

# How to Improve Your Compliance Program

By Michelle L. Jacko, Esq., Managing Partner and CEO, Jacko Law Group\*

*Posted to IAA Today on September 9, 2020*

Compliance is defined by Webster's dictionary in part as "conformity in fulfilling official requirements." When an investment adviser registers with the U.S. Securities and Exchange Commission ("SEC"), the registrant first learns about the importance of compliance under Section 203(e), which provides authority for the SEC to censure, limit, suspend, or revoke an investment adviser's registration based on its activities, and is guided by [Rule 206\(4\)-7](#) of the Investment Advisers Act of 1940, as amended ("Advisers Act"), commonly referred to as the Compliance Rule. The rule provides that, "[i]t is unlawful for an investment adviser registered with the Commission to provide investment advice unless the adviser has adopted and implemented written policies and procedures reasonably designed to prevent violation of the Advisers Act by the adviser or any of its supervised persons."

The purpose of compliance is simple – to prevent violations of securities rules and regulations so that investors can be protected and investment advisers can fulfill their ethical and fiduciary obligations to such investors. Accountability through supervision and a system of checks and balances is key to do just that.

In this article, we will be exploring ways to improve your Compliance Program regardless of work environment, be it onsite or remote. Through the adoption of risk mitigation techniques adopted in robust, customized policies and procedures, surveillance efforts and oversight, a Compliance Program can be enhanced to advance an organization's business.

## Introduction

If you ask a CEO of an investment



*Michelle L. Jacko, Esq.,  
Managing Partner and CEO,  
Jacko Law Group*

*"Through the adoption of risk mitigation techniques adopted in robust, customized policies and procedures, surveillance efforts and oversight, a Compliance Program can be enhanced to advance an organization's business."*

adviser "what do they fear most," one of the most common answers will be a down market. That could begin a spiraling series of events: an increased likelihood of lower performance, which could result in a loss of investor confidence that leads to closure of accounts, customer complaints, and potential regulatory inquiries and litigation, that results in financial liability and diminished goodwill and reputation of the company. In short, the firm could lose it all. Compliance, on the other hand, establishes a system of controls to help protect the business, harness goodwill, foster a positive reputation and elevate investor confidence because of the series of controls in place to help protect investors.

Therefore, it is important to evaluate and clearly define how the organization accomplishes compliance both in the office and in a teleworking setting. This is typically done through customized policies and procedures, supervision and oversight.

Rule 206(4)-7 sets forth that written compliance policies and procedures must be adopted by investment advisers to prevent, detect and promptly correct any material violation of federal securities laws, including the Advisers Act. To accomplish this, firms should consider how they supervise their employees and associated persons (to observe and direct the execution of their assigned duties and activities) and globally oversee the firm's operations and compliance efforts (to be vigilant and manage with care). This is achieved by, among other things, appointing a Chief Compliance Officer ("CCO") who is competent and knowledgeable, and annually tests the effectiveness of the adviser's policies and procedures. Collectively, this system of internal controls comprises the Compliance Program.

## The Tone of the Compliance Program is Set by Senior Management

To have an effective Compliance Program, a strong and competent CCO helps, and a senior management team that advocates compliance is better. The role of the CCO is multifaceted – he or she must be familiar with the securities laws which govern the business, help to formulate policies to comply with regulatory requirements, and implement a supervi-

*Continued on page 21*

sory oversight program, which is carried out by identified senior managers. To be effective, all employees and associated persons need to have a clear understanding of what to do, when, and how to do it. Therefore, having a strong tone at the top that echoes the importance of compliance and how it is everyone's responsibility is important. This should start with the CEO or President and trickle down throughout the organization.

Establishing this "tone at the top" may not happen overnight. The CCO will need to make concerted efforts to educate, train and make recommendations to the senior managers on how they can work together to advance the Compliance Program. For both larger and smaller organizations, it is important for the CCO to have a "seat at the table" so that he/she may have a voice at all critical meetings and discussions regarding investments, risks, operations, new hires, and other functional areas where important policy decisions are made that relate to a firm's regulatory compliance function. That way, regulatory considerations, conflicts of interest, oversight and supervision can be discussed concurrently as decisions are formulated which should increase the effectiveness and efficiency for getting "buy in" for the compliance policies relating to these areas.

Once policy is set, it is important to test its effectiveness and to assess whether violations of the policy are occurring. If transgressions are detected, the role of the CCO is to ensure that the violation is brought to the attention of senior management and recommend actions for senior management to take to help enforce the policy. This will include penalties, such as additional training with management, a written warning, fines, or potential termination of employment. Equal treatment amongst employees at various seniority levels (including officers, directors and senior managers) is important to demonstrate that non-compliance is unacceptable, regardless of a person's position.

*"Compliance ... establishes a system of controls to help protect the business, harness goodwill, foster a positive reputation and elevate investor confidence because of the series of controls in place to help protect investors ... it is important to evaluate and clearly define how the organization accomplishes compliance both in the office and in a teleworking setting. This is typically done through customized policies and procedures, supervision and oversight."*

### **The Compliance Program Must be Customized to the Adviser's Business**

Through the years, there has been much guidance from the SEC regarding the importance of the Compliance Program. When the Compliance Rule first went into effect, Lori Richards, then Director of the SEC's Office of Compliance Inspections and Examinations ("OCIE"), provided guidance in a June 28, 2004 speech entitled, "The New Compliance Rule: An Opportunity for Change," on what compliance staff should do to ensure that the Compliance Program is **dynamic**, noting that:

*"Compliance staff should continually be asking: Are we detecting problematic conduct with this policy? Based on what we've detected, should we alter our policy? Is there a better way to detect problematic conduct?... Were the actions we took, once problematic conduct was detected, adequate to deter problematic conduct by this individual or others?"*

Additional SEC staff speeches (e.g., Speech by Rosalind Tyson, Associate Regional Director of the SEC's Pacific Regional Office, "The SEC's CCO Outreach Program" (May 24, 2005)) followed on how this could best be accomplished, which included guidance on the need to:

- Identify and assess the *risks* of the firm;
- Implement *effective* policies and procedures; and
- Create policies and procedures that address and allow each risk to be *effectively managed*.

This guidance still applies today. To be effective, Compliance Programs must identify and address risks, including conflicts of interest. The risks at each organization will differ depending upon the products and services offered, how a firm's clients are billed, the advertising and social media activities done, the firm's readiness to activate a business continuity plan and have all staff work remotely for an indefinite period of time, the frequency and content of client communications, trading and operational practices and a firm's compensation arrangements.

Once the risks are identified, CCOs should then consider whether a policy exists to address and mitigate those identified risks. If not, a policy should be drafted to prevent potential violations, with input and buy-in from senior management. If the policy already exists, consider:

- Is the policy effective by having control procedures in place (such as the type and frequency of supervisory reviews, exception reports and records to track anomalies and outcomes, and escalation procedures for outlier results);
- Have past SEC deficiency letters and past annual review findings been con-

*Continued on page 22*

sidered to address potential weaknesses;

- Have current SEC priorities and guidance (including best practices) provided by OCIE been considered;
- Do the risks trigger the need for the policy to be rewritten due to operational or business changes; and
- Do the identified risks require additional client disclosures?

As part of this process, CCOs should determine what training may be needed for staff and third-party service providers on the firm's newly revised policies and procedures and determine the appropriate method and forum for conducting this training.

Finally, it is important to remember that the role of the CCO is to oversee the Compliance Program. So, while the CCO may not be the designated supervisor for every firm activity, the CCO is responsible for understanding the needs of the firm, including the regulatory risks within the business and protections needed by clients. Therefore, the CCO should take meaningful steps to identify those rules that apply to the adviser and help develop customized policies and procedures reasonably designed to mitigate risks and protect clients by preventing violations of applicable laws and regulations.

### The Importance of Surveillance and Supervision

Ongoing monitoring of higher risk activities at the investment adviser is critically important. In today's regulatory environment, surveillance and exception reports help to evidence the efforts taken by the organization to document that employees and associated persons are supervised, that vendor and investment due diligence is occurring and that supervisors and staff are complying with the firm's stated policies and procedures.

On August 12, 2020, OCIE issued a new [Risk Alert](#) on COVID-19 Compli-

*"For both larger and smaller organizations, it is important for the CCO to have a 'seat at the table' so that he/she may have a voice at all critical meetings and discussions regarding investments, risks, operations, new hires, and other functional areas where important policy decisions are made that relate to a firm's regulatory compliance function."*

ance Risks and Considerations. Among other things, the SEC focused on the need to consider how Compliance Programs need to adjust in response to the COVID-19 pandemic. This includes considering practices and what needs to be adjusted – such as ceasing to accept client checks as payment if the firm is not able to pick up mail daily, modifying supervisory and compliance procedures of how due diligence reviews are conducted, and use of and controls for using personal devices for a business purpose. Supervision of personnel, fees and expenses, investment fraud, protection of sensitive information and business continuity also must be considered and surveyed.

Technology helps to provide an effective and efficient means to save time, improve accuracy, and generate recordkeeping of surveillance efforts. Automation also allows the CCO to identify trends and patterns of potentially troubling behaviors that might not have otherwise been detected had the technology not been used. Some of the most common programs used for surveillance efforts include:

- Electronic record storage and surveillance software (for emails, social media posts, texting and instant messaging);
- Personal trading programs (that often extend to compilation of attestations, personal holding and quarterly trading reports, outside business activities reports, political contribution reporting and insider trading monitoring);
- Compliance trading programs (to evaluate trade aggregations, comply with client guidelines and restrictions, monitor best execution, and analyze account cash flows and active/inactive trading);
- Compliance calendars and monitoring systems (to help ensure all filing and reporting deadlines are met and reviews performed and documented);
- Advertisement and social media review tracking programs (for capturing requests for reviews and modifications sought from and approvals by Compliance);
- Cybersecurity monitoring and training systems;
- Proxy voting programs; and
- Branch office examinations (for advisers who have multiple office locations).

Dependent upon the size and complexity of the business, the SEC encourages advisers to use technology surveillance efforts to identify areas where the Compliance Program may be circumvented. But how the technology is used and the data output which it yields is critically important. If compliance automation is purchased but not effectively utilized, there is risk particularly when a violation could have been detected had the automation been set up properly. Moreover, if exception reports create data outputs which are overwhelming and not meaningful (e.g.,

*Continued on page 23*

due to the sheer volume of data generated), then adjustments must be made to develop more concise, meaningful results. Finally, cybersecurity controls, such as strong, unique passwords and multi-factor authentication, should be considered at the initial set-up stage and whenever software updates are made available. Work closely with your Information Technology team to identify potential vulnerabilities that could exist and address them directly with the technology vendor.

## Conclusion

Constantly reviewing and improving your Compliance Program is one of the most important duties that a CCO has. Compliance Program needs are constantly evolving as the business changes, new regulatory requirements emerge and enterprise risks present themselves. Consider the following list of do's and don'ts as you evaluate your Compliance Program:

- Do conduct and document a risk assessment every year to identify areas where policies have not formally been adopted.
- Do explore ways the firm can leverage technology to develop meaningful surveillance processes and reports.

*"[H]aving a strong tone at the top that echoes the importance of compliance and how it is everyone's responsibility is important. This should start with the CEO or President and trickle down throughout the organization."*

- Do consider whether your policies are truly customized to your firm and consider whether they are detailed enough; strongly consider OCIE's recent guidance as provided in both the SEC's examination priorities release and Risk Alerts.
- Don't assume everyone understands compliance requirements; take time to have smaller, more focused training sessions to engage in meaningful conversations to assess knowledge.
- Don't presume that the adoption of only those policies and procedures set forth in the Compliance Rule is enough; the SEC emphasized in its release of this rule that the listed policies are minimal requirements and each adviser is responsible for iden-

tifying risk exposures for the firm and its clients in light of the business operations and for adopting policies and procedures to address those risks.

- Don't believe "it can't happen to us." The SEC continues to bring enforcement actions against advisers that do not have adequate policies or procedures or lack internal controls to supervise certain personnel. (See, e.g., [In re James T. Budden and Alexander Budden](#) (IA Rel. No. 4225) (Oct. 13, 2015) and [In the Matter of Wedbush Securities, Inc.](#)) (Exchange Act Rel. No. 85309 (Mar. 13, 2019)).

*\*Michelle L. Jacko is Managing Partner of Jacko Law Group, PC. A version of this article first appeared as a Risk Management Tip on the Jacko Law Group website and was edited by Robert D. Conca, Esq., Partner, Jacko Law Group. Jacko Law Group works extensively with investment advisers, broker-dealers, investment companies, private equity and hedge funds, banks and corporate clients on securities and corporate counsel matters. For more information, please visit <https://www.jackolg.com/>. This article is for general information purposes and is not intended to be and should not be taken as legal or other advice. [IAA](#)*