protiviti®
Face the Future with Confidence

Proposed U.S. Interagency Guidance on Third-Party Relationships: Leveling the Playing Field for Third-Party Risk Management Requirements

July 19, 2021

On July 13, 2021, the Federal Reserve Board (FRB), the Office of the Comptroller of the Currency (OCC) and the Federal Deposit Insurance Corporation (FDIC) released a joint request for comment to their *Proposed Interagency Guidance on Third-Party Relationships: Risk Management*. The agencies have issued this proposed guidance in response to industry feedback requesting alignment among the agencies' third-party risk management (TPRM) guidance. The deadline for comments to be submitted is September 17, 2021.

Based primarily on previous OCC releases on the same topic (including OCC Bulletin 2020-10, *Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29* and OCC Bulletin 2013-29, *Third-Party Relationships: Risk Management Guidance*), the proposed guidance would establish uniform assessment standards for the three regulators. However, it does not reference the supplemental examination procedures included in OCC Bulletin 2017-7, which leaves open the question of whether uniform examination procedures will be released once the proposed guidance is finalized or whether each of the three agencies will develop and maintain its own examination standards.

The request for comment primarily asks whether any of the concepts in the OCC 2020 FAQ should be incorporated further into the final guidance and whether additional information should be included that would be helpful for banking organizations. In our analysis, the proposed guidance does update the original OCC 2013-29 guidance with some of the key talking points included within the OCC FAQ, such as the usage of industry consortiums. However, a significant amount of the detailed examples discussed in the FAQ are omitted from the proposed guidance, including examples of relationship types with data aggregators. We would expect that some of the omitted details will be included in the final guidance to help clarify some of the initial challenges the OCC had to address, which was why they subsequently have had to release two FAQS and their examination procedures.

Key takeaways that banks can act on now

TPRM Lifecycle Considerations

- Operational, compliance, reputation, strategic and credit risk are called out specifically as factors to consider within the scope of a TPRM program. Concentration and foreign provider risks are mentioned elsewhere. While not stated explicitly, our expectation is that, as we have seen with several recent examinations, organizations should be ready to demonstrate how they are assessing these individual risk categories throughout their TPRM lifecycle, specifically within their inherent risk assessment and due diligence processes. This includes having specific questions that address each risk category and resulting ratings for each of these categories of risk.

- As noted in previous guidance from the agencies, due diligence should be risk-based and commensurate with the third-party risk profile. That said, the inclusion of risk acceptance is a fundamental concept that is highlighted in the proposed guidance where third parties may not be able to provide or meet specific organizational requirements. Banks should begin reviewing current TPRM practices to ensure risks are formally accepted when third parties do not meet documented standards during the due diligence process.

- The proposed guidance addresses the use of industry utilities or consortiums, as well as consulting with other banking organizations and engaging in joint due diligence and ongoing monitoring efforts. While it's no surprise that the proposed guidance allows for the use of these approaches to support due diligence and ongoing monitoring efforts, the key message is that these efforts still must meet the bank's established assessment criteria. This reaffirms that the industry utilities and data enrichment providers will continue to be key support mechanisms for many in the industry. However, an organization cannot rely solely on those mechanisms as their only means of due diligence and ongoing monitoring.

    - Of note, items within several due diligence categories, including Strategies and Goals, Fee Structure and Incentives, and Complaint Management (ongoing monitoring), will be difficult to outsource given the nature of the topic.

- The proposed guidance formalizes the concept of Know Your Vendor within the Legal and Regulatory Compliance section of Due Diligence. While the basic sanctions screening process has been expected for years, the guidance formalizes the need to understand the ownership structure, including any beneficial ownership (whether public or private, foreign or domestic) and key principals. Organizations should be looking to obtain this information, if they don't have it already, and include it within their ongoing customer screening processes and negative news alerts.

- While best practice for several years, the proposed guidance formalizes the expectation that for riskier relationships, the financial analysis should be as comprehensive as that required by financial institutions to make a third-party loan. Banks should begin reviewing their approach to financial analysis to confirm that more robust measures are in place for those third parties supporting critical activities.

Data and Infrastructure

- Organizations should be reviewing their current technology infrastructure data models and reporting to determine if they can meet the expectations as laid out in the Documentation and Reporting section of the proposed guidance. While the proposed requirements are standard for most TPRM tools, the proposed guidance includes an expectation to have an "analysis of costs associated with each activity or third-party relationship, including any indirect costs assumed by the banking organization" and the executed contracts. Contract management has been a long-time pain point in many banking organizations, so now is the time to address that based on the proposed guidance. Additional considerations include:

    - The concept of sub-contractors is highlighted throughout the proposed guidance. Organizations should review their TPRM data models to support the cross referencing of subcontractors across third parties. They also should tag those relationships that are both third parties as well as fourth parties via other third parties.

    - A key concept in the proposed guidance around contracting includes the need to assess contracts periodically to ensure they address the pertinent risks, controls and related legal protections. This effectively requires organizations to begin to collect contract data in a reportable format for key terms and

conditions to be able to evaluate and assess quickly potential impacts of key program and legal changes.

Program Governance

- Staffing and requisite skills are noted throughout the proposed guidance, with the intention of highlighting that there is no one-size-fits-all approach to how third-party risk is managed. Rather, it's more important to make sure the TPRM program has the right skill sets and experience in each role to be effective. This is especially important for due diligence and ongoing monitoring activities related to specific risk domains where the business, or centralized TPRM function, may not have the requisite knowledge to support the applicable activities. We expect that a key component of future examinations will be the skills and experience of those involved throughout the TPRM lifecycle. Banks should be prepared to demonstrate the requisite skill sets are in place to assess and manage the applicable risks.

Opportunities for Comment

The comment period provides an opportunity for the industry to seek additional clarity on several key points, including the following:

- The proposed guidance does not address a common industry question, which is whether specialty third-party types (e.g., law firms, appraisers, professional services firms) or affiliate relationships can be managed through targeted risk management programs specific to those entities but outside the broader TPRM program. We understand that each of these entity types is included within the broader scope; however, a significant number of banks try to manage these relationships in specific ways outside the scope of the TPRM program while following the same principles. It would be beneficial for the regulatory bodies to affirm in the proposed guidance whether this is acceptable.

- The proposed guidance presents an opportunity to align on definitions with a key concept of operational resilience. However, the proposed guidance still leverages "Critical Activities" terminology, while the Sound Practices to Strengthen Operational Resilience (federalreserve.gov) guidance uses "Critical Operations" as its key term. In our view, the regulatory bodies should align on this key term to minimize the risk of redundant and potentially conflicting risk management programs within organizations. The key concept is the same across both and it is

important to align on these terms to allow for organizations to train on this concept across their business units and risk management teams.

- Concentration risks remain a key topic within the proposed guidance. However, a common industry challenge remains unaddressed in that the proposed guidance does not explain the regulators' expectations for how organizations should measure concentration risk. Including these expectations would allow organizations to build data models and reporting to help oversee and manage those risks.

- The proposed guidance expects organizations to reassess existing relationships periodically to determine whether the nature of an activity subsequently becomes critical. While the guidance focuses on the critical concept, we believe it's important to have change management processes in place that address, in real time, changes in the scope of the overall third-party relationship. Fundamentally, a periodic reassessment shouldn't be required if active monitoring is taking place. If regulatory bodies are going to hold organizations accountable for an annual risk assessment, it would be helpful to clarify this within the proposed guidance. Additionally, while the proposed guidance calls out the ability to change the frequency and type of monitoring, including service-level agreement performance reports, it is important to note that those changes typically are only in place via contract amendments, and therefore, changes as described in the proposed guidance may not be as operationally easy to execute as noted.

In closing

While the proposed guidance reads very similar to previous OCC bulletins, given the interagency nature of this new guidance, one can expect renewed emphasis on third-party risk management in the near future. We recommend that organizations, especially those that are not regulated by the OCC, review the proposed guidance and begin to address these key considerations to address any gaps in their TPRM programs.

About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independent and locally owned Member Firms provide clients with consulting and managed solutions in finance, technology, operations, data, analytics, governance, risk and internal audit through our network of more than 85 offices in over 25 countries.

Named to the 2021 Fortune 100 Best Companies to Work For® list, Protiviti has served more than 60 percent of *Fortune* 1000 and 35 percent of *Fortune* Global 500 companies. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

protiviti®