From: Matt Johnson <mjohnson@premierbankne.com>
Sent: Tuesday, August 31, 2021 12:10 PM
To: Comments
Subject: [EXTERNAL MESSAGE] July 19, 2021 - Proposed Interagency Guidance on Third-Party Relationships: Risk Management (RIN 3064-ZA26)

Dear Madam/Sir,

Based on Federal Register Vol 86, No 135 dated 19 July 2021, please see the information below in response for the request to comment on RIN 3064-ZA26.

Regards,
Matt

A. General

1. To what extent does the guidance provide sufficient utility, relevance, comprehensiveness, and clarity for banking organizations with different risk profiles and organizational structures? In what areas should the level of detail be increased or reduced? In particular, to what extent is the level of detail in the guidance's examples helpful for banking organizations as they design and evaluate their third-party risk-management practices?

The guidance provides flexibility for organizations to tailor to their unique attributes and risk profiles. The guidance could consider providing suggested criteria for organizations to determine inherent risks associated with their third-party risk management program. For example, criteria to evaluate overall third-party program risk could consider the following: degree of centralization/decentralization of the organization's vendor contract management and accounts payable functions; degree of centralization/decentralization of the organization's overall risk management program and/or maturity of the risk management related to third-party risk; maturity level of controls and processes for identifying third-party relationships and ensuring completeness of third-party relationships included in the third-party risk management program; level of reliance on third-parties to provide "critical activities"; the organization's overall or third-party risk appetite; level of insource vs. outsource for third party risk or overall risk management functions.

2. What other aspects of third-party relationships, if any, should the guidance consider?

Additional guidance could be considered for how the guidance distinguishes between related entities (e.g. affiliates, variable interest entities, related parties, etc.) and third-parties. Guidance could be included regarding ownership, controlling interests, or affiliations are to be managed differently as related entities or third parties. The guidance could expand on differing considerations for third parties with relations or affiliations with the organization (e.g. conflicts of interest, arm's length transactions, etc.). The guidance could consider indirect services provided to the organization's customers. For example, a Bank's customers could be involved with a data aggregator, where the Bank has not directly contracted for the services associated with data aggregators (e.g. Intuit providing data feeds from institutions to Quicken or QuickBooks). The guidance should also consider vendors' use of connectivity to the computing environment through application program interfaces or system accounts. As robotic process automation and artificial intelligence practices become more mainstream, the guidance should consider evaluation of the third-party's use of emerging technologies.

B. Scope

3. In what ways, if any, could the proposed description of third-party relationships be clearer?

Consider clarifying or providing examples of third-party relationships that can exist without a contract or remuneration. Providing additional guidance for organizations to identify and inventory third-party relationships would

help. For example, leveraging the organization's accounts payable information, contract management system, etc. as a source for ensuring the inventory of third-party relationships identified is complete and accurate. Depending on the nature of the business, additional information could be obtained by analyzing financial transactions on balance sheet or income statement accounts. Many organizations struggle with ensuring vendors in their third-party risk management programs are complete.

4. To what extent does the discussion of ''business arrangement'' in the proposed guidance provide sufficient clarity to permit banking organizations to identify those arrangements for which the guidance is appropriate? What change or additional clarification, if any, would be helpful?

Consider adding additional guidance of what constitutes a business arrangement and the application of the guidance to evaluate business arrangements. For example, PCI provides a process flow for identifying third parties in scope for PCI (page 5). Similarly, the guidance could provide a decision or process flow diagram by identifying the following elements: existence of a written contract; establishment of a verbal or informal agreement; monetary transfers; rights to goods or services; non-monetary economic benefits derived from the relationship; incurrence of monetary or non-monetary consequences for failure to deliver or perform; common ownership or related entities.

5. What changes or additional clarification, if any, would be helpful regarding the risks associated with engaging with foreign-based third parties?

Consider going away from the concept of 'foreign-based' third parties and focus the guidance on evaluating third parties subjected to different legal jurisdictions. For example, doing business with a third-party vendor in California could have more risk based on the California Consumer Privacy Act (CCPA). In addition, there is a trend for nations to join efforts to have regional or potentially global regulations (e.g. GDPR). Another consideration for evaluating risks with foreign based third parties could focus on if the third-party will access, store, or transmit protected information or if the foreign third-party will be remotely accessing information from the organization's domestic data centers. Additional guidance could be considered regarding domestic third parties that are subsidiaries of foreign entities or if there are foreign ownership interests associated with domestic third parties.

C. Tailored Approach to Third-Party Risk Management

6. How could the proposed guidance better help a banking organization appropriately scale its third-party risk management practices?

The guidance could consider having more information regarding categorization of vendors to manage the scale of the third-party risk management program. For example, banks could manage third parties classified as appraisers as a group instead of individually assessing each third-party appraiser. Guidance could be provided for including third parties in a category: same NAICS code; standard or substantially the same contractual agreements; similarities of duties to perform and consequences of non-performance. In addition, the guidance could consider presenting exceptions to grouping third parties into categories. For example, if an appraiser performs the majority of the bank's appraisals, where there would be a significant impact to the customers and to the bank's operations, the appraiser would not qualify for being managed in an overall category with other similar third-party vendors.

7. In what ways, if any, could the proposed guidance be revised to better address challenges a banking organization may face in negotiating some third-party contracts?

The FDIC could publish guidance for service providers or vendors' contractual agreements to achieve minimum standards established by the FDIC to be FDIC Third-Party Qualified Contracts. The qualifications requirements could be published by the FDIC for the minimum elements contracts must include to be FDIC Third-Party Qualified: scope; performance measures; responsibilities; right to audit; compliance with laws; confidentiality; operational resilience; insurance; termination; customer complaints; subcontracting. Many supervised institutions have problems ensuring vendors include certain provisions in the contract that allow the institution to perform its vendor oversight responsibilities. This would

help with contract negotiations since institutions could have a benchmark to indicate the vendor's contract is or is not qualified based on the FDIC minimum standards.

8. In what ways could the proposed description of critical activities be clarified or improved?

Consider providing considerations organizations can use for identifying critical activities based on the level of access within the organization's computing environment or pervasiveness of the third-party's access to sensitive information. For example, Target's HVAC vendor had pervasive access to Target's network. While the HVAC vendor might not rise to a critical level, implicit with the vendor's access permission level resulted in a critical operational impact. Specifically, the guidance should consider a subsection regarding guidance for engaging and managing risk associated outsourced IT and information security services (e.g. cloud providers, MSPs, MSSPs, etc.).

D. Third-Party Relationships

9. What additional information, if any, could the proposed guidance provide for banking organizations to consider when managing risks related to different types of business arrangements with third parties?

The guidance could be enhanced by providing information for organizations to establish and monitor key risk indicators for critical vendors. Often, it is challenging to quantify key risks associated with third-party vendors. Using key risk indicators could provide a measure of vendor risk using quantitative and qualitative inputs. Additional information on handing US governmental entities as third-party vendors (e.g. local, state, federal) that provide taxing authorities or governmental functions) could be provided. For example, banks must allow the FDIC, or other examiners empowered by law or regulation, access to sensitive, non-public information. Provided the governmental nature of the entities, the guidance could consider exclusion from scope of third-party risk management programs.

10. What revisions to the proposed guidance, if any, would better assist banking organizations in assessing third-party risk as technologies evolve?

The guidance could consider publishing a standard vendor technology risk questionnaire. For example, a standard list of questions for vendors to complete to measure the vendor's technology, business continuity, and cybersecurity risks. The burden on the vendors would be minimal since the same checklist could be used for the vendor's customers. Standard Information Gathering (SIG) questionnaires have helped; however, they have become complicated and could be tied to FIDC guidance more efficiently. The guidance should specify supervised institutions should supplement the standard vendor technology risk questionnaire based on how the supervised institution is connecting to the vendor, sensitivity of data, integration with internal or customer facing business operations, and other factors. The technology risk questionnaire could be periodically updated to continue evaluating the third-party vendor's use of emerging technologies.

11. What additional information, if any, could the proposed guidance provide to banking organizations in managing the risk associated with third party platforms that directly engage with end customers?

The guidance could reference FIL-55-2021, Authentication and Access to Financial Institution Services and Systems. While the importance of application interfaces, data aggregators, and customers' access to financial systems is paramount, including this in the third-party vendor risk management guidance could be duplicative. If the FDIC could provide a self-assessment template for third-party vendors who do or would like to do business with supervised institutions to complete, this would save both the vendor and the supervised institution time and resources.

12. What risk management practices do banking organizations find most effective in managing business arrangements in which a third party engages in activities for which there are regulatory compliance requirements? How could the guidance further assist banking organizations in appropriately managing the compliance risks of these business arrangements?

The best risk management practices are founded on establishing clear responsibilities and accountabilities with third-party vendors, agreed-upon measurements, and consequences for not achieving the agreed-upon measurements. Service level agreements have proven to be marginally ineffective to manage third-party vendor risk. For critical vendors, a higher degree of measuring both operational and compliance metrics should be employed to ensure vendors are held accountable for results. The guidance could introduce the concept of having compliance risk indicators to provide measurement and oversight for the execution of the third-party vendor's requisite compliance activities.

E. Due Diligence and Collaborative Arrangements

13. In what ways, if any, could the discussion of shared due diligence in the proposed guidance provide better clarity to banking organizations regarding third-party due diligence activities?

Shared due diligence could help alleviate the burden of third-party vendor risk management for both supervised institutions and third-party vendors. The guidance could include information on how the third-party vendor can demonstrate qualifications to do business with supervised institutions. The guidance should specify supervised institutions' responsibilities for evaluating third-party risks based on the institution's business model, controls, and risk appetite. For example, institutions using the same service with the same third-party vendor could have different risks management practices based on the institution's use of the vendor in its business operations or risk appetite. The guidance could consider setting standards for independent third-party risk management professionals performing standard due diligence and monitoring, allowing for multiple supervised institutions' reliance on the independent third-party.

14. In what ways, if any, could the proposed guidance further address due diligence options, including those that may be more cost effective? In what ways, if any, could the proposed guidance provide better clarity to banking organizations conducting due diligence, including working with utilities, consortiums, or standard setting organizations?

The guidance could provide alternatives for on-site visits to third-party vendors, often a large expense for supervised institutions with overseas third-party vendor operations. For example, the use of video conferencing to fulfill third-party risk management program requirements traditionally requiring a supervised institution's physical presence at the third-party vendor's operations. The proposed guidance could indicate how other risk management frameworks and due diligence or monitoring performed by independent parties or other customers of the third-party could be leveraged instead of supervised institutions performing separate, redundant third-party risk management diligence and monitoring.

F. Subcontractors

15. How could the proposed guidance be enhanced to provide more clarity on conducting due diligence for subcontractor relationships? To what extent would changing the terms used in explaining matters involving subcontractors (for example, fourth parties) enhance the understandability and effectiveness of this proposed guidance? What other practices or principles regarding subcontractors should be addressed in the proposed guidance?

The guidance should consider additional information for organizations to evaluate supply chain risks with their third-party vendors. Organizations who engage third-party vendors lack contractual privity with subcontractors or service providers engaged by third parties (e.g. fourth, fifth, sixth, etc. parties). The guidance could consider evaluating the third-party's vendor risk management program controls to identify and manage risks associates with the third-party's subcontractors. For example, evaluating the vendor's processes for identifying and managing third-party risks; level of oversight by the Board of Directors; etc.

16. What factors should a banking organization consider in determining the types of subcontracting it is comfortable accepting in a third-party relationship? What additional factors are relevant when the relationship involves a critical activity?

For critical activities, the guidance should consider the level of responsibility for supervised institutions' understanding of the third-party vendor's reliance and use of subcontractors. For example, evaluating if subcontractors access sensitive

data, lack of alternate subcontractors, lead time or risk to change subcontractors, subcontractor operations in foreign countries. The guidance should consider the third-party's use of subcontractors' impact on the supervised institution's reputational risks. For example, evaluating third-party vendor subcontractors to ensure operations or supply chains do not involved sanctioned countries, practices of questionable labor laws, and supply-chain risks.

G. Information Security

17. What additional information should the proposed guidance provide regarding a banking organization's assessment of a third party's information security and regarding information security risks involved with engaging a third party?

The guidance could consider practices associated with third-party vendor disengagement to ensue the third-party and the third-party's subcontractors properly destroy sensitive data obtained from the supervised institution. For example, many technology vendors use a shared tenant model, whereby supervised institutions do not have dedicated environments or separate storage areas for the institution's sensitive information. The guidance is generic regarding the destruction of sensitive information, where information can be retrieved from disposed technology equipment or shared storage devices that have not been overwritten. The guidance should consider having more information on the integration of the supervised institution and the third-party vendor's incident detection and management processes. For example, requiring more formal communications structures to ensure the supervised institution receives relevant information from third parties regarding potential security incidents.

H. OCC's 2020 FAQs

18. To what extent should the concepts discussed in the OCC's 2020 FAQs be incorporated into the guidance? What would be the best way to incorporate the concepts?

The best way to incorporate the FAQs would be to implement the concepts in appropriate sections of the guidance. Similar to the FFIEC Cybersecurity Assessment Tool, the guidance could consider developing inherent risk parameters for use of a third-party that can be compared to suggested controls to determine the intersection of inherent risks with third-party control maturity. The FFIC Cybersecurity Assessment Tool provides a good framework of generic controls ranging from maturities of baseline to innovative. Similar to cybersecurity, third-party risk management programs and controls could focus on similar generic risk management principles and have varying levels of maturity.

Matthew R. Johnson, CPA, CISSP, CISA

Senior Vice President & Chief Financial Officer
16802 Burke St.
Omaha, NE 68118
Phone: 402-715-4680
Cell: 402-212-6444
Fax: 402-715-4695
MJohnson@PremierBankNE.com

Our Mission:
To be the PREMIER community banking organization where employees, customers and shareholders can EXPECT MORE.