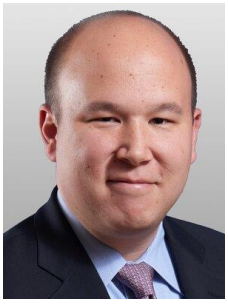
LAW360

Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Bank Agencies' 3rd-Party Risk Guidance: 6 Things To Know

By **Michael Nonaka, David Stein and Brandon Howell** (June 16, 2023, 10:57 AM EDT)


Michael Nonaka


David Stein


Brandon Howell

On Tuesday, June 6, the Board of Governors of the Federal Reserve System, Office of the Comptroller of the Currency and Federal Deposit Insurance Corp. issued final interagency guidance on managing risks associated with third-party relationships.

These risks include a bank's outsourced services, use of independent consultants, referral arrangements, fintech partnerships, merchant payment processing services, services provided by affiliates and subsidiaries, and joint ventures.

The final guidance represents the culmination of the agencies' efforts, which commenced formally in 2021, to outline consistent risk management principles for U.S. banking organizations to use in managing the risks associated with third-party relationships.

This final guidance rescinds and replaces the agencies' prior individual guidance on this topic.[1]

Compared to the agencies' proposed guidance, the final guidance includes more prescriptive detail in certain standards — e.g., due diligence and third-party selection and contract negotiation — and clarifying language emphasizing the risk-based and tailored approach that the agencies expect institutions to take in other standards, e.g., subcontracting and critical activities.

The precise impact of these changes will not become clear until banking organizations undergo examinations for third-party risk management practices and examination teams make judgments about how to apply the final guidance.

The final guidance is effective immediately as of June 6.

1. The final guidance remains principles-based and emphasizes the need for third-party risk management to be commensurate with risk.

The preamble to the final guidance indicates that commenters generally supported the proposed guidance and the use of a scalable, principles-based approach to third-party risk management.

A banking organization's risk management approach should be tailored to match the unique circumstances presented by the third-party relationship. The final guidance incorporates the same risk

management life cycle used in the proposed guidance: planning, due diligence and third-party selection, contract negotiation, ongoing monitoring, and termination.

Many of the changes adopted by the agencies were intended to streamline and clarify certain aspects of the final guidance. Examples of considerations for the various standards were added for illustrative purposes.

Also, the agencies made important clarifications requested by public commenters, including that:

- A banking organization's obligation vis-à-vis its third-party service providers' contractors, i.e., subcontractors, should focus on the third party's own processes for overseeing subcontractors and managing risks, rather than on the subcontractors themselves;

- A banking organization may have limited negotiating power with respect to certain third parties and therefore may be unable to insist upon the full complement of due diligence and contractual provisions set forth in the final guidance; and

- An activity that is critical for one banking organization may not be critical for all banking organizations.

2. The final guidance includes a section on governance to respond to public comment requesting better differentiation between board of directors and senior management roles with respect to third-party risk management.

The final guidance provides factors that are typically taken into account by a banking organization's board of directors in overseeing third-party risk management and the policies, procedures and practices implemented by senior management.

These factors include whether third-party relationships are managed in accordance with the organization's strategic goals and risk appetite and in compliance with laws and regulations.

The final guidance also identifies activities typically performed by management in carrying out its third-party risk management responsibilities, including integrating third-party risk management within the organization's overall risk management processes and providing that contracts with third parties are appropriately reviewed, approved and executed.[2]

The final guidance contains a subsection within the governance section on independent reviews.

Interestingly, compared to the proposed guidance's subsection on independent reviews, the agencies changed the phrasing of the subsection from "Banking organizations typically conduct periodic independent reviews of the third-party risk management process, particularly when third parties perform critical activities ..." to "[i]t is important for a banking organization to conduct periodic independent reviews to assess the adequacy of its third-party risk management processes."

This change in phrasing suggests that the agencies will expect or require banking organizations to have a process for conducting independent reviews of their third-party risk management processes.

The final guidance also deletes language in the proposed guidance specifying that an independent review may be performed by an internal auditor or independent third party.

3. The agencies rejected public commenters' attempts to streamline or reduce the due diligence provisions.

The proposed guidance's due diligence provisions "drew particular attention from commenters," with some raising concerns that the full range of diligence outlined in the proposed guidance was not feasible.

Commenters suggested various options for streamlining these provisions, including by facilitating collaboration among banking organizations and reliance on certifications, allowing for less stringent due diligence for certain third parties, and acknowledging shortcomings in accessing certain information.

In general, the agencies did not incorporate these suggestions. Instead, the agencies repeated their emphasis on the need to identify and evaluate the risks associated with each third-party relationship and to tailor risk management practices accordingly.

The final guidance's due diligence provisions are most susceptible to being converted into a mandatory checklist by agency examination teams. Banking organizations should pay attention to whether this due diligence guidance remains principles- and risk-based or begins to migrate to a mandatory checklist of requirements.

4. The agencies will offer additional resources for community banks to comply with the final guidance, although the content and timing for such resources are unclear.

Federal Reserve Gov. Michelle Bowman issued a statement of nonsupport for the final guidance because it is not accompanied by implementation aids or other tools designed to reduce the burden imposed on smaller banking organizations.

The Federal Reserve staff memorandum to the board of governors states that these additional resources will be offered in the future. Bowman criticized the final guidance for failing to provide the resources alongside the final guidance and failing to provide a timeline for such resources.[3]

5. The final guidance applies to bank-fintech partnerships and data aggregators.

The final guidance makes clear that the principles apply to a banking organization's relationship with a fintech company, stressing the need for a banking organization to understand how the arrangement with the fintech company is structured so that types and levels of risks can be assessed and controls can be implemented.

The final guidance also applies to data aggregators and states that the agencies are consulting with the Consumer Financial Protection Bureau with respect to the rulemaking required under Section 1033 of the Dodd-Frank Act pertaining to consumers' access to financial records.

6. Banking organizations should be prepared for greater supervisory focus on third-party relationships.

The final guidance applies to all banking organizations, regardless of an organization's size and complexity, and banking organizations should prepare for supervisory reviews focused on third-party risk management. The agencies enhanced the discussion in the final guidance's closing section on their

supervisory review practices for third-party relationships.

Although third-party risk management is already a standard supervisory consideration, the changes made to the final guidance indicate that banking organizations should expect a heightened focus on this area as the agencies incorporate the final guidance into their supervisory review activities.

For example, the final guidance states that examiners typically perform transaction testing or review results of testing to evaluate the third party's activities and compliance with applicable laws and regulations. With this express reference, it seems fair to expect greater reliance on transaction testing as part of the third-party risk management examination processes.

Even though the final guidance is intended to provide a uniform approach to third-party risk management examinations, the agencies' specific examination practices will continue to vary.

Michael Nonaka is a partner, David Stein is of counsel and Brandon Howell is an associate at Covington & Burling LLP.

[1] SR Letter 13-19/CA Letter 13-21, Guidance on Managing Outsourcing Risk (Dec. 5, 2013, updated Feb. 26, 2021); FIL-44-2008, Guidance for Managing Third-Party Risk (June 6, 2008); OCC Bulletin 2013-29, Third-Party Relationships: Risk Management Guidance, and OCC Bulletin 2020-10, Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29. The Final Guidance incorporates changes to reflect 15 of the 27 FAQs in OCC Bulletin 2013-29, which were an exhibit to the proposed guidance. The Final Guidance does not rescind and replace OCC Bulletin 2002-16, Bank Use of Foreign-Based Third-Party Service Providers: Risk Management Guidance (May 15, 2002).

[2] The Final Guidance acknowledges that there are many ways for banking organizations to structure their third-party risk management processes, observing that some organizations disperse third-party risk management among their business lines while others centralize processes under compliance, information security, procurement, or risk management functions.

[3] For the Agencies prior public resources, see Federal Reserve, Conducting Due Diligence on Financial Technology Companies: A Guide for Community Banks (Aug. 2021); Federal Reserve Publishes Paper Describing Landscape of Partnerships Between Community Banks and Fintech Companies (Sept. 9, 2021).