



Presented by Hardin Compliance Consulting LLC

Write the Best Annual Compliance Program Review EVER!

*By: Jaqueline M. Hummel, Partner and Managing Director
January 31, 2019*

Many chief compliance officers struggle every year with preparing the annual review and, based on the OCIE's summary of the [most frequently identified exam deficiencies](#); some are not up to the task. To help you out, here's our guide to writing your annual report.

First, look at what the rule requires. Under Advisers Act [Rule 206\(4\)-7](#), federally registered investment advisers are required to review their policies and procedures annually to determine their **adequacy** and the **effectiveness** of their implementation. As discussed in the [adopting release for Rule 206\(4\)-7](#), the review should "consider any compliance matters that arose during the previous year, any changes in the business activities of the adviser or its affiliates, and any changes in the Advisers Act or applicable regulations that might suggest a need to revise the policies or procedures." The review should answer these questions:

- Were recommendations from the prior year's annual review implemented?
- Were the firm's compliance policies and procedures adequate and followed consistently?
- Are there any operational or compliance risks or weaknesses that need to be addressed?
- Should any changes be made to the firm's policies and procedures?

Here's a basic outline for the report:

1. **Background:** Provide a brief description of the firm, including its main lines of business, client base, and assets under management. Usually the Form ADV Part 2A includes a description in the introduction and the section on the firm's advisory business which could be used for this purpose.
2. **Overview of the review process:** Identify who conducted the review (e.g., CCO, Management Committee, independent compliance consultant), when it was conducted, the period covered, and the scope. For example, the Chief Compliance Officer could be in charge of the process and require other areas of the firm to provide input, either on an ad hoc basis or through a formal

committee. The review process could cover the prior 12 months and include a review of (a) the compliance manual and (b) the results of compliance testing and monitoring over the past 12 months.

3. Identify the Principal Risks addressed through Compliance Policies and Procedures. In this section, discuss the principal risks specific to your firm and whether your compliance program addresses them.
4. Business, Industry and Regulatory Developments: In this section, discuss changes to your firm and changes made in the compliance program to address them. The section should also address any regulatory changes that required updates to your compliance program. Industry developments affecting your firm's business should also be addressed, if applicable. For example, significant cyber breaches may have caused your firm to re-evaluate its cybersecurity policies and procedures or engage an outside consultant to review your program.
5. Evaluation of the Adequacy and Effectiveness of Compliance Policies and Procedures, and Recommendations: This section should summarize the results of compliance testing and action items. This could include a spreadsheet with testing results or a written summary. Remember that the [Compliance Program Rule](#) requires that the firm review "the adequacy of the policies and procedures established pursuant to this section and the effectiveness of their implementation." Make sure that the written report specifically states whether the firm's compliance policies and procedures are adequate and effective.

Here are our recommendations on how to conduct the annual review of the compliance program.

Compliance Manual Review

The first step should be a review of the compliance manual. An investment adviser's compliance program should be designed to identify the firm's regulatory obligations, mitigate conflicts of interest that could result in harm to clients, and address risks to the firm and its clients. The SEC provided a list of risk areas that the compliance manual should address in the [adopting release](#) for the Compliance Program Rule:

- Portfolio management processes, including allocation of investment opportunities among clients and consistency of portfolios with clients' investment objectives, disclosures by the adviser, and applicable regulatory restrictions;
- Trading practices, including best execution, soft dollar arrangements, and trade allocation;
- Proprietary trading of the adviser and personal trading activities of its employees and access persons;
- The accuracy of disclosures made to investors, clients, and regulators, including account statements and advertisements;
- Safeguarding of client assets from conversion or inappropriate use by advisory personnel;
- The accurate creation of required records and their maintenance in a manner that secures them from unauthorized alteration or use and protects them from untimely destruction;
- Marketing advisory services, including the use of solicitors;
- Processes to value client holdings and assess fees based on those valuations;
- Safeguards for the privacy protection of client records and information; and
- Business continuity plans

Make sure your compliance manual covers all of these areas, as applicable. I would also include policies and procedures addressing the following areas in the compliance manual:

- Compliance with the Custody Rule, including Standing Letters of Authorization and inadvertent custody
- Required Regulatory Filings and Compliance with other regulatory regimes, if applicable, including:
 - Form ADV Part 1 and Part 2A/2B
 - Forms U-4 and U-5
 - Form PF
 - Schedules 13d, 13g, 13f, 13h and Section 16 Forms 3, 4, 5
 - Anti-Money Laundering
 - Form D and state blue sky filings
 - ERISA, FINRA rules surrounding “new issues,” CFTC “de minimis” exemption, Treasury filings, and
 - DOL Form LM-10
- Data Security and Cybersecurity (including Massachusetts data security requirements, SEC Regulation S-ID)
- Service provider oversight and due diligence
- Political contributions and compliance with the Pay to Play Rule
- Whistleblowing

After determining whether the firm has covered the bases, engage the other areas of the firm to review and sign off on the policies and procedures that cover their operations. The goal should be to determine whether the policies and procedures are adequate and followed consistently. Therefore, the people who are supposed to be following the procedures should answer these questions. For example, portfolio managers should review policies relating to the investment management process. Traders should review policies and procedures regarding trade allocation and aggregation. The IT department should confirm whether the description of the firm’s cybersecurity procedures is accurate. A full-blown cover-to-cover review is not always necessary; the frequency of the review depends on many factors, such as new regulations, added lines of business, use of new technology, operational changes, and changes in organizational structure. For example, a comprehensive review should take place after a merger with another firm. The compliance manual review the next year could be limited to any changes made since the last review.

If there are gaps in the manual, or inaccuracies in the policies and procedures, discuss them in the written report of the annual review and include recommendations to fix the issues. The SEC recognizes that compliance programs are iterative and expects to see changes.

Business and Regulatory Developments

The next step should be a consideration of any business developments and the effects on the compliance program. Has the firm entered into any new lines of business; opened new offices; changed its investment strategies or practices; experienced organizational changes, such as new ownership, new subsidiaries or affiliates, or loss of significant personnel; transitioned to a new portfolio management system (or similar firm-wide technology change); or changed key service providers? Any of these

developments can expose the firm to new risks and require changes to address them. For example, if the firm has recently adopted the Global Investment Performance Standards (GIPS®), the report on the annual review should include a discussion of the new policies and procedures adopted to ensure compliance.

Changes to the compliance team and its processes should also be included in the report. For example, if your firm appointed a new chief compliance officer, this should be discussed in the annual review along with a summary of the new CCO's credentials. When the firm adopts new compliance software, such as a personal securities transaction reporting system or email retention and review system, this should be discussed. Describe the service, how it's being used, and the due diligence performed to select the new service provider.

The annual compliance review should also address any key regulatory or industry developments over the past 12 months that have affected your firm. For example, in 2018, the SEC became increasingly aggressive against advisers for failing to disclose, or to adequately disclose, conflicts of interest. The big headline-grabbing cases have involved advisers and their affiliates receiving 12b-1 fees, revenue sharing, and other payments from other advisers and service providers. (Check out our [blog post](#) for a summary of key regulatory developments.) Given this development, many firms reviewed their Forms ADV Part 2A to see whether they adequately disclosed payments received from third parties and the conflict of interest such payments present. Firms may have also adopted a formalized process for selecting mutual fund share classes to be used in client accounts. A description of this new process should be included in the report.

Review Testing Results

The next step is a review of the compliance testing and monitoring performed throughout the year. This review should help the CCO determine whether the compliance policies and procedures are being followed and whether they were effective. The report could include a summary of tests performed along with findings and significant exceptions (e.g., in a spreadsheet) as an attachment to the written report.

The report should also address the recommendations made in the prior year's review. Discuss the progress made including changes to policies and procedures. If no progress has been made, then explain why not and any plans to remedy the situation.

The SEC will ask for this report during an examination, so choose your words carefully. This means report your results accurately and do not make promises you cannot keep. If one test revealed some minor issues that were resolved, do not report "no issues." It's more accurate to state "no material issues." For thornier issues where it's unclear when the firm will reach a resolution, be careful about setting a specific deadline; the SEC will hold you to it. Instead, it may be more productive to state that the firm will be exploring its options and will provide periodic reports to management on its progress.

Recommendations for Improvements

The written report of the annual review should include recommendations for improvement to the compliance program. As noted by the [SEC and the Department of Justice](#): “a good compliance program should constantly evolve. A company’s business changes over time, as do the environments in which it operates, the nature of its customers, the laws that govern its actions, and the standards of its industry. In addition, compliance programs that do not just exist on paper but are followed in practice will inevitably uncover compliance weaknesses and require enhancements.” Just because your program needs improvement does not mean it’s ineffective.

It is important that the report accurately discusses the findings of the annual review. Some firms are afraid of providing the SEC with a roadmap to their compliance failings. A successful compliance program, however, should be finding issues and resolving them. If there are no issues, then your compliance program may not be detecting problems. Even material issues indicating that the firm may have violated securities laws should be discussed. Do not engage outside counsel to write the report as a way to shield it from the SEC through a claim of legal privilege. First, it is unlikely that a claim of privilege would be successful under those circumstances, and second, the SEC can shut down your firm for failure to cooperate. Be honest. The SEC has shown much greater leniency to firms that admit their flaws and are working to correct them than firms that try to hide their issues.

The written report can also be used as leverage by the Chief Compliance Officer to request additional resources. As firms grow staff and assets under management, the compliance burden also increases. Regulatory burdens have also increased over the years and compliance officers are required to monitor for more risks. The SEC also expects more from the compliance function, as evidenced by OCIE’s risk alerts. By sharing examination findings and best practices, OCIE will now expect more from firms’ compliance programs and officers.

Asking for additional resources in the annual review can be risky. A CCO may be reluctant to cast his or her firm in a negative light. But when there are persistent, serious issues to be addressed, putting the request for help in writing can shield the CCO from personal liability. When the SEC goes after firms for inadequate compliance programs tend, CCOs that have asked for help are much less likely to be fined or censured.

Conclusion

Finally, the written report should conclude whether the firm’s compliance policies and procedures are adequate and effective. Remember, the program does not have to be perfect; it just has to be “reasonably designed to prevent violation of the Advisers Act by the adviser or any of its supervised persons.” (Rule 206(4)-7(a)) Look at your program as a whole to determine whether it is adequate and effective. If the program is generally meeting the goals of preventing violations of the securities laws, detecting violations that have occurred, and correcting promptly any violations that have occurred, then you should be able to come to that conclusion.

Partner with Hardin Compliance

Need help with your compliance program annual review or filing your Form ADV update? Hardin Compliance can help! Call us today at 1.724.935.6770, or visit our website at www.hardincompliance.com for more information.

Hardin Compliance Consulting provides links to other publicly-available legal and compliance websites for your convenience. These links have been selected because we believe they provide valuable information and guidance. The information in this e-newsletter is for general guidance only. It does not constitute the provision of legal advice, tax advice, accounting services, or professional consulting of any kind.