Federal Banking Agencies Extend Comment Period for Proposed Third-Party Risk Management Guidance

September 13, 2021

On July 19, 2021, the Board of Governors of the Federal Reserve System ("FRB"), Federal Deposit Insurance Corporation ("FDIC"), and the Office of the Comptroller of the Currency ("OCC" and together with the FDIC and FRB, the "Agencies") issued for comment proposed interagency guidance on managing the risks associated with third-party relationships ("Proposed Guidance").[1] The Proposed Guidance would apply to banking organizations supervised by the Agencies, regardless of size. On September 10, 2021, the Agencies extended the comment period by one month, from September 17, 2021 to October 18, 2021.

The Proposed Guidance is intended to provide "a framework based on sound risk management principles that banking organizations may use to address the risks associated with third-party relationships."[2] The Proposed Guidance would apply to any "business arrangement," including outsourcing arrangements, joint ventures and other ongoing relationships, with third parties or affiliates, potentially even when there is no contract or remuneration. The Proposed Guidance describes risk management processes for each stage in the life cycle of a third-party relationship, as well as governance and controls, including board of director and management oversight, applicable to all stages. Below, we provide a brief overview of the risk management processes and governance and control expectations outlined in the Proposed Guidance.

The Proposed Guidance "responds to industry feedback requesting alignment among the agencies with respect to third-party risk management guidance" and would replace each of the Agencies 'existing guidance.[3] The Proposed Guidance is based on, and largely tracks, the OCC's existing guidance contained in OCC Bulletin 2013-29, "Third-Party Relationships: Risk Management Guidance" ("Current OCC Guidance") and also is

---

1 "Proposed Interagency Guidance on Third-Party Relationships: Risk Management," 86 Fed. Reg. 38182 (Jul. 19, 2021), https://www.govinfo.gov/content/pkg/FR-2021-07-19/pdf/2021-15308.pdf.

2 86 Fed. Reg. at 38186.

3 FDIC, Press Release, Agencies Extend Comment Period on Proposed Risk Management Guidance for Third-Party Relationships (Sept. 7, 2021 10:30am ET), https://www.fdic.gov/news/press-releases/2021/pr21082.html?source=govdelivery&utm_medium=email&utm_source=govdelivery.

broadly consistent with, but more comprehensive and detailed than, the existing guidance of each of the FRB ("Current FRB Guidance") and the FDIC guidance ("Current FDIC Guidance").[4] For example, the Proposed Guidance would apply to a broader range of third-party relationships than does the Current FRB Guidance, which, by its terms, applies only to outsourcing arrangements.

The Proposed Guidance also is intended to respond to banking organizations' increasing use of third parties, especially financial technology-focused entities. The Agencies' requested comment on the extent to which content from the OCC's 2020 frequently asked questions to the Current OCC Guidance ("OCC FAQs"), which address the application of the Current OCC Guidance in light of technological innovations and new technology service providers (e.g., cloud computing providers, data aggregators), should be incorporated into the final version of the Proposed Guidance and appended to the OCC FAQs to the proposal.[5]

Risk-Based Tailoring and Compliance Implications

Although the Proposed Guidance describes extensive and detailed third-party risk management practices, the proposal also suggests that a banking organization should scale its third-party risk management program based on "its size, complexity and risk profile as well as the level of risk and number of third-party relationships."[6] Moreover, banking organizations should provide the most rigorous risk management and oversight of third-party relationships "that a banking organization relies on to a significant extent, relationships that entail greater risk and complexity, and relationships that involve critical activities. . . . "[7] The definition of "critical activities" is adapted from the Current OCC Guidance without significant revision and includes "significant bank functions" within the banking organization that "upon failure would result in a material loss of revenue, profit, or franchise value" and other activities that, whether performed internally or by a third party, implicate significant risk, require significant resource investment, or could have significant customer impacts.[8] Ostensibly, the Agencies ' promotion of risk-based tailoring of third-party risk management programs and practices indicates that they do not expect, as a matter of course, that a banking

---

4 *See* OCC Bulletin 2013-29, "Third-Party Relationships: Risk Management Guidance"; SR 13-19, "Guidance on Managing Outsourcing Risk"; FIL-44-2008, "Guidance on Managing Third-Party Risk."

5 OCC Bulletin 2020-10, "Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29."

6 86 Fed. Reg. at 38186.

7 *Id.* at 38184.

8 *Id.*

organization's third-party risk management practices include all of the processes described in the Proposed Guidance.

The Current FDIC Guidance and Current FRB Guidance similarly indicate that certain third-party relationships should be subject to greater oversight, although the factors for identifying such relationships do not overlap completely with those in the Proposed Guidance. For example, in FIL 44-2208, the FDIC indicates that "significant" third-party relationships include relationships that are new or involve new banking activities or where "the third party markets bank products or services."[9] The Current FRB guidance suggests that a banking organization's third-party risk management "focus on outsourced activities that . . . are critical to the institution's ongoing operations; involve sensitive customer information or new bank products or services; or pose material compliance risk."[10]

For banking organizations that are subject to the Current OCC Guidance or that manage their third-party risk management to the OCC's expectations as a best practice, the Proposed Guidance likely would not require significant changes from current risk management practices. The Proposed Guidance is nonetheless significant for these banking organizations because, among other things, it further solidifies and validates the granular supervisory expectations for risk management of third-party arrangements supporting "critical activities" outlined in the Current OCC Guidance. That the guidance would be interagency would seem to further diminish the likelihood of changes in the future because of the challenges associated with interagency rulemaking. For FRB- and FDIC-supervised banking organizations following the current guidance of their primary regulators, particularly those that outsource important functions (e.g., audit) and pursue partnerships, conformance with the Proposed Guidance may be a significant undertaking.

The Proposed Guidance clarifies that third-party risk management practices would be considered "when assigning the management component of the Federal Financial Institutions Examination Council's Uniform Financial Institutions Rating System."[11] Program deficiencies may be cited in examination reports as unsafe or unsound banking practices and result in informal or formal enforcement actions.

As the Proposed Guidance states: "[a]s the banking industry becomes more complex and technologically driven, banking organizations are forming more numerous and more

---

[9] FDIC, FIL-44-2008, Third-Party Risk Guidance for Managing Third-Party Risk (Jun. 6, 2008), https://www.fdic.gov/news/financial-institution-letters/2008/fil08044a.html.

[10] FRB, SR 13-19, Guidance on Managing Outsourcing Risk (Dec. 5, 2013), https://www.federalreserve.gov/supervisionreg/srletters/sr1319a1.pdf.

[11] 86 Fed. Reg. at 38195.

complex relationships with other entities to remain competitive, expand operations, and help meet customer needs."[12] The finalization of the Proposed Guidance would be important to banking organizations as they continue to expand their use of third parties, particularly financial technology-focused entities, to provide services to customers.

Overview of the Proposed Guidance

Stages of the Third-Party Risk Management Lifecycle

Below we summarize each stage of the third-party risk management lifecycle outlined in the Proposed Guidance, which closely tracks the Current OCC Guidance. The Current FDIC Guidance and Current FRB Guidance organize expectations for risk management processes into categories similar to the stages identified below.

Planning

- The Proposed Guidance suggests that, before entering into a third-party relationship, a banking organization develop a plan that "outlines the banking organization's strategy, identifies the inherent risks of the activity with the third party, and details how the banking organization will identify, assess, select, and oversee the third party."[13]

- The Proposed Guidance describes 11 "factors" or areas that "[a] banking organization typically considers" in planning for a third-party relationship, including, among other factors, the risks, complexity, costs, information security implications, and strategic purpose of the third-party relationship and its potential impacts on other strategies, employees, and customers.[14] A banking organization also considers its ability to manage and monitor the relationship and outlines contingency plans.

- The Proposed Guidance suggests that plans involving critical activities may be presented to and approved by the board.

Due Diligence and Third-Party Selection

- The Proposed Guidance describes 16 "factors" that, among other factors, a banking organization "typically considers" when evaluating a third party during the due diligence stage,[15] including the third party's strategies and goals, legal and regulatory

---

[12] *Id.* at 38187.
[13] *Id.* at 38185.
[14] *Id.* at 38188.
[15] *Id.* at 38189.

compliance, financial condition, business experience, fee structure and incentives, leadership, risk management, information security, management of information systems, operational resilience, incident reporting and management programs, physical security, insurance coverage, and potentially conflicting contractual arrangements with other parties.

- These areas closely track the areas outlined in the Current OCC Guidance, with certain additions. For example, consistent with the OCC FAQs, the Proposed Guidance addresses situations in which a banking organization "may not be able to obtain the desired due diligence information from the third party" and advises banking organizations to "identify limitations understand the risks, consider how to mitigate the risks, and determine whether the residual risks are acceptable."[16] The Proposed Guidance also suggests, alternative ways to assess a third party's likely financial condition when the third party does not have a long operational history by, for example, considering a third party's "expected growth, earnings, pending litigation, unfunded liabilities, or other factors that may affect the third party's overall financial stability."[17] Finally, as discussed in the OCC FAQs, the Proposed Guidance suggests that banking organizations consider cooperating with each other to supplement or enhance their respective due diligence efforts, but notes that any coordination would need to comply with antitrust laws.

- The Proposed Guidance clarifies that the "degree of due diligence should be commensurate with the level of risk and complexity of each third-party relationship."[18] Management would be expected to present the results of its due diligence to the board "when making recommendations to use third parties that involve critical activities."[19]

Contract Negotiation

- The Proposed Guidance describes 18 areas or contract terms that a banking organization typically focuses on when negotiating a written contract with a third party, including, among others, performance measures or benchmarks; responsibilities for providing, receiving, and retaining information; rights to audit and require remediation; responsibility for compliance with applicable laws and regulations; use of the banking organization's information, technology, and intellectual property; confidentiality and information security; operational resilience and business continuity; indemnification and insurance; limits on liability; handling

---

16 *Id.*

17 Id at 38189.

18 *Id.*

19 *Id.* at 38194.

of customer complaints; subcontracting; and choice-of-law and jurisdictional provisions when the third party is based outside of the United States.[20]

- The Proposed Guidance advises that the board, or a committee thereof, should approve contracts involving critical activities before their execution.

Ongoing Monitoring

- The Proposed Guidance outlines 13 factors that, among others, a banking organization typically considers for the ongoing monitoring of a third-party relationship. Monitoring includes assessing the third party's controls, and testing the banking organization's controls.

- The Proposed Guidance indicates that the extent of monitoring should be risk-based and typically includes adjusting monitoring as the level and types of risks presented by a relationship change over time.

- The Proposed Guidance suggests that significant issues should be escalated to the board of directors. The board also should review "the results of management's ongoing monitoring of third-party relationships involving critical activities" and confirm that management is "[taking] appropriate actions to remedy significant deterioration in performance or address changing risks or material issues identified through ongoing monitoring."[21]

Termination

- The Proposed Guidance outlines five factors that, among others, a banking organization typically considers when developing contingency plans and planning for terminating a third-party relationship. For example, a banking organization would be expected to consider "[c]apabilities, resources, and the time frame required to transition the activity while still managing legal, regulatory, customer, and other impacts that might arise" and "[r]isks to the banking organization if the termination happens as a result of the third party's inability to meet expectations."[22]

Oversight and Accountability

The Proposed Guidance describes oversight and accountability measures for a banking organization's third-party risk management program and the risk management of individual relationships, including board of directors and management responsibilities, documentation and reporting, and independent reviews. Although the Proposed

---

[20] *Id.* at 38191.

[21] *Id.* at 38193.

[22] *Id.* at 38195.

Guidance organizes these expectations in their own lifecycle stage, between contract negotiation and ongoing monitoring, they are applicable throughout the third-party risk management lifecycle.

Board of Director Responsibilities

The Proposed Guidance states that the board of directors is responsible for "overseeing the management of risks associated with third-party relationships" and describes six duties, including approving third-party risk management policies, the duties identified above relating to third-party relationships involving critical activities (e.g., approval of contracts), and generally overseeing the operation of the risk management program. [23]

The Proposed Guidance would represent a change in direction in terms of the FRB's supervisory expectations for board oversight of third-party relationships. As part of a broader initiative to focus supervisory expectations for the board on the board's core responsibilities, the FRB recently revised the Current FRB Guidance to remove explicit responsibilities assigned to the board, including the responsibility to approve outsourcing policies.[24] As such, the Current FRB Guidance does not include specific expectations for the board, other than that the board should receive from senior management "sufficient information about outsourcing arrangements so that [they] can understand the risks posed by these arrangements."[25]

The Current FDIC Guidance includes responsibilities for the board that generally align with the Proposed Guidance, including receiving reporting on management's risk assessment, approving contracts with significant third-party relationships and receiving reports on management's ongoing monitoring of third-party relationships.

Management Responsibility

The Proposed Guidance provides that "management is responsible for implementing third-party risk management" and describes 12 duties typically considered by management in executing and implementing third-party relationship risk management strategies and policies, including establishing responsibility and accountability for managing third parties

In various sections, the Proposed Guidance stresses the importance of appropriately staffing the functions responsible for third-party risk management activities.[26] Indeed, the Proposed Guidance notes that all "phases of the third-party risk management life

---

[23] *Id.* at 38193.

[24] FRB, SR 21-4, Inactive or Revised SR Letters Related to the Federal Reserve's Supervisory Expectations for a Firm's Board of Directors (Feb. 26, 2021), https://www.federalreserve.gov/supervisionreg/srletters/SR2104.htm.

[25] SR 13-19 at 2.

[26] 86 Fed. Reg. at 38194.

cycle . . . be performed by those with the requisite knowledge and skills" and that "[a] banking organization may involve experts across disciplines, such as compliance, risk, or technology officers, legal counsel[.]"[27] These expectations generally align with each of the Agencies' current guidance.

The Proposed Guidance indicates that banking organizations may use "external support where helpful to supplement the qualifications and technical expertise of in-house staff"[28] but notes that "[u]se of such external services does not abrogate . . . the responsibility of management to handle third-party relationships in a safe and sound manner and consistent with applicable laws and regulations."[29] None of the current guidance addresses the use of external support to supplement in-house staff.

Independent Reviews

The Proposed Guidance provides that banking organizations typically conduct internal audits or commission third-party audits of risk management processes, especially where a third party performs critical activities. "The results of independent reviews may be used to determine whether and how to adjust the banking organization's third-party risk management process, including policy, reporting, resources, expertise, and controls."[30]

Documentation and Reporting

The Proposed Guidance states that proper documentation and reporting "facilitate the accountability, monitoring, and risk management associated with third parties and will vary among organizations depending on their size and complexity."[31] Documentation and reports identified in the Proposed Guidance include approved plans for engaging third parties, due diligence results, executed contracts, risk management reports and reports of service disruptions or security breaches.

* * *

[27] *Id.* at 38188.

[28] *Id.*

[29] *Id.* at 38189.

[30] *Id.* at 38194.

[31] *Id.* at 38194.

Please do not hesitate to contact us with any questions.

NEW YORK

Gregory J. Lyons
gjlyons@debevoise.com

Caroline Novogrod Swett
cnswett@debevoise.com

Courtney Bradford Pike
cbpike@debevoise.com

WASHINGTON, D.C.

Satish M. Kini
smkini@debevoise.com