From: Audrey Kirkhoff <akirkhoff@bihbank.com>
Sent: Friday, September 03, 2021 2:52 PM
To: Comments
Subject: [EXTERNAL MESSAGE] July 19, 2021 - Proposed Interagency Guidance on Third-Party Relationships: Risk Management (RIN 3064-ZA26)

Based on the *Proposed Interagency Guidance on Third-Party Relationships: Risk Management* dated 19 July 2021, please see the information below in response for the request to comment on RIN 3064-ZA26.

The request for comment on the interagency guidance stated to consider whether: (1) Any of the concepts discussed in the OCC's 2020 FAQs should be incorporated in the final version of the guidance; (2) there are additional concepts that would be helpful to include in the guidance; and (3) there are any response considerations to the additional 18 questions provided in the request for commentary.

The focus of the commentary provided below addresses item #1 and #2 in the above paragraph, and also includes a subset of responses to the 18 questions, as warranted:

1. It is recommended that the OCC 2020 FAQs be incorporated in the final version of the guidance as these are an essential complement to the guidance. The FAQs add an element of clarity that would be most helpful in developing/enhancing a financial institution's (FIs) Third Party Risk Management (TPRM) Program. It would be more helpful for the content in the FAQ to be built directly into the guidance. It would be beneficial to create a 'definition' section within the guidance. Many of the FAQ's provide definitions or examples of the terms mentioned throughout the guidance. For example, the following terms could be included in a definition section built into the guidance, along with any complementary examples or commentary to aid in understanding:

    - 3rd party relationship
    - Business arrangement
    - Critical activities
    - Cloud computing provider
    - Data aggregator
    - FinTech company arrangement
    - Interagency technology service provider's (TSP) reports of examination
    - Service Organization Control (SOC) Report
    - 3rd Party assessment services (i.e., utilities).

2. We have recently 'exempted' a specialty third party entity-type relationship, i.e., appraisers, from the scope of the 'general' vendor management program requirements because this entity-type relationship is managed in a specific way as part of a specific risk management program in place within the Credit Department. What we were finding was that each appraiser was risk rated similarly as part of the broader TPRM program; however, the Credit Department had a targeted risk management program in place to monitor this vendor type, which included more tailored monitoring based on the specific vendor type. Can the guidance provide clarity as to the option to handle oversight of specialty third-party types such as appraisers, law firms, or professional services firms outside of the scope of the TPRM when they are managed/monitored as part of a targeted risk management program specific to the specific entity type?
3. The Sound Practices to Strengthen Operational Resilience (federalreserve.gov) guidance uses the key term of "Critical Operations" vs. the proposed guidance which uses the term "Critical Activities." Key concepts appear to

be the same for both terms. Can this terminology be aligned to minimize the risk of redundant and potentially conflicting risk management programs within FIs?

4. Explanation of regulator expectations as to how organizations should measure concentration risk. When a 3rd party vendor is used for the FIs core system, along with its ancillary products, this presents a significant concentration risk, especially for a community bank. Adding explanations of expectations for measurement of concentration risk would allow organizations to build data models and reporting to help oversee and manage the concentration risks repeatedly mentioned in the guidance.
5. Guidance addresses expectation for organizations to reassess existing relationships periodically to subsequently determine if an activity/operation has become critical. Should there be more emphasis on having a change management process in place that more proactively addresses any changes in scope of the 3rd party relationship services? This would allow for an FI to gain this knowledge in real time rather than when it performs an annual risk assessment. If active monitoring is taking place, a periodic assessment may not be required. This should increase the effectiveness and efficiencies of the FI's TPRM program.
6. It would be helpful to address within the guidance the due diligence and ongoing monitoring of third parties whose overall operations are not deemed to be high risk, but who may be storing, accessing, or processing non-public personal information for the FIs, resulting in a critical activity. This component of a 3rd party vendor's activities can pose a significant potential reputation risk to an organization. The operational risk is likely minimal to low; however, the damage to the FI's reputation could potentially harm its ability to attract customers, meet its strategic plan, or attract human talent because of the public's lack of confidence in keeping NPPI secure. Adding an appendix that includes a standardized vendor security questionnaire, as well as developing standards for reviewing SOC-2 reports, would assist FIs to assess these vendor's activities. This is touched upon in FAQ #8 and would be useful within the guidance
7. Management and the Board have ultimate oversight of the TPRM program. Should FIs be encouraged as to reporting the status of the ongoing due diligence performed as part of the TPRM program to the Board on a quarterly, or more frequent basis? This would keep management and the Board aware of potential TPRM program concerns/issues. Appears in OCC FAQs and is recommended to be included in the proposed guidance.
8. Discussion of cloud-based risk assessment would be helpful for technology vendors offering software as a service (SaaS). It is in the OCC FAQs and is recommended to be included in the proposed guidance.
9. Organizations who work with third-party vendors which then subcontract with subsequent 3rd parties (e.g. fourth, fifth, sixth, etc.) do not allow FIs to review the contracts or SOC reports for these subcontracted parties, making it difficult to fully understand the relationships and the risks of these subcontractors. Depending on the criticality of the activity (e.g., accessing, processing or storing NPPI or Bank confidential data) performed by the subcontractor, there should be guidance offered in relation to the evaluation of the third-party's vendor risk management program controls to identify and manage risks associates with the third-party's subcontractors. Disclosure of the right to have access to the 3rd party's vendor oversight monitoring/reporting should be included in the contract with the vendor, and could be added to the contract section of the guidance. FIs should be evaluating the 3rd party vendor's processes for identifying and managing their third-party (i.e., subcontractor) risks, as well as the level of governance by an oversight body, such as the Board of Directors or Risk Committee.
10. Regarding how the guidance can help FIs to appropriately scale its 3rd party risk management practices, it is recommended that the guidance suggest categorizing vendors by industry types that, by nature, considered to be low risk, such as landscaping, office suppliers, caterers, facility contractors, and other vendors that would not be a critical part of FIs operations and are in no way able to gain access to NPPI, inadvertently or otherwise. This would reduce the need to do an initial vendor risk assessment, since each would be assigned the low risk level based on the specific industry type.

Thank you for the opportunity to comment.

Audrey Kirkhoff CPA CERP CFE
Chief Risk Officer
717.929.2254

309 N Ronks Rd
Bird-in-Hand, Pa 17505

BANK OF
Bird-in-Hand
a full service community bank

[redacted]