an appropriate manner.

Examining ethical factors and reputational impacts can demonstrate the organization's commitment to ethical business conduct by providing support and guidance when employees are unsure what to do. By emphasizing the commitment to ethics as well as technical compliance, the organization is affirming that how business is conducted is just as important as the business itself. Such an approach is further supported by the Sentencing Guidelines' emphasis, when the guidelines were amended in 2004, on the importance of promoting "an organizational culture that encourages ethical conduct and a commitment to compliance with a law"[13].

A compliance and ethics risk assessment should therefore at minimum involve information concerning risks of:

- Criminal misconduct
- Direct legal liability (civil and criminal)
- Ethical and reputational harm

What is Not a Risk Assessment

It is worth noting what is *not* a risk assessment. A risk assessment is not intended to serve as an audit or investigation, although issues and circumstances that require a deeper examination may be brought to light from the process. A compliance and ethics risk assessment is not a financial or operational audit though it can be incorporated with these other processes.

---

[12] See The Conference Board, "Universal Conduct: An Ethics and Compliance Benchmarking Survey" by R.E. Berenbeim, p. 20 (2006).

[13] U.S. Sentencing Guidelines Manual 8B2.1(a)(2) (2004).

A compliance and ethics risk assessment should also not be confused with a compliance *program assessment* (or program audit), although the objectives and activities of both exercises can overlap:

- An evaluation or audit of the "program" entails a comprehensive review of the compliance processes and activities to assess the overall impact and effectiveness of the compliance and ethics program. A program evaluation can include a risk assessment, especially if one has not been performed before. Such an instance often involves a baseline effort to identify the range of compliance obligations and ethical risks the organization faces in order to determine if those obligations and risks are being addressed.
- By comparison, a risk "assessment" more specifically involves the identification and evaluation of compliance and ethics type risks, assessing their significance based on likelihood and consequence, determining the current and desired level of controls, and the acceptable level of risk.

Integration with Enterprise Risk Management Initiatives and Other Organizational Risk Assessments?

Risk assessments when performed from a compliance and ethics perspective do not delve into the full-range of business operational risks that a company experiences. But as noted, risk management has taken on more importance in the corporate environment spurring more risk assessment activities across organizations. The compliance and ethics professional should be cognizant of other risk assessment initiatives that may be taking place.

With the focus on Sarbanes-Oxley compliance and internal controls, regular risk assessments, along with the ranking and mapping of results, began taking place with business functions encouraged to evaluate their specific risks and contribute to a comprehensive understanding of the organization's overall risk profile[14].

Examples of other types of risk assessments taking place include:

- Disclosure controls under Sarbanes Oxley § 302 to material, non-financial, and financial information required to be disclosed
- Financial risks pursuant to Sarbanes Oxley § 404 internal controls over financial reporting

---

[14] A majority of organizations conduct periodic risk assessments, regardless of organizational size or headquarter-location. See Universal Conduct: An Ethics and Compliance Benchmarking Survey, *supra* note 12 at 21; Corpedia, "2006 Compliance Program and Risk Assessment Benchmarking Survey," p. 21; LRN, "The LRN Ethics and Compliance Risk Management Practices Report," p. 23 (2008).

- Fraud risks, including those performed as part of the external auditor's duties under Sarbanes Oxley and Auditing Standard 5 by the Public Company Accounting Oversight Board
- Other functional-specific risk assessments in high impact areas depending on industry (e.g., IT security controls, environmental risks, etc.)

Because ethics and compliance risks touch so many areas of the enterprise, organizations should consider integrating when possible the ethics and compliance risk assessment into an existing enterprise risk management process. Survey results indicate that, while companies perform formal risk assessments, the majority don't yet undertake them in an integrated manner that can offer useful benefits[15].

One obvious benefit of an integrated approach is consistency and uniformity with respect to terminology, criteria, process, and the risk information that is collected. When risk assessments are conducted separately by different business units, the use of different frameworks can result in the need and cost for reconciling the information collected across the organization. Integration can lead to a better quality of risk-based information upon which strategic and tactical decisions are based.

Integrating the assessment with other business processes can enhance its outcomes and observations, given that ethics and compliance concerns as a practical matter filter into every department and operation. Conducting enterprise-wide compliance and ethics risk assessments in conjunction with financial auditing, manufacturing, marketing, sales, IT, and other functions, ensures that a more complete range of risks are identified and correlated to ethics and compliance concerns.

Other advantages to a holistic risk management and assessment approach include:

- Efficiencies gained as risk issues and operational processes often overlap. More effective mitigation strategies can be developed if process interdependencies are understood.
- An integrated approach can also foster the perception that ethics and compliance is central to all the organization's activities rather than a stand-alone program outside of mainstream organizational concerns when a siloed assessment is performed (even if wide range of functions are involved in the compliance and ethics risk assessments).

---

[15] Nearly 2 in 10 surveyed companies (19%) did not integrate their risk assessments with other business processes. The LRN Ethics and Compliance Risk Management Practices Report, *supra* note 14 at 23.

There are some disadvantages to blending the compliance and ethics risk assessment into a broader enterprise-wide effort:

- Compliance and ethical risks may not be as obvious as operational risks and therefore may receive less attention from the majority of those involved.
- Involvement by the professional in an enterprise assessment will necessarily require more time, participation, and resources from program staff than when driving the assessment from purely a compliance and ethics perspective.

Risk Management Frameworks and Resources

While the U.S. Sentencing Guidelines are clear about the role and significance of risk assessments for an effective compliance and ethics program, the guidance is conspicuously meager on how to actually perform one. Generally the Sentencing Guidelines expects an organization to "scrutinize its operating circumstances, legal surroundings, and industry history to gain a practical understanding of the types of unlawful practices that may arise in future organizational activities[16]. As the commentary to the amended guidelines provides only minimal instruction, it can be valuable to look to other frameworks and standards for ideas on how to go about doing a risk assessment.

Examples of alternative risk management frameworks include:

- The Committee of Sponsoring Organizations of the Treadway Commission (COSO) issued a comprehensive enterprise risk management framework (ERM) in 2004 for companies to evaluate the broader universe of business risks[17]. Some commentators find COSO's ERM framework to be confusing and difficult to implement[18] and have turned to other standards.
- AU/NZS 4360, the Australian/New Zealand risk management standard uses a more concise definition of risk than COSO.
- ISO 31000, from the International Organization for Standardization is based on the AS/NZS 4360 risk management standard.
- The GRC Capability Model "Red Book 2.0 by the Open Compliance and Ethics Group (OCEG) seeks to integrate principles of effective governance, risk management, compliance and integrity (GRC) into tangible business practice[19] and provides an ERM

---

[16] Ad Hoc Advisory Group, *supra* note 5 at 91.

[17] Committee of Sponsoring Organizations of the Treadway Commission, "Enterprise Risk Management Framework" (2004).

[18] Forrester Research, "AS/NZ 4360 – A Practical Choice Over COSO ERM," by Michael Rasmussen (January 3, 2007).

[19] GRC Capability Model "Red Book 2.0" Open Compliance & Ethics Group (April 2009).

approach. OCEG comprises a multi-industry and multidisciplinary coalition of business leaders striving to provide a common framework and language for compliance and ethics professionals.

Each of the above-referenced sources provides a framework with guidance for conducting risk assessments as part of an overall risk management program. Other resources exist from professional associations and industry groups that the compliance and ethics professional should consider when designing a risk assessment approach. The following organizations have useful materials on risk assessments generally, and legal and compliance related risk assessments in particular:

- The Ethics and Compliance Officers Association (http://www.theecoa.org)
- The Society of Corporate Compliance and Ethics (http://www.corporatecompliance.org)
- Compliance and Ethics Leadership Council (https://www.celc.executiveboard.com)
- Association of Corporate Counsel (http://www.acc.com)
- Association of Certified Fraud Examiners (http://www.acfe.com)
- Institute of Internal Auditors (http://www.theiia.org)
- The Conference Board (http://www.conference-board.org)
- National Association of Corporate Directors (http://www.nacdonline.org)
- Open Compliance and Ethics Group (OCEG) (http://www.oceg.org/)

Whichever framework or approach that is ultimately adopted, the key is to utilize a systematic approach to the identification, classification, and prioritization of compliance and ethics risks.

Conducting the Compliance and Ethics Risk Assessment

The following sections provide practical suggestions for conducting the risk assessment. During the undertaking it will be valuable for management and all involved to have a clear understanding on the purpose and objectives of the risk assessment as company-wide resources and participation will be essential.

However, even with detailed planning, don't expect the process to run without glitches, especially if this is the organization's initial experience with a risk assessment. Don't let pursuit of perfection be the enemy of the good. It is important to recognize that implementing a risk assessment approach is not an exact science and there will be room for improvement in future iterations. Ideally the process will link the compliance and ethics function to key other departmental subject-matter-experts and resources to help drive the risk assessment process.

The commentary to the Sentencing Guidelines does set forth the basic steps that can serve as a starting outline for planning the process, and is revisited here:

1. First, the organization should identify the "criminal conduct" that might occur in conducting the organization's business, considering "the nature of the organization's business, the "prior history of the organization," criminal conduct common to the industry, and legal violations flagged by government regulations[20];
2. Next, the organization should assess the "nature and seriousness" of the legal risks as well as the "likelihood that [the] criminal conduct may occur."[21]
3. Third, the organization should prioritize its risks, addressing them in order of urgency[22].

Preliminary Risk Assessment Considerations

Before embarking on the process the following issues and questions should be considered carefully by the compliance and ethics professional. Answers to these questions will depend on your company's size, structure, operations, and regulatory environment.

Clarify the objectives and scope of the risk assessment:

Will you focus solely on the risk of criminal activity or will you address other forms of inappropriate conduct? How broad across the organization do you expect to touch?

- As discussed earlier, it is recommended that all major areas of misconduct be examined. The compliance and ethics risk assessment is better served by including a wide-range of risks, including those that are systemic to the typical organization and those unique to the industry in which the company operates.
- The lens from which the risk assessment is performed should take into account the articulated goals, values, and overall objectives of the organization. Risks (and their relative significance) that may not otherwise be identified will come into focus when taking into account the company's goals, values, and strategic objectives. For instance, a joint venture into a stringent regulatory environment may not make sense if the undertaking does not align with the organization's mission and strategy.
- As also previously discussed, should the compliance and ethics assessment be integrated into other risk assessment activities in the company? A related scope question is whether you should include all operations or apply a materiality threshold to determine inclusion in the process? It might be better to limit the scope to significant operations during an initial risk assessment so that the process does not become unwieldy, unless a smaller business area is operating in a highly risky environment.

---

[20] U.S. Sentencing Guidelines Manual 8B2.1, Application Note 6(A)(ii) (2004).

[21] *Id.*, Application Note 6(A)(i) and (ii).

[22] *Id.*, Application Note 6(B).

How granular will you go with each identified compliance and ethics risk area?

This point goes into examining risk areas contextually and how compliance and ethics are defined, which can determine how deep within the company you anticipate reaching within the organization. Looking at risks at a deep level will likely require some involvement by operational employees closer to the processes.

- How risks will be cataloged and structured may depend on whether the risk assessment is the first one being performed. If an initial or "baseline" assessment is taking place, you want to identify as best as possible *all* the compliance obligations (even if just at a high-level) encountered by the company. While this task can be arduous, especially for highly regulated companies, future ongoing assessments can build from this foundational labor.
- Are compliance and ethics "program" or organizational risks (e.g., tone at the top, awareness of the program, fear of retaliation, etc.) to be factored into the assessment in addition to subject-matter legal and regulatory categories? Program risks are discrete issues to be addressed comprising its own risk categories and requiring specific data collection (e.g., employee perception questionnaires). According to one survey, the general program risk areas most commonly identified from a risk assessment were: (i) internal policies and processes; (ii) employee awareness; (iii) understanding of compliance and ethics issues; and (iv) anonymous reporting system[23].

Should I hire an outside consultant to conduct the assessment?

The scope of the assessment and the maturity of the compliance and ethics program may dictate whether external support is useful. Programs just starting out and embarking on a baseline risk assessment can benefit from the expertise of an experienced consultant. An outside advisor also offers an independent and objective perspective which can prove valuable in managing multiple and competing perspectives from internal departments. Survey data suggests that about half of organizations have conducted their risk assessments entirely in-house, while the remainder used an outside advisor for at least part of the process[24].

Attorney-Client and Legal Privilege Considerations:

Whether or not an external consultant is engaged, the application of legal privileges should be kept in the forefront throughout the risk assessment despite the perceived erosion of the attorney-client privilege[25].

---

[23] Universal Conduct: An Ethics and Compliance Benchmarking Survey, *supra* note 12 at 22.

[24] Universal Conduct: An Ethics and Compliance Benchmarking Survey, *supra* note 12 at 24; Corpedia 2006 Compliance Program and Risk Assessment Benchmarking Survey, *supra* note 14 at 24.

[25] Universal Conduct: An Ethics and Compliance Benchmarking Survey, *supra* note 12 at 26.

Risk assessment materials can potentially be argued to be protected under evidentiary privileges and protections such as the federal self-evaluative privilege[26]. But it should be understood that even if the company attempts to protect the assessment by asserting a legal privilege (by outside counsel or the general counsel overseeing the process), such protection is uncertain and some courts may not recognize the privilege.

Understandably legal counsel will be concerned that information compiled during the risk assessment can be potentially damaging and may later be used against the organization—i.e., what did the company know and when did management know it (Example: a significant risk noted in the risk assessment is argued to have been ignored by the company). The following are observations on the practical application of legal privileges during the risk assessment process:

- Given this uncertainty, the better practice is to protect the attorney-client privilege and other discovery protections but to assume disclosure may be required. Assertion of the privilege can be achieved through careful document classification and process controls. Steps to protect the privilege will be discussed in the coverage of the risk assessment steps, below.
- As risk assessments have become more common, especially following the 2004 amendments to the Sentencing Guidelines, concerns regarding the lack of legal protections should not dissuade the company from undertaking a rigorous risk assessment. With the maturation of compliance and ethics programs, the benefits of a comprehensive assessment arguably outweigh the risks the information collected will be divulged. Self-disclosure of information is being promoted by regulators to establish a relationship of trust with governmental agencies or civil plaintiffs. In certain situations, it may be necessary and appropriate to waive attorney-client privileges and to provide access to evidence that might otherwise be privileged[27].
- Depending on the granularity of the information being gathered, a protocol to take an identified incident outside of the risk assessment process can provide a mechanism to assert the attorney-client privilege in appropriate circumstances. Such a protocol requires participation by experienced compliance and legal personnel to determine if an occurrence uncovered during the risk assessment should be treated separately from the process to better preserve potential legal protections for an uncovered event.

---

[26] The Ad Hoc Advisory Group Organizational Sentencing Guidelines Report discusses the self-evaluative privilege, and the risk of compliance program and audit materials serving as a litigation road map for prosecutors and private plaintiffs, *supra* note 5 at 113-121.

[27] For example, the Department of Defense (DoD) has a Voluntary Disclosure Program under which contractors who have discovered criminal or civil fraud and have reported the matter to the Inspector General have avoided prosecution by the U.S. Department of Justice. DoD Directive 5106.01 (April 13, 2006).

Experienced staff on the risk assessment team can help ensure that the documentation does not increase the risk to the organization if the assessment materials were to be disclosed. Information gathered should emphasize descriptive data and limit evaluative observations—particularly conjecture and opinion. Risk assessment data that is more descriptive and fact-based is less likely to supply litigants and investigators anything more than they would obtain through standard discovery and information requests.

Who should be involved? Establish a working group to lead the risk assessment: Successful risk assessments require the involvement of many individuals with a variety of areas of expertise. Their divergent business experiences, both in and out of the organization, add richness to the data collection and analysis, and ensures that the risk assessment is not the exclusive product of a single department or perspective. Benchmarks indicate that a wide range of functions participate, though not surprisingly, certain core departments are more commonly involved, with legal, compliance and ethics, internal audit, human resources, and finance leading the field of participants[28].

The compliance and ethics professional is well-equipped to lead the assessment process and certainly is the department most impacted. In some organizations, the legal department is the designated owner of the ethics and compliance risk assessment because with litigation history and sensitive evaluations as central aspects of any risk assessment, legal is better able to manage the assertion of legal privileges. For others, risk assessments are performed by the internal audit department, given that function's knowledge of the organization's control systems. Some have a freestanding risk department with its own chief risk officer. Whichever department owns the risk assessment process, senior management must ensure that it has adequate resources (e.g., time, staff, and organizational support) to complete its work.

Because the risk assessment is not a one-time event, the organization should also consider forming a management-level[29] risk steering committee to maintain continual oversight over the periodic performance of compliance and ethics risk assessments. The role of the risk committee can be undertaken by an existing compliance and ethics committee, or it can be a separate committee depending on the organization's structure and culture. For instance, a company may have a company wide risk committee as part of its ERM process where the compliance and ethics professional can participate.

---

[28] The LRN Ethics and Compliance Risk Management Practices Report, *supra* note 14 at 23-24.

[29] Legislators have proposed requiring a standing risk committee of the board of directors for all public companies. Although board-level risk committees are widespread in the financial services sector, it is less common for companies in other industries to have them.

Representation of the working group and steering committee can involve the same core functions with the working group focused on tactical implementation of the risk assessment, and the steering committee providing oversight for managing the identified risks, such as the responsibility for reviewing and approving mitigation plans submitted by risk owners.

Members of the risk assessment working group should be carefully selected. Apart from subject matter expertise, they should be advocates, facilitators, communicators and good listeners. Membership criteria can comprise individuals who:

- Believe in the value of the risk assessment process and in principles of risk management
- Are capable of building and maintaining buy-in for the risk assessment across different groups and disciplines
- Are able to aggregate and assimilate various types of information and data.

SAMPLE: Risk Committee Charter language

PURPOSE

The Risk Committee's primary purpose is to perform centralized oversight, policy-setting, information gathering, and communication to executive management and the Board of Directors, regarding [Company's] important risks and its related risk management activities. In addition, the Committee shall assist the [Management/Board of Directors] in fulfilling its oversight responsibilities related to the company's risk assessment and management processes.

RESPONSIBILITIES

The Risk Committee shall be responsible for the following activities:

a) Identify and monitor important existing and emerging risks to the achievement of the Company's strategic and operating objectives.
b) Formulate appropriate policies and monitoring and reporting frameworks to support effective management of important risks.
c) Review and evaluate the effectiveness of management processes and action plans to address such risks.
d) Advise on and recommend to executive management any significant actions or initiatives that the Committee believes necessary to effectively manage risk.
e) Ensure that activities of discrete risk management disciplines within the company are appropriately coordinated.
f) Report to executive management and the Board of Directors on the status of the company's important risks and related risk management processes.

Steps for Performing the Risk Assessment

With a team in place and the objectives confirmed, the organization should now be in a good position to begin the assessment starting with identifying the universe of risks to be evaluated. Companies use various combinations of methodologies to determine individual risks, as identifying the key areas of exposure can be a challenge.

1. Identifying the Risk Universe

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

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

A practical question in gathering this data is how to catalog and describe the risks in a meaningful way.

A. Establish basic risk terminology definitions

To assist in the cataloging of risks, it is useful to have a common taxonomy and categorization of risk types. The risk management community has provided several risk models to categorize risks into types for reporting and analysis purposes. With a common set of risk categories, risk assessment practitioners are better able to identify the organization's risks and can pull together risk information in a concise profile that helps users understand and monitor identified exposures.

Note that even seemingly basic terms like "risk" have a multitude of definitions with varying degrees of detail and precision. For example, COSO defines risk as "the possibility that an event will occur and adversely affect the achievement of objectives." Other definitions of risk emphasize the potential negative events that may be experienced as objectives are pursued, while others include both the protection of existing assets and the enhancement of future growth objectives[30].

[30] See GRC Capability Model "Red Book 2.0" Open Compliance & Ethics Group, April 2009, p. 9.

The organization should not let definitional nuances delay embarking on the risk assessment. Here are some basic working definitions of key terms distilled from various sources that can provide a starting point for the risk identification and the assessment process:

- ***Risk*** – The potential for loss caused by an event (or series of events) that can adversely affect the achievement of a company's objectives
- ***Compliance Risk*** – Risks that involve an uncertain legal or regulatory event that, if it occurs, has the potential to affect the achievement of a company's objectives
- ***Likelihood*** –The probability of the event occurring
- ***Impact*** or ***Severity*** –The potential consequences a realized risk may have on the organization
- ***Inherent Risk*** – The combination of expected likelihood and impact for any given risk; refers to the risk that exists *before* you address it—the risk in the absence of any actions you might take to alter either the likelihood or impact
- ***Mitigation*** and ***Controls*** – The measures taken to prevent, detect, minimize, or eliminate the identified risk
- ***Residual Risk*** – The net or remaining risk to the organization after consideration of mitigation or controls for the identified risk; also known as the company's "vulnerability" or "exposure" to the risk
- ***Compliance and Ethics Risk Assessment*** – The process of (i) identifying and defining compliance and ethical risks; (ii) determining their significance based on likelihood and impact; (iii) determining the current and desired level of controls for each risk; and (iv) monitoring remediation efforts.

B. Document reviews and public records research

Before convening a meeting of the working group, sources can be reviewed and consulted to begin developing a preliminary catalog of ethics and compliance risks. The risk assessment should include an examination of internal corporate documents, as well as industry information. To be sufficiently predictive, the risk assessment should include not only of known compliance breakdowns and failures, but also near misses. Types of material to review include:

- Litigation and claims history
- Issues raised via the hotline/helpline and to the compliance and ethics department
- Complaints received from customers, contractor, employees, and others
- Internal and external audit reports
- SEC filings
- Industry and government agency publications
- News reports and public information on compliance and ethics risks encountered by competitors

- Material on general legal risks applicable to all organizations (e.g., employment law).

This inventory of compliance and ethical risks should comprise a very thorough accounting of risks embodied in laws and regulations impacting the company. An effective ethics and compliance risk assessment takes into consideration risks that currently exist, as well as those activities that are currently legal but could reasonably be called into question in the future. The organization should be particularly attuned to gray zone areas or practices that may be common in the industry but may not be clearly defined as legal or ethical.

It is suggested that in compiling the types of events that can occur, try to list concrete actions that can be taken by employees or agents instead of abstract legal labels[31]. For example, instead of only labeling antitrust as a risk, specify "price-fixing" within the category of unfair competition. Practical descriptions will provide a more useful context for the remaining steps of the assessment and analysis.

C. Evaluate the types of compliance and ethics risks the organization is likely to face

With the scope of the assessment and definitions in mind, the working group needs to evaluate the nature of the risk information being collected. Beyond a listing of topics, here you want to drill down further to identify *behaviors* that create the greatest risk of violations of law, regulations, or company policy, and harm to the company's reputation.

In identifying areas where employees and others have either the capacity or the motivation to engage in wrongdoing, consider the following factors:

- Discretion – where are the company and individuals required to exercise judgment?
- Where do key decision-making and delegation authority reside?
- Are there areas lacking in supervision and internal controls?
- Are there internal pressures, temptations, and incentives?
- Are there external pressures from customers and complaints from vendors?
- Are there laws or policies that are not sufficiently understood or appreciated?

D. Other Inputs: Questionnaires, Interviews, Focus Groups

When identifying and assessing potential risk areas, the process should involve personnel across various disciplines and seniority levels. This can be accomplished through workshops, focus groups, surveys and interviews. After internal document reviews, the most popular methodology used in conducting risk assessment are "interviews of leadership and employees"[32].

---

[31] *ethikos*, "Thinking Inside the Box: Risk Analysis in Three Dimensions," J.M. Kaplan (Sept/Oct 2000).

[32] *Id.*; 2006 Compliance Program and Risk Assessment Benchmarking Survey, *supra* note 14 at 23.

Circulating a questionnaire that includes a listing of potential events can be an efficient way to identify compliance and ethics risks that apply to the organization. The working group and other participants can be asked to list every conceivable risk which would be later assessed (some risks will be ranked later in the prioritization phase and others may ultimately be excluded).

- Interviews are a valuable means for collecting risk information while imparting information about the compliance and ethics program. Who you talk to will depend on the scope of the assessment but generally you would include executive leadership and those in risk mitigation roles such as in-house and external counsel, internal and external auditors, risk managers and human resources—functional areas that comprise the working group. However, you should consider interviewing participants from all levels of the organization as front line operational employees can have useful observations and insights. It is preferable to include a broad cross-section of individuals to ensure that the opinions and perceptions about risk are as diverse and comprehensive as possible.

- Focus groups are another option and require a skillful facilitator to elicit input from the participants. The group interaction and dynamics can result in valuable observations and insights. Some organizations have used polling technology to allow focus group participants to vote confidentially on the likelihood and impact of listed risks.

Interviews are more prevalent than focus groups, likely in part due to the expense required to retain expertise to conduct an effective focus group. Interviews also permit a give-and-take that allows for follow up and more detailed information collection.

Interviews and focus groups should begin with an explanation of the purpose of the assessment. Short, open-ended questions tend to get longer, more useful answers. Focusing on the positive is sometimes more effective (e.g., "in what areas would the company benefit from additional training?"). It is crucial that the perceptions and opinions about risk be offered freely and without attribution.

If legal privileges are being sought, inform participants at the beginning of the interview that the risk assessment is being conducted under the direction of legal counsel and therefore the interview is privileged and must be treated as confidential. The interviewee should be reminded that involved attorneys represent the company and not the individual. The foregoing should be documented in the interview notes.

Again keep in mind that documentation of interview notes, memos, reports, etc. must all be drafted assuming disclosure. The compliance and ethics professional must be careful not to confuse opinion or conjecture with fact. Recommendations should be clearly stated and agreed-upon, and reviewed with counsel before finalizing and issued in writing.

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

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

Interview subjects can also be asked to identify areas where employees and others have either the capacity or motivation to engage in wrongdoing.

E. Organizing the risk categories

The company's historical risk data and information collected on the external legal, regulatory, business, and political environment should provide the working group sufficient detail to begin organizing and cataloging the identified risk areas. You will likely have a long list of risk areas in varying degrees of detail. Organize the risks in a hierarchy that is flexible as new risks will be identified in the future.

According to one survey, electronic data protection and privacy have become top concerns for compliance and ethics professionals due to expanding laws regarding data privacy in both the U.S. and Europe. Another challenge purportedly are anti-bribery laws and related risks[33]. The following is a summary of general legal, ethics and compliance risk categories that impact most organizations, including multinational companies. Note that organizational compliance and ethics program risks can be incorporated—in this example, "Whistleblower Protection" is captured as a risk area.

- *Bribery and Corruption.* Risk of national or international criminal investigation, indictment, and/or conviction and fines (of both the organization and employees involved) for

33 The LRN Ethics and Compliance Risk Management Practices Report, supra note 14 at 24.

paying bribes or engaging in other corruption with foreign officials to get business, retain business or receive some other undue advantage.

- *Antitrust and Unfair Competition.* Risk of violation of national or international civil or criminal laws concerning business collusion, conspiracy, and unfair competition.
- *Privacy and Data Security.* Risk of noncompliance with data privacy laws of a country in which the business operates, as well as the data privacy transfer protocols between countries.
- *Harassment and Discrimination.* Risk of violation of laws and organizational policies concerning workplace conduct pertaining to certain personal categories (gender, race, religion, ethnicity, age, sexual orientation, etc).
- *Human Rights.* Risk of violation of basic human rights concerning employees and others (especially in developing nations) including the use of child labor, slave labor, and other unfair labor practices.
- *Conflicts of Interest.* Risk that personnel, particularly upper and mid-level management, do not follow applicable conflict of interest rules, especially where there is potential adverse impact of the organization's reputation.
- *Environment, Health, and Safety.* Risk of violation of environmental or health and safety laws and policies with an adverse impact on people and/or property.
- *Whistleblower Protection.* Risk that an employee who raises good faith concerns about another employee, vendor, or customer faces retaliation for making such allegations.
- *Political Lobbying.* Risk that an improper contribution or political lobbying activity is undertaken on behalf of the organization or an individual employee in violation of the law.
- *Theft, Embezzlement, and Other Financial Misconduct.* Risk that one or more employees or agents engage in dishonest or criminal financial misconduct including misappropriation of property, and other misdeeds.
- *Fraud and Earnings Management.* Risk that management engages in the illegal or unethical manipulation or distortion of accounting, financial, or other records regarding the performance and results of the organization.
- *Money Laundering.* Risk that the organization knowingly or unknowingly engages in illegal transactions with third parties engaged in laundering funds from illicit activities.

2. Prioritizing the Risks

Following the data-gathering and discussions,, the working group should be prepared to prioritize the identified ethics and compliance risks in order to evaluate the controls in place and to recommend how to mitigate those risks. By prioritizing risks, the organization can focus its resources on those risks that occur most frequently and/or are likely to have the greatest impact on the organization.

The first factors to consider in prioritizing the risks are:

- The *likelihood* (the probability of the event occurring)
- The *impact or severity* (the potential consequences a realized risk may have)

A rare but significant harm will likely get priority over a more common but relatively trivial event. The majority of companies that conduct risk assessments appear to prioritize risk from both a probability of occurrence as well as severity of impact[34].

Information regarding the likelihood of a risk can come from many sources. The organization's own history already considered during the identification phase can provide data about how frequently a specific risk has arisen in the past. Past problems can prove to be a predictor of future issues and risks.

Regarding severity, the impact of a risk can be measured in several ways, including estimated economic loss, civil or criminal claim exposure, loss of customer or shareholder confidence, breach of employee loyalty, adverse publicity, and overall impact on the organization's ethical culture.

Assessment Criteria and Rating Scales

As with terminology and a robust methodology, the use of criteria and rating scales is critical to ensure an objective and consistent process. Issues of likelihood and severity are inherently subjective but can be made more reliable through the establishment of common criteria provided to those ranking the risks.

For example, a five point scale can be developed for the likelihood and frequency of the event occurring ranging from very low (one – highly unlikely and the probability, less than 1%) to very high (five – frequent occurrence, greater than once a week), with criteria and ratings in between those points.

Use of Surveys and Focus Groups to Rank and Rate

Some organizations augment the data from interviews and focus groups by administering surveys. Surveys can reach a broader population and are designed to elicit a wide range of perceptions about risks and their mitigating factors.

Similar to risk identification, it can be useful to implement a questionnaire or survey to allow others to provide their impressions of the relative priority of the risks that have been collected and organized. If your compliance and ethics risk areas have already been firmly established

---

[34] Universal Conduct: An Ethics and Compliance Benchmarking Survey, *supra* note 12 at 21; 2006 Compliance Program and Risk Assessment Benchmarking Survey, *supra* note 14 at 21.

and organized where the identification phase is focused on updating the universe of risks, you can consider also ranking them during the risk identification process—i.e., when sending out the questionnaire to list new risk areas, ask participants to further rate them according to likelihood and impact.

Some companies use group discussion or interviews to shed more light on opinions and ratings of risks. It can be difficult to elicit candid responses on the likelihood and severity of possible risks in a group setting, especially with senior leadership present. To encourage open and honest risk rankings, polling technology can be used to enable participants to freely rate risks during a focus group discussion without disclosing the actual rating that they gave.

Below is an example of a risk rating survey. Each participant is to assign each listed risk with a rating score. For example a score of one to five can be assigned to the likelihood or probability of the risk event occurring, with five for the most likely. A similar scale can be used for the impact depending on the detail and levels of the assessment criteria.

Sample Risk Rating Survey

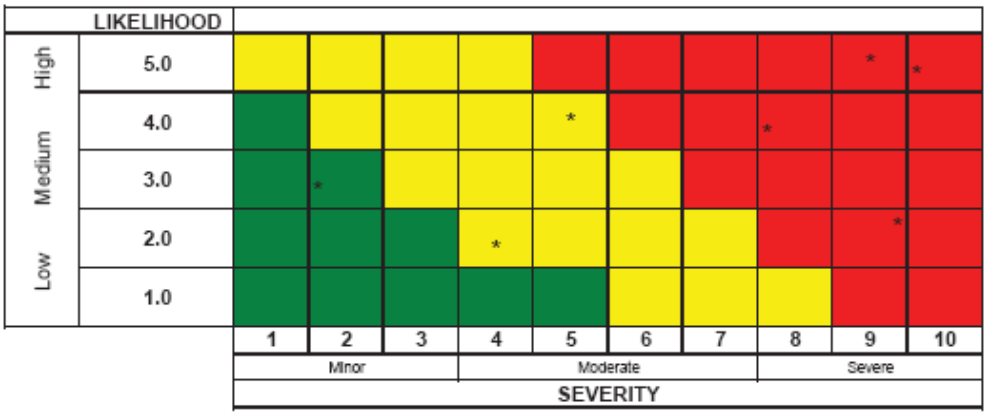
Risk	Impact	Probability	Comments
Bribery in foreign countries (FCPA)			
Export control			
Executive compensation			
Document retention/records management			
Maintaining Confidentiality			
Internal complaint resolution			
FMLA			
Government contracting			
Bid rigging			

The two scores can then be multiplied to provide a total score for each risk. The total scores can be ranked from highest to lowest to serve as a starting point for discussion. Surveys and scoring have their limits even with seemingly reliable criteria. Thus the scores should be reviewed to evaluate if they make sense to the working group.

Another approach is to plot each score for likelihood and severity on a matrix. In this manner you could designate that risks that are both more likely to occur and having the most severe

impact as possessing the highest priority. In the example below, red, yellow, and green levels of priority were determined along with the degree of action needed to address the risk.

Sample Risk Rating Matrix



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

3. Inventory the Compliance Environment and Other Key Controls

Once the top risks are identified, the next challenge is to identify existing compliance measures that address those risks. What are the appropriate and required responses to the identified and rated risks? Some risks are primarily employee awareness concerns that can be addressed through policies, training, and other guidance. Others may require more auditing and proactive monitoring or additional systems controls and other measures. The risk assessment work group will need to determine the business units and tasks involved with the identified risks.

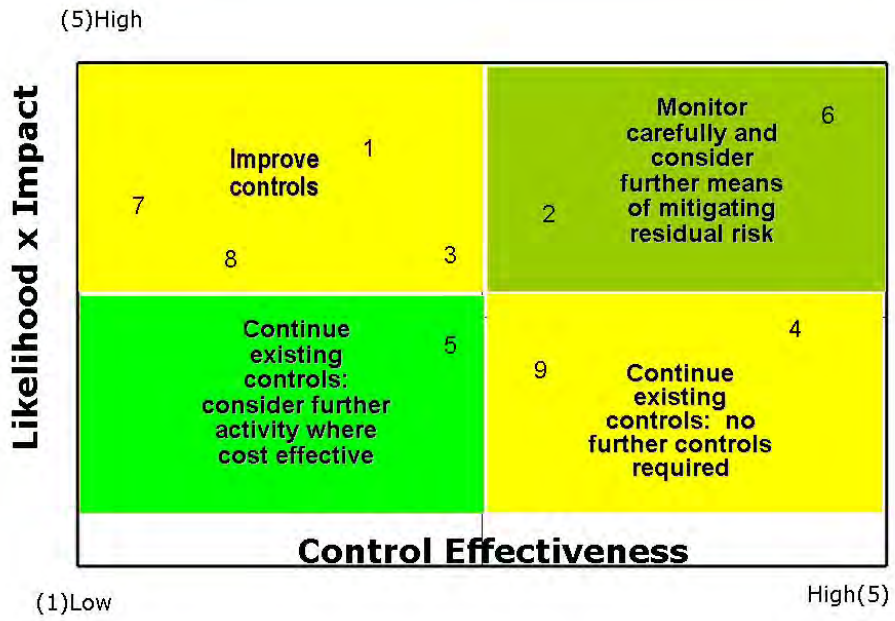
Each compliance and ethics risk can be further ranked by the sufficiency of current mitigation efforts and existing controls. The evaluation of compliance controls in place can similarly be made more reliable by the use of common criteria. Standard compliance controls can be introduced so that participants in the prioritization process will take into account the same types of activities and processes from the compliance and ethics program that address the risks, e.g., clear articulation of standards, accountability and assignment of responsibility, training and communication, preventative and detective controls noted by internal audit, etc.

Once the appropriate controls are identified, a gap and risk analysis can be performed. Essentially the process at this stage is to analyze within a business function and activity if there

is a need for compliance and ethics program type activities for a given risk. If a need exists, is it being met and if not, what type of controls are needed?

Another risk tool that can be utilized for the inventory and analysis is the residual risk chart.

Residual Risk Chart



Here, the combined likelihood and impact score that was measured is charted on one axis against the control effectiveness score. Risks with a high likelihood and severity of impact yet low control effectiveness will likely need to enhance existing controls and should do so on a priority basis. On the other extreme, risks scoring low on combined likelihood and impact with high control effectiveness measures can continue with existing controls with no further action required.

Recall the definition of *inherent risk*—the combination of expected likelihood and impact for any given risk; the risk that exists before you address it. The risk-likelihood severity matrix captures the inherent risk. When you factor the mitigation and controls in place, what remains is the *residual risk*—the net or remaining risk to the organization after consideration of the controls for the identified risk and depicted in the residual risk chart.

4. Remediate and Develop Action Plans

A state-of-the-art risk assessment is of no value if recommendations are not developed and implemented. Failing to act on the information collected could subject an organization to exposure in the event the information is disclosed during litigation or in connection with a government investigation.

Once the risks are scored and prioritized organizations then need to evaluate how to address each risk. There are four basic approaches to deal with risk:

- *Reject the risk*:. Some managers may choose to ignore difficult challenges with the hope that they will simply disappear. This approach will rarely result in a successful defense against the risk event occurring.
- *Accept the risk*: A common action to take is to accept the stated risk. For example, if the controls necessary to eliminate or mitigate key vulnerabilities are a greater financial burden to an organization than the actual risk impact, then it is probably a good idea to use budget dollars in other areas. For clearly stated legal obligations it would be extremely rare to accept a risk but may apply to gray areas of emerging regulations.
- *Transfer the risk*: An alternative to accepting a higher than reasonable risk when the cost of controls is too high is to purchase insurance to lower the business impact of an incident. This is a common risk management approach.
- *Mitigate the risk*: Risk mitigation typically focuses on managing the areas where the organization is most vulnerable. Risk mitigation involves the identification and management of risk mitigating controls.

For most significant compliance and ethics risk some level of mitigation will be required. The compliance and ethics professional with the working group can establish remediation plans for high priority risks and assign responsibility for mitigation. It is important to note that the risk assessment process does not change the ownership of the identified risks—it remains with the accountable executive.

Mitigation strategies and controls are developed to reduce the likelihood of adverse events; i.e., contain the impact should they occur and improve the ability of the organization to detect problems early. Mitigation steps can include activities such as education and training, new policies and procedures, increased audit activity, new equipment and materials, organizational change efforts, enhanced oversight, or changes in management and reporting structures. Mitigation may also require discontinuing a product line or ceasing to do business in a particular jurisdiction

Ultimately you will need to ensure the implementation of remediation plans that are developed from the risk assessment process. You will want to determine whether the remediation plan is actually effective at reducing the risk. Additionally it is important to document and report process improvements resulting from the remediation.

Some standard remediation steps to consider involving the compliance and ethics program include:

- Look for opportunities to revise compliance and ethics policies
- Adjust your communication plan with the risk information in mind and align communications with the effort expected under the Sentencing Guidelines to "promote an organizational culture that encourages ethical conduct and a commitment to compliance within the law.[35]"
- Update the training plan to target areas where employees do not understand or fully appreciate what is expected of them.
- Determine if there is a need for assignments of responsibilities in critical risk areas, or if additional resources are needed in the area to prevent and detect a given type of violation and risk. You may want to incorporate compliance and ethics components to job descriptions and incentives in a risk-based manner.
- Mitigate third-party risks through various due diligence activities. This can include ensuring background screenings, adding monitoring and auditing provisions in the contract, and requiring vendors to abide by your compliance and ethics program requirements.

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

- Review, revise and reissue policies on the U.S. Foreign Corrupt Practices Act
- Design targeted training and certifications of compliance for sales personnel involved in sales to government customers
- Issue guidance on how to retain foreign agents and representatives
- Require an approval process before a sale to a foreign government is consummated
- Require preapproval process for gifts, entertainment, or any expenditure on a foreign government official
- Review related policies on gifts and entertainment
- Develop and monitor gift and entertainment reports
- Audit and monitor risk mitigation efforts.

5. Reporting

A component of any remediation plan is ensuring that the action plan and mitigation strategies are communicated to those responsible for implementation. Senior management may also request regular updates on progress toward implementing the plan. Finally, the board of directors should be briefed on the risk-assessment process and its results. Providing the risk assessment report to the board or applicable board committee can support meaningful

[35] U.S. Sentencing Guidelines Manual, *supra* note 13.

program oversight by the board. The majority of compliance and ethics risk assessments appear to result in a written report[36].

Your final report will likely include discussion of risks identified during the document review, surveys, interviews or focus groups, and discussion amongst the risk assessment group. Recommendations for enhancements to the compliance and ethics program will also be based on the information collected and evaluated.

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

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

Supplemental Risk Management Principles

For the majority of compliance and ethics risk assessments, the basic steps—1. Identify the Risk Universe; 2. Prioritize the Risks; 3. Inventory the Compliance Environment and Other Key Controls; 4. Remediate and Develop Action Plans; and 5. Report—will suffice. But as risk management continues to become practiced, including the development of ERM programs, the following concepts are worth noting in the risk assessment process.

Risk Appetite and Risk Tolerance

Each organization has a different appetite and tolerance for risk, which may impact how risk areas are prioritized. Before performing a risk analysis of the collected risk data, it will be useful to understand the amount of risk, on a broad level, your organization is willing to accept in pursuit of stakeholder value.

Risk appetite defines the level of enterprise-wide risk that leaders are willing to take (or not take) with respect to specific actions, such as acquisitions, new product development, or market expansion. Where quantification is practical, risk appetite is usually expressed as a monetary figure or as a percentage of revenue, capital, or other financial measure (such as loan losses);

---

[36] Universal Conduct: An Ethics and Compliance Benchmarking Survey, *supra* note 12 at 25.

however, less quantifiable risk areas, such as ethical and reputational risk, should be considered when setting risk appetite levels. While management proposes risk appetite levels, the board ought to approve them—or challenge them and send them back to management for adjustments—based on an evaluation of alignment with business strategy and stakeholders' expectations.

Risk appetites may vary according to the type of risk under consideration. Some risks just come with the territory. If you are in the chemical business, there will inevitably be environmental spills and health and safety incidents. If you don't have the appetite for those types of risks, then you probably shouldn't be in that business. Once you have accepted this reality, you should do everything to prevent, detect, correct, respond to, and recover from any such incident.

Once the risk appetite is defined, management then should define specific *risk tolerances*, also known as risk targets or limits, that express the specific threshold level of risk by incident in terms that decision-makers can use (for instance, in completing an acquisition, the risk tolerance may be defined as a stop-loss threshold of a specified value). Management may have no tolerance for unethical business conduct or for environmental, health and safety incidents by adopting a zero incidents policy.

In most instances, there should be minimal tolerance regarding compliance and ethics related risks. The compliance and ethics professional should be available as a resource for helping senior executives understand and reconcile various views of risk within the organization.

The Myth of the Black Swan

One of the most feared risks of all is the *black swan* risk: the threat nobody had considered, and nobody can see coming[37]. Think of the September 11 terrorist attacks, the advent of Google, and the collapse of the financial markets.

But the black-swan risk is not what compliance and ethics professionals should be concerned about. The simple truth is that black-swan risks are, by definition, beyond our ability to perceive and anticipate. The much more pervasive and dangerous risk is that we fail to see the risks right in front of us, especially where they have always been, amplifying over time, until it is too late. The vast majority of compliance and ethical risks can be anticipated by understanding the regulatory environment in which your organization operates and closely monitoring government actions and industry trends.

Scenario Analysis

[37] See The Black Swan: The Impact of the Highly Improbable, by Nassim Nicholas Taleb (2008).

One way to evaluate high impact/low probability events is through scenario planning, which can augment statistical models and help companies prepare for specific events. Scenario planning enables executives to answer the questions: "What could disrupt our plans? And how vulnerable are we to it?"

The discipline of scenario analysis can be valuable to effective risk assessments because it forces one to ask, "What could go wrong in the future?" Scenario analysis is the process of analyzing a number of possible future events and focuses attention on all possible outcomes of an event occurring and the associated impacts. Proper scenario analysis improves decision-making by allowing management to more completely consider various outcomes and their implications to an organization.

For example, in considering the scenario of fraudulent trades occurring, the following questions could be evaluated:

1. Where does trading activity take place?
2. What kinds of trading takes place?
3. *What are all the ways unauthorized trading could take place?*
4. How up to date is our information?
5. Have we involved everyone with relevant knowledge in risk identification and control assessment?
6. *What would tell us if, in fact, unauthorized trades are occurring?*
7. How often do we formally analyze this scenario?
8. What issues have we identified in the past?
9. What losses have our industry competitors experienced?
10. *How could trades be hidden?*

To avoid scenario analysis becoming a time-consuming activity, management should focus on those risks that have been identified as the most material to the strategy of the business and that have the highest significance or likelihood of occurring.

Institutionalizing the Risk Assessment

The Sentencing Guidelines refer to an "ongoing" risk assessment. How often a specific risk must be monitored and re-assessed will depend on the risk itself. The continuing challenge is to be alert to when changed legal or business conditions require modifications to the compliance and ethics program and other controls.

The compliance and ethics professional should commit to updating and revising the risk-assessment process on a regular basis. You should receive reports of all issues and incidents of misconduct reported in the organization as this can reveal aspects of risk that were not

identified or foreseen. There should also be a mechanism for staying alert to the company's legal and regulatory environment.

The frequency with which an organization chooses to conduct such risk assessments may depend on the nature of the organization's industry. But if the methodology and process is adequately defined, it can reasonably be conducted annually and year-over-year results can be compared. Since operating environments, regulations and government enforcement priorities routinely change, it is inadvisable to conduct a formal risk assessment on a less frequent basis than every two years. Companies have begun to conduct risk assessments on a regular basis, either once per year or scheduled periodically along with regular audits[38].

A periodic assessment provides an opportunity to step back and assess how well the mitigation strategies have worked and to identify new or emerging risks that were not previously considered. If compliance and ethics program activities are well integrated into business activities, then ongoing monitoring of compliance risks should be occurring. A well-managed compliance and ethics program supported by a robust risk assessment process will result in a better use of organizational resources, improved outcomes, and fewer surprises.

[38] The LRN Ethics and Compliance Risk Management Practices Report, *supra* note 14 at 25.