WINSTON & STRAWN LLP

CLIENT ALERT

U.S. Federal Banking Regulators Release Final Interagency Guidance on Third-Party Risk Management

JUNE 14, 2023

Almost two years after their release of Proposed Interagency Guidance on Third-Party Risk Management, the Federal Deposit Insurance Corporation (FDIC), the Board of Governors of the Federal Reserve System (FRB), and the Office of the Comptroller of the Currency (OCC) (collectively, the agencies), on June 6, 2023, released final interagency guidance on the management of risks associated with third-party relationships. Importantly, and a result that will bring clarity and consistency for insured depository institutions and their financial technology (FinTech) partners, the final guidance rescinds and replaces each agency's existing guidance on third-party risk management. [1]

The guidance, which also became effective June 6, 2023, is designed to assist banking organizations with managing the risks associated with third-party relationships, including relationships with FinTech companies. Specifically, the guidance offers the agencies' views on sound risk management principles for banking organizations to consider when designing and implementing third-party risk management practices.

Takeaways from the Guidance

Third-party relationships have continued to multiply and evolve in the banking world, particularly with respect to bank-partnership programs between banks and FinTechs. Thus, it is no surprise that third-party risk management has become an increasing supervisory—and enforcement—focus of the agencies over the last few years.

While the guidance, by its own terms, "does not have the force and effect of law and does not impose any new requirements on banking organizations," in practice each agency (as the guidance *also* notes) will review its supervised banking organizations' risk management of third-party relationships as part of its standard supervisory processes, evaluating risks and the effectiveness of risk management to determine whether activities are conducted in a safe and sound manner and in compliance with applicable laws and regulations. Importantly, the guidance makes it clear that the agencies may pursue corrective measures, including enforcement actions, when necessary to address violations of laws and regulations or unsafe or unsound banking practices by the banking organization **or its third party.**

Accordingly, the Winston & Strawn LLP Financial Services team believes it is **critical** for financial institutions to design and implement sound risk management programs that are commensurate with the size, complexity, and risk profile of the banking organization, and the nature of its third-party relationships. This means developing and maintaining a comprehensive program that ensures the financial institution understands how each arrangement with a particular third party is structured in order to be able to assess the types and levels of risks posed, and to determine how to manage the third-party relationship accordingly.

Financial institutions or FinTechs with questions on the guidance, financial institutions that are looking to assess, develop, and/or enhance their third-party risk management programs, or FinTechs looking to understand their responsibilities and exposure when partnering with financial institutions, are encouraged to contact attorneys in the Financial Services Practice at Winston, who have both extensive in-house and external counsel experience in designing and implementing third-party risk management programs.

Summary of Key Points from the Guidance

Applicability and Scope

The guidance applies to any business arrangement[2] between a banking organization and another entity, by contract or otherwise. Consistent with the proposed guidance, the final guidance makes clear that a third-party relationship may exist even without a contract or remuneration.

The agencies specify that the guidance is intended to be broad-based to capture the full range of third-party relationships that could pose risks to banking relationships, especially as relationships may continue to evolve over time. The guidance includes the following nonexhaustive list of types of third-party relationships: outsourced services, use of independent consultants, referral arrangements, merchant payment processing services, services provided by affiliates and subsidiaries, and joint ventures. Within a footnote, the agencies additionally provide that the guidance is also relevant for situations in which a supervised banking organization provides services to another supervised banking organization.

Although the proposed guidance had generally excluded customer relationships from the definition of business arrangements, the final guidance removes that exclusion, explaining that some business relationships may incorporate elements or features of a customer relationship.

Tailored, Risk-Based Approach to Third-Party Risk Management

The overarching theme of the guidance is that banking organizations are expected to adopt sound risk management practices that are commensurate with the size, complexity, and risk profile of the banking organization, and the nature of its third-party relationships. To that end, banking organizations should ensure that they understand how each arrangement with a particular third party is structured in order to be able to assess the types and levels of risks posed, and to determine how to manage the third-party relationship accordingly.

The agencies indicate that banking organizations should engage in more comprehensive and rigorous oversight and management of third-party relationships that support higher-risk activities, including “critical activities.” The guidance acknowledges that activities that are considered critical by one banking organization may not be considered critical by another and leaves it to each banking organization to determine its critical activities and the third-party relationships that support those critical activities.

A few examples of characteristics of critical activities are provided in the guidance. Those are activities that: (1) cause a banking organization to face significant risk if the third party fails to meet expectations; (2) have significant customer impacts; or (3) have a significant impact on a banking organization’s financial condition or operations. The discussion on the proposed guidance notes that this list of examples differs from the list provided in the proposed guidance in that it is intended to remove imprecise concepts such as “significant investment” and “significant bank functions.” The discussion further reflects the agencies’ position that banking organizations can leverage definitions, approaches, and relevant terms and concepts applied in other relevant laws, regulations, and guidance to identify third-party relationships that support higher-risk activities, including critical activities.[3]

The agencies explain that, when applying classifications to third-party relationships, it is ultimately important (and constitutes a key element of effective risk management) for banking organizations to employ a "sound methodology" to identify the activities and third-party relationships that require more-comprehensive oversight.

Third-Party Relationship Risk Management Life Cycle

According to the agencies, effective third-party risk management generally follows a continuous life cycle through each of its stages: planning, due diligence and third-party selection, contract negotiation, ongoing monitoring, and termination. The guidance provides risk management principles applicable to each stage of the life cycle and purports to address several concerns, questions, and suggestions that had been raised by commenters to the proposed guidance, relating to topics such as:

- A banking organization's inability to obtain desired due diligence information from a third party.
- The use of collaborative efforts and shared due diligence among banking organizations to reduce the burdens of due diligence and supplement ongoing monitoring of third parties.
- The need for greater flexibility in certain contract negotiations.
- The level of oversight and risk management a banking organization should employ over its third parties' subcontractors.
- The scope and frequency of ongoing monitoring of third parties.

Ultimately, the steps taken by a banking organization throughout the life cycle should aim to ensure, among other things, that the third party: (1) can perform the activity in a manner consistent with its contractual obligations, and in compliance with the banking organization's policies and practices, strategic goals, objectives, risk appetite, and risk profile; (2) has the expertise, processes, and controls to enable the banking organization to remain in compliance with applicable laws and regulations; and (3) appropriately responds to any compliance issues (including violations of law or regulatory actions) with applicable supervisory agencies and self-regulatory organizations, as appropriate.

Governance

The guidance dedicates a section to governance over third-party risk management, which identifies the typical practices expected of banking organizations, commensurate with risk and complexity: oversight and accountability, independent reviews, and documentation and reporting.

- **Oversight and Accountability**. The agencies emphasize the importance of proper oversight of, and accountability for, banking organizations' third-party risk management processes for the entirety of the risk management life cycle. The guidance distinguishes between the responsibilities of a banking organization's board of directors and those of its management. From the agencies' perspective, management bears responsibility for developing and implementing third-party risk management policies, procedures, and practices. The board of directors, in turn, bears the responsibility to oversee the organization's third-party risk management processes and to hold management accountable. The guidance lists a number of factors that both the board and management should consider when fulfilling their respective responsibilities.
- **Independent Reviews**. The guidance indicates that banking organizations should conduct periodic independent reviews to determine the adequacy of their third-party risk management processes. To the extent a banking organization discovers issues or concerns through its reporting, it should identify and escalate those concerns to its board of directors, as appropriate.
- **Documentation and Reporting**. According to the agencies, banking organizations should maintain proper documentation and reporting concerning their third-party relationships. However, the agencies recognize that documentation and reporting will vary among organizations depending on the risk and complexity of their third-party relationships.

Supervisory Reviews of Third-Party Relationships

The final section of the guidance includes information on the nature and scope of the agencies' reviews of their supervised banking organizations' third-party risk management processes. The agencies indicate that they will each incorporate the review of third-party risk management processes as part of their standard supervisory processes. The reviews will focus on the effectiveness of a banking organization's third-party risk management process, and the scope of their reviews will be influenced by the degree of risk and complexity associated with a banking organization's activities and third-party relationships.

The agencies list a few factors that they will typically consider when performing their supervisory reviews, some of which include the ability of bank management to oversee its organization's third-party relationships, and the impact that third-party relationships have on the banking organization's risk profile and on the organization's compliance with applicable laws and regulations.

To the extent the agencies' reviews uncover material risks and deficiencies in their supervised banking organizations' risk management processes, the agencies note that they will take such steps as: (1) consulting with the banking organization's senior management and board of directors, as appropriate; (2) reviewing the banking organization's plan for remediation; and (3) considering their findings when assigning the components of the applicable rating system and highlighting the risks and deficiencies in their Report of Examination.

---

[1] FDIC's FIL-44-2008; OCC Bulletin 2013-29 and the frequently asked questions ("OCC FAQs") subsequently published in 2020; and the FRB's Supervisory Letter SR 13-19/CA 13-21. Notably, although the OCC FAQs have been formally rescinded, the agencies included several concepts from the OCC FAQs within the final guidance. Further, the release of the guidance prompted the FDIC to finally withdraw its proposed guidance on third-party lending, FIL-50-2016, that had been issued for comment in July 2016 and remained in proposed status ever since.

[2] The agencies note that the terms "business arrangement" and "third-party relationship" are synonymous in the guidance and are meant to be interpreted broadly.

[3] An example of potentially relevant guidance that the agencies mention in their discussion is the Interagency Paper on Sound Practices to Strengthen Operational Resilience.

8 Min Read

Related Locations

Charlotte | Miami | New York

Related Capabilities

Transactions | Financial Innovation & Regulation | Employee Benefits & Executive Compensation | Financial Services | FinTech, Banking & Payments

Related Regions

North America

Related Professionals

Juan Azel

Kobi Kennedy Brinson

Carl Fornaris

Jennifer Olivestone