Davis Polk

Proposed interagency guidance on risk management of third-party relationships

August 20, 2021 | Client Update | 19-minute read

The Federal Reserve, FDIC and OCC jointly issued proposed guidance on banking organizations' risk management of third-party relationships. The proposed interagency guidance would replace existing third-party risk management guidance that was issued separately by each agency. Our client update summarizes the proposal and explains how it builds on, and deviates from, the existing guidance.

Background

On July 13, 2021, the Board of Governors of the Federal Reserve System (Federal Reserve), the Federal Deposit Insurance Corporation (FDIC), and the Office of the Comptroller of the Currency (OCC, and together with the Federal Reserve and the FDIC, the Agencies), requested comments on proposed interagency guidance on how banking organizations should manage the risk associated with their third-party relationships (the Proposed Guidance). Comments on the Proposed Guidance are due by September 17, 2021.

If adopted, the Proposed Guidance would replace the Agencies' existing, separate third-party risk management guidance:

- 2008 FDIC guidance titled "Guidance for Managing Third-Party Risk" (the FDIC Guidance);
- 2013 Federal Reserve guidance titled "Guidance on Managing Outsourcing Risk (the Federal Reserve Guidance); and
- 2013 OCC guidance titled "Third-Party Relationships: Risk Management Guidance" (the OCC Guidance).

As a result, the Proposed Guidance would harmonize the third-party risk management expectations for banking organizations supervised by the FDIC, Federal Reserve and OCC. The Proposed Guidance represents a joint effort by the Agencies to respond to the continued and growing prevalence of relationships between banking organizations and third parties, including both traditional outsourcing relationships with service providers and partnership arrangements with financial technology (fintech) companies.

The Proposed Guidance is broadly consistent with the Agencies' existing guidance. Like the Agencies' existing guidance, the Proposed Guidance emphasizes that a banking organization is ultimately responsible for conducting its activities—including activities conducted through a third party—in a safe and sound manner. In addition, like the Agencies' existing guidance, the Proposed Guidance provides that a banking organization should adopt risk management practices that are commensurate with the risk posed by its third-party relationships. Further, the risk management life cycle outlined in the Proposed Guidance—with planning, due diligence, contract negotiation, monitoring and termination phases—is generally consistent with the frameworks outlined in the Agencies' existing guidance.

Practically speaking, banking organizations that currently adhere to applicable Agency guidance, and particularly banking organizations with mature compliance and third-party risk management processes and policies, would likely need make relatively minimal updates to their third-party risk management frameworks to ensure adherence to the Proposed Guidance. For smaller institutions that are currently subject to the Federal Reserve or FDIC Guidance, which is generally less prescriptive and detailed than the Proposed Guidance and the OCC Guidance on which it is based, the Proposed

Guidance may represent a more meaningful change.

The issuance of the Proposed Guidance and associated request for comment may signal that third-party risk management is an area of increasing supervisory focus for the Agencies. The Proposed Guidance concludes by explaining that "[a] banking organization's failure to have an effective third-party risk management process that is commensurate with the level of risk, complexity of third-party relationships, and organizational structure of the banking organization may be an unsafe or unsound practice." It further explains that the Agencies may "pursue appropriate corrective measures, including enforcement actions, to address violations of law and regulations or unsafe or unsound banking practices by the banking organization or its third party."

Proposed interagency guidance

Scope of third-party relationships

Like the existing OCC Guidance on which it is modeled, the Proposed Guidance broadly defines a third-party relationship as "any business arrangement between a banking organization and another entity, by contract or otherwise." Such relationships "may exist despite a lack of a contract or remuneration" and "can include relationships with entities such as vendors, fintech companies, affiliates, and the banking organization's holding company." According to the Proposed Guidance, the term "business arrangement" is "meant to be interpreted broadly," but "third-party business arrangements generally exclude a banking organization's customers."

The scope of relationships covered by the Proposed Guidance is broader than that of the Federal Reserve Guidance, which is limited to outsourcing relationships with service providers and so would not necessarily apply to, for example, partnership arrangements with fintechs.

Tailored approach

Consistent with the approach of the Agencies' existing guidance, the Proposed Guidance explains that "[a] banking organization's third-party risk management program should be commensurate with its size, complexity, and risk profile as well as with the level of risk and number of the banking organization's third-party relationships."

According to the Proposed Guidance, banking organizations should devote the most "comprehensive and rigorous oversight and management of third-party relationships that support 'critical activities.'" Critical activities are defined in the Proposed Guidance as "significant bank functions" (i.e., "any business line of a banking organization, including associated operations, services, functions, and support, that upon failure would result in a material loss of revenue, profit, or franchise value") or other activities that:

- "could cause a banking organization to face significant risk if the third party fails to meet expectations;
- could have significant customer impacts;
- require significant investment in resources to implement the third-party relationship and manage the risk; or
- could have a major impact on bank operations if the banking organization has to find an alternate third party or if the outsourced activity has to be brought in-house."

This proposed definition of critical activities differs slightly from the OCC Guidance, which has the same four prongs, but applies those prongs to "significant bank functions (e.g., payments, clearing, settlements, custody) or significant shared services (e.g., information technology), or other activities."

Neither the Federal Reserve Guidance nor the FDIC Guidance uses the term "critical activities" or a similar defined term. The Federal Reserve Guidance states that a banking organization's third-party risk management program should "focus on outsourced activities that have a substantial impact on a financial institution's financial condition; are critical to the institution's ongoing operations; involve sensitive customer information or new bank products or services; or pose material compliance risk." The FDIC Guidance states that "[a] third-party relationship should be considered significant if the institution's relationship with the third party is a new relationship or involves implementing new bank activities; the relationship has a material effect on the institution's revenues or expenses; the third party performs critical functions; the third party stores, accesses, transmits, or performs transactions on sensitive customer information; the third party markets bank products or services; the third party provides a product or performs a service involving subprime lending or card payment transactions; or the third party poses risks that could significantly affect earnings or capital." As a result, the Proposed Guidance would require Federal Reserve- and FDIC-supervised banking organizations to apply a new

approach to identifying their most important third-party relationships.

Stages of the third-party risk management life cycle

The Proposed Guidance reflects the same five-stage continuous third-party risk management life cycle as the existing OCC Guidance: (1) planning; (2) due diligence and third-party selection; (3) contract negotiation; (4) ongoing monitoring; and (5) termination. The Proposed Guidance also reflects the same three principles as the OCC Guidance that apply throughout the life cycle: (1) oversight and accountability; (2) documentation and reporting; and (3) independent reviews. [1] This organizational framework differs from the Federal Reserve and FDIC Guidance, which outline core elements of an effective third-party risk management program rather than stages of a continuous life cycle, but the content of the risk management activity under the Proposed Guidance is still broadly consistent with those elements.

Planning

According to the Proposed Guidance, before entering into a third-party relationship, a banking organization should "evaluate the types and nature of risks in the relationship and develop a plan to manage the relationship and its related risks." Greater advance planning is required for certain third-party relationships, including those involving critical activities.

The Proposed Guidance outlines various factors that a banking organization should consider in planning for a third-party relationship, including, among other factors, the risks, complexity, and financial impact of the business arrangement; the potential impact of the arrangement on the organization's other strategic initiatives, employees, customers; and the organization's ability to provide adequate oversight and management of the relationship on an ongoing basis. In the existing Federal Reserve and FDIC Guidance, the first step of the recommended third-party risk management process is a "risk assessment" that is broadly similar to the planning phase described in the Proposed Guidance.

Due diligence and third-party selection

According to the Proposed Guidance, before selecting and entering into any relationship with a third party, a banking organization should conduct due diligence commensurate with the risk and complexity of the relationship. A banking organization should conduct more extensive due diligence on a third-party relationship that is higher risk or that involves critical activities. If the banking organization cannot obtain the desired information in the diligence process, it should identify limitations, understand the risks, consider how to mitigate the risks, and determine whether the residual risks are acceptable. The Proposed Guidance contemplates the use of external services, industry utilities, or consortiums, as well as coordination with other banking organizations, when conducting due diligence.

The Proposed Guidance states that a banking organization typically considers the following factors (each of which is described in further detail in the Proposed Guidance) when conducting due diligence on a third party with which it may enter into a relationship:

- the third party's overall business strategy and goals;
- the third party's ownership structure and legal and regulatory compliance capabilities;
- the third party's financial condition (including via review of audited financial statements and other filings);
- the third party's depth of resources and prior business experience;
- the third party's fee structure and incentives;
- the qualifications and backgrounds of the third party's principals;
- the effectiveness of the third party's own risk management;
- the third party's information security program;
- the third party's management of information systems, particularly those that will be used to support the relationship;
- the third party's operational resilience in the face of potential disruptions and hazards;
- the third party's incident reporting and management programs;
- the third party's physical security and environmental controls;
- the third party's human resource management, including training;

- the degree to which the third party relies on subcontractors;
- the scope of the third party's insurance coverage; and
- any conflicting contractual arrangements that the third party has entered into with other parties.

The Proposed Guidance mirrors the OCC Guidance in terms of enumerated areas that banking organizations should focus on during the due diligence process, but reflects some additional expectations for certain areas for due diligence. For example, with respect to reviewing a third party's legal and regulatory compliance capabilities, the Proposed Guidance reflects an expectation that banking organizations will "[c]onsider whether the third party has identified, and articulated a process to mitigate, areas of potential consumer harm, particularly in which the third party will have direct contact with the bank's customers, develop customer-facing documents, or provide new, complex, or unique products." The list of due diligence topics in the Proposed Guidance is more extensive than in the existing Federal Reserve Guidance and FDIC Guidance. New topics include the third party's fee structure and incentives, incident reporting and management programs, and degree of physical security and environmental controls.

There are other differences in the due diligence process described in the Proposed Guidance and the Agencies' existing guidance. For example, the Agencies' existing guidance does not expressly contemplate coordination and cooperation among banking organizations on the due diligence of third parties. And unlike the FDIC Guidance, which states that due diligence "should also be performed periodically during the course of the relationship, particularly when considering a renewal of a contract," the Proposed Guidance focuses squarely on due diligence to be conducted before selecting and entering contracts or relationships. Overall, however, the due diligence process recommended in the Proposed Guidance is broadly consistent with the Agencies' existing guidance.

Contract negotiation

Negotiation of the contract that governs the anticipated relationship is the third step in the life cycle described in the Proposed Guidance. Where a banking organization is unable to negotiate for contractual terms that it desires, the banking organization should evaluate whether the contract would satisfy its needs or result in an unacceptable level of risk.

The Proposed Guidance reflects heightened expectations for particularly important contracts. A banking organization's board of directors (or a committee thereof) should be aware of and pre-approve contracts involving critical activities. According to the Proposed Guidance, "a material or significant contract with a third party typically prohibits assignment, transfer, or subcontracting by the third party of its obligations to another entity without the banking organization's consent," implying that a material contract that does not contain such prohibitions could be problematic from the Agencies' perspective.

The Proposed Guidance states that a banking organization typically considers the following factors (each of which is described in further detail in the Proposed Guidance) when negotiating a contract with a third party:

- the nature and scope of the arrangement, include any ancillary services to be provided;
- measures or benchmarks used to assess performance under the contract;
- responsibility for providing, receiving and retaining information;
- the banking organization's rights to audit, monitor performance, and require remediation of identified issues;
- responsibility for compliance with applicable laws and regulations;
- cost, compensation, and methods for the calculation thereof;
- ownership and license of the banking organization's information, technology, and intellectual property;
- confidentiality and integrity of the banking organization's information;
- operational resilience and business continuity in the event of problems affecting the third party's operations;
- indemnification clauses;
- the third party's insurance coverage;
- the dispute resolution process;
- limitations on the third party's potential liability;
- default and termination provisions;

- responsibility for responding to customer complaints;
- whether the third party may engage subcontractors;
- in the case of foreign-based third parties, choice-of-law and jurisdictional provisions; and
- where applicable, provisions stipulating that the performance of activities by the third party for the banking organization is subject to regulatory examination oversight.

The Agencies' existing guidance recommends that banking organizations focus on a very similar set of factors during contract negotiations with a third party, and the Proposed Guidance is therefore generally consistent with the existing guidance on contract negotiation. The Proposed Guidance does, however, reflect some heightened or more prescriptive expectations for specific contractual provisions as compared to the Agencies' existing guidance. For example, the Proposed Guidance states that a banking organization's contract with a third party should address the third party's procedures for notifying the banking organization *immediately* in the event that a service disruption, security breach, compliance lapse, enforcement action, regulatory proceeding, or other event poses a significant risk to the banking organization. This is more prescriptive than any of the Agencies' existing guidance. The OCC Guidance addresses a similar scope of notifications but does not reflect any timing expectation for those notifications. The Federal Reserve Guidance only addresses notifications of breaches involving the disclosure of non-public personal information and notifications of contractual events of default. The FDIC Guidance addresses notifications of contractual events of default and states that management should "consider" requiring exception-based reports from third parties "that would serve as notification of any changes or problems that could affect the nature of the relationship or pose a risk to the financial institution."

Ongoing monitoring

The Proposed Guidance explains that ongoing monitoring is "an essential component" of third-party risk management. Like other aspects of third-party risk management, the Proposed Guidance states that monitoring should be commensurate with the level of risk and complexity of a third-party relationship, and the degree of monitoring may need to be re-calibrated over time based on changed circumstances.

The Proposed Guidance states that a banking organization typically considers the following factors in conducting its ongoing monitoring of a third party:

- evaluate the overall effectiveness of the third-party relationship and the consistency of the relationship with the banking organization's strategic goals;
- assess changes to the third party's business strategy, legal risk, and its agreements with other entities that may pose conflicting interests, introduce risks, or impact the third party's ability to meet contractual obligations;
- evaluate the third party's financial condition and changes in the third party's financial obligations to others;
- review the adequacy of the third party's insurance coverage;
- review relevant audits and other reports from the third party, and consider whether the results indicate an ability to meet contractual obligations and effectively manage risks;
- monitor for compliance with applicable legal and regulatory requirements;
- assess the effect of any changes in key third party personnel involved in the relationship with the banking organization;
- monitor the third party's reliance on, exposure to, performance of, and use of subcontractors, as stipulated in contractual requirements, the location of subcontractors, and the ongoing monitoring and control testing of subcontractors;
- determine the adequacy of any training provided to employees of the banking organization and the third party;
- review processes for adjusting policies, procedures, and controls in response to changing threats and new vulnerabilities and material breaches or other serious incidents;
- monitor the third party's ability to maintain the confidentiality and integrity of the banking organization's systems and information, including the banking organization's customers' data if received by the third party;
- review the third party's business resumption contingency planning and testing and evaluate the third party's ability to respond to and recover from service disruptions or degradations and meet business resilience expectations; and

– evaluate the volume, nature, and trends of consumer inquiries and complaints and assess the third party's ability to appropriately address and remediate inquiries and complaints.

Termination

Finally, the Proposed Guidance notes that where a banking organization terminates a third-party relationship, management should do so in an efficient manner and consider how to transition services by bringing them in-house or contracting with another third party.

The Proposed Guidance states that in preparing for termination of a third-party relationship, a banking organization typically considers the following factors:

– capabilities, resources, and the time frame required to transition the activity while still managing legal, regulatory, customer, and other impacts that might arise;

– potential third-party service providers to which the services could be transitioned;

– risks associated with data retention and destruction, information system connections and access control issues, or other control concerns that require additional risk management and monitoring during and after the end of the third-party relationship;

– handling of joint intellectual property developed during the course of the business arrangement; and

– risks to the banking organization if the termination happens as a result of the third party's inability to meet expectations.

The discussion of termination preparation in the Proposed Guidance is broadly similar to that in the existing OCC Guidance, but differs from the Federal Reserve and FDIC Guidance, which both address termination procedures in the context of contract negotiation but not as a standalone stage of the risk management life cycle. As such, when compared to the Federal Reserve and FDIC Guidance, the Proposed Guidance is more prescriptive regarding termination of a third-party relationship.

Expectations throughout the risk management life cycle

Oversight and accountability

The Proposed Guidance would provide that a banking organization's management and board of directors are responsible for implementing third-party risk management processes and for overseeing the overall risk management framework, respectively. As described further below, with respect to oversight and accountability, the Proposed Guidance outlines: (1) the responsibilities of the board of directors; (2) the responsibilities of management; (3) expectations for independent reviews of third-party risk management processes; and (4) expectations for documentation and reporting.

The Proposed Guidance is more prescriptive on this topic than the existing Federal Reserve and FDIC Guidance. For example, the Proposed Guidance distinguishes the responsibilities of the board of directors and management in far more detail than existing guidance.

Board of directors

In overseeing the management of risks arising from the third-party relationships, boards of directors of banking organizations typically consider:

– confirming that risks related to third-party relationships are managed in a manner consistent with the banking organization's strategic goals and risk appetite;

– approving the banking organization's policies that govern third-party risk management;

– approving, or delegating to, an appropriate committee reporting to the board, approval of contracts with third parties that involve critical activities;

– reviewing the results of management's ongoing monitoring of third-party relationships involving critical activities;

- confirming that management takes appropriate actions to remedy significant deterioration in performance or address changing risks or material issues identified through ongoing monitoring; and
- reviewing results of periodic independent reviews of the banking organization's third-party risk management process.

Management

In carrying out third-party relationship risk management, management of a banking organization typically considers:

- developing and implementing the banking organization's third-party risk management process;
- confirming that appropriate due diligence and ongoing monitoring is conducted on third parties and presenting results to the board when making recommendations to use third parties that involve critical activities;
- reviewing and approving contracts with third parties;
- providing appropriate organizational structures, management, and staffing (in terms of level and expertise);
- confirming that third parties comply with the banking organization's policies and reporting requirements;
- providing that third parties be notified of significant operational issues at the banking organization that may affect the third party;
- confirming that the banking organization has an appropriate system of internal controls and regularly tests the controls to manage risks associated with third-party relationships;
- confirming that the banking organization's compliance management system is appropriate to the nature, size, complexity, and scope of its third-party business arrangements;
- providing that third parties regularly test and implement agreed-upon remediation when issues arise;
- escalating significant issues to the board;
- terminating business arrangements with third parties that do not meet expectations or no longer align with the banking organization's strategic goals, objectives, or risk appetite; and
- maintaining appropriate documentation throughout the third-party risk management life cycle.

Independent reviews

The Proposed Guidance explains that banking organizations typically engage their internal auditor or an independent third party to conduct periodic independent reviews of their third-party risk management processes, especially where third parties perform critical activities. Senior management confirms the results of such reviews and reports them to the board. These reviews assess adequacy of the organization's internal policies and procedures for:

- confirming third-party relationships align with the banking organization's business strategy;
- identifying, measuring, monitoring, and controlling risks of third-party relationships;
- understanding and monitoring concentration risks that may arise from relying on a single third party for multiple activities or from geographic concentrations of business;
- responding to material breaches, service disruptions, or other material issues;
- involving multiple disciplines across the banking organization as appropriate during each phase of the third-party risk management life cycle;
- confirming appropriate staffing and expertise to perform risk assessment, due diligence, contract negotiation, and ongoing monitoring and management of third parties;
- confirming oversight and accountability for managing third-party relationships (for example, whether roles and responsibilities are clearly defined and assigned and whether the individuals possess the requisite expertise, resources, and authority); and
- confirming that conflicts of interest or appearances of conflicts of interest do not exist when selecting or overseeing third parties.

Documentation and reporting

The Proposed Guidance states that a banking organization should properly document and report on its third-party risk management processes and business arrangement throughout the entire third-party risk management life cycle. Documentation may vary among banking organizations based on their size and complexity, as well as that of their third-party relationships, but may include:

- a current inventory of all third-party relationships, which clearly identifies those relationships that involve critical activities and delineates the risks posed by those relationships across the banking organization;
- approved plans for the use of third-party relationships;
- risk assessments;
- due diligence results, findings, and recommendations;
- analysis of costs associated with each activity or third-party relationship, including any indirect costs assumed by the banking organization;
- executed contracts;
- regular risk management and performance reports required and received from the third party, which may include reports on service level reporting, internal control testing, cybersecurity risk and vulnerabilities metrics, results of independent reviews and other ongoing monitoring activities; and
- reports from third parties of service disruptions, security breaches, or other events that pose a significant risk to the banking organization.

2020 OCC FAQs

The OCC issued a set of frequently asked questions on the OCC Guidance in 2020 (the OCC FAQs). The OCC FAQs are appended to the Proposed Guidance as an exhibit thereto, and the Agencies request comment on the degree to which the contents of the OCC FAQs should be incorporated into the body of the Proposed Guidance.

The OCC FAQs clarify various aspects of the OCC Guidance on which the Proposed Guidance is based. The OCC FAQs address, among other things:

- the breadth of the arrangements that qualify as a "third-party relationship," including with respect to cloud- and other technology-based services;
- the permissibility of collaboration among banking organizations when carrying out the due diligence, contract negotiations, and monitoring described in the OCC Guidance; and
- the applicability of the OCC Guidance to various third-party relationships with fintechs.

If you have any questions regarding the matters covered in this publication, please reach out to any of the lawyers listed below or your usual Davis Polk contact.

Dana Seesel Bayersdorfer
+1 212 450 3423
dana.bayersdorfer@davispolk.com

Luigi L. De Ghenghi
+1 212 450 4296
luigi.deghenghi@davispolk.com

Adam M. Greene
+1 212 450 4857
adam.greene@davispolk.com

Kirill Lebedev
+1 212 450 3232
kirill.lebedev@davispolk.com

Eric McLaughlin
+1 212 450 4897
eric.mclaughlin@davispolk.com

Margaret E. Tahyar
+1 212 450 4379
margaret.tahyar@davispolk.com

[1] The OCC Guidance and the Proposed Guidance each include an identical visual depiction of both the five stages of the third-party risk management life cycle, as well as the three principles that apply throughout the life cycle. However, in the body of the Proposed Guidance, a discussion of oversight and accountability, documentation and reporting, and independent reviews is inserted between the discussions of the contract negotiation and ongoing monitoring stages of the life cycle. In contrast, the OCC Guidance discusses oversight and accountability after addressing the termination stage. We believe the intent of the Proposed Guidance is to convey that oversight and accountability, documentation and reporting, and independent reviews are principles that should guide banking organizations during the entirety of the life cycle, and not to introduce those topics as a new, standalone stage of the life cycle.