OUTLINE:
IA/HF TESTING AND RISK ASSESSMENT

Prepared by

Lorna A. Schnase
Attorney at Law

for the

IA/HF Testing / Risk Assessment Lab

2011 NSCP Southern Regional Meeting/Labs

Dallas, Texas
April 12, 2011

THE BIG PICTURE

Q1: How do "testing" and "risk assessment" relate to one another?

A1: **Risk assessment** is the fundamental exercise of identifying what risks a firm faces and evaluating how significant the identified risks are to the firm and its clients or investors. For purposes of the SEC compliance rules,[1] this includes the risk that the firm will commit a violation of the federal securities laws or engage in conduct posing a conflict of interest that is not properly disclosed or consented to by clients or investors. For purposes of a firm's broader risk management effort, this should also include the risk that other threats faced by the firm will result in harm.

Risk assessment helps firms to properly design their compliance programs, which by rule must be "reasonably designed" to prevent, detect and correct violations. In order to ensure their programs are "reasonably designed," firms must identify the risks they face and target scarce resources to those areas posing greater risk.

Testing, on the other hand, is a quality control measure undertaken to assess the effectiveness of a firm's compliance program and whether the compliance procedures instituted by the firm are in fact working. The results of testing should be used to continually improve a firm's compliance program and make it more robust. Testing is often done in conjunction with, or as part of, a firm's annual review of its compliance program.

HOW TO DO A RISK ASSESSMENT

Q2: How should firms go about doing a risk assessment?

A2: There is no prescribed approach for doing a risk assessment. Firms vary widely, so different approaches may be suitable for different firms. However, a risk assessment would typically include at least the following 4 basic steps:

STEP 1: Prepare a risk inventory, listing all the risks posed by the firm's business. Consider the potential for legal and regulatory violations, conflicts of interest, breaches of contract, failures to adhere to investment guidelines, and so on. This list will be better and more complete if the process is a firm-wide effort.

STEP 2: Assign a risk "rating" to each risk, considering both the likelihood of the risk occurring and the potential for harm if it does. Use a rating system that makes sense for the firm and its compliance personnel.

STEP 3: "Map" the risks identified to procedures implemented to address those risks. In other words, show how the compliance procedures instituted at the firm are designed to address risk by correlating specific risks to specific procedures.

STEP 4: Review and update the risk assessment at least once a year. Consider changes, regulatory developments, testing results and other factors that have occurred since the last update to determine whether risks should be added or deleted.

Each of these steps – along with the entire risk assessment process – is discussed in far greater detail in the paper provided as part of the materials for this Lab, entitled "A 4-Step Risk Assessment Process for Investment Advisers,"[2] which also provides a sample Risk Matrix and sample Risk Inventory.

Q3: What does it mean to "follow the money"?

A3: Firms are often told to "follow the money" [3] as part of their compliance effort. This means "money" – revenues, compensation and non-cash benefits alike -- flowing into and out of the firm (and the hands of firm personnel) should be scrutinized, until the underlying arrangements are well understood, including what risks they pose and how firm procedures can be fashioned to ensure that the arrangements stay in compliance with the law and firm policies.

While it does not take an accounting degree to "follow the money," personnel should have at least a basic understanding of the firm's accounting system, financial statements and financial controls when scrutinizing these areas. If in-house personnel are not strong with these concepts, assistance from outside auditors or consultants might be warranted.

COMING UP WITH A GAME PLAN FOR TESTING

Q4: Why should firms plan their compliance testing?

A4: Planning offers many benefits, among them:

- Providing a beginning and end to the process with guideposts along the way, to steer and measure progress.
- Allowing personnel/outside parties to have input into the process, ensuring that it is as robust and efficient as it can be given available resources.
- Coordinating "to-do" tasks among inside and outside personnel, offering greater efficiency.
- Helping to make sure that important items do not slip between the cracks.
- Providing continuity from year to year and a catch-point for where improvements and enhancements can be introduced from year to year.

Q5: What resources might firms draw on in planning and implementing their testing?

A5: Aside from resources available in-house (prior year documentation and the like), firms can now find a large number of outside resources available to help them plan and implement their compliance testing, such as templates, sample checklists, guides, articles, SEC releases and more. Many of these resources are available for free on the Internet.

A list of resources can be found at the end of the paper provided as part of the materials for this Lab, entitled "Investment Adviser Compliance Program Annual Reviews."[4]

Q6: How should firms go about planning their compliance testing?

A6: The law does not dictate when and how firms should test their compliance procedures, aside from the basic compliance rule requirement that procedures be "reviewed" at least annually. Nonetheless, the SEC expects firms to conduct a certain amount of testing in order to make sure that their compliance programs are "reasonably designed" to detect, prevent and correct violations.[5]

Testing will be more robust if it incorporates a variety of different types of tests, such as transactional, periodic and forensic tests. Each of these types of tests is explained in the article provided as part of the materials for this Lab, entitled "Focus On: Adviser Compliance Testing."[6]

Because firms vary so widely, there is no "one-size-fits-all" testing program suitable for all firms. However, these basic steps will be useful in the planning process:

FIRST, using a list of the firm's compliance procedures, decide which procedures and areas should be tested.

NEXT, decide the following:

- What kind of test will be used to test each procedure (for example, transactional, periodic and/or forensic) and specifically what test will be used (for example, checking X against Y). Refer to the "Focus On: Adviser Compliance Testing" article[7] for an extensive list of tests that might be used to test in various different areas. Depending on the area, testing might consist of reviewing documentation, calculating or recalculating numbers, interviewing personnel, comparing information from various sources, checking processes that were followed, conducting simulations and so on.

- How frequently the test should be conducted (for example, quarterly or yearly) and, where appropriate, using what sample size.

- Who should conduct the various tests (such as in-house personnel, outside consultants, auditors and so on), keeping in mind the benefit of "functional separation" (having tests done by individuals other than those with day-to-day responsibilities in each area).

THEN, create a plan (perhaps on a spreadsheet or using project management software) incorporating these various elements to keep track of what will be tested, how, when and by whom.

Q7: What is the single most important thing firms should keep in mind in testing?

A7: Compliance personnel should know what they are testing for.

For example, if compliance personnel are testing trading data for window dressing, they must know what patterns might be indicative of window dressing. This provides context and purpose for the test and makes it more likely that the particular violation will be detected. Too often, compliance personnel review data, make calculations and complete checklists without having a clear understanding of what they are looking for.

At the same time, compliance personnel should keep a skeptical and open mind to detect potential violations that may not have been considered or anticipated beforehand. For example, if testing trading data for window dressing, personnel should be educated about and keep an open mind for other violations that might be revealed by trading patterns, such as portfolio pumping, insider trading, unfair allocations and other violations, even if the risk of those violations might be considered low.

Q8: How should firms incorporate technology in their testing?

A8: While much testing still goes on manually, particularly at smaller firms, technology is becoming increasingly ubiquitous in testing. This ranges from using fairly inexpensive, commonplace technology like Excel spreadsheets for analyzing data, to using fairly expensive, sophisticated software suites that can automate large portions of a compliance program, such as:

- insider trading testing,
- personal trading pre-clearances,
- brokerage placement,
- trade allocations,
- pre-trade screening trades against restricted lists and for adherence to investment restrictions,
- calculating risk metrics (such as VaR (value at risk), alpha, beta and other volatility measures),
- detection of suspicious trading patterns,
- valuations testing for stale prices and comparing valuations against next sale prices,
- email surveillance,
- pre-clearance and reporting of gifts, entertainment and outside business activities,
- pre-clearance and reporting of political contributions under "pay to play" restrictions, and
- checks at account opening against OFAC and similar lists for anti-money laundering purposes,

just to name a few.

SAMPLING – WHAT TO PICK AND HOW MANY

Q9: Does every trade, every document or every item need to be tested for testing to be effective?

A9: No. Indeed, testing a sample of items is typical when there are too many items to test individually. Sampling is a widely accepted technique, even in formal financial and compliance audits.

Q10: How should a firm decide what to pick and how many?

A10: SEC rules do not dictate what to pick for testing and how many.[8] They simply require the firm's compliance program to be "reasonably designed" to prevent, detect and correct violations. (Testing is aimed in particular at "detecting" violations.) Unfortunately, there is no "bright line" defining how much testing is enough to ensure that a compliance program is "reasonably designed." This can be seen as a matter of judgment that can be improved with experience.

Firms are not required to follow rigid statistical sampling techniques when testing, although having some familiarity with sampling concepts is helpful. Some firms decide what to pick for testing by:

- random sampling (picking with an eye toward each item having an equal probability of selection), or
- systematic sampling (based on a fixed interval, such as every third case).

Other methods for picking what to test (generally considered less reliable) include:

- haphazard sampling (picking without a structured method, but avoiding conscious bias or predictability), and
- judgmental sampling (picking based on a known bias, such as all items over a certain value, all items showing a specific type of exception and so on).

Firms may find stratifying large groups of testable items to be useful. For example, if a firm is testing the completeness of client account opening documentation and the firm has both retail and institutional clients, it would be more effective to test documentation from both groups.

How many items should be tested will of course vary by firm. The number tested should be reasonable under the circumstances, taking into consideration the size of the firm, the nature of its business, the types of clients it serves and other key characteristics of its business model, as well as the regulatory sensitivity of the area being tested. Other common sense factors should also be considered, such as:

- Has a problem or issue come to light in the course of testing in a particular area? If so, more cases ought to be tested to determine how widespread the problem is.
- Has there been an issue detected in this area in the past? If so, common sense would suggest testing more cases than if not.
- Is the area a "hot topic" for the SEC or the industry? If so, more attention should be paid to testing that area.

- Has there been a change in personnel or change of procedure in certain areas, suggesting a greater risk for errors to have occurred? If so, more rigorous testing in that area may be warranted.
- Is the area subjected to more than one type of testing? If so, selecting a smaller number of items for one particular type of test may be reasonable. For example, if a firm surveils email electronically on an on-going basis using a lexicon-based system, it may be reasonable for the firm to select a smaller number of messages for its quarterly manual review than if the quarterly manual review was the only testing method used.

Ideally, the method used to select items and the number of items tested would provide reasonable confidence that the sample group results are representative of the group as a whole. There are many free technology tools available on the Internet – such as sample size calculators – that can help firms determine what sample size might be right for their testing and help them to understand the relationships between sample size, population size, margin of error and confidential level.

REPORTING THE FINDINGS AND DOING THE FOLLOW-UP

***Q11: How should testing results be documented*?**

A11: Tests and their results should be clearly documented in order to coordinate the effort, mount appropriate responses and satisfy regulatory inspectors. Documentation does not have to be formal, but should be complete and clear. Documentation might take many different forms, for example:

- copies or lists of the specific procedures or items that were tested;
- data sheets, spreadsheets or calculations documenting the mechanics of the test and the results;
- manual or automated exception reports;
- checklists laying out testing protocols, evidencing completion and spelling out results;
- notes from or summaries of interviews conducted with employees or others who were consulted in connection with testing in various areas; or
- copies or summaries of reports from auditors, consultants, service providers or others that may be used as outside testing resources (audit reports from accountants, SAS 70 reports, SOP 07-2 reports, reports issued in connection with AT section 601 compliance attestations, etc.).

Ideally, documentation would also evidence who conducted the test and when, so that delays or omissions in the test scheduling can be detected and any problems corrected.

***Q12: Do tests and their results have to be included in a written report, like an annual review report*?**

A12: No, but they probably should be (at least in summary form). The adviser compliance rule – Rule 206(4)-7 – requires that a firm's compliance procedures be "reviewed" not less than annually. Annual reviews can, and typically do, include testing, which might be conducted at the time of the annual review or on a rolling basis throughout the year. Although the compliance rule does not specifically require advisers to prepare a written report of the annual review, firms should consider

preparing one. A well written report will evidence that the firm satisfied its regulatory obligation to conduct the review and allow the results to be effectively communicated within the firm, including to senior management who are responsible for making decisions about the firm's direction and future.

Firms unable to provide adequate written documentation of their compliance reviews risk being found deficient and subjected to closer SEC staff scrutiny or more frequent SEC inspections. Evidently, most firms understand this. According to a recent industry survey, nearly 80% of the responding firms indicated that they memorialize their annual review in a written report.[9]

Adequate documentation is prudent given the view of some regulators that "if it isn't in writing, it didn't happen." At the same time, documentation should be prepared with appropriate care understanding that it might well become subject to SEC inspection and/or public disclosure in connection with a lawsuit or otherwise.

***Q13: What are the adviser books & records requirements specifically related to testing documentation*?**

A13: Any records that are created to document an adviser's compliance program review (including testing) must be maintained and preserved in an easily accessible place for not less than 5 years from the end of the fiscal year during which the last entry was made on the record. During the first 2 years, the record must be maintained in an appropriate office of the adviser.

***Q14: How should firms follow up on compliance testing*?**

A14: Promptly.[10] Among firms surveyed, 6% reported that testing revealed "significant" compliance issues; another 69% reported "minor" compliance issues revealed.[11] Any testing that indicates a potential problem should be addressed and resolved with due speed. Minor problems would likely result in a less full-scale response as compared to larger or more serious problems, which would be best brought to the attention of senior management immediately. However, even minor problems should be viewed in context to see whether a pattern is developing that suggests a more serious problem may exist.

Whenever testing reveals a "red flag," an action plan should be formulated taking into consideration all relevant issues, including among them:

- Should outside counsel be engaged to investigate specific issues or violations and provide legal advice, in an engagement intended to be protected by the attorney-client privilege?
- What can be done to enhance procedures and eliminate the discovered weakness? If a compliance program "loophole" is discovered or conduct is found flying under the compliance "radar screen," firms should assess, implement and document their response eliminating those problems.
- Has any client been harmed due to the weakness or violation and, if so, in what way, how much, for how long and what can be done to make them whole?
- Which personnel were involved in the situation and what were their role, responsibility and level of culpability? Should they be terminated, put on leave or reassigned pending resolution of the issue?
- What should clients or investors be told about the issue and when?

- Should the firm "self-report" to the SEC or other regulators or otherwise contact authorities about the issue?
- Must or should the firm or its clients disclose the matter publicly, in SEC filings or otherwise and, if so, when?
- Should the firm's or client's fidelity bond carrier or E&O insurance carrier be notified of the problem, in order to preserve a possible claim under those policies? (Failure to notify a carrier of potential claims in a timely fashion may void otherwise available coverage.)
- Should the firm engage the services of a public relations firm to assist with outside contacts and relations?
- Must or should a contingency be booked on the financial statements of the firm and/or any affected clients?

Firms vary in their approach to follow-up, including self-reporting. Of the small percentage of firms (6%) reporting in a recent survey that testing had detected "significant" compliance issues, the majority (68%) said that they did not report the issues to the SEC and did not intend to raise them at their next SEC exam because they had resolved the issues internally.[12] Another 20% said they did not self-report to the SEC, but plan to raise the issues during their next SEC exam. Only 12% said that they had reported the matters to the SEC.[13]

Q15: What are the potential consequences of failing to follow up?

A15: In addition to the potential for violations to get progressively worse before being fixed, failing to follow up on "red flags" is one of the surest ways to get the attention of the SEC, and not in a good way. It is clear from public statements and enforcement actions[14] that the Staff takes a very dim view of firms that know something is wrong and do nothing to address it (in a timely fashion), particularly if the problem is repeated or recurring (i.e., recidivism).

Firms should consider follow-up one of the most important aspects of their compliance program. According to the head of OCIE, unresolved problems should be a compliance professional's worst nightmare.[15] This emphasizes that the compliance program is in place not just to catch problems after they occur, but to CORRECT them as well and PREVENT them from occurring again. This goal can only be achieved with appropriate follow-up.

[1] Rule 206(4)-7 under the Investment Advisers Act of 1940 ("Advisers Act"). There is a parallel rule for registered investment companies under the Investment Company Act of 1940, Rule 38a-1.

[2] A copy of "A 4-Step Risk Assessment Process for Investment Advisers" by Lorna A. Schnase (dated January 8, 2010) is included either in the printed materials provided with this Lab or on the NSCP's website available for download by Lab participants after the conference.

[3] See, for example, Speech by SEC Staff: Remarks Before The National Regulatory Services Investment Adviser and Broker-Dealer Compliance/Risk Management Conference by Stephen M. Cutler, Director of the SEC Division of Enforcement, Charleston, South Carolina (September 9, 2003) at http://www.sec.gov/news/speech/spch090903smc.htm.

[4] A copy of "Investment Adviser Compliance Reviews & Testing" by Lorna A. Schnase (updated through July 13, 2010) is included either in the printed materials provided with this Lab or on the NSCP's website available for download by Lab participants after the conference.

[5] See, for example, Compliance Programs of Investment Companies and Investment Advisers; Final Rule, Release Nos. IA-2204 and IC-26299 (Dec. 17, 2003) (Adopting Release) at fn. 15 ("Where appropriate, advisers' policies and procedures should employ, among other methods of detection, compliance tests that analyze information over time in order to identify unusual patterns…."); and the SEC Staff-prepared CCOutreach handout entitled "Questions Advisers Should Ask While Establishing or Reviewing Their Compliance Programs" (May 2006), in particular the questions under the "Quality control and forensic testing" heading ("Do you regularly conduct transactional or quality control tests to determine whether your activities are consistent with your compliance policies and procedures?" and "Do you conduct periodic tests to detect instances in which your policies and procedures may be circumvented or where there may have been attempts to take advantage of the gaps in your policies and procedures?").

[6] A copy of "Focus On: Adviser Compliance Testing" by Lorna A. Schnase, *The Investment Lawyer* (March-April 2010), is included either in the printed materials provided with this Lab or on the NSCP's website available for download by Lab participants after the conference.

[7] See footnote 6 above for the full citation.

[8] See FINRA Regulatory Notice 07-59 (December 2007), which provides guidance to broker-dealers on testing electronic communications. While not directly applicable to advisers or funds, that guidance includes valuable perspective on many of the issues discussed in this outline, including sampling.

[9] See the 2010 Investment Management Compliance Testing Survey, Summary Report, at http://www.investmentadviser.org/eweb/dynamicpage.aspx?webcode=PN_RB (p. 3).

[10] See Speech by SEC Staff: Compliance Professionals Play Proactive Defense, Remarks by Lori A. Richards, Director of the SEC's Office of Compliance Inspections and Examinations, National Society of Compliance Professionals National Membership Meeting (Washington, D.C., October 18, 2001) (emphasis added): "In the SEC's examination program we are giving a lot of attention to how we can fix problems more quickly. We think you should do the same. Unresolved problems should be a compliance professional's worst nightmare."

[11] See the 2008 Investment Management Compliance Testing Survey, Summary Report, at http://www.investmentadviser.org/eweb/dynamicpage.aspx?webcode=PN_RB (p. 14).

[12] See the 2008 Investment Management Compliance Testing Survey, Summary Report, at http://www.investmentadviser.org/eweb/dynamicpage.aspx?webcode=PN_RB (p. 15).

[13] Id.

[14] See, for example, CapitalWorks Investment Partners, LLC and Mark J. Correnti, Inv. Advisers Act Release 2520, 2006 SEC LEXIS 1306 (June 6, 2006) (among other things, repeated failures to correct deficiencies supported claim that firm's compliance program did not meet the required Rule 206(4)-7 standard). See also Western Asset Management Co. and Legg Mason Fund Adviser, Inc., Advisers Act Rel. No. 1980 (September 28, 2001): "Supervisors must also respond vigorously to indications of possible wrongdoing…. Supervisors must inquire into red flags and indications of irregularities and conduct adequate follow-up and review to detect and prevent future violations of the federal securities laws"; and In Re Rhumbline Advisers and John D. Nelson, Advisers Act Rel. No. 1765 (September 29, 1998): "Red flags and suggestions of irregularities demand inquiry as well as adequate follow-up and review. When indications of impropriety reach the attention of those in authority, they must act decisively to detect and prevent violations of the federal securities laws." Also, see Letter From the Office of Compliance Inspections and Examinations: To Registered Investment Advisers, on Areas Reviewed and Violations Found During Inspections (May 1, 2000): "The examination staff closely reviews the actions that advisers have taken to remedy the deficiencies cited during past examinations. Examiners have found instances where advisers have failed to correct violations cited during prior examinations, even after representing to the staff in writing that such violations would be corrected promptly. These violations may be subject to enforcement action, if appropriate."

[15] See the quotation from Lori Richards' speech, cited in footnote 10 above.