Managing Third-Party Risk – Tips and Best Practices

By Madison Dewey

About the Author:
Madison Dewey is a Business Risk Assurance Associate with Fairview Cyber. She can be reached at madison.dewey@fairviewcyber.com.

Importance of Managing Third-Party Risk

Vendors / third-parties are a critical part of any organization. They provide essential services to assist with everyday business. Many vendors have access to and / or store sensitive company data that may include personally identifying information ("PII"). Security breaches often affect organizations through one of their vendors. If a vendor has inadequate security protocols or is a victim of a cybersecurity incident, its clients' data may be at risk. To prevent these kinds of security incidents, it is critically important that companies monitor their vendors and thoroughly research the information security safeguards in place.

This article focuses on the SEC's guidance and best practices for registered investment advisers ("RIAs"). The information is largely applicable to broker-dealers as well. In addition, FINRA has provided multiple specific releases for member firms. These releases are referenced throughout the article including FINRA's Regulatory Notice 21-29 which provides guidance surrounding managing third-party risk and reminds firms of their obligations related to third-party risk.
A vendor management program enables a company to address and define the risks associated with certain critical vendors to (1) safeguard confidential information and (2) secure critical systems from misuse, disruption, and unauthorized access. Roles and responsibilities are also assigned to personnel as part of this program to help manage critical vendors and the risks associated with them.

Vendor management programs have also become a common focus area in SEC exams. Recent SEC Cyber Exam request lists for RIAs include a section related to vendor management that requests detailed documentation surrounding firms' vendor due diligence procedures. Commonly requested materials include:

- Policies, procedures, and standards for third-party vendors;
- List of all vendors with a brief description of the services the vendors provide, whether the firm has access to client NPI, whether an executed contract is in place with that vendor;
- Most recent due diligence questionnaire provided to, or status report prepared by, vendors managing client information that interact with the firm's internal systems that discuss data security protocols at the vendor and / or results of audits performed of such controls;
- Written contingency plans that the firm has with vendors in case of bankruptcy, development of conflicts of interest, or other issues that might put the vendor out of business;
- Sample documentation or notification the firm requires (or has received) from third-party vendors prior to such vendor implementing significant changes to their systems, components, or services that could potentially have security impacts to the firm and its data containing NPI;
- List of terminated vendors during the examination period;
- Information obtained by the firm regarding any actual or suspected breaches of the vendor's data security protocols;
- Internal communications with vendors concerning any suspected / actual breaches;
- Information on any actual or suspected breaches of the firm's data security protocols related to the use of video conferencing software;
- Internal communications with clients or other stakeholders concerning any suspected / actual breaches.

Below are questions observed from SEC Cyber Exam Interviews of RIAs

- Explain the third-party vendors submitted and walk us through how these providers were chosen and are supported by your IT partner.
- What process was used to identify the selection of vendors? Do any social security numbers reside with these vendors, and what types of data live where?

- Any ongoing due diligence after onboarding the service providers performed during the review period?
- Maintaining any documentation for the due diligence process, process for documenting the conversations and vendor requests?
- Ongoing due diligence for the vendors?
- All data related to customers which resides with other vendors. Do the vendors have the same retention policies or do these vary?
- Records created in using third party vendors, are you recreating for books and records purposes or grabbing that info to somewhere else?

Step-by-Step Guide to Developing a Vendor Management Program

Creating a vendor management program can seem like a daunting task, especially for firms that might have numerous critical vendors. Below is a step-by-step guide for developing a vendor management program that can be used as a starting point. Eventually, this should turn into a formal vendor management policy and procedure.

1. Establish a Vendor Management Committee
    - This committee typically includes a firm's Chief Compliance or Operations Officer and any additional designees deemed necessary.
    - The vendor management committee can be responsible for maintaining an approved vendor lList and implementing the policies and procedures pertaining to vendor due diligence.
2. Determine What Constitutes a Critical Vendor
    - It is important to define what constitutes a critical vendor because it allows a firm to identify which vendors require additional review.
    - In the past, firms had to assess this on their own, however, the Proposed Cyber Rules (Rule 206(4)-9 under the Investment Advisers Act of 1940 and Rule 38a-2 under the Investment Company Act of 1940 offer a new definition that firms can use
        - The proposed rule provides, "a risk assessment must also identify service providers that receive, maintain, or process adviser or fund information, or that are permitted to access their information systems, including the information residing therein and the cybersecurity risks they present."
3. Identify the Documentation to be Maintained. This might include:
        - Approved vendor list;
        - Risk Assessment that includes ratings related to data, operation, and due diligence risks;
        - Additional items reviewed during the review (SOC reports, security policies, Certificate of Insurance);
        - A list of alternate vendors to prepare the firm in case a current critical vendor experiences a significant business disruption or is deemed a high-risk vendor;
        - Vendor agreements;
4. Establish a Time for Annual Reviews
    - Critical vendors should be reviewed when engaged initially as well annually thereafter to ensure the firm remains up to date regarding risks the vendor may pose..
    - An annual Vendor management meeting is a great way for a firm to meet and discuss findings.

Together, these steps will act as your firm's vendor management policy and procedures and comprise your vendor management program. The policy and procedures can be used as a guide when conducting vendor due diligence and determining risk ratings.

FINRA issued a report in 2015 that provides valuable information to consider when creating a vendor management program. One area addressed by the report is the level of due diligence warranted for different vendors. The report advises that firms should correlate the level of due diligence to the level of risk inherent in the relationship with the. Vendors with access to low level data and minimally relied upon by the firm might only be required to complete due diligence questionnaires. Vendors with access to sensitive data and greatly relied upon might be required to provide additional due diligence materials such as SOC reports, vulnerability reports, or security policies and procedures.

Tips & Best Practices

- Review your Vendor Management Policy and Procedures annually to ensure it remains current and applicable to industry risks.
- Stay informed of important industry topics and update or supplement the questionnaire as appropriate.
- Remain aware of important industry topics and include additional questions to the questionnaire as needed or send a separate questionnaire.
- Reach out to vendors immediately when a breach or vulnerability is identified to inquire if they were affected by a widely reported breach. i.e., Log4j vulnerability.
- Vendor agreements should typically address the following;
    - The sensitivity of information and systems the vendors will have access to;
    - Scope of arrangement, services offered, and activities authorized;
    - Responsibilities of all parties;
    - Penalties for lack of performance;
    - Ownership, control, maintenance, and access to financial and operating records;
    - Audit rights and requirements;
    - Data security and member confidentiality;
    - Acceptable methods for the return, destruction, or disposal of firm information in the vendor's possession at the end of the contract;
    - Statement requiring the vendor to only use firm data and information systems for purposes detailed within the agreement and / or approved statement of work;
    - Breach notification responsibilities.
- Firms should note that some states and countries have specific requirements regarding PII. Additional requirements may apply and be included in contracts if PII from the person in those jurisdictions will be accessed.
- Develop a meaningful Vendor Due Diligence questionnaire that asses the controls a vendor has in place. These controls should include:
    - Limits on data accessed by employees;
    - Virus protection;
    - Encryption of data at rest or in transit;
    - Controls in place regarding subcontractors;
    - System patch management;
    - Change management processes;
    - Business recovery / continuity practices;

FINRA has put together a cybersecurity checklist to assist firms in developing and documenting a cybersecurity program. Section 3 of the checklist specifically addresses managing third-parties and vendor management.

Challenges of Vendor Due Diligence

A critical part of a vendor management program is reacting to challenges encountered when sending requests and following up with vendors. Firms often face unresponsive vendors or when faced with gaps in a vendor's cybersecurity review, firms may be reluctant to make the proposed changes. Ultimately, the onus is on advisers to maintain proper documentation of vendor due diligence reviews.

Tips for Managing Unresponsive Vendors

Some vendors, especially large vendors (i.e., Microsoft O365), may not respond to firms' due diligence requests. As an alternative, firms should exhaust publicly available resources and check for SOC reports posted on the vendor's website. Larger vendors often post security documents or certification attestations on their website that are available either for download or by request.

Small vendors also might be reluctant to respond to a due diligence request. Firms should check the vendors' website for due diligence materials or additional contacts. Another option is to schedule a call with the vendor to discuss the security measures in place. Smaller vendors may lack the resources to complete due diligence requests, however, they could be able to provide insight regarding their security measures in place during a phone call. Firms should note this deviance from their typical vendor due diligence process in their review and determine if they want to incur the risk of a vendor that completes a request via a phone call instead of providing documentation of the security measures in place.

Third parties can also be engaged to conduct assessments of vendors using publicly available information to provide a baseline security rating and / or to conduct an external vulnerability scan on the vendors. Firms should be aware that if they outsource their vendor due diligence reviews to a third-party, they may have to conduct due diligence on the third-party. The review should be easier to complete as the third-party should be familiar with this request.

Tips for Resolving Gaps in Vendor Reviews

When material gaps are identified in your review, consider requesting the vendor take remedial action. Vendors may not want to make such changes or may lack the means to comply with them. To adequately document the vendor due diligence conducted, firms should adopt processes to navigate these difficulties.

From a regulatory perspective, firms should maintain vendor due diligence documentation for all critical vendors and implement a process to oversee any changes required to address material security gaps identified during the review.

If a vendor does not offer an adequate explanation regarding the security gaps identified or does not adopt proposed changes, firms should reference the steps taken to resolve the security gaps and any correspondence between them and the vendor in their due diligence review and determine if they would like to continue to incur the risk of working with the vendor. A firm could also turn to its alternate vendors at this time to determine if their security practices are better.

Recent SEC Proposed Rule & the Potential Impact on Vendor Due Diligence

The SEC proposed a new rule with oversight requirements for registered investment advisers on third-party service providers on October 26th, 2022. Outsourcing specific business functions can greatly benefit investment advisers, but clients' PII can be compromised if advisers do not conduct oversight regarding the service providers' controls. The SEC's proposed rule identifies

specific monitoring requirements for registered investment advisers outsourcing "covered functions" to a service provider.

The SEC's proposed rule on outsourcing by investment advisers will bring to light the importance of conducting reviews on service providers and identifying the controls service providers have in place to protect clients' PII. Registered investment advisers who currently do not prioritize vendor due diligence will be expected to do so, and advisers who do already monitor service providers may have to shift their procedures in accordance with the final rule.

As mentioned previously, there are multiple roadblocks that a firm can incur when conducting vendor due diligence. The proposed rule may highlight these roadblocks as conducting reviews on third-party service providers becomes more common and expected. Advisers should be aware of these roadblocks when building out their vendor management program to ensure that they can comply with the final rule and mitigate gaps incurred when conducting their reviews.

Conclusion

Engaging vendors is a necessary part of conducting business for most firms. The SEC has made its expectations clear: vendor due diligence is a necessary part of an adviser's compliance program. Recent proposed regulation has shown that vendor due diligence is a focus area and, in the future, will be a requirement. Vendor due diligence is challenging because there is not a one-size fits all approach and it is common to face challenges both in the vendor due diligence request process and in the remediation process.

Developing and maintaining a thorough but flexible vendor management program will enable your firm to meet regulatory expectations and stay ahead of industry threats associated with vendors. ■