BCLP. Client Intelligent

Insights

SUPERVISION OF VENDORS WHEN OUTSOURCING – THE BUCK STOPS WITH FINRA MEMBER FIRMS

Aug 17, 2021

SUMMARY

Key Takeaways:

- On August 13, 2021, FINRA issued Regulatory Notice 21-29 ("RN 21-29") to remind member firms that they must establish and maintain an adequate supervisory system, including written supervisory procedures ("WSPs"), to address any core business activities or regulatory functions outsourced to third-party vendors and/or sub-vendors (collectively "Vendor" or "Vendors").
- FINRA emphasized throughout RN 21-29 that the notice is not intended to create new rules or requirements – rather, its guiding principles are established by existing FINRA and industry rules which were set forth previously in Notice To Members 05-48 , and reiterated in a number of FINRA Enforcement cases since FINRA published that release. FINRA did determine, however, that RN 21-29 is necessary as a refresher for member firms based on its observations of numerous recent exam deficiencies.
- In essence, outsourcing an activity or function to a third party does not relieve members of their ultimate responsibility for compliance with all applicable federal securities laws and regulations, and FINRA rules require that the outsourced activities are properly supervised by a licensed individual, where appropriate, within the member firm.
- RN 21-29 identifies key topics for consideration in ensuring compliance with the applicable rules, including the development of an adequate corporate governance structure that memorializes the decision to outsource and manages the lifecycle of the engagement (from onboarding the Vendor to dissolution). This governance structure should also: ensure adequate supervision, proper registration and cybersecurity protections; include provisions for the maintenance of adequate books and records; and include the creation of a business continuity plan that takes into consideration the outsourcing of the respective business functions to Vendors. These topics are outlined in further detail below.

According to FINRA, member firms are increasingly using third-party Vendors to perform core business and regulatory functions over a wide range of activities.[1] During examinations occurring between 2017 and 2021, FINRA observed numerous compliance deficiencies on this topic. Accordingly, this alert is intended to be a checklist of key concepts for member firms to consider when assessing their outsourcing programs and it is based on guidance derived from FINRA's RN 21-29 and 05-48.

Key Thoughts and Considerations Based on FINRA's Guidance.

1. Adequate Corporate Governance. Member firms may have a variety of reasons for outsourcing certain business functions, including cost considerations and/or efficiencies. FINRA's regulatory notice reminds members that they should have an established corporate governance structure, memorialized in WSPs, which evaluates and documents essential risk data points during the decision making process, and that outlines the responsibilities of the respective parties during the lifecycle of the Vendor relationship. Below is a checklist of some key thoughts, among others, to consider when selecting a third-party Vendor:

WSPs. Design and implement WSPs that clearly outline the decision to outsource and will govern the lifecycle of the engagement (from onboarding to dissolution of the relationship).

Justification. Have an adequate justification for the decision to outsource the business function, and document the decision-making process in writing, taking into account the related risks.

Stakeholders. Ensure the right stakeholders participate in the decision making process, including representatives from the line of business, legal, compliance, risk, IT, and supervision departments.

Selection Process. When selecting the Vendor:

a. Consider whether the activity or function is appropriate for outsourcing;

b. Consider multiple alternative Vendors before the selection occurs; and

c. Consider the Vendor's reputation, financial condition and operational capabilities in addition to the impact to the member firm if the Vendor fails in carrying out its duties.

Due Diligence. Conduct due diligence on the Vendors on the front end and periodically throughout the lifecycle of the relationship, including on-site visits to observe and monitor the Vendor's activities.

Documentation/Contract. Memorialize in writing:

a. The relationship with the Vendor through a contract;

b. The Vendor's legal and regulatory responsibilities and the firm's overall expectations of the Vendor; and

c. A written nondisclosure agreement to ensure protection of customer data.

Conflicts of Interest. Put controls in place to address potential conflicts of interest in the decision making process.

Vendor Disclosure. Ensure the contract requires the Vendor to disclose material changes in business practices, financial hardships including default or bankruptcy, the existence of legal and regulatory matters, as well as any potential settlements, cybersecurity breaches, and other risks or changes in circumstances that may have a material impact on the member firm or its reputation.

2. Supervision. FINRA Rule 3110 (Supervision) requires member firms to establish and maintain a system to supervise the activities of their associated persons that is reasonably designed to achieve compliance with federal securities laws and regulations, as well as FINRA rules, including maintaining written procedures to supervise the types of businesses in which it engages and the activities of its associated persons. This supervisory obligation extends to member firms' outsourcing of certain "covered activities," which are activities or functions that, if performed directly by a member firm, would be required to be the subject of a supervisory system and WSPs pursuant to FINRA Rule 3110.[2] Important considerations include:

WSPs. Design and implement WSPs that identify the staff of the member firm required to supervise the Vendors and ascertain that all of the staff's roles and responsibilities are clearly defined.

Monitor. Periodically monitor and assess the accuracy and quality of work provided by the Vendor.

Vendor Certification. Require that Vendors:

a. Attest or certify completion of their assigned tasks; and

b. Attest or certify that they are conducting self-assessments to ascertain that the work being performed is completed timely and accurately.

Awareness and Vigilance.

a. Become and remain aware of any operational or compliance related problems and investigate any such problems periodically;

b. Conduct on-site visits of the Vendors to observe, review and monitor their business practices; and

c. Investigate customer complaints involving the Vendor's work product or performance.

Training. Affirmatively take part in training the Vendor and its staff to ensure that the proper red flags are being dispositioned adequately and/or the communication process between the Vendor and the member firms is open and functioning appropriately.

3. Registration. In general, any parties conducting activities or functions that require registration under FINRA rules will be considered "associated persons" of the member, absent the service provider separately being registered as a broker-dealer and such arrangements being contemplated by FINRA rules (such as in the case of clearing arrangements), MSRB rules, or applicable federal securities laws or regulations. Outsourcing an activity or function to a third party does not relieve members of their ultimate responsibility for compliance with all applicable federal securities laws and regulations and FINRA and MSRB rules regarding the outsourced activity or function. Accordingly, members may need to adjust their supervisory structure to ensure that an appropriately qualified person monitors the arrangement with the Vendor.[3]

Proper Licensure.

a. Review every activity and business function outsourced carefully to determine whether it requires licensure according to federal and state law and/or FINRA rules.

b. Determine whether the Vendor is registered as a broker-dealer and the performed activity is contemplated by FINRA rules (such as in the case of clearing arrangements), MSRB rules, or applicable federal securities laws or regulations.

c. Determine whether the member firm needs to adjust its supervisory structure to ensure that an appropriately qualified person monitors the arrangement.

4. Cybersecurity. Member firms must establish written policies and procedures that address administrative, technical and physical safeguards for the protection of customer records and information that are reasonably designed to: (1) ensure the security and confidentiality of customer records and information; (2) protect against any anticipated threats or hazards to the security or integrity of customer records and information; and (3) protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer.[4]

Vendor Governance. When evaluating a prospective Vendor:

a. Consider whether the Vendor is SOC 2 certified or has gone through a similar widely recognized audit procedure to test the strength of its cybersecurity systems;

b. Obtain copies of its SSAE 18 or other audit reports and review such to ascertain that it performs to the level of expectation; and

c. Consider whether the Vendor has any prior security breaches or data loss incidents.

WSPs - Design and Implementation.

a. Determine which Vendors should have access to sensitive customer non-public data and/or critical firm systems and determine to what degree access is appropriate; and

b. Design and implement WSPs with controls in place to ensure Vendors safeguard customer information.

Controls - Design and Testing.

a. Determine whether it is appropriate to implement multi-factor authentications before granting data access to Vendors;

b. Periodically evaluate and test the controls to assess continued strength; and

c. Evaluate periodically whether continued access is required for the outsourced business function and/or whether the Vendor's access to certain data is outdated and can be restricted or revoked.

Protocol for Security Breaches.

a. Ensure procedures are in place in the event of a data breach, including notification to the member firm, law enforcement, regulators and/or firm clients, and that there is a clear incident response plan;

b. Monitor and test changes to systems and applications to ascertain that controls are not compromised and customer data remains protected; and

c. As noted above, ensure that Vendors are required to promptly notify the member firm of any security breaches, threats or data loss incidents.

5. Books and Records. Member firms are required to maintain certain business records including blotter data, correspondence, customer complaints, among others, in varying different formats, and to make those documents readily available to regulators upon request.[5] Similarly, member firms are required to ensure their Vendors keep required records and can make those available to regulators for review and inspection upon request.

WSPs - Design and Implementation.

a. Design and implement WSPs which describe the books and records requirements for each outsourced activity.

Testing and Review.

a. Periodically monitor and test the Vendor's compliance with the books and records requirements;

b. Ascertain the Vendor is correctly calculating and maintaining adequate record retention policies;

c. Ensure that the Vendor is creating records that are WORM compliant (write once, read many) where necessary; and

d. Have procedures in place to purge a Vendor's access to client records and information and business records upon dissolution of the Vendor relationship.

6. Business Continuity Plans ("BCP"). Member firms must create and maintain a written BCP with procedures that are reasonably designed to enable member firms to meet their existing obligations to customers, counterparties and other broker-dealers during an emergency or significant business disruption, including provisions that are specific to outsourcing functions to third-party Vendors.[6]

WSPs - Design and Implementation.

a. Design and implement WSPs that clearly address the responsibilities of the member firm and its Vendors during the time of an emergency or significant business disruption.

Testing and Review.

a. Periodically test the BCP, including Vendors, to ensure the parties know their respective roles and responsibilities and to ensure functionality;

b. Ensure that each Vendor has sufficient staff dedicated to the member firm and its business operations; and

c. Ensure that the member firm and its Vendors review and update their BCPs periodically, as needed, in light of changes to operations, structure, systems, business or location.

Conclusion

While outsourcing certain business functions may be advantageous for a variety of reasons, the firm is still responsible for the underlying regulatory responsibilities surrounding those activities. Simply put, the buck stops with the member firm. There are countless risk considerations associated with relying on Vendors and it is important that firms take those risks into consideration within the decision making process. It is also important for firms to develop a compliance program which addresses the related risks throughout the lifespan of the Vendor relationship. If you have questions on this topic or need assistance with securities regulatory or litigation matters, please reach out to us as we would be delighted to help with your needs.

1. FINRA notes in Regulatory Notice 21-29 that common outsourced activities include accounting/payroll functions, legal and compliance, information technology, operations functions, and administrative functions.

2. *FINRA's Regulatory Notice* 05-48 reminds member firms that "outsourcing an activity or function to … [a Vendor] does not relieve members of their ultimate responsibility for compliance with all applicable federal securities laws and regulations and [FINRA] and MSRB rules regarding the outsourced activity or function." Further, *Notice* 05-48 states that if a member outsources certain activities, "the member's supervisory system and [WSPs] must include procedures regarding its outsourcing practices to ensure compliance with applicable securities laws and regulations and [FINRA] rules."

3. See FINRA Regulatory Notice 05-48.

4. See SEC Regulation S-P Rule 30 which addresses cybersecurity concerns.

5. See FINRA Rules 3110 and 4510 and SEC Exchange Act Rules 17a-3 and 17a-4.

6. See FINRA Rule 4370 which addresses Business Continuity Planning and Emergency Contact Information.

RELATED PRACTICE AREAS

- Financial Regulation Compliance & Investigations
- Regulation, Compliance & Advisory
- Broker-Dealer and Investment Advisor Regulatory Enforcement, Disputes and Investigations

MEET THE TEAM

Shea O. Hicks

St. Louis

shea.hicks@bclplaw.com
+1 314 259 2659

Jeffrey A. Ziesman

Kansas City

jeff.ziesman@bclplaw.com
+1 816 374 3225
