Chapter 13

Performing Due Diligence and Oversight of Third-Party Service Providers

By Michelle L. Jacko, *Jacko Law Group, PC*
Robert Boeche, *Jacko Law Group, PC*
Tina Mitchell, *Core Compliance & Legal Services, Inc.*
Craig Watanabe, *Core Compliance & Legal Services, Inc.*

I. INTRODUCTION

For various reasons, a financial firm may choose to partner with external third-party service providers (TPSPs) for the performance of essential tasks, rather than performing such tasks internally. Working with TPSPs opens a financial firm up to various types of risks—operational, legal, and regulatory. Costs associated with failing to properly address and monitor such risks not only include monetary losses plus loss of reputation and/or market share, but can also lead to injunctions, sanctions, suspensions, or permanent disbarments by regulators. Nevertheless, there are numerous reasons to use TSPSs whose synergies and benefits often outweigh such risks, especially if risks are properly mitigated. Financial firms often engage a TPSP because of the vendor's experience in performing certain tasks, cost and time considerations, and common industry practice.

Regardless of the impetus for these relationships, regulators require financial firms to conduct initial and ongoing due diligence on TPSPs. This chapter will discuss the regulatory requirements of financial institutions for performing due diligence on TPSPs; the types of due diligence reviews available; common challenges for evaluating service providers; and how to best structure, document and maintain a thorough due diligence program.

II. REGULATORY EXPECTATIONS FOR INITIAL DUE DILIGENCE AND ONGOING MONITORING OF TPSPS

"Due diligence" is the level of prudence, judgment, activity and care a reasonable person exercises under particular circumstances in order to avoid harm.[1] For the past

[1] From http://definitions.uslegal.com/d/due-diligence/

several years, regulators such as the U.S. Securities and Exchange Commission (SEC) and the Financial Industry Regulatory Authority (FINRA) have placed a high priority on ensuring that financial institutions have strong due diligence programs in place covering their use of external TPSPs.[2]

SEC and FINRA Requirements and Interpretations

The practice of performing due diligence on and ongoing oversight of TPSPs is not viewed as a "best practice" by regulators. Rather, such practices are viewed by regulators to be mandatory, as stated by regulators in written interpretations and guidance regarding compliance rules and regulations. When enforcing this requirement, regulators, among other sources, typically rely upon guidance described here.

Rule 206 and Rule 206(4)-7 under the Investment Advisers Act of 1940. Section 206[3] and Rule 206(4)-7 thereunder of the Investment Advisers Act of 1940, as amended (the "Advisers Act"), require investment advisers to adopt written policies and procedures reasonably designed to prevent violations of federal securities laws. Part of this requirement is for investment advisers to conduct due diligence on TPSPs to ensure any tasks outsourced by the adviser to such third-parties are being conducted pursuant to federal law. Although the SEC's formal guidance does not give a great amount of detail as to the extent and scope of such due diligence requirements, the SEC generally looks for due diligence "reasonably designed" to detect and prevent violations of federal securities laws.

Rule 38a-1 Under the Investment Company Act of 1940. Similar to the rules imposed on investment advisers by the Advisers Act, Rule 38a-1 under the Investment Company Act of 1940 requires investment companies to adopt written policies and procedures reasonably designed to prevent violations of federal securities laws. Stipulations of this rule include implementing procedures governing the performance of due diligence on TPSPs. In April 2016, the SEC emphasized this requirement as part of a *Guidance Update* and stated therein, "because funds…outsource critical functions to third parties, the [SEC] staff believes that they should consider conducting thorough initial and ongoing due diligence of those third parties."[4]

FINRA Notice to Members 05-48.[5] FINRA Rule 3010 requires members to design a supervisory system and corresponding written supervisory procedures that are appropriately tailored to each member's business structure.[6] In its Notice to Members 05-48 (NTM 05-48), FINRA[7] established that "outsourcing an activity or function to a third party does not

---

[2] FINRA's 2016 Regulatory and Examination Priorities Letter (Jan. 6, 2016), http://www.finra.org/sites/default/files/2016-regulatory-and-examination-priorities-letter.pdf

[3] Section 206 outlines those prohibited transactions of investment advisers, which include, among other provisions, antifraud provisions that generally prohibit an adviser from engaging in any practice that is fraudulent, deceptive or manipulative.

[4] SEC, *IM Guidance Update* No. 2016-04 (June 2016), https://www.sec.gov/investment/im-guidance-2016-04.pdf

[5] National Association of Securities Dealers, *Notice to Members, Outsourcing* (July 2005), http://www.finra.org/sites/default/files/NoticeDocument/p014735.pdf

[6] *See FINRA Rule 3010(a) and (b)*; and *Notice to Members (NTM) 99-45 (June 1999)*.

[7] The Notice to Members was actually promulgated by NASD in 2005. The NASD would later consolidate with the member regulation, enforcement, and arbitration operations of the New York Stock Exchange to form FINRA in 2007.

relieve members of their ultimate responsibility for compliance with all applicable federal securities laws and regulations."[8] As a result, for those members who outsource parts of their business, Rule 3010 supervisory procedures must also include procedures regarding such outsourcing practices to ensure compliance with applicable laws and rules. NTM 05-48 states that these supervisory procedures must be structured to ensure such arrangements are monitored, including "conducting a due diligence analysis of the third-party service provider."[9] NTM goes on to remind members that such due diligence should not only occur at the time a service provider is selected, but that members have "a continuing responsibility to oversee, supervise, and monitor the service provider's performance of covered activities."[10]

Notably, more recent guidance appears in Notice to Members 11-14, and Letters to Members March 9, 2009, and March 1, 2010.[11]

Regulatory Guidance and Considerations for Features of a Due Diligence Program

Codified regulations and written guidance are not the only sources financial professionals should review when developing a robust due diligence program ensuring TPSPs are performing services compliantly. SEC speeches and past precedent of enforcement actions also provide valuable insight into other topics a due diligence program should cover. The following highlights provide a sampling of such guidance.

SEC Comments and Guidance Statements. For the past several years, the SEC has continued to stress the importance of conducting thorough due diligence on TPSPs. As part of the SEC's 2009 "CCOutreach Regional Seminars,"[12] the SEC noted that "advisers should review each service provider's overall compliance program for compliance with the federal securities laws and should ensure that service providers are complying with the firm's specific policies and procedures." The SEC stated examiners will assess the adviser's "disclosures, contracts with clients, and contracts with service providers to determine whether the services and reporting obligations are consistent with disclosures and that all obligations are adequately addressed and overseen by the adviser." The SEC noted specific risk factors to be examined including, but not limited to:

- An adviser relying too heavily on a TPSP;
- An adviser changing TPSPs; and
- Whether an adviser is a "related person"[13] to the TPSP.

---

[8] FINRA, *Notice to Members, Outsourcing* (July 2005), http://www.finra.org/sites/default/files/NoticeDocument/p014735.pdf

[9] *Id.*

[10] *Id.*

[11] The complete text of the Notice to Members and Letters to Members referenced may be found at http://www.finra.org/sites/default/files/NoticeDocument/p123398.pdf, https://www.finra.org/sites/default/files/Industry/p118113.pdf, and http://www.finra.org/sites/default/files/Industry/p121004.pdf, respectively.

[12] SEC CCOutreach Regional Seminars, *The Evolving Compliance Environment: Examination Focus Areas* (Apr. 2009), https://www.sec.gov/info/iaiccco/iaiccco-focusareas.pdf?inf_contact_key=07351db9b4125acf3f4299fd40614c744fbfea546bef99d0fa64a529ed41d25f

[13] As part of its Form ADV Glossary, the SEC has defined "related persons" as any person that is under common control with an adviser.

More recently, as part of the SEC's September 2015 National Examination Program Risk Alert, the Office of Compliance Inspections and Examinations (OCIE) launched a cybersecurity effort, wherein vendor management was specifically called out. The staff specified:

> Some of the largest data breaches over the last few years may have resulted from the hacking of third-party vendor platforms. As a result, examiners may focus on firm practices and controls related to vendor management, such as due diligence with regard to vendor selection, monitoring and oversight of vendors, and contract terms. Examiners may assess how vendor relationships are considered as part of the firm's ongoing risk assessment process as well as how the firm determines the appropriate level of due diligence to conduct on a vendor.[14]

This emphasis alone is a call to action for the industry to focus risk management programs on due diligence of TPSPs.

Further, the SEC has proposed rules for transition planning, which among other emphases, stresses the importance of ensuring TPSPs understand their role within an advisory firm's business continuity plan,[15] particularly if they are a critical service provider to the adviser. This further emphasizes that due diligence of TPSPs must be a critical component of a financial institution's compliance program.

Enforcement Actions. The SEC has taken a number of financial institutions to enforcement over failure to conduct adequate due diligence of its TPSPs. More recent cases include the following.

- *In the Matter of Cantella & Co.*, IA Rel. No. 4338 (Feb. 23, 2016): The SEC found[16] that Cantella, a registered investment adviser, took insufficient steps to confirm the accuracy of F-Squared Investments, Inc.'s historical data and other information contained in advertising materials distributed by Cantella. Adequate due diligence on F-Squared's proposed data and calculation methodologies, such inaccuracies would have been identified. Because Cantella failed to perform due diligence, the advertisements showed results that were inflated substantially over F-Squared's actual performance. Cantella consented to the entry of the order finding that it violated, among other infringements, Section 206(4) of the Advisers Act, and, without admitting or denying the findings, agreed to pay a $100,000 penalty. Subsequently the SEC sanctioned 13 additional advisers in a series of SEC orders[17] who had also relied upon F-Squared for marketing purposes without properly performing due

[14] OCIE's 2015 Cybersecurity Examination Initiative, *National Exam Program Risk Alert,* Volume IV, No. 8 (Sept. 15, 2015), https://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf

[15] *Adviser Business Continuity and Transition Plans,* Rel. No. IA-4439, File No. 87-13-16, https://www.sec.gov/rules/proposed/2016/ia-4439.pdf

[16] Per the SEC, the findings in this matter were pursuant to Cantella & Co.'s offer and not binding on any other person or entity in the referenced proceeding or any other proceeding.

[17] For a list of the related orders, *see* https://www.sec.gov/news/pressrelease/2016-167.html

diligence on F-Squared, its calculation methodologies and/or obtaining proper documentation to verify such calculations. The penalties assessed against the firms ranged from $100,000 to a half-million dollars based upon the fees each firm earned from the related strategies. As stated by Andrew J. Ceresney, director of the SEC Enforcement Division, "when an investment adviser echoes another firm's performance claims in its own advertisements, it must verify the information first rather than merely accept it as fact."[18] This message clearly illustrates the SEC's position that due diligence of third-parties is the responsibility of the adviser;

- *In the Matter of Calhoun Asset Management, LLC, and Krista Lynn Ward,* IA Rel. No. 3428 (Jul. 9, 2012): The SEC alleged that materially false and misleading statements were made by Calhoun, the investment adviser to two funds of funds, and Ward, its principal and sole employee, about the firm's due diligence process. Calhoun touted due diligence process in marketing materials and the firm's website, particularly on the selection of investment managers, but failed to conduct such due diligence. Instead, Calhoun outsourced the services to a third-party vendor, on whom Calhoun did not perform due diligence or monitor in any capacity. As a result, Calhoun received a $50,000 penalty (joint and several basis with Ward), and Ward was barred from brokerage and advisory business with right to reapply in five years;
- *In re Merrill Lynch, Pierce, Fenner & Smith Incorporated,* FINRA Letter of Acceptance, Waiver and Consent No. 2008014187701 (Jun. 24, 2012): Merrill Lynch outsourced some of its proxy functions for certain accounts of its adviser programs to a TPSP. The TPSP misdirected proxy ballots, used outdated proxy delivery designations, and conducted clerical errors. FINRA alleged that Merrill Lynch had, among other infringements, failed to establish a supervisory system to reasonably supervise the delivery of proxies to certain customers. FINRA argued that had such due diligence processes been in place, Merrill Lynch would have been detected such errors. Merrill Lynch consented to the imposition of various sanctions, censure, and a $2.8 million fine.

II. TYPES OF DUE DILIGENCE REVIEWS

A firm can conduct a TPSP due diligence review in various ways. This section explores:

- Considerations for using internal versus external resources for conducting TPSP due diligence;
- How to effectively use checklists and questionnaires; and
- Tips for conducting onsite evaluations.

Internal Versus External (Third-Party) Due Diligence

Options for Performing Due Diligence. Due diligence requires knowledge and understanding of the type of product and service a firm seeks to evaluate. In some cases, a firm may not have the internal resources to conduct the due diligence because of lack of time or knowledge. In other instances, an external due diligence provider may not

[18] *Id.*

understand the intricate details of what needs to be performed and what circumstances apply. Thus, before a firm commences any type of due diligence, it is important to determine whether the party selected (in the form of an internal staff person or an external provider) has sufficient knowledge and experience to know the right questions to ask and the right red flag areas to explore prior to beginning the due diligence process.

Notably, many external resources are available to conduct *product* due diligence (particularly in direct participation programs). However, fewer providers offer due diligence on TPSPs. Consequently, many financial firms likely turn to a compliance consultant or attorney to provide such services.

From a practical standpoint, outsourcing due diligence can be costly. It can also be a more complex process than internal investigations. It is often difficult to assess the quality of due diligence performed by an external source and to evaluate whether the external source "got it right." Furthermore, the work required is highly dependent on the nature of the services provided. For example, information technology (IT) consultants, fund accountants, and custodians are critical service providers; the services they offer are complex, requiring a significant amount of effort by a firm to perform due diligence. On the other hand, due diligence of other TPSPs, such as a compliance consultant or attorney, will focus on different areas and may not be as complex to perform. Later, this chapter explores how due diligence checklists and questionnaires can direct inquiries to relevant areas pertaining to that particular TPSP.

For these and other reasons, firms often opt to perform their own due diligence on third-party service providers. It is imperative to understand that performing due diligence is complex and requires skill. Firms that handle the due diligence internally must have personnel with the requisite knowledge and skill to perform effective reviews. Such staff needs to know what documents to request, what questions to ask, and how to detect potential problems. Performing effective due diligence requires recognition skills. Issues must be vetted and identified as potential red flags requiring follow-up. Firms that have less experienced staff may need to invest in training staff members who will perform due diligence. Although due diligence is addressed at industry conferences, most often these skills are acquired through experience. Therefore, it is essential to have a knowledgeable, experienced professional oversee the process.

Table 1 compares the major advantages and disadvantages of the two paths due diligence may take.

TABLE 1. ADVANTAGES AND DISADVANTAGES OF THE TWO AVENUES FOR TPSP DUE DILIGENCE

	Advantages	Disadvantages
Internal	Lower cost and more control	Firm may not have expertise or experience
External	Convenient and generally performed by knowledgeable and experienced individuals	High cost and quality of the review may be difficult to independently assess

SOC Reports. In many cases when performing due diligence, a firm will receive and rely upon externally derived reviews such as service organization control (SOC) reports. A service auditor develops a SOC report to report on the controls at an organization that provides services to and is relied upon by other user entities. For the financial industry, the most commonly seen is the Statement on Standards for Attestation Engagements No. 16(SSAE 16) report as required under the American Institute of Certified Public Accountants (AICPA) for practitioners at service organizations.[19]

Some due diligence officers rely heavily on SOC reports, almost treating them as external due diligence reviews. SOC reports can be extremely helpful in providing valuable insight into the TPSP's controls, but like most tools, there are certain limitations as to what the report covers. For example, the SOC report is based on accounting standards that measure the financial controls at an organization. For SSAE 16, there are two types of SOC reports: Type 1 (SOC 1) and Type 2 (SOC 2). In a SOC 1 engagement the auditor reviews the controls in the subject organization as of a particular date, and thus is a snapshot of the control environment. In a SOC 2 engagement the auditor examines how the controls were designed, implemented, and managed over a period of time (typically six months.) Auditors performing a SSAE 16 engagement must examine the financial, operational, and compliance controls using the five Trust Services Principles and Criteria, which include:

- *Privacy:* examination of the collection, use, retention, disclosure, and disposal of personal information;
- *Availability:* examination of controls to ensure the subject is available for operation and use as agreed or committed to customers;
- *Processing integrity:* examination of whether system processing is complete, accurate, timely, and authorized;
- *Confidentiality:* examination of whether information designated as confidential is protected; and
- *Security:* examination of whether the system is protected against unauthorized access, use, or modification.[20]

SOC reports vary greatly in length.[21] A typical report is technical and not easy for a layperson to understand. When a firm reviews a SOC report, it is important to focus on the independent service auditor's report and any assertions made by the company. If the auditor's opinion is qualified, the TPSP could prove to be a nonstarter.

Although a SOC report provides useful information for conducting due diligence, it may not be all-encompassing, particularly for the unique services that a TPSP could provide for the organization. Therefore, thoughtful consideration must be made as to

[19] SSAE 16 is the accounting standard that became effective in June 2011 and superseded the Statement on Auditing Standards 70 (SAS 70).

[20] The Security principle was updated in 2014 to reflect today's greater awareness of cybersecurity and includes seven categories of review: organization and management, communications, risk management and design and implementation of controls, monitoring of controls, logical and physical access controls, system operations, and change management.

[21] A typical size SOC report is 100 pages.

what the next steps should be in the assessment. Because SSAE 16 reports are costly, only the larger TPSP will likely be able to provide them.

Using Checklists and Questionnaires

As with so many areas within a compliance program, checklists provide a valuable tool in standardizing what information the firm should collect and consider in assessing any TPSP. A due diligence checklist is designed for use by the due diligence officer for overseeing what areas must be reviewed. On the other hand, a due diligence questionnaire (DDQ) is designed to be sent to the subject company for a response to a request for information. Both serve separate and distinct, yet complementary purposes.

Typical types of information sought during a due diligence review include the following:

- Background information on the service provider;
- Services provided;
- Qualifications of the firm and firm personnel;
- Recent changes at the firm;
- Disclosure of litigation, regulatory inquiries, or customer complaints;
- Disclosure of material conflicts of interest;
- References;
- Privacy policy;
- Data security policy;
- Business continuity plan;
- Information relevant to applicable regulatory requirements (e.g., requisite licensing);
- Proof of insurance;
- Financial records;
- Sample contract; and
- SOC reports.

Figure 4 at the end of this chapter provides a sample due diligence checklist.

In some instances, the TPSP may have updates to these topics completed in a due diligence report that the provider will automatically forward to the user firm. In other instances, the user firm must create its own DDQ to seek these responses. A due diligence officer should periodically review the DDQ to update records based on changes in regulation, servicing needs, and risk profiling of the TPSP.

Onsite Evaluations

Purely documentary reviews have their limitations, so a comprehensive review will include an onsite visit. The qualitative information obtained during an onsite interview can be a valuable complement to the quantitative information gleaned from a documentary review. For example, consider *Moneyball: The Art of Winning an Unfair Game,* a novel by Michael Lewis.[22] This story was based on Billy Beane, the general manager of the

[22] In 2011, this real-life story was made into a movie featuring Brad Pitt, Jonah Hill, and Philip Seymour Hoffman.

Oakland Athletics, who for a time revolutionized baseball scouting by relying solely on statistics (such as on-base percentage) to evaluate players. Traditional scouting combined both statistical (quantitative) analyses and an experienced scout's subjective evaluation of seeing the player in action (qualitative) to evaluate the talent. Billy Beane's contribution to baseball undeniably proved the worth of quantitative analytics, but most successful teams still augment their scouting with qualitative judgments from scouts. Likewise, with vendor due diligence, an onsite visit can provide valuable insights that augment the evaluation of a vendor and the responses the TPSP provides on paper.

Five primary objectives for the onsite visit enable the due diligence officer to:

- Observe business operations;
- Validate information provided;
- Review documents and systems;
- Develop relationships; and
- Detect red flags.

Although an officer may not be able to assess the quality of the services provided by the vendor until the TPSP is engaged, he or she can discern a lot by observing how the provider works with other clients. What is the environment of the workplace? Is it organized? Do employees seem engaged, enthusiastic, and knowledgeable? Does the vendor have well-thought out responses on how it would service the firm's needs and handle any issues that might arise?

Importantly, an onsite visit provides an opportunity to validate information provided. Does the documentation align with the due diligence officers' understanding of the vendor's business practices? Are key employees able to articulate more than a sales pitch? Do their responses give the officers confidence in the services the TPSP will be providing? How much experience and expertise does the firm have in handling clients similar to this firm?

In some instances, the vendor may be unwilling to share certain information in response to a due diligence questionnaire but will allow visitors to review such information onsite. In other instances, IT and other systems would require demonstrations, which are best viewed while onsite.

Developing a good working relationship with critical service providers is important. In most cases, firms have few opportunities to meet face-to-face with their TPSP; and telephone calls and emails are no substitute for direct human interaction in developing good working relationships. Understanding the firm, its needs, and the people that the TPSP will interact with will help establish a strong foundation for good service by that vendor.

As indicated earlier, performing due diligence is complex. Specifically, it requires a set of skills—one of which is the ability to spot potential red flags. It is the due diligence officers' job to probe, dig deep, and get the requisite information to make a determination of the match of the firm with the TPSP. Some skills in detecting red flags are familiarity with the types of issues that may be encountered and open-mindedness to

issues that may be atypical. For example, customer service may be a high priority for a clearing firm or custodian. What are the TSPS's response times? What is the ratio of customer service agents to clients? Some red flags can be detected from documentary reviews, but others only become apparent at the provider's site. The officers should know the difference and during the onsite visit focus on those that can only be detected onsite, such as observations of workflow issues or vague/evasive responses to pointed questions.

Key to a good outcome for the onsite review is proper preparation. The due diligence officers should have performed a thorough documentary review so they have a good understanding of the service provider and can ask intelligent, probing questions. Moreover, the documentary review may reveal clues about potential red flags, for example, ones signaled by vague responses in a DDQ. The due diligence officers should arrive onsite prepared with an agenda and a list of questions. They should interview key personnel independently, if possible. Independent interviews may uncover contradictions or additional information that may not come out in a group interview.

Onsite visits are time-consuming and costly, so they are typically reserved for critical service providers such as clearing firms and custodians. However, when performed skillfully, onsite reviews are an invaluable component of a comprehensive due diligence review.

III. COMMON CHALLENGES FOR EVALUATING SERVICE PROVIDERS

Risk Profile for the TPSP

Each TPSP should be assigned a risk level for monitoring purposes. The factors considered when officers assign a risk level to a TPSP will vary, but the significance of the risk level should be commensurate with each service provider's applicable overall risks and conflicts. For example, all else being equal, a subadviser that has regulatory disciplinary history should be assigned a higher risk level than a subadviser that doesn't have disciplinary history. The example provided here is simple to understand, but in other cases, evaluation and acceptance of risk varies greatly dependent upon facts and circumstances and therefore requires careful analysis and consideration.

How to Begin Risk Profiling. Risk profiling should begin at the enterprise level of the TPSP and take into consideration the following areas:

- Financial risk;
- Operational and resource risk;
- Key personnel turnover risk;
- Privacy/information security risk;
- Legal/compliance risk;
- Business continuity/succession plan risk; and
- Affiliate risk.

Next, officers should consider whether the services performed by the TPSP are critical to the firm and providing services to clients (dubbed the critical provider risk). The officers consider whether the TPSP has direct contact/relationship with the firm's clients, such as a custodian, subadviser, solicitor, or associated broker-dealer. Then the profilers consider whether any TPSP is providing more than one type of service to the firm and/or the firm's clients. For example, an investment adviser that uses a custodian with a broker-dealer affiliate that provides trade execution for the adviser's clients would be a more "critical" service provider due to the multiple services provided.

Thereafter, the profilers consider the services provided (service risk), looking at the strengths and weaknesses attributable to that service provider in performing the services. Profilers ask:

- Does the service provider have extensive expertise in providing the services?
- What is the level of customer satisfaction achieved?
- Is the service one that is currently under regulatory scrutiny (e.g., independence of third-party auditors)?

The final step is identifying conflicts of interest that are specific to each service provider and the services they provide (conflict risk), which is discussed in detail later in this chapter.

For each of these areas, the profilers assign a risk level (such as high, medium, and low). The risk level assigned to each factor in many cases could be subjective and within a firm's discretion of its risk appetite. The profile should document the analysis, and determine the probability or likelihood of whether any of the identified risks will occur and the damaging effects it would have if not handled properly.

Conflicts Surrounding Use of Service Providers

Outsourcing services to a TPSP is very common in the financial services industry, and in some cases, is mandatory in order to adhere to applicable federal and/or state regulations.[23] However, whether a provider is required or not, certain material conflict areas need to be considered and addressed as part of a firm's service provider evaluation process. This discussion describes some higher risk areas, with examples of conflicts for each.

Compensation Flow/Revenue Sharing. Compensation arrangements tied to services can often lead to finding conflicts. One common example is when a firm uses an affiliated service provider, wherein the owner(s) of both companies are the same or under common control. This arrangement creates a conflict of interest because the owner(s) receive a benefit when the affiliated firm receives the service fee. Another example is an advisory firm using a broker-dealer to execute client transactions and certain employees of the advisory firm also serve as registered representatives of

[23] For example, Rule 206(4)-2 under the Advisers Act requires investment advisers that are considered to have custody (other than for fee debiting authority) to obtain annual surprise audits from an independent accounting firm.

the broker-dealer who receive transaction and/or trailing commissions (e.g., 12b-1 fees) based on those transactions. As further discussed later, such conflicts necessitate action steps by the financial institution to disclose and mitigate or eliminate the conflict.

Direct and Indirect Benefits. A conflict also presents itself when the firm hiring the TPSP receives direct or indirect benefits as a result of the service provider arrangement. This comes into play, for example, when smaller advisory firms enter into arrangements with certain custodian/brokers to provide custody and trading services to its clients (e.g., Charles Schwab, Fidelity, Pershing, or TD Ameritrade). Under these bundled arrangements, in addition to the services and benefits received by the firm's clients, the firm also receives benefits and services, but at no additional cost. These services and benefits generally include access to client data via an online portfolio accounting system, a dedicated trading desk, access to real time market data, investment research, recordkeeping services, facilitation of the payment of advisory fees, and other business and management support. Although these arrangements are permissible, advisers must address the applicable conflicts.

Relationships with Key Personnel. Nepotism is not necessarily a bad thing, but it is a conflict that must be identified and addressed when a firm hires a family member as a TPSP directly or engages a company that employs a family member as a service provider. The term "family member" should be applied in a very broad sense and not only include immediate blood relatives, but also certain nonrelated persons, including but not limited to long-term friends, adult children of close friends or clients, and domestic partners. This approach was driven home in two 2016 SEC enforcement actions.[24] London-based public accounting firm Ernst & Young (E&Y), along with a senior partner and an auditor, agreed to pay approximately $9.3 million in settlement charges. SEC investigations determined that there had been violations of auditor independence rules due to undisclosed close personal relationships between the E&Y auditors and personnel at the E&Y clients being audited.

Affiliations. Compensation arrangements, and use of firm affiliates and/or close family members as TPSPs present inherent conflicts. Moreover, conflicts also may exist with certain TPSP affiliations (such as ownership affiliations as well as strategic partnerships within the financial industry) that should be reviewed and disclosed. An example of such a strategic partnership would be a situation in which an advisory firm enters into a solicitation arrangement with an individual who is employed at an unaffiliated investment advisory firm or a broker-dealer.

When a firm handles conflicts, the best practice is to eliminate the conflict. However, in some cases, elimination only switches one conflict for another. For example, hiring an unaffiliated service provider would eliminate the compensation conflict that arises

---

[24] *In the Matter of Ernst & Young LLP and Gregory S. Bednar, CPA,* Rel. No. 3802 & 78872 (Sept. 19, 2016) and *In the Matter of Ernst & Young LLP and Robert J. Brehl, CPA, Pamela J. Hartford, CPA, and Michael T. Kamienski, CPA,* Rel. No. 3803 & 788783 (Sept. 19, 2016).

from hiring an affiliated service provider, but if the unaffiliated service provider were owned by the son of the firm's largest client, there would still be a relationship conflict that would need to be addressed.

Numerous mitigation steps can be taken; many revolve around the type and materiality of each conflict. Although there are too many to list in this chapter, some core mitigation steps can be applied to all service provider conflicts:

1. Provide clients with detailed disclosures in relevant documents (e.g., client agreements, marketing collateral, Forms ADV, and offering documents) that include information outlining the conflict(s), along with a summary of how the firm addresses the conflict(s).
2. Maintain documentation outlining the reason(s) why elimination of the conflict was not a viable solution (i.e., why it was believed to *not* be in the best interest of clients).
3. Assign a higher risk level to service providers that have one or more material conflicts.
4. Implement heightened oversight (e.g., more frequent reviews) for service providers with higher risk levels.
5. Implement conflict of interest policies and procedures, identifying material conflicts and how the firm addresses the conflicts.

Contract Language Considerations

Each service provider arrangement should be memorialized in a written contract and include, at a minimum, an outline of the services being provided and the role of each party. Importantly, a contract is a legal document that should be drafted and/or reviewed by legal counsel that is well versed in federal and state securities laws. Even so, there are a few topics that should be considered for inclusion in a contract with a service provider that may not be standard in all contracts. These include:

- Disclosure of applicable conflicts of interest and how addressed;
- Authorization of performing periodic due diligence reviews and access to relevant records;
- Requirement for notification of material changes to firm and key personnel;
- Limits on authority to act on behalf of firm and marketing activities for the firm;
- Outline of books and records to be maintained (including time period and method of retention);
- Certifications of compliance/legal/financial viability;
- Confirmation of E&O insurance;
- Required disclosures to be provided to ERISA clients under ERISA Rule 408(b)(2);
- Cybersecurity and safeguarding controls (if the TPSP will be receiving or transmitting data related to a client account);
- Responsibility and limitation regarding sub-contractors used by service provider; and
- Return of records upon termination of relationship and destruction of confidential information in the TPSP's possession.

Service Provider's Industry Experience

Engaging an experienced and knowledgeable TPSP is critical. This is especially true when a financial institution is required by regulation to hire a TPSP. Such is the case when an investment adviser must have annual surprise audits performed by an accounting firm because it has custody of client assets. The challenge, of course, is finding a service provider that has the necessary depth of experience in the specialized area needed.

There is a never-ending list of TPSPs in the financial industry. In fact, there are a number of TPSPs that specialize in niche areas. Given this fact, where does one start when there are a plethora of service providers to choose from?

The following resources are helpful consider for gathering information about the service provider's experience:

- *Industry referrals:* ask the TPSP for a list of clients to contact;
- *Internet searches:* Google the name of the service provider to see what shows up;
- *Website review:* review the TPSP's website to gather information on firm history;
- *Referral services:* research service provider referral services for a list of applicable TPSPs to consider;
- *Staff interviews:* talk with service provider staff members that perform the specific services and also determine employee turnover rate; and
- *Industry networks:* check with industry peers to obtain recommendations.

IV. HOW TO STRUCTURE A DUE DILIGENCE PROGRAM

What to Review

During the due diligence process, a variety of documents and information will need to be gathered from each TPSP. Initially, requests should be made covering core areas, such as:

- Corporate structure and company history;
- Affiliates;
- Products and services;
- Operational structure;
- Financials and corporate accounting;
- Insurance coverage;
- Key employees (new and terminated); and
- Legal and compliance (including regulatory exams, as applicable).

Next, the information requested should focus on the type of TPSP and the specific services that will be used by the firm. Following are some examples (this list is not all-inclusive):

- Custodians (custody of client assets)
  - Classification and holding of client assets,
  - Use of subcustodians,
  - Process for securing safety of assets,
  - Securities lending practices,
  - Settlement processes, and
  - Reporting on account holdings and transactions;
- Accounting firms (annual financial audits and surprise exams)
  - Status of registration with the Public Company Accounting Oversight Board (PCAOB),
  - Process for monitoring adherence to auditor independence requirements,
  - Types of clients, and
  - Experience in performing acquired services;
- Subadvisers (investment management services)
  - Regulatory registration status,
  - Compliance program structure,
  - Biographies of investment personnel,
  - Firm/strategy performance,
  - Other services offered,
  - Brokerage practices,
  - Proxy voting practices, and
  - Service providers used;
- Solicitors (client/investor referrals)
  - Industry licenses and state registration status,
  - Process for finding potential clients,
  - Employment history, and
  - Other solicitation arrangements;
- Broker-dealers (brokerage and trade execution services)
  - Regulatory registration and FINRA membership status,
  - Compliance program structure,
  - Other services offered,
  - Securities investor protection corporation (SIPC) coverage,
  - Best execution assessments, and
  - Market making practices.

It's also extremely important to determine and review the procedures and controls each TPSP has in place covering:

- Risk and conflict identification and management;
- Confidentiality and safeguarding of nonpublic information (including identity theft);
- Cybersecurity;
- Anti-money laundering;
- Business continuity; and
- Prevention of violations of applicable regulatory and/or firm requirements.

Gathering and reviewing certain information regarding competitors also should be included in the process, during both initial and subsequent reviews.

How to Conduct a Due Diligence Review

The method for gathering the information can vary, but the most common ways include:

- Performing onsite visits;
- Interviewing key personnel (in person and via teleconferences);
- Using questionnaires (both internal and external);
- Reviewing websites, social media, blogs;
- Perform internet searches;
- Requesting copies of various documents; and
- Obtaining industry/client reference letters.

A due diligence process should begin by ranking each TPSP by risk and conflict level, and the same approach can be used when reviewing all the information and documentation gathered. In other words, commence with reviewing the materials covering the highest risk and conflicts areas for the service provider ranked with the highest risk level.

Also, when gathering information from a TPSP, the reviewer(s) should verify the accuracy of verbal assertions made. The reviewer shouldn't be reluctant to ask pointed questions when interviewing senior managers and always ask for clarification when needed. The reviewer should consider the reliability of the source of information, especially when it appears too good to be true or when it's from an unknown third party.

Once the review process is over, the reviewer(s) should have a clear understanding of the TPSP's business practices, along with risk and mitigation controls, and be able to make an informed recommendation to senior management on whether to continue using the service provider.

Who Should Perform the Review. A strong due diligence program takes time and effort, and requires involvement from more than just the firm's compliance personnel. A number of factors are considered when the reviewer makes a determination, including:

- The size of the firm;
- The number of service providers used;
- The person(s) or department managing the arrangements; and
- The frequency of reviews needed.

Larger firms should opt for having a due diligence committee in charge of performing reviews. For smaller firms, it's usually best to have the reviewer(s) be the personnel responsible for managing the TPSP relationship, with oversight by the firm's chief compliance officer (CCO) or equivalent.

When a reviewer assigns responsibility, the roles, required steps, and expectations should be clearly outlined. A committee can accomplish this by having a written charter that provides the framework for the reviews. Individual reviewers can develop standard operating desktop procedures and review them periodically with senior management.

Frequency of Reviews. Once the compliance professional performs an initial due diligence review, the frequency of subsequent reviews should not be a "one size fits all" approach. It's always a good rule of thumb to perform formal due diligence reviews on an annual basis, but a firm should have a review process in place that appropriately corresponds with each TPSP. Timing depends on a number of factors that will affect the frequency of reviews. These factors include, but are not limited to:

- The risk level assigned to the service provider during the initial or most recent due diligence;
- The extent of identified conflicts surrounding the relationship;
- Amount of client facing involvement;
- Changes to regulations affecting the service provider or the firm;
- The type of service/product being provided;
- The terms of the contract;
- Changes to the firm's business and/or services being provided; and
- Legal and/or disciplinary history.

The service providers with high risk levels, material conflicts, and historical legal and/or disciplinary events should be reviewed more frequently and before those with a lower risk level (as was discussed for assigning risk profiles for service providers).

There also are certain factors that may mandate an ad hoc review, such as:

- Departure of key employee(s);
- Regulatory action;
- Widespread disaster (e.g., earthquake, hurricane); and
- Cybercrime.

Depending on the issue warranting the impromptu review, the reviewer may want to consider whether a surprise onsite visit is justified.

Notably, a firm's risk ranking for service providers will most likely change over time, which may prompt a change to the frequency of reviews. For example, a core TPSP was recently the subject of a regulatory proceeding for law violations directly resulting from a lack of adequate procedures and controls. In this scenario, the service provider should be ranked as "high risk" and an ad hoc review performed to determine the steps the TPSP is taking to correct the violation and ensure the same (or similar) violation does not happen again. Also, because this is a core TPSP some form of due diligence (e.g., questionnaires or telephone interviews with senior management) should be performed periodically in between and in addition to an annual review. This will enable the reviewer

to confirm that updated controls and procedures are being followed and that no other violation has occurred. Then, after a couple of years if the service provider has shown that the additional procedures and controls are adequate and appear to be effectively preventing another violation, the risk level can be lowered to "medium" and less frequent reviews performed, unless other high-risk factors are associated with the service provider.

The person(s) performing due diligence reviews should implement an ongoing monitoring process. This not only helps determine when routine reviews are necessary but also helps track events that trigger unscheduled reviews.

Developing a Standardized Flow and Monitoring System

In developing an ongoing monitoring program, the best place to start is with a list of all current TPSPs used by the firm, listing the name and type of service provider, the date of the service contract, a brief summary of the services provided, and—last but not least—the assigned risk level. From there, the reviewer should set up electronic files for maintaining all documents, correspondence, and reports. This can be done by using data-storing software or by creating files on the firm's network system. Whichever method is used, it is imperative that security measures be implemented to help preserve the integrity of the information and to limit the sharing to only personnel required or allowed to have access. Also, the data should be segregated by TPSP and stored in a manner that enables easy retrieval of specific documents. When it comes to data storage, organization is key.

A systematic process for reviews is the next essential step. Wherever possible, the reviewer should automate reminders. For example, smaller firms can set up a due diligence calendar using Microsoft Outlook or equivalent program, which allows for electronic tracking of both past and future due diligence activity and will provide automated alerts on upcoming reviews for to enable due diligence team members to adequately prepare. For large firms with numinous service providers, software is available that has a multitude of capabilities, including but not limited to notification of upcoming reviews, the provision of due diligence reports, and retention of data.

Importantly, as noted above, service providers with high risk levels should be scheduled for more frequent reviews.

Lastly, a tracking system that captures the firm's completed due diligence reviews should be put into place. This system should capture the following information:

- The date each review was performed;
- The type of reviews performed (e.g., initial, quarterly, annual onsite, etc.);
- The method of each review (e.g., questionnaire, internet search, third-party provider, telephonic Q&A, or offsite versus onsite);
- The date and type of report provided to senior management; and
- The location of documents and data collected related to the review.

Although there are a few choices on how best to structure a tracking system, using technology will create many efficiencies (including time and money), particularly if the firm has a large number of service providers. This a technologic approach enables the firm to most easily run specific reports based on the information maintained in the software, which can further help to identify gaps or potential areas of concern that require follow-up.

Perform Periodic Assessments of Your Due Diligence Program

Due diligence programs should be dynamic and evaluated from time to time to evaluate their effectiveness. Firms need to ensure that they are asking the right questions, assessing high-risk areas and gathering meaningful data in order to ascertain the strength of a service provider. When a reviewer performs this assessment, he or she should consider the following:

- Is the current due diligence process efficiently generating appropriate and timely responses from service providers?
- Are reviews being performed in accordance with firm written policies and procedures?
- Does it appear that information related to risk and conflicts of interest is being effectively solicited and obtained from service providers?
- Are reviewers spending sufficient time on each review?
- Are the correct employees performing the reviews?
- Does the report and documentation maintained reflect the full process? A due diligence report should include
  - The amount of time spent to conduct the due diligence review,
  - A description/summary of what was reviewed,
  - The identity of the reviewer(s),
  - Whether any additional requests for information were made, and
  - The findings and recommendations from the due diligence team.

Firms also should consider having an evaluation of their due diligence program performed by a third party from time to time, because this assists senior management in confirming whether the program aligns with the firm's needs and is structured effectively.

Employee Training

The first consideration is who should be trained and how frequently. Depending on the size of the organization and the sharing of responsibilities for gathering and assessing due diligence information, it could be prudent to provide general training to all employees. For those employees intimately involved in the due diligence process, more frequent training is required to review overall firm protocols, regulatory requirements (as applicable), and detection of red flags.

Training can be delivered using a variety of methods. Webinars from reputable providers, desktop training (using case examples), classroom instruction, and one-on-one mentoring are just a few commonly used methods. To document that such training occurred, the trainer should use and maintain a sign-in sheet and agenda to help demonstrate what was discussed and when. This will be particularly helpful during a regulatory examination.

The trick to good training is to engage the audience. This can be accomplished in a few different ways. A first consideration is using a roundtable type setting so attendees can ask questions at any time. Next, real life examples help to "personalize" the experience. The trainer can conduct an advance survey for attendees about the firm's current due diligence practices by using a survey system. Having a survey's results may help to inspire a more dynamic discussion. In turn, results also may alert the trainer to any potential gaps to address real-time during the training.

V. BEST PRACTICES FOR DOCUMENTING A DUE DILIGENCE REVIEW

Information to Capture

There is a saying in compliance: "If you didn't document it, it didn't happen," which stresses the importance of documenting reviews; and this certainly applies to due diligence of service providers.

When formulating a typical computer folder structure, the reviewer may use the sample in Figure 1.

FIGURE 1. SAMPLE FOLDER STRUCTURE

<Compliance>
<Due Diligence>
<Product Due Diligence>
<Investment Manager Due Diligence>
<Service Provider Due Diligence>
<Name1>
<Name1 2016 Due Diligence Review>
<Name1 2017 Due Diligence Review>
<Name2>
<Name2 2017 Due Diligence Review>

Within this folder configuration, there should be certain subfolders. For example, within the 2017 Due Diligence Review folder, a best practice is to include the following types of data and information:

- Due diligence questionnaire;
- Due diligence report (summarizing the review and results);
- Completed due diligence checklist;
- Service Organization Control (SOC) report;
- Policies and procedures manual;
- Business continuity and cybersecurity plan(s);
- Marketing collateral;
- Website screenshots;
- Internet search screenshots;
- Internal notes from discussions and interviews; and
- Reports and other collateral provided by the TPSP.

A sample due diligence checklist is given later in this chapter; it provides the structure for the review and ensures that reviews are comprehensive and consistent. The other items, with the exception of the due diligence report, are incorporated into the checklist as the procedure for performing due diligence. Finally, the report written by the due diligence officer will highlight any findings, make a recommendation, and provide the rationale for the recommendation. The reports are often relatively brief: one page or less.

Two factors differentiate a thorough due diligence effort: a well-annotated checklist and copious notes from discussions and interviews. Notes can also be appended to Adobe Acrobat files such as SOC reports or internet search results. These notes all demonstrate that the documents were reviewed and not just collected and filed.

Identifying Red Flags

The ability to identify red flags is a critical skill for due diligence best practices. Because red flags come in all shapes and sizes, recognition can be challenging. To make this point, here are some examples.

Example 1: Damaged Reputation. Alan Thackery is performing due diligence on Shareset, a file-sharing vendor under consideration for his firm's client portal. The due diligence seems to be going well when Alan discovers that an internet search reveals Shareset changed names recently. Drilling down in the search pages he discovers the firm has suffered a recent catastrophic failure that resulted in several client lawsuits. The name change was to mitigate reputational damage from the incident. Had Alan not conducted this type of search, this red flag could have been undetected.

Example 2: Omitted Contract Term. As part of an initial due diligence review of a CRM vendor, Marie Padella reviews the contract. Per her due diligence checklist, the two key provisions are the confidentiality and data ownership provisions. The contract

is silent with regard to data ownership. This is an invisible red flag; most omissions are not apparent and can be very difficult to detect. Some firms have lost all of their CRM data when changing vendors because of data ownership issues. Thus, for Marie the data ownership clause is a critical part of the due diligence review for this vendor.

Example 3: Decreased Customer Service. Pete Labuda's firm has been using the same order management system, SalesTracker, for the past several years. As part of his ongoing due diligence, Pete reviews the vendor's sales literature and skims the biographies of "Our Team." He notices many new team members and is curious about the level of service SalesTracker is providing. When Pete interviews his firm's traders, he discovers that they believe SalesTracker's customer service has dramatically declined. This is a red flag that requires further investigation in order for Pete to determine whether to continue using this TPSP.

These illustrations are just a sampling of the breadth of issues a due diligence officer may encounter in performing due diligence. Spotting red flags is a recognition skill and, like most skills, it is generally developed through experience. If the firm does not have someone experienced in performing due diligence, the officer should consider external resources that can offer mentoring and other assistance, such as attorneys and compliance consultants.

Developing Firm Protocols for Initial and Ongoing Due Diligence

Due diligence is an important duty of financial institutions, which should be addressed in the firm's policies and procedures manual. Figure 2 offers a template for developing protocols.

FIGURE 2. SAMPLE DUE DILIGENCE POLICY

[Firm name] uses unaffiliated TPSPs to assist it in providing certain services to the firm for the servicing of our clients. Upon entering into agreements with such TPSPs, [firm name] will oversee that these TPSPs are completing those services for which they are contracted. Failure by the TPSPs to meet their obligations could not only subject [firm name] to a situation wherein we are not fulfilling our obligations, but moreover, could subject our clients to unnecessary risks associated with the inadequate or failed completion of the contracted services.

In conducting due diligence and evaluating the soundness of a TPSP, [firm name] considers the material risks associated with its reliance on those services provided by the TPSP. The firm will analyze and consider, among other things, the following:

- The TPSP's ability to adequately meet their contractual servicing obligations;
- Any material changes to the TPSP's business or services;
- The continued satisfaction of our team with the TPSP's product or services (including response times and communications); and
- Overall specific performance.

Figure 3. shows a sample procedure useful for the first-time and continued evaluation.

FIGURE 3. SAMPLE EVALUATION PROCEDURE

[Firm name] will conduct due diligence of our TPSPs and oversee those services outsourced to the TPSP, particularly for those which assist in the furnishing of advisory services to our clients.

[Firm name] will evaluate such TPSPs by conducting the following.

Initial Due Diligence

- Request the TPSP to complete [firm name's] Due Diligence Checklist [Questionnaire]; the firm will thereafter evaluate the responses and consider the TPSP's proposed services and any risks posed by outsourcing services to the vendor.
- [Firm name] will determine the exact services to be provided by the TPSP and will ensure that clear descriptions of these services appear in the TPSP's contract.
- Designated [firm name] employees to write a report summarizing the due diligence review, which will include a recommendation about whether or not the TPSP appears to meet XYZ's due diligence standards. The firm will include any recommendation for the frequency of ongoing due diligence to be performed on the TPSP based on its risk profile.

Ongoing Due Diligence

- Employees that use the TPSP's product or service should be kept apprised of the required components of the service and [firm name's] expectations of the service. Should the TPSP not meet this servicing standard, employees should escalate this information to the designated person overseeing the vendor relationship.
- The designated person overseeing the TPSP is responsible for working with the due diligence team to pinpoint areas requiring review. Should the designated person learn of an issue with the TPSP, that person should report the issue to the [designee].
- [Firm name] should conduct due diligence on all TPSP on a systematic basis utilizing the firm's due diligence checklist [questionnaire]. The frequency of the review will be determined at the inception of the relationship (based on the TPSP's risk profile), which shall be reviewed no less than annually.
- To evidence our due diligence efforts, [firm name] will author and maintain a written report summarizing the type of due diligence review conducted and include any recommendation(s) in terms of further reviews or investigations needed and whether the firm should or should not use the services of the vendor.

Depending on the type of TPSP and their risk profile, due diligence can be very time-consuming. Therefore, it is important to develop a protocol for determining how often each vendor should be reviewed, and the methodology to use for such review (e.g., through reports, onsite visits, telephonic interviews, or all three). Consequently, the due diligence officer should develop a due diligence calendar to ensure that critical TPSPs are being reviewed as needed.

VI DUE DILIGENCE QUESTIONNAIRES

One of the primary ways to capture and maintain pertinent information concerning TPSPs is through the use of DDQs. They bring efficiency to the due diligence process by standardizing the diligence questions posed to TPSPs most frequently. They questionnaires also give insight into the specific TPSP's services, risk processes, management, and performance. With it, an adviser can better determine whether a particular TPSP can effectively support the adviser's business activities.

Considerations for Drafting Due Diligence Questionnaires

An adviser must recognize and take into consideration applicable securities laws and its responsibilities under those laws when creating its standard DDQ template. The DDQ should be sufficiently customized and detailed to cover areas related to the TPSP's services and operations that may create risks, conflicts, or other effects on the firm's business.

Understand the Role of the TPSP. Prior to drafting a DDQ, the adviser should understand the role the TPSP will (or does) occupy on behalf of the adviser. For instance, if using the services of a subadviser to manage some or all of an adviser's assets, the adviser should carefully evaluate the TPSP's performance, adherence to guidelines and its portfolio model, reputation, management team, business continuity plan, succession plan, compliance program, and marketing, to just name a few.

Identify Risks. The types of risks inherent to a given TPSP differ greatly depending upon the services provided. For instance, when dealing with TPSPs that have access to nonpublic client information, the firm will want to ensure the TPSP has taken measures to safeguard such information. In furtherance of this, as part of the DDQ, advisory firms will want the TPSP to provide responses to such questions as:

- What personnel of the TPSP will have access to the client information?
- What types of safeguards are currently in place to protect client information?
- Does the TPSP employ a cybersecurity program, and if so, what does it entail?
- What, if any, breaches have occurred in the past that resulted in client information being shared?

Some additional risks may include: geographic location, industry experience, background of TPSP owners, the TPSP's lack of internal policies and procedures, type of

reports/documentations/services provided, and compensation structure. The DDQ should ask questions that address these risks and the steps taken by the TPSP to address such risks.

Ongoing Reviews. Typically, the information collected in response to a DDQ represents a snapshot of the activities of a TPSP at a certain point in time and is current only as of the date the DDQ is completed. No due diligence program is perfect. Each due diligence process undertaken for a potential or active TPSP will reveal strengths and weaknesses of the due diligence program. That discovery is why it is important for advisers to continuously monitor TPSPs to ensure they are sufficiently performing the services for which they were contracted, and that no new risks to the advisers have become evident since the prior DDQ. This ongoing review is expected by regulators[25] and is an important piece of the due diligence program.

Reviewing DDQ Responses

As mentioned above, DDQs are designed to provide a basis for advisers to commence their due diligence reviews of TPSPs, but are neither designed to be an exhaustive list of questions that may be relevant to a given TPSP, nor the sole tool used in performing due diligence. Once the DDQ has been created and customized to fit the services provided by a given TPSP, an advisory firm must effectively distribute and review responses to the DDQ. This can be a robust process that entails multiple facets beyond simple delivery and receipt of the DDQ. It is recommended that firms design internal policies and procedures (or "standard operating procedures) governing such activities. For example, consider the following review processes.

Designating a Point Person. The due diligence officer should designate a single point of contact or a small dedicated group to oversee the distribution, collection and review of DDQs. Channeling information can often simplify the process. Having someone familiar with such aspects as the timing, plus the manner and means of delivering a DDQ can reduce inefficiencies. Additionally, having a single point of contact also promotes consistent recordkeeping practices and establishes a liaison for TPSPs to contact should they have any questions when completing the DDQ.

Trust But Verify. This should be the mantra for any compliance program, but it is especially true for firms when conducting due diligence on any TPSP. DDQs are a great way to gather lots of information about a TPSP in an expeditious fashion. However, simply relying upon the answers to the DDQ itself is not always sufficient. Firms need to take additional steps to be sure that the information provided by the TPSP in the DDQ is accurate and verifiable. Such sentiments were articulated by Andrew J.

[25] As discussed as part of FINRA Regulatory Notice 11-14, a firm's supervisory procedures should include "an ongoing due diligence analysis of each current or prospective third-party service provider to determine, at a minimum, whether: (1) the third-party service provider is capable of performing the activities being outsourced; and (2) with respect to any activities being outsourced, the member firm can achieve compliance with applicable securities laws and regulations and applicable FINRA and MSRB rules."

Ceresney, former director of the SEC's Enforcement Division, when he stated, "When an investment adviser echoes another firm's…claims…, it must verify the information first rather than merely accept it as fact." [26] With this in mind, firms should be proactive and wherever possible, investigate whether the responses provided by the TPSP in a DDQ are truly accurate.

Onsite Due Diligence. Going hand-in-hand with the "trust but verify" mantra is the recommendation to perform onsite due diligence of TPSPs when possible. The purpose of onsite due diligence, described previously, is to verify and cross-check the information that has been collected and analyzed as part of the DDQ and other means. Additionally, this personal interaction gives the firm an opportunity to interview TPSP personnel to clarify any questions the firm may have regarding TPSP's responses given as part of the DDQ and to allow the TPSP to demonstrate that the services contracted are being effectively performed. Firms should be thorough and structured in their approach to onsite due diligence in order to prevent wasted energies. Such preparation should include, but is not limited to: understanding processes of the TPSP, knowing who serves in management roles for the TPSP, and having an agenda set beforehand. It is important to remember that even though the firm's due diligence team is a visitor in these meetings, they are also the agenda-setters and should be the ones leading the onsite review.

Going Beyond the TPSP. Just as advisers use TPSPs to perform certain services on behalf of their firm, so too, do TPSPs use certain vendors to assist in their business operations. Well-drafted DDQs should ask questions not only in regard to the TPSP itself, but also as to whom, when, and how that TPSP may make use of the services of other vendors. Depending on the responses received, the due diligence reviewer may need to take additional steps to perform due diligence on the TPSP's critical vendors. This is especially true when the firm is dealing with third-parties responsible for the safeguarding of client information. The level of due diligence to be performed will vary depending on the due diligence program of the TPSP itself, and whether it is viewed as sufficient to identify and address risks associated with such third parties.

Drafting a Due Diligence Report. A firm must document its internal controls to demonstrate the dynamics of the protocol. This is particularly true when it comes to due diligence. A due diligence report should summarize the process used to conduct due diligence as well as all findings related to the examination of the TPSP. Generally, the report includes a profile of the TPSP highlighting the description of its services, business model, operations, compliance program, and management. The report should also include an overview of the industry in which the TPSP operates and how the adviser plans to use its services. It is important to include within the findings any outside vendors the TPSP materially relies upon in performing its services on behalf of the

[26] SEC, Investment Advisers Paying Penalties for Advertising False Performance Claims (Aug. 25, 2016), https://www.sec.gov/news/pressrelease/2016-167.html

adviser. Included as attachments to the report should be those documents collected throughout the due diligence process, including but not limited to:

- Any and all contracts between the adviser and the TPSP;
- The business continuity and cybersecurity plans;
- Succession plan;
- Confidentiality terms and conditions;
- Most recent audited financial and regulatory filings of the TPSP (if applicable); and
- All other pertinent documents demonstrating the TPSP's ability to effectively perform services on behalf of the adviser.

Red Flags and Requests for Additional Information

Once the DDQ responses and supporting documentation have been properly vetted and analyzed, the due diligence team will need to decide whether to either move forward, continue with, or terminate the TPSP relationship. An important factor in reaching this determination is to assess whether the information collected shows any potential "red flags" relating to the TPSP. Red flags refer to circumstances suggesting conflicts of interest, corruption risk, or other factor that should be properly identified and mitigated through adequate safeguards.

If red flags have been identified, it is critical that further inquiry be undertaken prior to engaging or continuing with the TPSP. Any red flags identified need to be considered in the context of the industry and jurisdiction in which the TPSP operates. An effective due diligence program allocates resources by ranking risks. Higher risk TPSPs should be evaluated more frequently and scrupulously than a lower-risk profiled vendor. Based upon the level of risk associated with a given TPSP, the firm should assign monitoring tools congruent with addressing such risks (e.g. audits, unannounced visits or meetings, and annual training).

Although all red flags should be carefully considered by the firm, not all will lead to a termination of relationship. For example, a TPSP's failure to respond to a particular question on a DDQ should be deemed a red flag. However, the TPSP may have not understood the question or intentionally omitted its response due to trade secret or confidentiality concerns. If a red flag is discovered, the due diligence reviewer must be sure to escalate this issue to the appropriate designated person for further action.

For TPSP relationships that require more in-depth due diligence, the firm should consider using outside counsel for investigation and/or resolution of red flags. Such actions are typically reserved for critical third-party partners that present a higher degree of risk or for situations when numerous red flags are discovered.

In addition to the identification of red flags, firms also need to consider whether the information collected throughout the due diligence process provides enough information to effectively determine whether or not to engage or continue retaining the TPSP.

Often, additional information is required to help fill any gaps that may exist. To that end, it is imperative to establish due diligence procedures and then review them often to address gaps within the process.

VII. OTHER DUE DILIGENCE CONSIDERATIONS

A situation may arise that leads the firm to determine that it is best to terminate the relationship with the TPSP. This outcome typically arises when:

- The due diligence responses are incomplete, inadequate, or not truthful;
- The servicing needs of the firm have changed and the TPSP can no longer satisfy the current requirements of the firm;
- The management team or financial condition of the TPSP has materially changed; or
- The services provided by the TPSP are unsatisfactory and are insufficient or substandard.

If it is the firm terminating the relationship, the due diligence officer should follow the notification provisions for termination as set forth in the TPSP servicing agreement (e.g., such as providing a written 30-day notice). If, on the other hand, the TPSP is terminating the relationship with the firm, the officer must be sure to do the following:

- Get all books and records the TPSP maintained on the firm's behalf for the duration of the relationship, particularly if there are regulatory requirements to maintain said records;
- Attempt to download or obtain all critical data that the firm owns;
- Determine whether notification is required to clients (e.g., custodian or broker-dealer changes); and
- To the extent the TPSP had access to confidential client information and/or trade secrets of the firm, review how they will be returning or destroying such information; be sure to review the terms of the TPSP and comply with them accordingly.

VIII. DUE DILIGENCE CHECKLIST

Due diligence is a dynamic process that involves careful deliberation. Recent enforcement actions highlight that firms must take reasonable steps to ask intelligent, customized questions designed to delve into whether anything is suspect or awry.[27] Failure to conduct an adequate investigation, particularly when red flags are present, is a compliance program failure that will likely lead to formal actions being taken—by the regulators and/or the firm's clients. Figure 4 provides a sample checklist.

---

[27] See, for example, *In the Matter of Neal R. Greenberg,* https://www.sec.gov/litigation/admin/2010/33-9139.pdf and *In the Matter of Paul H. Heckler and Yosemite Capital Management,* https://www.sec.gov/litigation/admin/2010/ia-3005.pdf

FIGURE 4. SAMPLE CHECKLIST TO USE IN SERVICE PROVIDER DUE DILIGENCE PROCESS

[Name of firm]

SERVICE PROVIDER DUE DILIGENCE FORM

The following form should be used for reviewing service providers that will provide services to [insert name of firm] (the "firm"). This form should be retained in a file that includes copies of all documents used to conduct due diligence on the service provider.

SERVICE TO BE OUTSOURCED

1. Type of service to be outsourced:

☐ Accounting/Finance: _____ ☐ Compliance Consulting: _____

☐ Legal Services: _____ ☐ Administrative Functions: _____

☐ Information Technology: _____ ☐ Operations/Support Functions: _____

☐ Other: _____

2. Is this service essential to the operation of the firm (i.e. transaction order entry; custody and prime brokerage; service designed to promote rapid recovery of operations etc.)?

☐ Yes ☐ No

APPROPRIATENESS OF OUTSOURCING

1. Potential impact on firm if service provider fails to perform:

Financial Impact:	☐ High	☐ Medium	☐ Low	☐ N/A
Reputational Impact:	☐ High	☐ Medium	☐ Low	☐ N/A
Operational Impact:	☐ High	☐ Medium	☐ Low	☐ N/A
Customer Service Impact:	☐ High	☐ Medium	☐ Low	☐ N/A
Potential Losses to Customers:	☐ High	☐ Medium	☐ Low	☐ N/A
Comply with Regulatory Requirements:	☐ High	☐ Medium	☐ Low	☐ N/A
Costs to firm:	☐ High	☐ Medium	☐ Low	☐ N/A
Degree of Difficulty Replacing Service Provider:	☐ High	☐ Medium	☐ Low	☐ N/A

Comments:

_____

_____

_____

2. Is there an affiliation or other relationship between the firm and the service provider?

☐ Yes ☐ No

If yes, please describe the relationship and any potential conflicts of interest:

_____

_____

_____

3. Is the service provider a regulated entity subject to independent supervision?

☐ Yes ☐ No

If yes, name of regulator: _____

SERVICE PROVIDER INFORMATION

1. General Information

Firm Name: _____

Firm Address: _____

_____

Contact Name(s): _____

CRD # (if applicable): _____

Phone: _____ Fax: _____ Website: _____

2. Is the service provider owned/controlled by a Parent Co.?

☐ Yes ☐ No

If yes, name: _____

3. Personnel:

Approximate number of employees: _____

Does the service provide hire independent contractors? ☐ Yes ☐ No

4. Background Information:

How many years has the service provider been in business? _____

How many years has the service provider provided the outsourced function? _____

Is the service provider known to the firm or employees of the firm? ☐ Yes ☐ No

If yes, please name the individual(s) and describe any prior experience each had with the service provider:

_____

_____

DUE DILIGENCE

1. What methods did the firm use to verify the service provider's information? (Choose all that apply; attach relevant documents to this report.)

☐ FINRA Public Disclosure
☐ Entity Formation Documents
☐ Credit/Background Check
☐ Form BD/ADV
☐ Personal Referral
☐ 10K
☐ Policies and Procedures Manual(s)
☐ Marketing Materials
☐ Onsite Inspection
☐ Internet Research
☐ SEC Public Disclosure
☐ Independent Research
☐ Media/News Reports
☐ Business Plan
☐ RFP
☐ Personal Interviews
☐ Financials
☐ Sales Materials
☐ Confidentiality Procedures and Contracts for Not Sharing Information

Other _____

2. **If the service is outsourced, does that represent any special risks to the firm if the vendor does not perform as contracted (e.g., loss of data, etc.)?**

   _____
   _____
   _____

3. **Should the vendor's office be visited?** ☐ Yes ☐ No

4. **Please describe the background and experience of individuals who will be performing the services:**

   _____
   _____
   _____

5. **Based on your review of the information, has the service provider and/or its principals been subject to any regulatory, criminal or civil disciplinary issues?**

   ☐ Yes ☐ No

   If yes, please describe:

   _____
   _____
   _____

6. **Based on your review of the information, please describe the service provider's ability and capacity to perform the outsourced activities effectively, reliably, and to a high standard (include in your description relevant technical, financial, human resources, and/or other assets of the service provider):**

   _____
   _____
   _____

7. **Does the service provider have a business continuity plan?**

   ☐ Yes ☐ No

   If yes, please describe:

   _____
   _____
   _____

8. **Is privacy and protection of non-public information a factor in outsourcing?**

   ☐ Yes ☐ No

   If yes, comment on the adequacy of the service provider's for safeguarding non-public information:

   _____
   _____
   _____

   Does the firm maintain notes from personal interviews and onsite inspections; printouts from public disclosure sites, etc.)? ☐ Yes ☐ No

   If yes, please identify where this evidence is maintained: _____

   _____

9. After reviewing the information, are there any questionable issues or potential conflicts of interest?

☐ Yes ☐ No

If yes, please describe:

_____

_____

_____

CONTRACTS AND AGREEMENTS

1. Has (or will) the firm entered into a written agreement with the service provider?

☐ Yes ☐ No

If yes, please identify the relevant provisions and disclosures in the contract (choose all that apply).

- ☐ Provides for firm and regulator access to records
- ☐ Defines responsibilities of all parties subject to contract
- ☐ Provide quality services measures
- ☐ Defines how responsibilities will be monitored
- ☐ Disclosure of breaches in security
- ☐ Requirement to maintain a disaster recovery plan
- ☐ Firm and client confidentiality
- ☐ Liabilities of the parties
- ☐ Payment arrangements
- ☐ Guarantees and indemnities
- ☐ Term and termination date
- ☐ Information security provisions (i.e., data to remain uncorrupted and secure)

Other relevant provision(s):_____

2. Was the written agreement reviewed by legal counsel?

☐ Yes ☐ No ☐ N/A

If yes, name of legal counsel: _____

Date of Review: _____

3. Was the written agreement reviewed by the manager responsible for outsourcing functions?

☐ Yes ☐ No

If yes, name of manager: _____

Date of Review: _____

OVERSIGHT AND PERIODIC REVIEW

1. Who is responsible for the periodic oversight and review of the outsourced service?

_____

2. Identify the individual(s) who will monitor the outsourced service.

_____

3. Identify the tools that will be used to monitor the outsourced service:

- ☐ Service delivery reports prepared internally
- ☐ Service delivery reports supplied by the service provider
- ☐ Publicly available resources
- ☐ Performance levels established in written agreement
- ☐ Internal auditor
- ☐ Onsite inspection
- ☐ External auditor
- ☐ Attestations by service provider
- ☐ Other: _____

_____

4. Frequency of monitoring:

☐ Daily ☐ Weekly ☐ Monthly ☐ Quarterly ☐ Annually

Other: _____

5. If deficiencies are found, are procedures in place to respond to such deficiencies (i.e., communicate with the service provider; terminate the contract)?

☐ Yes ☐ No

DOCUMENTATION REVIEW AND APPROVAL

1. Individual(s) responsible for completing this due diligence review:

_____

☐ The firm has elected to use the service provider above.

☐ The firm will not use the service provider above.

_____ _____

Signature Date

IX. CONCLUSION

It is essential to keep improving and evolving the due diligence process. To that end, the firm should establish a due diligence committee, identify what is working, and what requires improvement. The firm should conduct periodic risk assessments on due diligence processes and assess whether the firm is doing enough, asking the "right" questions, and collecting meaningful data. Management should review which employees are best suited to analyze due diligence data and assess periodically if they continue to be the most qualified to do so. For new products, a due diligence officer should ensure that the product is understood, that training and surveillance systems are established, and that suitability considerations are evaluated as necessary. For new services, the officer should check the terms of servicing agreements with the TPSP to

ensure it is fulfilling its obligations—from a servicing, contractual, and legal perspective. Importantly, the firm must remember to train. Training is the key to success for any effective due diligence program. The due diligence team members must understand why due diligence is being conducted and identify how it can continuously improve. They should review DDQs frequently and not allow them to go static. By keeping this process continuous, the firm will be in a position to advance its due diligence of TPSPs as the financial industry and its regulations continue to progress.

ABOUT THE AUTHORS

Michelle L. Jacko, Esq.,. is the managing partner and CEO of Jacko Law Group, PC, which offers corporate and securities legal services to broker-dealers, investment advisers, investment companies, hedge/private funds and financial professionals. In addition, Ms. Jacko is the Founder and CEO of Core Compliance & Legal Services, Inc., a compliance consultation firm.

Ms. Jacko specializes in investment advisory and broker-dealer firm formation, hedge and private fund development, mergers and acquisitions, transition risks, and investment counsel on regulatory compliance and securities law. Her practice is focused on the areas of corporate and compliance risk management, contracts, policies and procedures, testing of compliance programs (including evaluation of internal controls and supervision), performance advertising, soft dollar arrangements, best execution, separation agreements, and much more.

Previously, Ms. Jacko served as of counsel at Shustak & Partners, PC. Prior to that, she was vice president of compliance and branch manager of the Home Office Supervision team at LPL Financial Services, Corporation (Linsco/Private Ledger). Ms. Jacko also served as legal counsel of investments and CCO at First American Trust, FSB and held the position of compliance manager at Nicholas-Applegate Capital Management. In addition, Ms. Jacko was with PIM Financial Services, Inc., and Speiser, Krause, Madole & Mendelsohn, Jackson.

Ms. Jacko regularly presents at conferences throughout the nation, and is a frequent contributor to various industry journals. In 2013, Ms. Jacko was appointed to the Editorial Advisory Board for the Wolters Kluwer publication *Practical Compliance and Risk Management for the Securities Industry*. She is cofounder of the Southern California Compliance Group and is involved in the American Bar Association (Business Law Section), State Bar of California (Corporations Committee, where she serves as vice-chair of education), and San Diego County Bar Association. She also is a FINRA arbitrator. Ms. Jacko was named as a Top 20 Rising Star for "Who's Who" in Upcoming Compliance Professionals by *Compliance Reporter* magazine in 2006. In 2014, Ms. Jacko was named as a finalist for San Diego Magazine's 2014 Woman of the Year Award. She was also recognized as a finalist for San Diego Business Journal's 2014 Women Who Mean Business Awards.

Ms. Jacko received her juris doctor degree from St. Mary's University School of Law and bachelor of arts in International Relations from the University of San Diego. She is admitted to the State Bar of California and United States District Court, Southern District of California. Ms. Jacko is a past two-term board member for the National Society of Compliance Professionals (NSCP), holds NSCP's certified securities compliance professional (CSCP) designation, and is an active member and presenter.

Robert R. Boeche II provides strategic legal counsel at the Jacko Law Group to investment advisers, broker-dealers, private funds, and other financial professionals. Mr. Boeche advises clients on all aspects of formation, registration, and ongoing operations. He regularly counsels clients regarding the legal issues surrounding all matters of business entity formation, including state filings, document preparation, and general corporate governance matters, as well as succession planning. Mr. Boeche is responsible for drafting contracts, sales agreements, and client disclosure documents, as well as reviewing/preparing regulatory responses. He has extensive experience in all matters of investment adviser registration and compliance, including advising clients on solicitation and marketing activities.

Mr. Boeche regularly presents at conferences throughout the nation, and is a frequent contributor to various industry journals such as those of Schwab and Wolters Kluwer and others. He is involved in the State Bar of California (Corporations Committee) and the San Diego County Bar Association (where he serves on the Business and Corporate Law's Advisory Board). Mr. Boeche also was named as one of San Diego Transcript's 2014 Top Attorneys for corporate transactional law in 2014.

Mr. Boeche received his juris doctor degree from the University of San Diego School of Law, where he was involved as a member of the school's "National Mock Trial Team" and was the recipient of such awards as "Best Oral Advocate" and "Cali Award." Prior to his joining JLG, Mr. Boeche worked at the law firm of Wilson, Sonsini, Goodrich and Rosati in their Corporate Division, where he focused on transactional law related to corporate finance, corporate governance, debt and equity financing, and mergers and acquisitions. Mr. Boeche is admitted to the State Bar of California.

Tina Mitchell, practicing at Core Compliance & Legal Services, has more than 30 years of securities experience providing practical compliance solutions for clients. Her practice focuses on investment adviser compliance risk management, including performing marketing and advertising reviews, annual reviews and focused risk assessments, SEC mock audits, authoring/assessing policy and procedure manuals, drafting codes of ethics and evaluating trading and portfolio management operations. Ms. Mitchell also specializes in mentoring and training CCOs and other compliance personnel and assists them with maintaining their firm's compliance programs.

In addition, Ms. Mitchell frequently authors articles and periodically presents in webinars and at conferences.

Prior to joining CCLS, Ms. Mitchell was the senior vice president and CCO for Engemann Asset Management, a federally registered investment adviser owned by the Phoenix Companies. Engemann managed assets for registered investment companies, wrap programs, and high-net-worth clients. During most of her 14-year employment at Engemann, Ms. Mitchell was responsible for the firm's continued compliance with federal and state securities laws. She also served as the secretary of the Phoenix Engemann Funds (part of the Phoenix Family of Funds) and compliance liaison between Engemann and the Phoenix Engemann Funds board of trustees.

Ms. Mitchell has served as a FINRA arbitrator for the past 20 years and served as president of the Southern California Compliance Group for three years. She also is a member of the California 40' Act Group.

Craig Watanabe serves as a senior compliance consultant for Core Compliance & Legal Services, with particular focus on practical, risk-based compliance solutions. Mr. Watanabe is also a financial advisor at Penniall & Associates, Inc., bringing extensive experience in investments and wealth planning. With more than 30 years of industry experience as a financial planner, branch manager, operations manager, CCO and chief operating officer (COO), Mr. Watanabe provides our clients with a high level of compliance consulting support in areas of broker-dealer and investment adviser compliance, investment banking, insurance, commodities, retail investment advisory, and ERISA plans.

Prior to his joining CCLS, Mr. Watanabe worked at Advisor Solutions Group as a senior compliance consultant. In this capacity, Mr. Watanabe provided comprehensive compliance consulting and outsourcing to retail RIAs. Prior to that, Mr. Watanabe served as the COO and CCO at Penniall & Associates. During his six-year tenure, Mr. Watanabe implemented an outcomes-oriented approach to protect investors, advisers, and the firm.

Mr. Watanabe served on the FINRA District 2 Committee from 2008-11 and was chairman of the Committee in 2011. Mr. Watanabe served six years on the NSCP board of directors and was chairman of the board in 2013. Mr. Watanabe is a frequent speaker at compliance conferences and has authored numerous articles and training modules for compliance professionals.