Why Investment Advisers Should Perform Risk Assessments at Least Annually

Practical Steps for Assessing Risks

By Michelle L. Jacko, Jacko Law Group, PC, and Tina Mitchell, Core Compliance & Legal Services, Inc.*

The beginning of a new year is a great opportunity to perform a detailed risk assessment, before any unidentified risks cause client harm or reputational and financial damage to your firm. In recent years, more and more investment advisers are electing to conduct a risk assessment as part of an annual compliance program check. Not only does a risk assessment help in the development of policies and procedures, but also can serve as a mitigation tool to help identify and proactively address potential threats to lower risk exposure.

Risks applicable to investment advisers also continue to be a high priority focus for the Securities and Exchange Commission ("SEC"). To that end, the SEC's Office of Compliance Inspections and Examinations is tasked with the responsibility of, among other things, monitoring risk applicable to its registrants. Some areas with associated risks that the SEC has focused on include custody, cybersecurity, business continuity/disaster recovery, employee personal trading, political contributions, safeguarding non-public information, trading practices, valuation and fee billing, marketing and advertising, conflicts of interest, firm affiliations, compensation arrangements and portfolio management process.

In this article, we give an overview of the components that make a risk assessment program effective, explore the starting points for creating a risk inventory, provide tips and factors for evaluating risks, discuss tools and systems to use as risk management controls and summarize actions to help you implement an effective risk assessment and monitoring program.

Michelle L. Jacko, Jacko Law Group, PC

Tina Mitchell, Core Compliance & Legal Services, Inc.

Implementing a Solid Risk Assessment Process

For a risk assessment program to be effective, it should include (at a minimum) the following four components:

1. ***Review*** – Performing a review of business practices should be one of the first steps, along with considering the firm's services and product offerings. Performing a risk review should take place when: new services or products are introduced, annually, any time there is a change, and when new or revised regulations are implemented. This helps ensure that applicable risks are identified both initially and thereafter. In essence, reviews are an ongoing process.

2. ***Implementation*** – Once the risks are identified, they need to be either eliminated or mitigated depending on the type of risk and risk appetite of the firm. Implementing policies and procedures on reviewing and addressing risks is essential and should include documenting reviews and findings, along with ensuring appropriate disclosures to clients.

3. ***Supervision*** – Senior managers and compliance personnel should continually supervise the firm's risk management process to help ensure risks are

Continued on page 13

"The goal of a risk assessment is to establish quantifiable data points that can serve as a qualitative analysis of existing controls to determine residual risk."

addressed properly and in line with policies and procedures. Each applicable risk that is not eliminated should be categorized and ranked so that supervision efforts are spent appropriately. Importantly, a risk can have more than one category assigned. For example, the risk of a trade error could be a financial risk due to the potential costs; an operational risk if the error was due to systems used; and a compliance risk since it needs to be handled in line with firm policies and procedures, regulatory requirements and in the best interest of the client. Because of these factors, this type of risk should have a higher ranking.

4. ***Knowledge*** – To be able to accurately identify related risks, senior managers and compliance personnel need to be knowledgeable of the types of risks that are associated with their firm's business practices and offerings. The SEC's website (www.sec.gov) provides a wealth of information, in addition to other regulators' websites, such as FINRA (www.finra.org), CFTC (www.cftc.gov), and Municipal Securities Regulatory Board (www.msrb.org). Another resource includes signing up for newsletters from legal firms and compliance consulting firms.

Starting Points for Creating a Risk Inventory

The goal of a risk assessment is to establish quantifiable data points that can serve as a qualitative analysis of existing controls to determine residual risk. Prior to undertaking this task, however, you will need to understand what you are trying to accomplish. Large organizations tend to have a risk department that analyzes risks at an enterprise level – taking into consideration market risks, operational risks, regulatory risks, compliance risks and financial risks. Smaller firms generally do not have the resources or infrastructure to accomplish this, but instead, will focus on the enterprise's compliance risks. To conduct a compliance risk review, consider taking the following steps:

- Step 1: **Inventory your compliance obligations** under both the federal securities laws and pursuant to your disclosures to clients and investors.

- Step 2: **Identify areas of conflicts of interest**. As you approach this, think about, in very realistic terms, what could go wrong? How could clients be harmed? Write these possible problems down. Consider the types of abusive conduct that have already been identified by the SEC in enforcement actions – but be more expansive in your analysis. Think about your service providers, too, and how their conduct – or misconduct – might harm your clients. Your goal here is to identify conflicts of interest that, if unmitigated, could lead to violations of any type.

- Step 3: Match existing compliance practices to your inventory of obligations and conflicts of interest, and **find any gaps**.

"It is all about having a process that helps eliminate, or at least lessen the impact of a risk. One size does not fit all."

- Step 4: **Assess the effectiveness of existing compliance functions**. In this stage, determine whether a particular compliance function makes violations less likely, and results in the prompt identification of violations.

- Step 5: **Identify additional compliance procedures** that are warranted based on changes to the firm's business model and products or services, and consider new regulatory requirements.

Similar approaches should be taken for the evaluation of market, credit and operational risks, which are typically conducted by line managers, portfolio managers, operations personnel and/or a risk management officer. For smaller firms, this analysis could also be overseen by the Chief Compliance Officer.

To capture these data points, consider developing a risk inventory spreadsheet and determine the metrics for measurement. For example, many firms opt to use a high, medium and low risk measurement or a numeric system (such as 1-5). Generally, a focus area is assigned a "high" risk assessment level if the reviewer believes that an area is not in full compliance with the regulatory requirements or if a deficiency was noted in a prior regulatory exam or annual review report and was not corrected or addressed. A focus area is assigned a "medium" risk assessment level if the reviewer believes that an area is one which will likely draw attention to the SEC due to a lack of some internal control. A focus area is assigned a "low" risk assessment if the reviewer believes that the internal controls appear adequate.

Continued on page 14

Continued from page 13

SAMPLE:

Focus Area	Line Manager	Identified Risk	Severity Level	Firm Priority (1-5, 1 being top priority)	Notes
Marketing	Joe	Use of social media for prospecting	Low (just audited; only uses one account - LinkedIn)	3	Will limit content to announcing firm events and new hires
Sales	Susan	Rolled out new offering	Medium	2	Mitigate through training
Compliance	Alex	Failed to conduct 2017 Annual Review	High	1	Engaged compliance counsel this month

Evaluating Risks

Once the risk inventory is complete, it is important to take steps to assess the risk management framework. If the firm has a Chief Risk Officer, then the findings should be compiled by the line-managers and delivered to that individual; in smaller firms, typically the Chief Compliance Officer assumes that role and escalates to senior management.

When assessing risks, several subject matters should be considered, including:

- Whether the firm's policies and procedures address the risk area;
- Findings from past SEC/regulatory examinations and annual reviews;
- Gaps identified by area managers throughout the year;
- Exception reports generated from risk management and monitoring systems;
- Customer complaints / litigation;
- Conflicts of interest (including dual roles of supervisors);
- Compensation arrangements;
- Use of key service providers;
- Insurance coverage;
- Internal controls for privacy, cybersecurity, Code of Ethics and Code of Conduct;
- Books and records retention; and
- Supervisory structure.

Once a risk is identified and prioritized, several outcomes can occur:

- Minimize
- Monitor
- Control
- Avoid
- Reject
- Accept
- Transfer
- Reduce
- Mitigate

The outcome decision is based on the information available and must be responsive to change. The decision should also be based on the firm's goals, processes, systems, resources, capabilities and skills. It is all about having a process that helps eliminate, or at least lessen the impact of a risk. One size does not fit all.

Tools and Systems: Developing Risk Management Controls

As risks are assessed, discussions should ensue about what controls, tools and technology should be leveraged to assist in addressing risk management concerns. Often these controls involve technology solutions, which may require additional funding from the business. To this end, Senior Management may request that Compliance conduct an evaluation as to why one control is better than another and may request alternatives to be considered for a variety of reasons, including costs. Consequently, in this role, Compliance is tasked with collecting data and mapping that to the internal control and potential risks associated with the product or activity in order for the risk managers to make a strategic business decision.

Other tools which frequently are used by Compliance in their risk management efforts include:

- Calendars
- Checklists
- Internal audits and forensic testing
- Participation in Committee Meetings (Risk Management, Operations, Best Execution and Ethics Committee discussions)
- Training on risk management and compliance obligations

Take action by starting with the highest risks first and discuss with line managers how the firm can drive something down from a high to a low risk. Develop protocols and test whether those internal controls are working; if gaps remain, address and try again. As appropriate, report progress to the Board of Directors (or equivalent) and/or Senior Management.

Conclusion

For the risk assessment process to be successful, Senior Management and the Board of Directors must be fully engaged. Policies, systems and processes must be dynamic and customized

Continued on page 15

to support the firm's risk culture. The risk appetite of the organization must be clearly defined with respect to the risk tolerances and business boundaries. There should be a method to evaluate the risks and summarize the results in a measurement that is easily communicated and understood. To be effective, risk management should be incorporated into strategic planning, business processes, performance measurement and incentive compensation, with the overall process reviewed annually. Ideally, a compliance risk assessment should be conducted each year to help advance the compliance program agenda and prioritize efforts. Documenting results will help senior management to understand what is needed in terms of resources – from personnel to technology and training. Through forward thinking and timely recognition, many risks can be effectively mitigated.

"Ideally, a compliance risk assessment should be conducted each year to help advance the compliance program agenda and prioritize efforts."

**Michelle L. Jacko, Esq., is Managing Partner of Jacko Law Group, PC and Tina Mitchell is Lead Senior Compliance Consultant of Core Compliance & Legal Services, Inc. They work extensively with investment advisers, broker-dealers, investment companies, hedge funds, private equity firms, banks and corporate clients on securities and corporate counsel matters, as well as regulatory compliance issues. Ms. Jacko can be reached at info@jackolg.com or (619) 298-2880. Ms. Mitchell can be reached at info@corecls.com or (619) 278-0020.*