CORE COMPLIANCE

**Risk Management Update**
**February 2017**

## Why Investment Advisers Should Perform Annual Risk Assessments

Risks applicable to investment advisers 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 ("OCIE") is tasked with the responsibility of, among other things, monitoring risk applicable to its registrants. In the release of the SEC's 2017 examination priorities,[1] OCIE's then Director Marc Wyatt stated, "OCIE's priorities identify where we see risk to investors so that registrants can evaluate their own compliance programs in these important areas and make necessary changes and enhancements."

Since 2011, OCIE has been issuing written "Risk Alerts" to the financial industry covering certain risk areas they've identified though examinations of registrants. To date, they have published 24 Risk Alerts[2] with almost half of those being issued in 2015 and 2016. In this month's Risk Management Update, we discuss some of the higher priority risk areas pertaining to investment advisory firms and also provide guidance on addressing these risks and outline steps for implementing an effective risk assessment and monitoring program.

### High Profile Risk Areas

#### *Custody*

In 2010, the revisions to Rule 206(4)-2 of the Investment Advisers Act of 1940 (the "Custody Rule")[3] became effective, which included the removal of certain exemptions and the implementation of additional safeguarding steps that investment advisers with custody are required to follow. The SEC revised the Custody Rule to address the risks that came to light after certain fraud cases in 2008, including Madoff.[4]

Just two years later, the SEC published a Risk Alert[5] outlining "significant" deficiencies surrounding custody that they had uncovered during investment adviser exams.[6] Ironically, the first deficiency listed was the failure of advisers to recognize when they have custody. The SEC had found that some investment advisers had not identified certain activities as causing custody, which included:

---

[1] *See* https://www.sec.gov/news/pressrelease/2017-7.html.

[2] *See* https://www.sec.gov/ocie.

[3] "Custody of Funds or Securities of Clients by Investment Advisers" (Release No. IA-2968) (Mar. 12, 2010), found at https://www.sec.gov/rules/final/2009/ia-2968.pdf.

[4] *See* https://www.sec.gov/news/press/2008/2008-293.htm.

[5] *See* https://www.sec.gov/about/offices/ocie/custody-risk-alert.pdf.

[6] Notably, some of the deficiencies led to enforcement cases.

- Serving as trustee or co-trustee of a client's account;
- Bill paying and check writing services;
- Acting as general partner of a limited partnership;
- Online access to a client's account; and
- Receipt of checks made payable to clients from third parties.

The SEC Risk Alert also noted deficiencies under the surprise exam and qualified custodian requirements, along with audit approach issues.

*Risk Management Tip:* Chief Compliance Officers should provide periodic training to employees on custody. Providing examples during training that are based around the firm's practices are helpful. For example, if the firm allows "Standing Letters of Authorization" to be maintained with clients' custodians, training should be provided on when such letters have the potential to impart custody to the firm.

***Cybersecurity***

In 2014, OCIE announced the launch of their cybersecurity preparedness exam initiative[7] and this risk area has been on the SEC's examination priorities list every year since that time. The exam initiative consisted of the SEC performing sweep exams on several registrants to determine the strength of each firm's cybersecurity policies, procedures and controls. In February 2015, the SEC issued a Risk Alert[8] that provided a summary of their findings from the cybersecurity exams performed. Later that same year, the SEC came out with another Risk Alert announcing that they would be performing a second set of sweep exams on cybersecurity.[9] During 2015, the SEC also published written guidance on cybersecurity that included certain recommended steps for registrants to consider as part of their cybersecurity efforts.[10]

In their 2017 exam priorities letter, the SEC outlined their continued focus on examining registrants' cybersecurity compliance preparedness. Given the fact that businesses continue to rely more heavily on technology, cybersecurity will likely remain a very hot topic with the SEC for at least the next few years.

- Financial Services - Information Sharing and Analysis Center (fsisac.com)
- National Initiative of Cybersecurity Education (csrc.nist.gov)
- Securities and Exchange Commission (sec.gov)
- Financial Industry Regulatory Authority (finra.org)
- Department of Justice (justice.gov)

---

[7] *See* https://www.sec.gov/ocie/announcement/Cybersecurity-Risk-Alert--Appendix---4.15.14.pdf.
[8] *See* https://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf.
[9] *See* https://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf.
[10] *See* https://www.sec.gov/investment/im-guidance-2015-02.pdf.

*Risk Management Tip:* Firms should perform at least annual assessments of their cybersecurity protocols and provide ongoing training to employees. There are online resources that can provide a wealth of information on cybersecurity and cybercrimes, some of which include:

***Business Continuity/Disaster Recovery***

Since September 11, 2001, the ability of financial firms to recover from a disaster has been high on the radar of the SEC and other regulators, including the Financial Industry Regulatory Authority ("FINRA") and the Commodities Futures Trading Commission ("CFTC"). After 9-11, there have been a couple of natural disasters that have provided regulators with a back door look in to the strength of firms' business continuity plans.
For example, after Hurricane Sandy, the SEC, FINRA and the CFTC performed focused reviews of firms' business continuity plans and the steps taken during the disaster.
Shortly thereafter, they distributed a joint release on their findings,[11] and included recommended steps for firms to help ensure strong business continuity plans are in place. Around that same time, the SEC separately issued a Risk Alert,[12] which included their "observations and lessons learned" during their business continuity exams.

More recently, the SEC has proposed a rule on "Adviser Business Continuity and Transition Plans"[13] that if adopted, would require investment advisers to have both types of plans in place.

*Risk Management Tip:* Remember to cover wide spread and longer term business disruptions, such as earthquakes, tornados, and hurricanes in your business continuity plan, and also address protocols to follow during cyberattacks.

***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. ***R****eview* – 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. ***I****mplementation* – 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.

---

[11] *See* https://www.sec.gov/about/offices/ocie/jointobservations-bcps08072013.pdf.
[12] *See* https://www.sec.gov/about/offices/ocie/business-continuity-plans-risk-alert.pdf.
[13] *See* https://www.sec.gov/rules/proposed/2016/ia-4439.pdf.

3. ***S**upervision* – Senior managers and compliance should continually supervise the firm's risk management process to help ensure risks are 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. ***K**nowledge* – 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.

**Conclusion**

This RMU only provides a brief look at three of the areas that the SEC considers to have associated risks. Additional areas include, but aren't limited to, employee personal trading, political contributions, safeguarding non-public information, trading practices, valuation and fee billing, marketing and advertising, firm affiliations, compensation arrangements and portfolio management process.

If you haven't performed a detailed risk assessment, now is the time to begin before any unidentified risks cause client harm or reputational and financial damage to your firm.

For assistance, please contact us at info@corecls.com, at (619) 278-0020 or visit us at www.corecls.com for more information.

**Author: Tina Mitchell, Lead Sr. Compliance Consultant; Editor: Michelle Jacko, CEO, Core Compliance & Legal Services ("CCLS"). CCLS works extensively with investment advisers, broker-dealers, investment companies, hedge funds, private equity firms and banks on regulatory compliance issues.**