CONDUCTING A RISK ASSESSMENT*

This article should be read in conjunction with the attached "Risk Identification Questionnaire" and "Sample Risk Identification & Assessment Chart."

Many firms are preparing for and conducting annual reviews of their compliance programs as required by the Advisers Act.[1] During this review process, many advisers are identifying various risks to their firms and client accounts and ensuring that the firm's compliance program addresses adequately these risks. While the compliance rule does not explicitly require an adviser to conduct such a risk assessment, the Commission and SEC staff nonetheless expect advisers to do so.[2] As a result, advisers have many questions regarding the assessment process, including: (i) what is the SEC's rationale for expecting a firm to adopt a risk assessment program; (ii) what does an assessment entail; (iii) when and how often should an adviser conduct an assessment; (iv) who should be responsible for conducting the assessment; and (v) how should a firm document the assessment to balance the firm's potential liability against SEC staff expectations? The discussion below addresses these questions and other matters in an effort to assist advisers in developing and implementing their risk assessment process.

INCLUDING RISK ASSESSMENT IN A COMPLIANCE PROGRAM

Advisers were required to implement a compliance program, reasonably designed to prevent violation of the Advisers Act, by October 5, 2004.[3] In meeting this deadline, many advisers identified existing and potential conflicts of interest between the adviser and its clients and designed a compliance program to address these conflicts.[4] The SEC staff also advocated that advisers conduct a comprehensive risk assessment of firm operations to identify, in addition to conflicts of interest, risks to the interests of the firm and its clients.[5] The SEC staff considers this assessment to be an important tool in helping to prevent further scandals and improve a firm's overall compliance program.[6]

Based on the foregoing, the SEC staff will most likely expect to see evidence of an adviser's risk assessment process.[7] Firms are encouraged, therefore, to (i) understand the SEC's concept of risk assessment; (ii) delegate the risk assessment function to an appropriate person or team; and (iii) improve policies and procedures in an effort to mitigate or eliminate risks to the firm and its clients.

DEFINING RISK ASSESSMENT

A risk assessment involves identifying and prioritizing issues, conflicts and other matters regarding a firm's operations that may create risk to the interests of the firm and/or its clients.[8] This process requires a firm to consider carefully its vulnerabilities.[9] The assessment should also include a review of the processes surrounding identified risk areas (*e.g.*, policies, procedures and business practices) in order to identify and eliminate or mitigate any gaps or weakness in these processes.

DELEGATING RISK ASSESSMENT DUTIES

Firms delegate the risk assessment function to various persons, including: (i) a CCO and/or other appropriate person(s), (ii) a risk committee or team, and (iii) an independent third party. Firms with only a few employees may find it necessary to delegate risk assessment to one or two individuals, whereas larger firms may find it appropriate to create a risk committee or employ an independent third party to assist in conducting the assessment. Many firms involve the CCO to some extent in the assessment process and some firms rely solely on the CCO to conduct the entire risk assessment. While the latter approach may be a function of firm resources, firms should endeavor, nonetheless, to involve other business people in the assessment process. For example, a firm's president, CEO, CFO, CIO, portfolio managers, traders, analysts, *etc*. should be involved in the assessment process since they will have firsthand knowledge of the firm's operations and any corresponding risks, and insights into how an employee might circumvent the company's compliance program to further his own interests. If a firm utilizes a risk committee, it should consist of high-level management and employees who carry out the day-to-day operations. Often, the people who perform a firm's day-to-day functions are most likely to observe a weakness or gap in the firm's processes. The person(s) selected to conduct the assessment, whether an individual or committee, should have sufficient knowledge of the firm and its business lines.

Once it is established who will conduct the risk assessment, an adviser should also determine whether the risk committee or individual(s) will review risk on a firm-wide basis or will divide the review process on a business-unit basis or other basis.

TIMING OF RISK ASSESSMENT

Some risk committees or individual(s) incorporate the risk assessment process into the firm's annual review. Others meet quarterly or less often to discuss risk. Still others have unscheduled impromptu risk meetings or add "risk" as an agenda item to another meeting, such as a board meeting or compliance staff meeting. Ideally, the risk assessment process should occur on a regular basis and as triggering events occur. A triggering event may include entering into a new line of business, transacting in securities new to an advisory client's account, and learning of a recent legal or regulatory action against a similarly situated adviser.

For each triggering event, a firm should assess the risks and conflicts that might arise and ensure that the adviser has a process in place to address those potential risks and conflicts. For example, if an adviser intends to establish and manage a hedge fund along side other accounts it should consider, among other things, the following: (i) incentives to allocate choice investments to the hedge fund in an effort to increase performance and garner higher performance fees, (ii) whether disclosure of valuation methods, trading strategies and performance of the hedge fund is accurate, and (iii) whether the adviser is marketing to appropriate sophisticated clients. If a firm wishes to transact in securities new to an advisory client's account, for example, credit swaps or collateralized debt obligations, the adviser should consider, among other things, whether (i) the portfolio manager, investment officer, investment committee, and/or research department has an adequate understanding of the security type, (ii) the security is suitable for the client's account,

(iii) new disclosures should be made about the security type and any corresponding risks, (iv) the adviser has sufficient systems and back-office support to accommodate trading of the security, and (v) the adviser has sufficient capabilities with respect to pricing or fair valuing the security. In addition, advisers should consider any enforcement, criminal or civil action or unfavorable press report regarding another firm and determine whether the adviser has a process in place to prevent a similar situation from developing at the adviser. For example, if the SEC were to sanction a firm because it failed to adequately segregate duties and supervise key personnel, an adviser should review its processes regarding these matters, as appropriate.

IDENTIFYING RISKS

The advisory business involves many types of risks that may potentially harm the interests of a firm and its clients. Advisers may group risk into broad categories such as operational, strategic, financial, compliance, and reputation. Some risks may fall into more than one category. Operational risk arises from the potential that inadequate information systems, operations systems, transaction processing, systems development, *etc*., will result in unforeseen losses. Strategic risk arises from inadequate current and prospective business decisions or responsiveness that might harm a firm's financial condition or create conflicts among a firm's clients. For example, this category may include risks associated with an adviser's (i) affiliations with broker-dealers or other businesses, (ii) lines of business such as managing mutual funds along side hedge funds, or (iii) non-U.S. business activities. Financial risk is the risk that a firm may be unable to meet its financial obligations. This category may include risks associated with (i) counterparty creditworthiness, (ii) firm leveraging, or (iii) cash flow management and revenue cycles. Compliance risk arises from the possibility that a breach of internal policies or procedures, laws, rules, regulations or ethical standards may impact negatively or disrupt firm operations or condition. For example, insider trading or failure to segregate duties or properly supervise employees may lead to regulatory enforcement actions, litigation, breached contracts, *etc*. Finally, reputation risk arises from the potential that inappropriate employee or management actions or inactions may cause the press or public to form a negative opinion of the firm and/or its products and services.

A risk committee or individual(s) may identify these and other risks by brainstorming about possible threats to the interests of the firm and its clients. A risk committee or individual(s) might also identify risks by reviewing the firm's financials and questioning the source and appropriateness of payments, profits and assets. In other words, "follow the money" and question whether firm pressure to increase income, profits and assets is causing employees to place the interests of the firm ahead of clients or to place the interests of certain clients before other clients.[10]

When identifying possible risks it is imperative that advisers "think outside the box."[11] It is easy to spot risk areas that regulators have already identified (*e.g*., late trading and market timing). However, firms must also assess new risk areas that could significantly affect client assets and firm viability.[12] Attached is a Risk Identification Questionnaire that may assist a risk committee or individual(s) in identifying risks. The questionnaire addresses the broad categories of risk discussed above, but presents predominately questions related to compliance risk.

After identifying possible risks, the risk committee or individual(s) should assign a person or team to (i) examine the policies, procedures, day-to-day business processes and/or systems surrounding the risks; (ii) ascertain the level of risk (*e.g.*, low, medium or high) to the firm and its clients; and (iii) propose reasonable compliance solutions to eliminate or decrease the risk, if necessary.[13] An adviser may determine the level of risk by assessing the probability of the risk's occurrence and the impact of this occurrence on the interests of the firm and its clients. Certain factors may decrease the level of risk, such as controls that identify the risk before it materializes, low probability of profits, and policies and procedures that provide all employees with clear guidance on the scope of permissible and impermissible conduct.[14] The level of risk may also be increased by certain factors, such as policies, procedures and operations that fail to detect the risk, the likelihood of significant profits, the belief that "everyone is doing it," and a lack of clear regulatory or supervisory guidance.[15] Based on these factors, the risk committee or individual(s) should prioritize all identified risks and allocate firm resources to the highest risk areas in an effort to mitigate or eliminate the risk.

REPORTING

A firm should establish to whom the risk committee or individual(s) will report regarding identified risks and possible solutions to lessen or dispose of the risks. For example, some advisers may require the risk committee or individual(s) to report periodically to the CCO or other senior executive. Whatever the reporting structure, each person involved in the risk assessment process should have a clear understanding of what to report (*e.g.*, "red flags," gaps in controls, new risks) and when to report to the CCO or other senior management.

DOCUMENTING THE ASSESSMENT PROCESS AND RESULTS

An adviser might consider creating a written report describing the firm's risk assessment process and results. The report should be in concise plain English and highlight any material problems and related resolutions. The report, although not required by SEC rules, may indicate to senior management, a fund board, an institutional client or the SEC staff that the firm has undertaken to identify possible risk areas and has committed to resolving any problems or gaps in the firm's compliance program that are identified during the assessment process.

Attached is a Sample Risk Identification and Assessment Chart, which may serve as an attachment to or reference in a risk assessment report. The chart tracks the priority and resolution of identified risks. Many advisers question whether risk assessment documentation will provide the SEC staff with a roadmap to possible firm weaknesses, tempt the SEC staff to ask probing questions, or send the SEC staff on a "fishing expedition." Regardless of these concerns, it is likely that the SEC exam staff will expect to see some indication that a firm is conducting a risk assessment of its operations.[16] Therefore, it may benefit a firm to have something in writing regarding its risk assessment process and results. Advisers should seek, however, advice from counsel in order to ensure that the documentation balances SEC staff expectations with the firm's potential liability.

DISCLOSING CONFLICTS

An adviser should review separately any conflicts of interest identified during the risk assessment process to determine if the adviser adequately disclosed these conflicts to its clients. An adviser should disclose all material conflicts to its clients on Form ADV. In addition, firms should consider whether other conflicts might necessitate amending client contracts or drafting some type of client specific disclosure. Some conflicts may also require advisers to acquire client consent of the matter.

RECORDKEEPING

The recordkeeping rule requires all advisers to maintain copies of all compliance rule "policies and procedures" that are in effect or were in effect at any time during the last five years.[17] If a firm has adopted or maintains risk assessment policies and procedures pursuant to the compliance rule, it must maintain copies of these policies and procedures in accordance with the recordkeeping rule. Moreover, it is possible that the SEC staff will expect to see risk assessment policies and procedures maintained under the recordkeeping rule since the staff would likely view risk assessment as necessary to comply with the compliance rule. The recordkeeping rule also requires advisers to keep any "records" documenting the adviser's annual compliance program review. If a firm incorporates a risk assessment into its annual review process, the SEC will expect to see any records documenting the risk assessment.

SELF-REPORTING

If a risk assessment committee or individual(s) uncovers a material matter during the assessment, a firm might consider self-reporting this matter to the SEC staff. Self-reporting may aid an adviser in reducing charges, obtaining lighter sanctions, or mitigating language in SEC documents used to announce and resolve enforcement actions.[18] Although SEC staff encourages self-reporting,[19] firms should seek the advice of counsel before reporting any matter to the SEC staff.

* The Investment Adviser Association does not intend for this article and/or any corresponding attachments to be a (i) comprehensive treatment of each issue that an adviser may need to address in its risk assessment process, or (ii) substitute for legal advice. Each advisory firm must tailor its risk assessment process to the firm's own operations and business. The Investment Adviser Association undertakes no responsibility to update this article.

[1] Rule 206(4)-7 under the Investment Advisers Act of 1940, as amended (Advisers Act).

[2] *Compliance Programs of Investment Companies and Investment Advisers; Final Rule*, Rel. Nos. IA-2204 and IC-26299, 74716 (Dec. 17, 2003) (stating that advisers should "identify conflicts and other compliance factors creating risk exposure for the firm and its clients in light of the firm's particular operations, and then design policies and procedures to address those risks"); Gene Gohlke, Associate Director, Office of Compliance, Inspections and Examinations (OCIE), U.S. Securities and Exchange Commission (SEC), *Remarks at the Managed Funds Association Educational Seminar Series 2005 – A Job Description for CCOs of Advisers to Private Investment Funds* (May 5, 2005) (stating that the process of risk identification and assessment is an important starting point for establishing effective compliance programs); Lori A. Richards, Director, OCIE, SEC, *Remarks before the National Society of Compliance Professionals 2004 National Membership Meeting – Instilling Lasting and Meaningful Changes in Compliance* (Oct. 28, 2004) ("Richards NSCP Speech") (stating that all firms must be proactive in identifying risk areas and in endeavoring to mitigate or eliminate those risks).

[3] Although Section 206(4)-7(a) of the compliance rule specifies the prevention of violations under the "Advisers Act," for practical purposes many advisory firms expand the scope of their compliance program to encompass all U.S. securities laws.

[4] Failure to mitigate, eliminate and/or disclose conflicts of interest may cause an adviser to violate, among other things, the anti-fraud provisions and disclosure requirements of the Advisers Act.

[5] Paul F. Roye, Director, Division of Investment Management, SEC, *Remarks before the Mutual Fund Directors Forum Fifth Annual Policy Conference: Critical Issues for Investment Company Directors* (Feb. 17, 2005) ("Roye Speech"); Lori A. Richards, Director, OCIE, SEC, *Remarks at NRS Annual Spring Compliance Conference – The Need for More Proactive Risk Assessment* (Apr. 14, 2004) ("Richards NRS Speech").

[6] *Id*. *See also*, Richards NSCP Speech, *supra* n. 2.

[7] In fact, the SEC staff included in a July 2005 examination request list the following request:

> Provide the following documents pertaining to the [r]egistrant's compliance program:
>
> a. A copy of the standard operating procedures ("SOP") for the risk identification and assessment process, which is the process by which registrant identifies risks and problems likely to be present at the adviser/fund.
>
> b. A copy of the minutes of any risk committee meetings that were held during the inspection period. Please note that advisers and funds are not required to have a risk committee.
>
> c. A current inventory of compliance risks. If changes were made to this inventory of risks during the inspection period, please indicate what these changes were and the corresponding date of the change….

f. Any document registrant has, such as a matrix or a spreadsheet, that maps its inventory of risk identified above to its written policies and procedures.

[8] Richards NSCP Speech, *supra* n.2 (encouraging firms to be proactive in identifying conflicts of interest that might incentivize illegal and unethical behavior); Mary Ann Gadziala, Associate Director, OCIE, SEC, *Remarks before the NYSE Regulation First Annual Securities Conference - Rebuilding Ethics and Compliance in the Securities Industry* (June 23, 2005) ("Gadziala Speech") (noting that a comprehensive risk analysis typically includes the assignment of the level of inherent risk and identification and rating of controls or mitigates); Roye Speech, *supra* n. 5 (suggesting that firms prioritize identified risks, but cautioning managers to not overlook the obvious or assume too much).

[9] Richards NSCP Speech, *supra* n. 2 (stating that a careful analysis of a firm's vulnerabilities is necessary to make a proactive change in the firm's compliance program that will foster ethical behavior and decision-making).

[10] Stephen M. Cutler, Director, Division of Enforcement, SEC, *Remarks before the National Regulatory Services Investment Adviser and Broker-Dealer Compliance/Risk Management Conference* (Sept. 9, 2003) ("Cutler Speech") (urging firms to "follow the money" to identify whether the interests of a potential more lucrative category of customers are being placed above those of another, less profitable group of customers).

[11] Roye Speech, *supra* n. 5 (urging fund directors to anticipate problems and areas where there could be issues within management firms and to be prepared to "think outside the box"); Cutler Speech, *supra* n. 10 (urging firms to be creative in their search for conflicts).

[12] Richards NSCP Speech, *supra* n. 2 (stating that firms that have only identified conflicts that have previously been identified by regulators have not really done a serious self-analysis to identify conflicts of interest in their operations).

[13] This approach is based on the SEC's method of identifying risks in the mutual fund and advisory industries. For example, OCIE staff engages in "risk mapping" whereby all examiners participate in small focus group-like discussions about the compliance risks that they have perceived in the securities industry. Participants identify risks, map them to relevant mitigating and aggravating conditions, and propose possible compliance and regulatory solutions. *See* Lori A. Richards, Director, OCIE, SEC, *Testimony Concerning SEC's Mutual Fund Oversight*, Before the U.S. House Subcommittee on Commercial and Administrative Law (June 7, 2005); *See also*, Roye Speech, *supra* n. 5 (suggesting that management companies engage in the type of risk assessment exercise that has been instituted at the SEC).

[14] Lori A. Richards, Director, OCIE, SEC, *Remarks before Financial Services Institute: First Annual Public Policy Day - An Update on the SEC's Examination Program* (Oct. 13, 2004).

[15] *Id*.

[16] Gadziala Speech, *supra*, n. 8 (stating that an evaluation of how an enterprise identifies and deals with compliance risks is a key aspect of a comprehensive SEC compliance examination); Richards NRS Speech, *supra* n. 5. *See also* 2005 SEC Staff Inspection Request List, *supra* n. 7.

[17] Rule 204-2(a)(17) under the Advisers Act.

[18] *Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934 and Commission Statement on the Relationship of Cooperation to Agency Enforcement Divisions*, Rel. No. 34-44969 (Oct. 23, 2001) (setting forth criteria that the SEC will consider in determining whether, and how much, to credit self-policing, self-reporting, remediation and cooperation -- from the extraordinary step of taking no

enforcement action to bringing reduced charges, seeking lighter sanctions, or including mitigating language in documents used to announce and resolve enforcement actions).

[19] *Id*. *See also*, Richards NSCP Speech, *supra* n. 2 (stating that firms will be better off by being forthcoming with the SEC than if the SEC staff detected the problem themselves); Cutler Speech, *supra* n. 10 (suggesting that firms notify the SEC staff of any "violative conduct" since the consequences will be worse if the SEC staff discovers this conduct on its own).