NSCP Currents

February 13, 2025

Getting by with a Little Help from Friends: The Use & Management of Outsourced Service Providers

By Paul Felsch

Executive Summary

- Outsourcing of key services continues to be on the rise, with some 2024 studies showing that certain market registrants plan to increase the level of outsourcing between 25% and 50% over the next three years. For any registrant, whether an investment adviser or broker-dealer, while outsourcing can certainly have certain benefits, it can also carry potential risks that should be evaluated and overseen carefully.
- Registrants should be clear within their organizations regarding what the outsourcing risks are generally, as well as risks attached to certain third-party service providers that may be under consideration for outsourcing or are actively in use.
- Registrants should also have clear, explainable, and documented due diligence and oversight methodologies for outsourced service provider engagements.
- Additionally, depending on their level of complexity, registrants should consider implementing some form of a third-party risk management governance framework (depending on, and commensurate with, the size and complexity of their organization) to ensure that outsourced engagements are subject to appropriate vetting and monitoring.
- Registrants should not discount potential regulatory scrutiny on their third-party risk management practices and programs even in the absence of specific rules on this topic.

Introduction

This article is intended to build on other literature from the National Society of Compliance Professionals and provide investment advisers and broker-dealers with insights and refreshers of what effective third-party oversight methods and protocols can – and possibly, should — look like from the perspective of employing sound risk management practices irrespective of prescribed regulatory standards. To these ends, this article provides the following (among other content):

- The types of outsourced functions that may warrant more robust oversight;
- Types of third-party outsourcing risk considerations;
- Common third-party due diligence and ongoing oversight practices;
- Typical elements of a third-party engagement life cycle; and
- Third-party risk management governance framework components.

Critical Functions

Below is a non-exclusive list of functions that have a high probability of being tied not just to an investment adviser's or broker-dealer's (referred to here as a "registrant") general obligations to clients (depending on the nature of their relationship with a client), but also to those areas where, should there be a failure of some kind, client harm could result. Accordingly, registrants may want to more closely examine their oversight practices when outsourcing any of the following activities:

CRITICAL FUNCTIONS	
Adviser/Sub-adviser	Reconciliation
Client Servicing	Regulatory Compliance
Cybersecurity	Trading Desk
Investment Guideline/Restriction Compliance	Trade Communication & Allocation
Investment Risk	Valuation
Portfolio Management (excluding adviser/sub-adviser)	Pricing
Portfolio Accounting	Other (facts & circumstances dependent)

Outsourcing Conditions

Prior to and while outsourcing any of the abovementioned functions, a registrant should make certain determinations to ensure outsourcing a particular function, and to a particular party, is appropriate with attendant risks reasonably mitigated. The application of these conditions has the potential to enable registrants to more effectively identify the types of risks attached to any potential outsourced function and relationship. Such conditions can include any number of the following:

Outsourcing Conditions	

Pre-Engagement Due Diligence	• Nature & Scope of Covered Function
	  • Identify the nature and scope of the covered function the service provider is to perform
	• Risk Analysis & Management
	  • Identify and determine how the registrant will mitigate and manage the potential risks to clients or the registrant's ability to perform its services resulting from engaging a service provider to perform a covered function
	• Competence, Capacity & Resources
	  • Determine that the service provider has the competence, capacity, and resources necessary to perform the outsourced function
	• Sub-Contracting Arrangements
	  • Determine if the service provider itself has any sub-contracting arrangements that would be material to the provider's performance of the outsourced function, and if so, identify and determine how the registrant will manage and mitigate the risks attendant to such sub-contracting
	• Compliance Coordination
	  • Obtain reasonable assurance from the service provider that it is able to and will coordinate with the registrant for purposes of the registrant's compliance with federal securities laws that may be applicable to the covered function
	• Orderly Termination
	  • Obtaining reasonable assurance from the service provider that it is able to and will provide a process for orderly termination of its performance of the covered function (should the time come)
	• Recordkeeping

Outsourcing Conditions	
	• If applicable, obtain reasonable assurance from the service provider that it is able to fulfill the registrant's obligations to comply with books & records requirements of applicable federal securities laws • Also maintain records of the due diligence that has been conducted to evidence such due diligence
Ongoing Monitoring	• After an engagement has begun, periodically monitor the service provider's performance of the covered function to assess the items noted as part of the pre-engagement due diligence process • Determine that it is appropriate to continue outsourcing generally, and outsourcing to the specific service provider • The manner and frequency of the ongoing monitoring may be determined by the registrant

Due Diligence Considerations & Methodologies

Service Provider Risk Considerations. The nature, breadth, and depth of a registrant's due diligence should generally be determined by a combination of the nature of the covered function being performed, along with the particulars of a given service provider itself. While specific practices an adviser or broker-dealer can employ are discussed below, some examples of the types of risks registrants should account for when calibrating their initial and ongoing due diligence process – either in terms of their likelihood or even basic relevance/applicability – are as follows:

Risk Considerations

- **Information Misuse:** The service provider misusing sensitive or material non-public information to which it has access
- **Complexity:** The complexity of the function being outsourced
- **Reliability:** The reliability and accuracy of the service or function delivered by the service

provider

- **Concentration:** Extensive use of the service provider by the registrant, the registrant's affiliates, or industry as a whole
- **Alternatives:** Available alternatives in the event the service provider fails or is unable to perform the service
- **Speed:** The speed with which a function could be moved to a new service provider
- **Conflicts:** Conflicts of interests of the service provider
- **Transparency:** The service provider's unwillingness to provide transparency and access to information needed to understand how the service provider (a) performs its functions and (b) is performing its functions
- **Proprietary Technology:** The extent to which the service provider is using proprietary technology to perform a critical covered function for the registrant, and therefore, the criticality of the service provider to the registrant
- **Control Environment:** The service provider's documented control environment
- **Violation History:** The service provider's audit, compliance violation, and regulatory examination history
- **Litigation:** Private action history against the service provider in relation to the services being provided
- **Financial:** The financial soundness and stability of the service provider
- **Information Security:** The service provider's information and cybersecurity practices and their effectiveness
- **Business Continuity:** The service provider's business continuity planning program and its effectiveness
- **AI/GenAI:** The service provider's use of AI or GenAI in the performance of the covered function
- **Sub-Contractors:** The service provider's own use of sub-contractors to perform a covered function and its attendant oversight methodology and framework

Pre-Engagement Due Diligence & Ongoing Oversight/Monitoring Methodologies. There are common, long-established practices registrants may employ that would assist them in selecting service providers, monitoring their performance, and understanding the risks attached to certain service provider relationships. For ongoing monitoring and oversight in particular, it is important to note that the nature of the monitoring and oversight performed can modulate depending on the service provider's performance of the outsourced function, as well as any increase or decrease in a service provider's risk profile. Commonly employed pre-engagement due diligence and ongoing oversight and monitoring practices include:

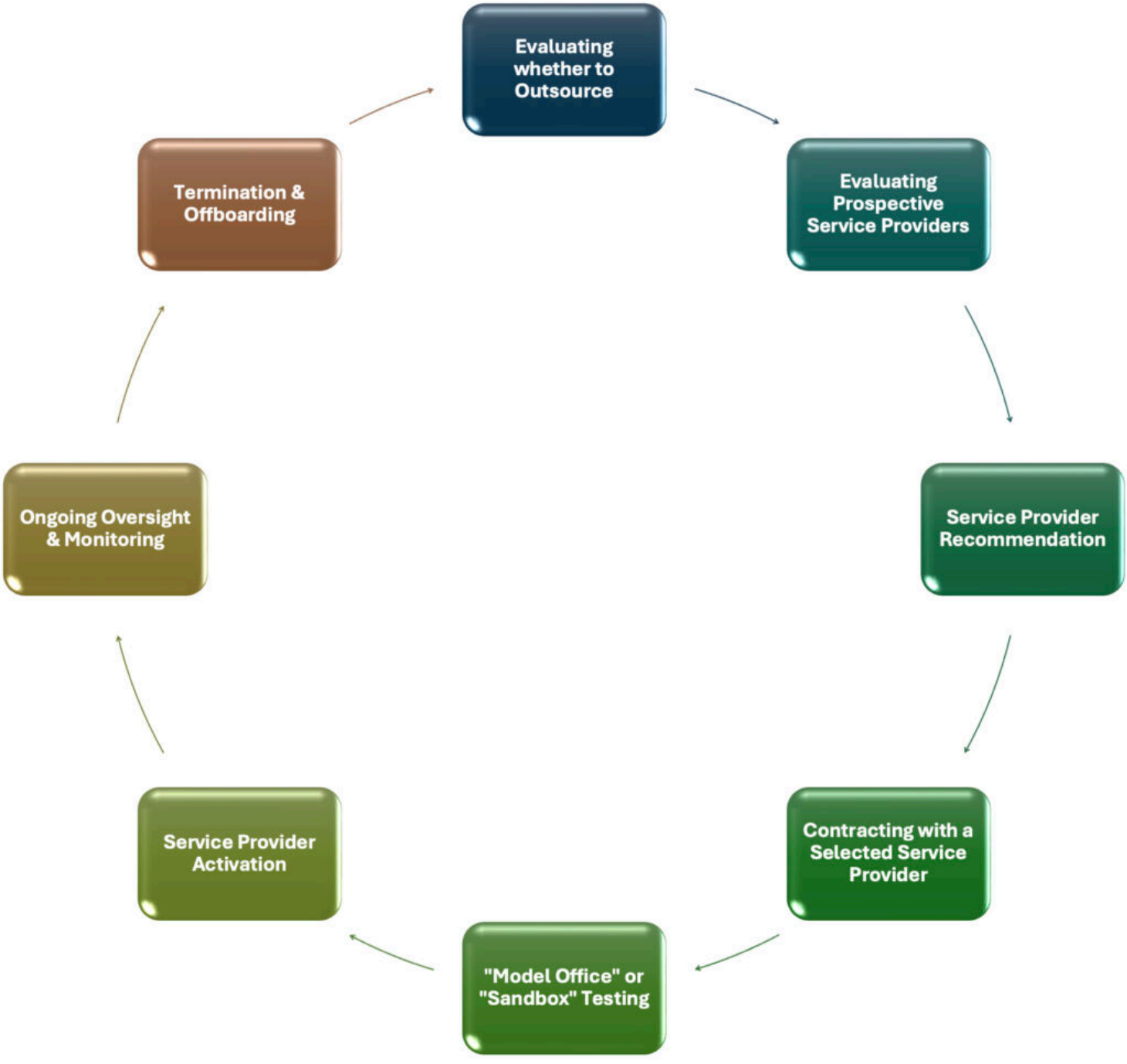
Third-Party Due Diligence Practices	
PRE-ENGAGEMENT DUE DILIGENCE	ONGOING MONITORING & OVERSIGHT

Third-Party Due Diligence Practices	
Use of Due Diligence Questionnaires (narrative-based with supporting documentation)	Use of Compliance Certifications & Periodic Questionnaires (changes or exception-based with supporting documentation as needed, such as for policy & procedure changes, etc.)
Reviews of Policies & Procedures	Daily, Weekly, Monthly or Other Periodic Monitoring, as Appropriate (e.g. if the outsourced function is a daily function such as trading, reconciliation, etc.)
Systems Demonstrations	Review of Policy & Procedure Changes
Process Walk-Thru's (including onboarding, live-relationship, offboarding)	Review of Policy, Procedure, or Contractual Violations (if any)
Review of Policy Violations & Regulatory Examination Deficiencies (e.g. exam letter inspections)	KPI Reviews
Review of Independent Audit Results (e.g. SOC1's, etc.)	Issues & Errors Tracking & Reporting
Onsite or Virtual Meeting with Key Personnel (including "boots on the ground")	Review of Independent Audit & Regulatory Examination Results
Premises Security and "Walling" Inspections	Periodic Onsite or Virtual Meetings with Key Personnel, as well as Ad Hoc Meetings (as needed)
Commemoration of Due Diligence Observations	Commemoration of Ongoing Monitoring Observations

Third-Party Risk Management Life-Cycle & Frameworks

Third-Party Life Cycle. At a very practical level, a registrant should think of all outsourced/third-party engagements in the context of a life-cycle, ranging from the initial evaluation phase regarding whether it

makes sense to outsource, all the way through to the termination or cessation of an outsourced relationship. The following diagram depicts the typical elements of the third-party risk management cycle:



Third-Party Risk Management Framework. Each stage of the third-party life cycle should typically fall into a framework that governs each stage. Third-party risk governance frameworks are designed to ensure intentional and informed decision making occurs before an outsourced relationship may progress to the next stage in the life-cycle. Third-party risk governance frameworks also help ensure that a registrant is aware of various risks and performance metrics that a particular service provider may have.

In order to ensure that all stakeholders who have an obligation or interest in evaluating a prospective or a service provider are sufficiently involved in the outsourcing life-cycle, an adviser or broker-dealer should consider establishing a structured third-party risk management framework, irrespective of an adviser's size or organizational complexity. The construct of such a framework should be tailored to and right-sized for the particular needs and business of a given registrant. Such a framework could even be as simple as a single policy or procedural document that speaks to what is required at each phase. Potential governance

considerations for each stage of the third-party risk management life-cycle can include a combination of one or more of the following, depending on the nature of an adviser's organization and business model:

Potential Governance Framework	
Outsourcing Evaluation	• Area within registrant considering outsourcing a covered function (relationship owner) evaluates whether such function is appropriate to outsource • Determination to outsource covered function documented with rationale, including benefits and risks • Determination to outsource may be unilateral or rest in cross-functional governance group
Service Provider Evaluation	• Relationship owner assembles prospective service providers to be considered • Other areas within registrant have ability to opt in or out for whether their functional expertise is needed to assess prospective service provider candidates (e.g. operations, compliance, legal, technology, finance, etc.) • Relationship owner and cross-functional stakeholders conduct due diligence
Service Provider Recommendation	• Relationship owner makes recommendation to cross-functional governing body regarding recommended service provider (which includes justification for outsourcing the functional generally) • Cross-functional group may approve or deny for contracting • Risk rating is assigned to selected service provider, which in part drives frequency and methodology for ongoing monitoring and oversight
Contracting	• Legal works with service provider on contractual terms (substantive terms to be approved by relationship owner, interested stakeholders, and ultimately cross-functional governing body) • Terms of relationship documented by relationship owner to ensure adherence by service provider and adviser
Model Office/Sandbox	• Prior to service provider "going live" with performance of function, service provider's performance of the function has been validated in "model office"/"sandbox" environment

Potential Governance Framework	
	• Cross-functional governing body sets criteria for sufficient “model office”/“sandbox” testing/validation
Activation	• Service provider “going live” with performance of function occurs after cross-functional group within adviser approves based on satisfactory “model office”/”sandbox” results
Monitoring	• Relationship owner and cross-functional stakeholders conduct ongoing oversight and monitoring • KPI’s, issues, and errors are documented, remediated, and reported to cross-functional governing body with set frequency
Termination	• Relationship owner recommends termination of engagement – may be unilateral or rest in cross-functional governance group (service provider may themselves terminate as well) • Relationship owner facilitates offboarding of function, and if need be, onboarding of new service provider (subject to the third-party life cycle and governance framework)

Parting Thoughts

The exact nature of a registrant’s third-party risk management practices and program will and should depend on the nature, size, and complexity of its business. There is no need to turn third-party risk management into more of a bureaucracy than needed. Any practices – be they due diligence methodologies or governance constructs – ultimately need to be designed to best facilitate the assessment of outsourced engagements to ensure the registrant’s clients are not harmed, and also that the registrant’s rendering of services is optimized.

Thanks for lending me your ears.

Bibliography

- Audet, Chris et al., “Stay Ahead of Growing Third-Party Risk,” https://www.gartner.com/smarterwithgartner/a-better-way-to-manage-third-party-risk, August 16, 2019.
- Federal Register Vol. 88, No.111, June 9, 2023.
- “Fund Managers Increasingly Reliant on Outsourcing,” https://www.ocorian.com/news-press-releases/fund-managers-increasingly-reliant-outsourcing, January 23, 2024.

- Hicks, David et al., “Third-Party Risk Management Outlook 2022,” https://kpmg.com/xx/en/home/insights/2022/01/third-party-risk-management-outlook-2022.html, January 2022.
- Itoh, Tasuku, “Conducting Effective Third-Party Risk Management,” Risk Management, April 2, 2024.
- Mikkelsen, Daniel et al., “Improving Third-Party Risk Management: A Joint Study between ORIC International and McKinsey & Company, https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Risk/Our%20Insights/Improving%20third%20pc third-party-risk-management.ashx, October 2017.
- Moog, Matthew et al., “Global Financial Services Third-Party Risk Management Survey: Is It Time to Shift Your Perspective of Third-Party Risk?,” https://globaltaxnews.ey.com/news/2018-5743-global-financial-services-third-party-risk-management-survey-is-it-time-to-shift-your-perspective-of-third-party-risk, June 7, 2018.
- Stephen, Lesley. “Deloitte’s 2023 Global Third-Party Risk Management Survey Shows Resiliency, Building Trust Top Priorities for Leaders,”https://www.deloitte.com/global/en/about/press-room/deloittes-2023-global-third-party-risk-management-survey-shows-resiliency.html, October 16, 2023.

About the Author:

Paul Felsch is a Chief Compliance Officer..
He can be reached at pwfelsch3@gmail.com.
