



## Implementing and Reviewing SEC-Mandated Compliance Programs

### INTRODUCTION

In a national sweep inspection begun at the end of October 2004, Securities and Exchange Commission staff began telephoning investment companies to gauge their compliance with the SEC's new chief compliance officer ("CCO") rules. We understand those surveyed were asked to describe the firm's risk assessment process—both in terms of the initial design of the compliance program and identification of new risks going forward—and also to discuss, among other things:

1. Whether the CCO believes he or she has sufficient resources to implement the new compliance program;
2. Whether the CCO search process had been challenging and which qualifications were emphasized during the search;
3. Whether the fund's CCO serves in the same capacity with respect to the fund's adviser;
4. Whether the anticipated nature of the working relationship between the fund's board of directors and the CCO had been considered;
5. Whether the fund's board had been consulted in the design of the fund's compliance program and what types of materials had been reviewed by the board during the approval process; and
6. As of what date the fund's board had approved the fund's compliance program and appointed its CCO.

An on-site inspection from the SEC's inspection staff is a distinct possibility for those who provided unsatisfactory answers.<sup>1</sup> Moreover, given the speed with which the SEC instituted the sweep after the

effective date of the compliance rules, there is a sense among funds and advisers that the SEC staff is likely to conduct enforcement investigations and seek sanctions for violation of the compliance rules quite swiftly.<sup>2</sup>

The sweep, together with a steady drumbeat of public commentary by the SEC staff, appears calculated to ensure that ongoing implementation and review of firm compliance programs remain an asset management industry priority. Stated plainly, the staff's message is, as outgoing SEC Division of Investment Management Director Paul Roye said in November: "Don't ease up on your compliance efforts now that your procedures are in place."<sup>3</sup> Roye added: "The importance of the [new compliance rules] cannot be overstated, and many industry observers believe [they] will in time prove to be among the most significant of the industry reforms the Commission has put in place over the past year."<sup>4</sup> This Memorandum is intended to help firms meet that expectation with practical advice regarding implementing and reviewing their compliance programs.

### OVERVIEW OF THE COMPLIANCE RULES

In December 2003, the SEC adopted rules that require each federally registered investment company and investment adviser to adopt and implement written policies and procedures reasonably designed to prevent violation of the applicable federal securities laws and to review those policies and procedures at least annually for adequacy and effective implementation.<sup>5</sup> These rules also require that each fund and adviser

<sup>1</sup> While the results of the sweep are not public, Lori Richards, Director of the SEC's Office of Compliance Inspections and Examinations, has said that not all firms polled met her office's expectations. See Chris Frankie, "SEC Brass: No Complacency on Compliance," *Ignites* (March 1, 2005) (citing comments by, in addition to Ms. Richards, outgoing SEC Division of Investment Management Director Paul Roye and OCIE Associate Director Gene Gohlke, all speaking to the Investment Adviser Compliance Best Practices Summit (Feb. 28, 2005)).

<sup>2</sup> See, e.g., Chris Frankie, "SEC Seen Taking Hard Line on CCO Rule," *Ignites* (Dec. 1, 2004).

<sup>3</sup> Paul Roye, Director of the SEC's Division of Investment Management, Keynote Address, at 22nd Annual Advanced ALI-ABA Conference on Life Insurance Products (Nov. 4, 2004).

<sup>4</sup> *Id.*

<sup>5</sup> *Compliance Programs of Investment Companies and Investment Advisers*, SEC Release Nos. IA-2204, IC-26299 (Dec. 17, 2003) (the "Adopting Release").

designate a CCO to be responsible for administering its compliance program.

Rule 206(4)-7 under the Investment Advisers Act of 1940 requires an adviser's compliance program to address the responsibilities of the adviser within the scope of the Investment Advisers Act.<sup>6</sup> Rule 38a-1 under the Investment Company Act of 1940 more broadly directs funds to adopt and implement a compliance program reasonably designed to prevent violation of the federal securities laws by the fund, including policies and procedures that provide for the oversight of key fund service providers (*e.g.*, each investment adviser, principal underwriter, administrator and transfer agent).<sup>7</sup>

The remainder of this Memorandum assumes familiarity with the basic requirements of Rule 206(4)-7 and Rule 38a-1. A lengthier summary of the two rules is available on our firm's website at [http://www.shearman.com/publications/asset\\_pubs.html](http://www.shearman.com/publications/asset_pubs.html).

## RISK-BASED IMPLEMENTATION AND DESIGN

Senior staff of the SEC Office of Compliance Inspections and Examinations ("OCIE") have said that a CCO can expect the following four questions at the beginning of a routine inspection:

1. Tell us about your business.
2. What conflicts and risks have you identified?
3. What are your compliance goals (and how are they tailored to your business and to preventing, detecting and correcting problems related to your identified conflicts and risks)?
4. Describe recent compliance concerns and how your compliance program responded to them.<sup>8</sup>

<sup>6</sup> In addition to the Investment Advisers Act, an adviser is subject to certain other regulatory regimes relating to its advisory business, such as those governing insider trading and protection of customer information. An adviser's compliance program reasonably would cover those requirements as well.

<sup>7</sup> For purposes of Rule 38a-1, the term "federal securities laws" means (i) the Securities Act of 1933, (ii) the Securities Exchange Act of 1934, (iii) the Sarbanes-Oxley Act of 2002, (iv) the Investment Company Act of 1940, (v) the Investment Advisers Act of 1940, (vi) Title V of the Gramm-Leach-Bliley Act, (vii) the Bank Secrecy Act (as applicable to funds) and (viii) any SEC or other agency's rules under each of these.

<sup>8</sup> John Walsh, OCIE Chief Counsel, at the National Regulatory Services "Building Compliance Programs" Conference (Aug. 2, 2004). To this last point in Mr. Walsh's list of questions, OCIE Associate Director Gohlke has said: "It's surprising the number of firms that have come to us and said 'We haven't had any [mistakes]. We simply don't believe them. Every firm has compliance issues. It's just a fact of life. Our goal is to see how the problems were corrected.'" Gene Gohlke, *supra* n.1.

The thrust of these questions illustrates that each fund and adviser should consider its unique business needs, conflicts and risks when implementing its own compliance program. Reliance on, and conformity with, industry "best practices" in identifying and responding to conflicts or risks is not enough.<sup>9</sup>

Firm management and compliance personnel therefore should devote greater ongoing attention and resources to matters identified as presenting meaningful conflicts or other risks *for their firm* and less attention to those identified as presenting little or no risk. A possible approach to the individualized analysis this requires would be to organize a designated risk assessment committee to meet periodically and as necessary to consider significant matters as they arise.<sup>10</sup> Such a committee structure would be supplemented by frequent meetings between compliance personnel and senior management, portfolio managers, members of a fund's board of directors, department heads and other firm employees.<sup>11</sup> The ideal outcome in the eyes of the SEC staff will be an institutionalized "culture of compliance" in which risk assessment and risk management are part of the daily life of all employees.<sup>12</sup>

## TESTING THE COMPLIANCE PROGRAM

Because no new compliance program will be perfect from the start, senior SEC staff have urged funds and advisers to commence testing their compliance programs.<sup>13</sup> Especially during the initial implementation phase, employee feedback and focused testing of this nature is important to ensure the program's various parts work together as planned. Testing should include:

1. Frontline reporting and regular review of the same by supervisory personnel;

<sup>9</sup> OCIE Director Lori Richards, at the National Society of Compliance Professionals National Membership Meeting (Oct. 28, 2004) (the "October NSCP Meeting").

<sup>10</sup> OCIE Director Richards commented approvingly regarding such a committee in response to a question from the audience when speaking at the October NSCP Meeting. Matters mentioned by Ms. Richards at that forum as potentially requiring reassessment of a firm's risk profile include changes to the firm's business model, turnover among key personnel, and growth or changes in the firm's client base. In other contexts, regulators have formally recommended the use of risk assessment committees. *See, e.g.*, Interagency Statement on Sound Practices Concerning Complex Structured Finance Activities, SEC Release No. 34-49695 (May 17, 2004).

<sup>11</sup> Lori Richards, *supra* n.9.

<sup>12</sup> This culture of compliance is a common SEC staff theme. *See, e.g.*, Tom Leswing, "SEC Director: All Staff Should Help Spot Risks," *Ignites* (Nov. 10, 2004) (citing remarks by Charles Fishkin, Director of the SEC's Office of Risk Assessment).

<sup>13</sup> Lori Richards, *supra* n.2; Paul Royce, *supra* n.3.

2. Analysis of information collected, which may include analysis by outside sources. Information should be analyzed over time to identify unusual patterns that may point to compliance problems or deficiencies;<sup>14</sup>
3. Prompt investigation of any patterns of compliance exceptions, customer complaints or other suspicious activities; and
4. Reporting up the chain as required by the compliance program or as otherwise appropriate. As the SEC is looking for a compliance-oriented “tone at the top,”<sup>15</sup> ensuring ongoing participation in this process by senior management is vital.

## ANNUAL REVIEW OF POLICIES AND PROCEDURES

The compliance rules require that each compliance program be reviewed at least annually for adequacy and effective implementation. The first such review must be completed within 18 months of a program’s adoption, with subsequent reviews to be completed at least every 12 months thereafter.

The annual review requirement has been characterized as “among the most powerful tools” available to CCOs under the new compliance rules.<sup>16</sup> Yet in a survey of 70 fund directors conducted late last year, half said their companies had not figured out how to put their annual reports together and nearly a quarter said they had not even considered the matter yet.<sup>17</sup>

This suggests, of course, that it is time to begin planning the annual review. In any event, given the variety of topics to be covered in the review, many firms are likely to opt for a rolling review schedule in which different components of the program will be assessed on an interim basis (say, quarterly or semi-annually), thereby lessening the “crunch” that would otherwise result from doing everything at the same time on a purely annual basis.

<sup>14</sup> Paul Royce, *supra* n.3.

<sup>15</sup> See, e.g., “Compliance Program Q&A with OCIE Director Lori Richards,” *Fund Directions* (Aug. 2004); Alison Sahoo, “SEC Lists Indicators of Good Compliance,” *Ignites* (Dec. 1, 2004) (citing remarks by Gene Gohlke).

<sup>16</sup> John Walsh, *supra* n.8.

<sup>17</sup> “Poll: Compliance Anxiety Persists,” *Ignites* (Nov. 15, 2004).

## Scope of the Annual Review

The Adopting Release states that the annual review should include an evaluation of (1) the effectiveness of the implementation of the compliance program; and (2) the need to revise the compliance program as a result of any compliance matters that arose during the previous year, any changes in the business activities of the adviser or its affiliates, and/or any relevant regulatory developments.

1. *Evaluation of the effectiveness of the implementation of the compliance program.* In addition to “overall firm compliance” and any firm-specific compliance needs, the review should focus on the effectiveness of the compliance program in addressing those matters identified in the Adopting Release as critical to most firms’ compliance efforts.<sup>18</sup> In the staff’s view, the evaluation process should include a self-assessment by the CCO of his or her role in the organization. In performing this self-assessment, a CCO should ask whether he or she has been a “key player in the process of getting business done the right way” and whether he or she has the necessary respect, resources, access and authority within the organization.<sup>19</sup>
2. *Evaluation of the need to revise the policies and procedures.* OCIE staff have said that the policies and procedures constituting a compliance program should not be static and that a review must question past practice.<sup>20</sup> The goal is always to improve on the existing approach to detecting and preventing compliance violations. Going forward, Rule 38a-1 does not require board approval of amendments to a fund’s or its service providers’ policies and procedures, but “material changes” must be discussed in the CCO’s annual report to the board.<sup>21</sup>

<sup>18</sup> The list for advisers addressed portfolio management, brokerage practices, proprietary and personal trading, accuracy of disclosures, including account statements, safeguarding assets, accuracy of books and records, marketing, valuation, privacy of client information, and business continuity. The list for funds added pricing of fund shares, processing of fund shares, identification of affiliated persons, protection of nonpublic information, fund governance and market timing.

<sup>19</sup> Lori Richards, *supra* n.9 and n.15. With regard to resources, a recent study by Cerulli Associates estimates smaller investment advisers will increase their compliance budgets for 2005 by 10% to 20% over 2004. Cecily O’Connor, “Smaller Managers Feel Pinch of Compliance, Regulation Costs,” *Pensions & Investments* (Dec. 13, 2004).

<sup>20</sup> Lori Richards, *supra* n.1 and n.9; John Walsh, *supra* n.8.

<sup>21</sup> *Adopting Release*, n.33.

As part of the annual review process, it may be helpful first to establish a preliminary “compliance profile” for each business unit reviewed and to use the profile as a fact-finding guide. Such a profile might incorporate the following:

#### Business Matters

- Has the unit entered new lines of business, developed significant new customers or modified its investment practices or strategies?
- Has the unit hired any new professionals whose activities should be covered by the compliance program?
- Has the unit implemented new software or automation initiatives?
- Has the unit’s ownership changed (as a result of a sale of the business or merger)? Has the unit acquired any new subsidiaries?
- Have there been any other business or organizational changes?

#### Industry Developments

- Have there been any changes in industry “best practices” or other standards? Has the SEC, NASD or another relevant regulator proposed or adopted any rules relating to the unit’s business?<sup>22</sup>

#### Complaints and Compliance Exceptions

- Is there a pattern of client complaints or compliance exceptions?
- Were remedial actions taken promptly? Is there a pattern in the remedial actions taken?
- Were complaints or exceptions escalated properly?

#### Problems with the Compliance Program

- Have there been any issues with interpretation or confusion about the application of specific policies and procedures?
- Have there been any compliance concerns not anticipated by the compliance program or violations of specific policies and procedures for which a remedial process was not identified?
- Have there been any problems in enforcing the compliance program (e.g., difficulties with respect to specific individuals or matters)?

<sup>22</sup> Regulatory enforcement actions and public comments by a regulator’s senior staff also should be considered.

### Who Conducts the Annual Review?

Neither of the compliance rules states who should conduct the annual review, and there is no “one size fits all” approach.<sup>23</sup> Generally, however, for both advisers and funds, if the review is conducted internally, the CCO should conduct or supervise the review. If an independent firm is retained (whether to conduct the review in full or in part), the CCO would be expected to supervise that external review.

In short, it is important that the CCO visibly “lead” the annual review process. Anything less may give the impression that the CCO does not have sufficient institutional stature.

There are advantages and disadvantages to engaging an independent firm to conduct the annual review:

#### Pros

- Independence and fresh perspective of the reviewer (which may, among other things, be persuasive for a regulator that the firm is implementing its compliance program in good faith).
- Opportunity for increased insight into industry practice.

#### Cons

- Limited familiarity of the reviewer with the firm’s specific business needs and compliance practices. A danger in retaining an independent reviewer is that the reviewer will miss important issues; thus, the CCO must carefully monitor the process and ensure that gaps in the independent reviewer’s knowledge of the company do not lead to oversights.
- Cost (which may be reduced by limiting the scope of the independent review).

### Documenting the Annual Review

The compliance rules require an adviser and fund to maintain any records documenting their compliance program annual review. Relevant documentation may include:

- An inventory of policies/procedures reviewed;
- An inventory of files and other records reviewed;
- Employee, service provider or other certifications, acknowledgments or representations reviewed;

<sup>23</sup> Rule 38a-1 does *not* require fund boards to conduct the annual review of the fund’s and its service providers’ policies and procedures. That review instead may be performed by the fund’s CCO, and its results would be described in the CCO’s annual report to the board.

- Checklists, reconciliation workbooks, exception records and similar material reviewed;
- Records of approvals of variations from established policies/procedures;
- Records of interviews (identifying persons involved and topics covered);
- A list of remedial actions reviewed; and
- Changes made to specific policies/procedures during the previous year.

There are no requirements in Rule 206(4)-7 as to either the necessity of a written report as part of the annual review of an adviser's compliance program or the content of such a report. Rule 38a-1 relating to funds, however, provides useful guidance. That Rule requires a fund's CCO to submit an annual report to the fund's board, which report must include: (1) any material changes in the policies and procedures since the last report, (2) any recommendations for material changes in the policies and procedures as a result of the annual review, and (3) any material compliance matters since the date of the last report.<sup>24</sup>

A written report of this nature, even in brief form, supplements the documentation listed above and more clearly establishes that the firm has qualitatively evaluated the effectiveness of its compliance program. *It should be noted, however, that no attorney-client privilege or work product doctrine protects the documentation or report of the annual review from review by the SEC staff.*<sup>25</sup> Care therefore must be taken in the management and presentation of this material.

### To Whom Does the CCO Report His or Her Findings?

Unlike Rule 38a-1, which requires annual reporting to the fund board, Rule 206(4)-7 by its terms does not require any reporting by the CCO relating to the annual review. Reporting to key executives and otherwise involving senior management in the review process, however, may help demonstrate to the SEC (and to management) that the adviser is actively

<sup>24</sup> Rule 38a-1(e)(2) defines "material compliance matters" as those compliance matters about which the board reasonably needs to know in order to oversee fund compliance.

<sup>25</sup> In the Adopting Release, n. 94, the SEC stated with respect to Rule 38a-1: "All reports required by our rules are meant to be made available to the Commission and the Commission staff and, thus, they are not subject to the attorney-client privilege, the work-product doctrine, or other similar protections." Expanding on this theme, SEC staff have said that judicious use of attorney-client privilege is an indicator of how seriously a firm takes compliance. Gene Gohlke as cited by Alison Sahoo, *supra* n.16.

seeking to assure its compliance with Rule 206(4)-7. This also demonstrates a positive "tone at the top."

- If an adviser is very small, senior firm officers presumably will know the results of the annual review, and may well have been closely involved in performing it, as part of their basic supervisory functions. Even in this case, documentation that a final report by the CCO, whether oral or written, was provided to these officers is suggested.
- For firms with more than a few employees, the CCO presumably will report the findings of the annual review to an executive officer or senior management body.

In addition to reports to senior management, the annual review is an opportunity to remind personnel throughout the organization of the importance of their compliance efforts. Interviews conducted as part of the review, as well as training sessions relating to any revisions to the compliance program following the review, may provide useful vehicles for disseminating this message.

## PROBLEMATIC CONDUCT

Problematic conduct, such as possible violations of law or of the firm's compliance program, should be discussed with internal or external counsel promptly. This is so regardless of whether the conduct is uncovered during the annual review process or through more routine testing or interaction.

- Sanctions should be applied as required, with deviations from established escalation and sanction processes considered carefully. SEC inspection staff have been charged with asking probing questions about exceptions allowed under a compliance program (e.g., who can authorize an exception, whether a fund's or adviser's board will be notified, etc.).<sup>26</sup> Exceptions benefiting senior personnel, or other potentially favored constituents such as family members or "star" portfolio managers, will bring added scrutiny. As OCIE Associate Director Gene Gohlke recently said: "It's important that if serious breaches occur, the [firm] not give high-level managers a slap on the wrist when they might throw the book at a lower-level staffer who committed a similar infraction."<sup>27</sup>
- Upon discovery of problematic conduct that is anything more than isolated and non-material, the compliance program should be reviewed as to whether revisions are necessary to prevent

<sup>26</sup> Paul Roye, *supra* n.3.

<sup>27</sup> Gene Gohlke as cited by Alison Sahoo, *supra* n.15.

recurrence. Revisions will require training as to the new requirements for relevant personnel. If a problem appears to be isolated, additional training may be warranted even if amendments to the procedures are not necessary.

- If the firm is subject to Sarbanes-Oxley Act financial reporting standards, as are SEC-registered investment companies, the persons responsible for certifying the efficacy of the firm's financial reporting procedures should be advised of problematic conduct relevant to their certifications.
- Targeted follow-up testing should be conducted to ensure the conduct has ceased.

### **PARTNERING WITH THE SEC?**

SEC officials insist they "are not looking to nail CCOs to the wall for early issues related to the recently enacted rule."<sup>28</sup> To the contrary, they are encouraging CCOs "not to live in fear of making a mistake" since "there will be a learning curve for both the SEC and the industry."<sup>29</sup>

In fact, the SEC and its staff have said they want CCOs to be their "partner[s] in the protection of investors" and therefore to communicate compliance problems with the SEC more readily than in the past. Doing so will, they say, help the staff make sure that CCOs have the support they need from both their firms and the SEC.<sup>30</sup> This message comes from the highest levels, with SEC Chairman William Donaldson asking firms to maintain open lines of communication with the SEC so that it can "fashion solutions that are meaningful and workable before an emerging [compliance issue] becomes a significant problem."<sup>31</sup>

Most recently, OCIE Director Richards announced plans, jointly with the Division of Investment Management, to develop a formal SEC staff outreach program targeted at CCOs.<sup>32</sup> Under consideration are regular SEC-sponsored "Dear CCO" newsletters describing new rules and regulatory interpretations. Also under consideration are annual or semi-annual panel discussions or conferences, which the staff sees as opportunities to interact and exchange views on good industry practices with CCOs. Ms. Richards also wants the planned program to be a vehicle for providing CCOs with information as to what the staff is finding during exams and illustrate responses to potential compliance pitfalls. While Ms. Richards acknowledges that the SEC is "always going to be an enforcement agency," she says the new outreach program should be understood as an effort to "marry that enforcement approach with a more proactive approach to help keep firms out of trouble."<sup>33</sup>

The opportunity for CCOs to converse directly with their primary regulator about compliance initiatives, industry-wide pitfalls and suggested best practices offers CCOs the potential for an additional compliance tool. This evolving relationship with the SEC and its staff will clearly be on uncharted waters, however, and must be managed carefully.

<sup>28</sup> Chris Frankie, "SEC Tries to Calm CCO Fears," *Ignites* (Dec. 8, 2004) (citing remarks by Division of Investment Management Associate Director Robert Plaze).

<sup>29</sup> *Id.*

<sup>30</sup> *Id.*

<sup>31</sup> Chairman William Donaldson, Remarks at Independent Directors' Council (Oct. 21, 2004).

<sup>32</sup> Chris Frankie, "New SEC Program Aims to Build CCO Trust," *Ignites* (Feb. 1, 2005) (citing remarks by Ms. Richards and Associate Director Plaze).

<sup>33</sup> *Id.*

This memorandum is intended only as a general discussion of these issues. It should not be regarded as legal advice. We would be pleased to provide additional details or advice about specific situations if desired. For more information on the topics covered in this issue, please contact:

Paul S. Schreiber  
New York, NY  
(+1 212) 848-8920  
pschreiber@shearman.com

Craig S. Tyle  
Washington, D.C.  
(+1 202) 508-8016  
craig.tyle@shearman.com

Nathan J. Greene  
New York, NY  
(+1 212) 848-4668  
ngreene@shearman.com

**[www.shearman.com](http://www.shearman.com)**

©2005 SHEARMAN & STERLING LLP

599 Lexington Avenue, New York, NY 10022

As used herein, "Shearman & Sterling" refers to Shearman & Sterling LLP, a limited liability partnership organized under the laws of the State of Delaware.