DEPARTMENT OF THE TREASURY

Office of the Comptroller of the Currency

[Docket ID OCC-2026-0793]

RIN 1557-ZA18

FEDERAL RESERVE SYSTEM

[Docket No. OP-1881]

FEDERAL DEPOSIT INSURANCE CORPORATION

RIN 3064-ZA58

NATIONAL CREDIT UNION ADMINISTRATION

[Docket No. NCUA-2026-1684]

RIN 3133-ZA54

Proposed Third-Party Risk Management Guidance

AGENCY: The Office of the Comptroller of the Currency (OCC), Treasury, the Board of Governors of the Federal Reserve System (Board), the Federal Deposit Insurance Corporation (FDIC), and the National Credit Union Administration (NCUA).

ACTION: Proposed interagency guidance and request for comment.

SUMMARY: The OCC, Board, FDIC, and NCUA (collectively, the agencies) invite comments on this proposed third-party risk management guidance. The proposed guidance would reflect the agencies' supervisory experience and lessons learned through examining banking organizations' third-party risk management practices. In particular, the proposed guidance would discuss the potential benefits that may accrue when a banking organization aligns its third-party risk management practices in relation to the reasonably assessed risk levels specific to each of its third-party relationships. This

approach may assist banking organizations in the prioritization of third-party risk management based on material financial risks, compliance with laws and regulations, and resource allocation. The proposed guidance also would help banking organizations consider potential strategies for tailoring their third-party risk management practices according to the banking organization's size, complexity, and risk profile, as well as the nature of its third-party relationships.

The agencies plan to rescind and replace existing guidance on third-party risk management to promote consistency and innovation in the banking industry.

DATES: Comments must be received on or before **[INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*]**.

ADDRESSES:

OCC: Commenters are encouraged to submit comments through the Federal eRulemaking Portal. Please use the title "Third-Party Risk Management Guidance" to facilitate the organization and distribution of the comments. You may submit comments by any of the following methods:

- *Federal eRulemaking Portal – Regulations.gov:*

  Go to *https://regulations.gov/*. Enter Docket ID "OCC-2026-0793" in the search box and click "Search." Public comments can be submitted via the "Comment" box below the displayed document information or by clicking on the document title and then clicking the "Comment" box on the top-left side of the screen. For help with submitting effective comments, please click on "Commenter's Checklist." For assistance with the *Regulations.gov* site, please call 1-866-498-2945 (toll free) Monday – Friday, 9 a.m. – 5 p.m. ET, or e-mail *regulationshelpdesk@gsa.gov*.

- *Mail:* Chief Counsel's Office, Attention: Comment Processing, Office of the Comptroller of the Currency, 400 7th Street, SW, Suite 1E-216, Washington, DC 20219.
- *Hand Delivery/Courier*: 400 7th Street, SW, Suite 1E-216, Washington, DC 20219.

Instructions: You must include "OCC" as the agency name and Docket ID "OCC-2026-0793" in your comment. In general, the OCC will enter all comments received into the docket and publish the comments on the *Regulations.gov* website without change, including any business or personal information provided such as name and address information, e-mail addresses, or phone numbers. Comments received, including attachments and other supporting materials, are part of the public record and subject to public disclosure. Do not include any information in your comment or supporting materials that you consider confidential or inappropriate for public disclosure.

You may review comments and other related materials that pertain to this action by the following method:

- *Viewing Comments Electronically – Regulations.gov*:

Go to *https://regulations.gov/*. Enter Docket ID "OCC-2026-0793" in the search box and click "Search." Click on the "Dockets" tab and then the document's title. After clicking the document's title, click the "Browse All Comments" tab. Comments can be viewed and filtered by clicking on the "Sort By" drop-down on the right side of the screen or the "Refine Comments Results" options on the left side of the screen. Supporting materials can be viewed by clicking on the "Browse Documents" tab. Click on the "Sort By" drop-down on the right side of the screen or the "Refine Results" options on the left side of the screen checking the "Supporting & Related Material"

checkbox. For assistance with the Regulations.gov site, please call 1-866-498-2945 (toll free) Monday-Friday, 9 a.m.-5 p.m. ET, or e-mail *regulationshelpdesk@gsa.gov*.

The docket may be viewed after the close of the comment period in the same manner as during the comment period.

Board: You may submit comments, identified by **Docket No. OP-1881**, by any of the following methods:

- *Agency Website: https://www.federalreserve.gov/apps/proposals/*. Follow the instructions for submitting comments, including attachments. ***Preferred Method.***
- *Mail:* Benjamin W. McDonough, Secretary, Board of Governors of the Federal Reserve System, 20th Street and Constitution Avenue NW, Washington, DC 20551.
- *Hand Delivery/Courier:* Same as mailing address.
- *Other Means: publiccomments@frb.gov.* You must include docket number in the subject line of the message.

Comments received are subject to public disclosure. In general, comments received will be made available on the Board's website at *https://www.federalreserve.gov/apps/proposals/* without change and will not be modified to remove personal or business information including confidential, contact, or other identifying information. Comments should not include any information such as confidential information that would be not appropriate for public disclosure. Public comments may also be viewed electronically or in person in Room M-4365A, 2001 C St. NW, Washington, DC 20551, between 9 a.m. and 5 p.m. during Federal business weekdays.

FDIC: You may submit comments to the FDIC, identified by ZRIN 3064-ZA58, by any of the following methods:

- *Agency Website: https://www.fdic.gov/federal-register-publications.* Follow instructions for submitting comments on the FDIC's website.
- *Email: comments@FDIC.gov.* Include ZRIN 3064-ZA58 in the subject line of the message.
- *Mail:* Jennifer M. Jones, Deputy Executive Secretary, Attention: Comments—ZRIN 3064-ZA58, Federal Deposit Insurance Corporation, 550 17th Street NW, Washington, DC 20429.
- *Hand Delivery/Courier:* Comments may be hand-delivered to the guard station at the rear of the 550 17th Street NW building (located on F Street NW) on business days between 7 a.m. and 5 p.m.
- *Public Inspection:* Comments received, including any personal information provided, may be posted without change to *https://www.fdic.gov/federal-register-publications.* Commenters should submit only information they wish to make available publicly. The FDIC may review, redact, or refrain from posting all or any portion of any comment that it may deem to be inappropriate for publication, such as irrelevant or obscene material. The FDIC may post only a single representative example of identical or substantially identical comments, and in such cases will generally identify the number of identical or substantially identical comments represented by the posted example. All comments that have been redacted, as well as those that have not been posted, that contain comments on the merits of this notice will be retained in the public comment file and will be

considered as required under all applicable laws. All comments may be accessible under the Freedom of Information Act.

NCUA: Comments may be submitted in one of the following ways. **(Please send comments by one method only)**:

- *Federal eRulemaking Portal: https://www.regulations.gov*. The docket number for this proposed guidance is NCUA-2026-1684. Follow the "Submit a comment" instructions. If you are reading this document on federalregister.gov, you may use the green "SUBMIT A PUBLIC COMMENT" button beneath this rulemaking's title to submit a comment to the regulations.gov docket. A plain language summary of the proposed guidance is also available on the docket website.
- *Mail:* Address to Melane Conyers-Ausbrooks, Secretary of the Board, National Credit Union Administration, 1775 Duke Street, Alexandria, Virginia 22314–3428.
- *Hand Delivery/Courier:* Same as mailing address.

Mailed and hand-delivered comments must be received by the close of the comment period.

Public Inspection: Please follow the search instructions on *https://www.regulations.gov* to view the public comments. Do not include any personally identifiable information (such as name, address, or other contact information) or confidential business information that you do not want publicly disclosed. All comments are public records; they are publicly displayed exactly as received and will not be deleted, modified, or redacted. Comments may be submitted anonymously. If you are unable to

access public comments on the internet, you may contact the NCUA for alternative access by calling (703) 518-6540 or emailing *OGCMail@ncua.gov*.

FOR FURTHER INFORMATION CONTACT:

OCC: Graham Bannon, Counsel, Chief Counsel's Office, 202-649-5490; Office of the Comptroller of the Currency, 400 7th Street, SW, Washington, DC 20219. If you are deaf, hard of hearing, or have a speech disability, please dial 7-1-1 to access telecommunications relay services.

Board: Juan Climent, Deputy Associate Director, (202) 460-2180, Jeff Ernst, Manager, (202) 369-9439, Brock Kannan, Manager, (202) 924-0665, Allison Boller, Sr. Financial Institution Policy Analyst II, (202) 253-4686, Division of Supervision and Regulation; or Claudia Von Pervieux, Special Counsel, (202) 469-1020, Benjamin Nuyens, Senior Counsel, (202) 909-7574, Legal Division; Board of Governors of the Federal Reserve System, 20th Street and Constitution Avenue NW, Washington, DC 20551.

FDIC: Division of Risk Management Supervision: Sumaya Muraywid, Section Chief, (202) 898-3904; Division of Depositor and Consumer Protection: Monika Jansen, Senior Policy Analyst, (202) 898-6781; Legal Division: Kate Marks, Senior Counsel, (202) 898-3896.

NCUA: Office of Examination and Insurance: Simon Hermann, Senior Credit Specialist, *shermann@ncua.gov* or (703) 518-6360; *Office of General Counsel:* Ian Marenna, Associate General Counsel for Regulations and Legislation, *imarenna@ncua.gov* or (703) 518-6540; National Credit Union Administration, 1775 Duke Street, Alexandria, Virginia 22314.

SUPPLEMENTARY INFORMATION:

I. Introduction

Banking organizations[1] routinely rely on third parties for a range of products, services, and other activities. These third-party relationships vary widely in form and in the degree of operational functions outsourced to the third party. The agencies have long acknowledged both the benefits associated with third-party relationships and the potential that these relationships may present or, in some cases, heighten certain risks. Third-party relationships have varying levels of importance to a banking organization's operations and delivery of products and services, and accordingly may warrant different levels of risk management.

In order to assist banking organizations in identifying and managing risks associated with third-party relationships and in complying with applicable laws and regulations, the Board, FDIC, and OCC published the *Interagency Guidance on Third-Party Relationships: Risk Management* in 2023 (the 2023 Guidance).[2] The agencies continue to believe that the principles-based, tailored approach outlined in the 2023 Guidance remains a relevant tool to assist banking organizations in considering their

[1] For a description of the banking organizations supervised by each agency, refer to the definition of "appropriate Federal banking agency" in section 3(q) of the Federal Deposit Insurance Act (12 U.S.C. 1813(q)). For purposes of this proposed guidance, banking organizations also include insured credit unions as defined in the Federal Credit Union Act (12 U.S.C. 1752(7)). Use of this guidance may also be relevant to any other entity supervised by the agencies.

[2] 88 FR 37920 (June 9, 2023). The 2023 Guidance is supplemented by the OCC for its supervised entities by guidance specific to foreign-based third-party service providers (OCC Bulletin 2002-16, "Bank Use of Foreign-Based Third-Party Service Providers: Risk Management Guidance" (May 15, 2002)). The 2023 Guidance is also supplemented by the Board, FDIC, and OCC with a statement on bank-fintech arrangements (OCC Bulletin 2024-20, Board SR Letter 24-5, and FDIC FIL-45-2024, "Joint Statement on Banks' Arrangements with Third Parties to Deliver Bank Deposit Products" (July 25, 2024)), and the Board, FDIC, and OCC have published a resource for community banks (OCC Bulletin 2024-11, Board SR Letter 24-2/CA Letter 24-1, and FDIC FIL-19-2024, "Third-Party Risk Management: A Guide for Community Banks" (May 3, 2024)) (collectively, the Supplemental TPRM Resources).

third-party risk management practices. However, based on feedback from stakeholders and supervisory experience, the agencies believe the 2023 Guidance frequently has been interpreted in an overly broad manner and with an insufficient focus on tailoring its risk management principles.

The 2023 Guidance is susceptible to such an interpretation for several reasons, notwithstanding language disclaiming any prescriptive intent or checklist approach. First, because it attempts to address a broad range of third-party relationships, banking organizations have reported that they have often struggled to understand (i) which of the extensive list of considerations apply to specific contexts (*e.g.*, relationships with core providers vs. financial technology companies (fintechs) vs. facilities maintenance vendors); and (ii) how to tailor their approach in practice, as many of the examples the 2023 Guidance provides may prove effective for one banking organization but impractical or infeasible for another. This is in part due to overly detailed examples and idealized factual scenarios that may not align with the real-world experiences of banking organizations when dealing with third parties. While examples can be valuable for illustrating how risk management principles translate into effective strategies, they can undermine a principles-based approach by suggesting a one-size-fits-all checklist.

Second, while the 2023 Guidance sets forth an expectation that banking organizations apply more comprehensive and rigorous oversight of third-party relationships supporting "critical activities," it is focused more on the activity conducted by the third party rather than either the third-party relationship or the magnitude or likelihood of harm related to the risks implicated by the relationship. Banking organizations have reported applying heightened risk management practices to a wide

range of third-party relationships without regard to the magnitude and likelihood of the risks actually posed by each relationship.

Third, the 2023 Guidance has been interpreted as establishing prescriptive requirements for banking organizations. Supervisory experience has shown use of words like "should" when discussing examples has failed to convey the importance of tailoring risk management to the actual risks a banking organization faces, commensurate with the banking organization's size, complexity, and risk profile and the nature of its third-party relationships. The 2023 Guidance unintentionally incentivized overly-process-driven approaches that fail to prioritize higher-risk relationships and focus risk management efforts and resources where they are needed.[3]

Finally, the 2023 Guidance has been read to discourage arrangements with newer and innovative third parties because it indicates they may present elevated risks. However, these firms can provide innovative services and solutions that enhance access to financial products and services and create economic opportunities for banking organizations and their customers.[4] To the extent the 2023 Guidance has implied an impossible goal of risk elimination, rather than risk management, banking organizations have reported maintaining relationships with third parties that may not best meet their needs, including where the third party cannot provide the banking organization with best-in-class products and services, has breached contract terms, or offers above-market pricing.

---

[3] As third-party risk management may at times involve multiple business functions within a banking organization (*e.g.*, cybersecurity, resilience, and data privacy, as well as various subject-matter experts), a failure to allocate and prioritize resources in a risk-based manner may also have unintended consequences on the effectiveness of risk management functions outside of the third-party risk management context.

[4] *See generally* E.O. 14405 "Integrating Financial Technology Innovation into Regulatory Frameworks," 91 FR 30475 (May 19, 2026) (E.O. 14405).

The proposed guidance would address these concerns by emphasizing risk identification and assessment as the foundation of a risk-based approach. This would enable banking organizations and examiners to focus on material financial risks and violations of laws and regulations rather than ineffective and counter-productive check-the-box exercises. Banking organizations that appropriately prioritize their risk management efforts—tailoring the level and detail of oversight to correspond with assessed risk levels—are better positioned to effectively manage third-party risk.

The proposed guidance would also encourage responsible innovation, consistent with Executive Order 14405, by emphasizing a risk-based and tailored approach to third-party risk management and removing broad-based and overly prescriptive language from the 2023 Guidance that may unduly impede fintechs from entering partnerships with banking organizations.

The agencies invite comments on all aspects of the proposed guidance. Any finalized guidance would replace the 2023 Guidance and the Supplemental TPRM Resources.[5]

II. Regulatory Analysis

Paperwork Reduction Act

The Paperwork Reduction Act of 1995 (44 U.S.C. 3501-3521) (PRA) states that no agency may conduct or sponsor, nor is the respondent required to respond to, an information collection unless it displays a currently valid Office of Management and Budget (OMB) control number.

[5] The agencies invite comments on whether any additional guidance documents, interpretive letters, or other resources relevant to third-party risk management should also be rescinded.

The guidance does not revise any existing, or create any new, information collections pursuant to the PRA. Rather, any reporting, recordkeeping, or disclosure activities mentioned in the guidance are usual and customary and should occur in the normal course of business as defined in the PRA.[6] Consequently, no submissions will be made to the OMB for review.

Executive Order 12866 (as Amended)

Executive Order 12866, titled "Regulatory Planning and Review," as amended, requires the Office of Information and Regulatory Affairs (OIRA), OMB, to determine whether a proposed guidance is a "significant regulatory action" prior to the disclosure of the proposed guidance to the public. If OIRA finds the proposed guidance to be a "significant regulatory action," Executive Order 12866 requires the relevant agency to conduct a cost-benefit analysis of the proposed guidance and for OIRA to conduct a review of the proposed guidance prior to publication in the *Federal Register*. Executive Order 12866 defines a "significant regulatory action" to mean a regulatory action that is likely to (1) have an annual effect on the economy of $100 million or more or adversely affect in a material way the economy, a sector of the economy, productivity, competition, jobs, the environment, public health or safety, or State, local, or tribal governments or communities; (2) create a serious inconsistency or otherwise interfere with an action taken or planned by another agency; (3) materially alter the budgetary impact of entitlements, grants, user fees, or loan programs or the rights and obligations of recipients thereof; or (4) raise novel legal or policy issues arising out of legal mandates, the President's priorities, or the principles set forth in Executive Order 12866.

[6] 5 CFR 1320.3(b)(2).

OIRA has determined that this proposed guidance is not a significant regulatory action under section 3(f) of Executive Order 12866 and, therefore, is not subject to review under Executive Order 12866.

Executive Order 14192

Executive Order 14192, titled "Unleashing Prosperity Through Deregulation," requires that an agency, unless prohibited by law, identify at least 10 existing regulations to be repealed when the agency publicly proposes for notice and comment or otherwise promulgates a new regulation with total costs greater than zero. Executive Order 14192 further requires that new incremental costs associated with new regulations shall, to the extent permitted by law, be offset by the elimination of existing costs associated with at least 10 prior regulations. This proposed guidance, if finalized as proposed, is expected to be a deregulatory action under Executive Order 14192 because it would provide supervisory clarity that may result in greater efficiencies and streamlining in banking organizations' third-party risk management functions.

III. Text of Proposed Guidance

The text of the proposed guidance on third-party risk management is as follows:

Third-Party Risk Management Guidance

A. Overview

B. Risk Management Components

1. Risk Identification and Assessment

i. Third-Party Relationship Identification

ii. Risk Identification

iii. Risk Assessment

2. Risk Oversight

i. Due Diligence and Third Party Selection

ii. Contract Negotiation

iii. Ongoing Monitoring

iv. Termination

v. Cross-Cutting Oversight Topics

3. Residual Risk Acceptance

4. Governance

A. Overview

Banking organizations[7] routinely rely on third parties for a range of products, services, and other activities. These third-party relationships come in a variety of forms and involve services related to many aspects of a banking organization's business. The degree of discretion granted to a third party can vary significantly in different types of relationships.

Banking organizations of all sizes rely on third-party relationships to operate effectively and meet evolving customer expectations. Community and mid-size banking organizations, which play an outsized role in lending and are vital to the strength of the U.S. economy, may be particularly reliant on such relationships to remain competitive in a rapidly evolving marketplace. Third-party relationships benefit banking organizations by allowing access to or facilitating technological advances; strategic business

[7] For a description of the banking organizations supervised by each agency, refer to the definition of "appropriate Federal banking agency" in section 3(q) of the Federal Deposit Insurance Act (12 U.S.C. 1813(q)). For purposes of this proposed guidance, banking organizations also include insured credit unions as defined in the Federal Credit Union Act (12 U.S.C. 1752(7)). Use of this guidance may also be relevant to any other entity supervised by the agencies.

innovations; new or improved products, services, and delivery channels and engagement with new or expanded markets; and operational efficiencies.

At the same time, use of third parties may introduce new risks or amplify existing risks to banking organizations and their customers.

A banking organization has ultimate responsibility to establish and maintain sound risk management practices and comply with applicable laws and regulations. A banking organization's use of third parties does not diminish its responsibility to meet these requirements to the same extent as if the activities were performed by the banking organization internally, including where the third-party relationship involves affiliates, service providers that are themselves highly-regulated entities, or subcontractors, or where elements of the banking organization's risk management practices are performed by a third party. The proposed guidance provides sound risk management principles to assist banking organizations in identifying, assessing, and managing risks associated with third-party relationships.[8]

Third-Party Relationships

For purposes of this guidance, a third-party relationship is a business arrangement between a banking organization and an entity or individual for the provision of one or more products, services, and other activities that support the banking organization.[9] The use of subcontractors alone does not typically create an independent third-party

[8] Banking organizations' third-party relationships may raise additional consumer compliance considerations that may be relevant to, but that are not directly addressed in, this proposed guidance.

[9] The agencies have observed that third-party relationships typically involve written agreements. Where a banking organization lacks a written agreement with a third party, or where no clear consideration underlies an activity, that activity is unlikely to constitute a third-party relationship. What would be the advantages and disadvantages of a banking organization applying the proposed guidance only to third parties that are subject to a written agreement with the banking organization to which it provides services? Would this approach, or an alternative, help clarify the scope of the proposed guidance and, if so, how?

relationship or create a presumption of direct banking organization oversight of any subcontractors.

These third-party relationships vary widely in form and in the degree of operational functions outsourced to the third party. Some third parties provide services central to the banking organization's operations. These include core processing service providers that provide comprehensive back-end applications and infrastructure that support the operation and essential functions of one or more of a banking organization's business lines; firms that provide other services that support a banking organization's essential operating functions, such as cloud processing, cloud storage, and compliance tools; and fintechs that partner with banking organizations to provide access to financial services. Other third-party relationships involve varying levels of interaction with a banking organization's operations. These include third parties that provide assistance with business-line- or product-specific activities (*e.g.*, software or data providers); perform administrative or clerical tasks (*e.g.*, operators of call centers or recordkeeping services); offer professional support services (*e.g.*, auditors, lawyers, or consultants); and maintain office support services (*e.g.*, physical security providers).

Principles-Based Approach

Each banking organization is responsible for operating in a safe and sound manner and adopting risk management practices that are best suited to managing the specific risks that it faces, commensurate with the banking organization's size, complexity, and risk profile and with the nature of its third-party relationships (including the risk and complexity of those relationships and type of activities performed by the third party). Not all third-party relationships present the same level of risk, and a similar relationship at different banking organizations may present different risks. Accordingly,

there is no one-size-fits-all approach to effective risk management. Banking organizations are experienced in determining, and are ultimately responsible for establishing, third-party risk management practices that are appropriate for the banking organization, consistent with safe and sound banking practices and in compliance with applicable laws and regulations. The agencies will give due consideration to a banking organization's reasonable decisions in matters of third-party risk management supervision.

Non-Enforceable Guidance

This proposed guidance does not set forth enforceable standards or prescriptive requirements;[10] accordingly, non-compliance with this guidance will not result in supervisory action against a banking organization. Any supervisory criticism will be specific to a banking organization's operations, financial condition, or other relevant factors, consistent with the applicable legal standards. Deviation from or inconsistency with this proposed guidance or any examples herein, including where an examiner believes that deviation or inconsistency is contrary to best practices, will not alone be a basis for supervisory action. However, the agencies may take action for violations of laws or regulations, unsafe or unsound practices, or other material risks that result from insufficient management of third-party risk (consistent with applicable rules and guidance on agency enforcement and supervisory standards).

B. Risk Management Components

The proposed guidance presents four components that banking organizations may consider when managing third-party risk: (1) identifying and assessing applicable risks;

[10] *See* 12 CFR Part 4, Subpart F, Appendix A (OCC); 12 CFR Part 262, Appendix A (Board); 12 CFR Part 302, Appendix A (FDIC); 12 CFR Part 791, Subpart D (NCUA).

(2) overseeing risks proportionate to their significance; (3) making informed decisions about residual risks and risk acceptance; and (4) establishing appropriate governance practices.

1. Risk Identification and Assessment

i. Third-Party Relationship Identification

Sound third-party risk management commonly begins with identifying and categorizing third-party relationships. Maintaining an inventory of third-party relationships may be useful for managing third-party risks. For example, a large or complex banking organization with multiple higher-risk third-party relationships may benefit from a periodically updated and detailed inventory that maps individual subcomponents of a third-party relationship to various banking organization business units, reporting lines, or other accountability mechanisms, while a community bank may benefit from a simpler or streamlined format that allows its management to quickly assess relevant third-party relationships at a higher level. Banking organizations may decide not to maintain extensive inventories of relationships posing limited risk, such as those related to administrative or clerical tasks, professional support services (including auditing and legal advice), or office support services (including physical security).

ii. Risk Identification

After identifying its prospective or existing third-party relationships, a banking organization generally identifies relevant risks. Risks presented by third-party relationships are varied and may change over time or may not be immediately apparent. For example, a core service provider, given the extent of its services, is likely to touch on many components of a banking organization's operational risk, in addition to other risks. A facilities maintenance third party, by contrast, may implicate only a relatively limited

range of risks, such as physical access risk. A banking organization typically has the experience and relevant information for identifying the most salient risks, especially where relevant staff members, such as subject-matter experts, are included in the risk identification process. It is unlikely that a banking organization could identify all possible risks and it is not expected to do so; however, identifying the most relevant risks is generally part of effective third-party risk management.

iii. Risk Assessment

Not all third-party relationships present the same level of risk, and there is not only one way to properly conduct risk assessments. Risk assessments commonly take into account both the magnitude of harm the third-party relationship could cause the banking organization or its customers and the likelihood that the harm will occur. A banking organization's higher-risk third-party relationships could include those (1) that, if disrupted, subjected to attack, conducted in breach of the terms of any applicable contract, or otherwise performed in a manner in which non-business-as-usual circumstances prevail, could cause the banking organization to incur an actual non-trivial violation of law or regulation, pose material harm to the financial condition of the banking organization, or result in a significant disruption to the banking organization's operations or customers; and (2) where there is a material likelihood that such legal or regulatory violation, financial harm, or operational disruption may occur under current or reasonably foreseeable conditions.

While certain third-party relationships, such as core processing service provider relationships, are likely to be assessed by most banking organizations as higher risk,[11] other relationships may be assessed as higher risk by one banking organization but not by another.[12] Some banking organizations may conduct a risk assessment for an overall third-party relationship, considering all activities conducted by the third party, while other banking organizations may conduct the assessment on a per-activity basis.[13]

Certain third-party relationships may be less likely to be assessed as higher risk. For example, many banking organizations contract with affiliated entities that operate within an enterprise-wide risk management framework to perform various services. Use of such affiliate arrangements can help a banking organization and its related entities more efficiently organize operations and maximize efficiencies. Such services, when conducted within an organization-wide enterprise risk management framework with which the banking organization is familiar, may be lower-risk and can enable the banking organization to rely on alternative oversight mechanics such as staff overlaps.

Additionally, certain third parties may themselves be entities that are heavily regulated and supervised by one or more state or federal regulators. As such, in certain

[11] As risk assessments are typically tailored to an individual banking organization's circumstances, a banking organization may determine, for example, that a core bank processor that provides services for only a limited portion of the banking organization's business represents a relatively lower-risk relationship compared to a core bank processor that provides services for the majority of a banking organization's business, depending on the relevant factors.

[12] Relatedly, many third parties may connect to a banking organization's information technology systems and networks, including through application programming interfaces, vendor portals, or other means. These access points may be exploited; however, a third party with access to a banking organization's systems or networks that do not hold critical data and are appropriately segmented is not necessarily higher risk, and banking organizations may, for example, be able to manage any related risks primarily through safe and sound cybersecurity risk management rather than through extensive third-party risk management.

[13] The agencies have also observed, for example, that banking organizations will commonly take the overall third-party relationship into account in circumstances where the bank is exposed to concentration risk from a third party due to relying on the third party for extensive services.

circumstances, a banking organization may consider a third party's regulatory status and regulatory obligations as part of its risk assessment. However, supervisory and regulatory schemes may differ materially between entity types and with regard to applicable legal requirements, regulatory or supervisory authority, the nature of the activity, or other factors, and thus the mere presence of a regulatory scheme may not necessarily serve to mitigate risks relevant to a banking organization.[14] Further, even regulated entities could nevertheless operate in a less than satisfactory condition, which could increase the risk they pose to the banking organization.

A banking organization may obtain further information that warrants adjusting its initial risk assessment after it performs due diligence and engages in contractual negotiations. Additionally, changing circumstances, an expanded or a renegotiated contract, or a banking organization's experience overseeing a third-party relationship, among other factors, may be indicators that a third-party relationship's risk has changed since the banking organization's initial assessment and may benefit from being reassessed. The decision of whether and how frequently to re-assess a banking organization's risks related to a third-party relationship may take into account additional factors such as changes in reliance on the third party, any new or existing identified concerns with the third party, or a change in the level(s) and type(s) of services provided by the third party.

Banking organizations typically have extensive experience assessing risks as part of their business. As such, examiners will give due consideration to a banking

[14] No supervisory or regulatory agency is responsible for a banking organization's third-party risk management. Banking organizations should not rely on the existence of any agency supervision or regulation as a substitute for managing third-party risk or as a proxy for whether such third parties provide services in a safe and sound manner.

organization's reasonable judgment regarding the banking organization's risk assessments.[15]

2. Risk Oversight

Effective risk management involves overseeing third-party relationships in a manner proportionate to the risks they present and consistent with the banking organization's risk appetite and tolerances. Banking organizations typically prioritize oversight of higher-risk third-party relationships and establish more rigorous oversight practices for such relationships. A banking organization may tailor its oversight in a manner commensurate with the banking organization's size, complexity, and risk profile, as well as with the nature of the third-party relationship. For example, the level of oversight appropriate for a banking organization with multiple business lines, operating subsidiaries, and a diversified customer base may not be appropriate for a banking organization with a less complex business model. Risk management practices that do not prioritize and tailor according to risk could increase the magnitude and likelihood of harm arising from higher-risk relationships due to inappropriate levels of attention and oversight.

The following discusses oversight at a high level. The examples provided are illustrative only, may not be relevant to all banking organizations or relationships, and are not comprehensive.

i. Due Diligence and Third Party Selection

Due diligence is the process by which a banking organization assesses a third party's ability to perform the activity as expected, adhere to the banking organization's

[15] To what extent would it be helpful for the guidance to include a list of characteristics that generally indicate that a third-party relationship is high risk, and if so, what characteristics should be included?

policies, comply with applicable laws and regulations, and conduct the activity in a safe and sound manner. As with all third-party oversight, the amount of due diligence that is warranted depends on the risk presented by the third-party relationship and the banking organization's individual business needs. In the case of lower-risk third-party relationships, a banking organization may be more comfortable with relying either on less-detailed due diligence information or on public or alternative sources, as compared to its higher-risk relationships. Depending on the circumstances, this relatively less-detailed level of due diligence may be sufficient for the banking organization to determine that the third party is likely able to perform the services being contracted for (including, for example, that the third party has sufficient staffing and capabilities) and that further due diligence may not provide appreciable benefits to the banking organization.

Depending on the circumstances, due diligence may involve assessing a third party's financial condition; business experience and key personnel; staffing capabilities and qualifications, including training relevant to the banking organization's business; legal and regulatory compliance; insurance coverage; and information security and cybersecurity capabilities and track record, as applicable. Due diligence may also evaluate the effectiveness of the third party's relevant risk management practices and capabilities, including policies, procedures, and internal controls and whether there is an alignment with the banking organization's own applicable policies, procedures, controls, strategies, and expectations.

In some cases, a banking organization may not be able to obtain certain due diligence information from a third party. For example, a third party may not have a long

operational history, may not permit on-site visits, or may not share (or is not permitted to share) information that the banking organization requests, but a banking organization may determine that other factors offset or compensate for those limitations. A banking organization may also have limited negotiating power with some third parties, which may amplify these difficulties. Even when unable to meet all of its due diligence objectives, a banking organization may still collect sufficient information, including from supplemental sources, to be able to determine that engaging with the third party is within the banking organization's risk appetite and tolerances. Outside information sources may be relied upon in certain contexts, including, for example, information or feedback obtained through banking organizations or trade groups, review of available public sources, or, in the case of a third party with a limited operational history, the overall qualifications and experience of management and employees of the third party in performing the services that would be provided. Similarly, external industry experts familiar with the third party, the relevant industry, or with market standard terms and practices may also supplement or help a banking organization conduct due diligence. However, where the third party is unable or unwilling to provide information or other cooperation reasonably necessary for the banking organization to conduct due diligence, ongoing monitoring and risk assessments, the alternative sources described above may not be sufficient to allow the banking organization to engage with the third party within its risk appetite and tolerances.

ii. Contract Negotiation

Effective third-party risk management generally involves negotiating contract provisions designed to facilitate effective risk management, oversight, and performance, in line both with the banking organization's risk identification and assessment and with

the results of its due diligence, and that specify the expectations and obligations of both the banking organization and the third party.

There are no generally applicable expected contract terms for third-party relationships—even for higher-risk relationships—and banking organizations typically tailor their contract negotiations and provisions to their individual needs and circumstances, commensurate with the banking organization's size, complexity, and risk profile and the nature of its third-party relationships. As such, the presence or absence of a specific contractual term that an examiner may believe to be contrary to best practices would not alone be a sufficient basis for an examiner to communicate an adverse finding related to a banking organization's third-party risk management practices.

Depending on the circumstances, the terms of the contract may allocate responsibility between the parties. A service level agreement can define performance measures, which can assist banking organizations in evaluating a third party's performance and compliance with applicable laws and regulations. Other items that may be relevant for a banking organization to consider during contract negotiations include, depending on the circumstances, confidentiality and information security, and, as discussed below, use of subcontractors, operational resilience plans, and termination provisions.

Third parties often offer standard contracts. Banking organizations can assess whether these standard terms adequately address their specific circumstances and risks. For example, banking organizations may determine that they need to request modifications, additional contract provisions, or activity-specific addenda to strengthen oversight for areas that pose higher risk to the banking organization. For lower-risk

relationships, a banking organization may determine that standard form contracts are sufficient. Alternatively, a banking organization may focus negotiations on a narrow subset of contractual provisions most relevant to the risks presented by the third-party relationship and that could provide the banking organization sufficient comfort that the services provided through the third-party relationship will be conducted in a manner that meets its needs and that is within its risk appetite and tolerances.

When a banking organization has limited negotiating power relative to a third party, it may be unable to negotiate all of its desired contractual provisions. The banking organization may still reasonably proceed with the relationship if, for example, the banking organization has a reasonable understanding of the risks relevant to the third-party relationship and any residual risks are in line with the banking organization's risk appetite and tolerances, especially if there are limited alternative options. In certain circumstances, banking organizations may also be able to gain an advantage by negotiating contracts as a group with other organizations, as discussed below.

Maintaining an inventory of and periodically reviewing third party contracts may assist a banking organization in confirming that existing provisions continue to address pertinent risks. If new risks are identified, a banking organization may consider whether it is appropriate to renegotiate or terminate a third-party relationship.

iii. Ongoing Monitoring

Ongoing monitoring is the process by which banking organizations assess and monitor third-party performance and changes in the risks posed by third-party relationships. It also includes any associated reporting to the board and senior management, as appropriate, in line with the banking organization's size, complexity, and risk profile, as well as the nature of its third-party relationships. Ongoing monitoring

may enable a banking organization to: (1) confirm the quality of a third party's controls and its ability to meet contractual obligations and perform as expected; (2) identify significant issues or concerns, such as material or repeat audit findings, deterioration in financial condition, security breaches, data loss, service interruptions, compliance issues, customer complaints, changes to insurance coverage, or other indicators of increased risk; and (3) respond to such significant issues or concerns when identified.

Examples of monitoring activities may include: (1) reviews of updates to information utilized in due diligence and reports or data regarding the third party's performance and the effectiveness of its controls, including audits conducted by the third party (or an independent entity hired by the third party);[16] (2) periodic visits and meetings with third-party representatives to discuss performance and operational issues; (3) periodic testing of the banking organization's controls that manage risks from its third-party relationships and, in certain circumstances, periodic testing of the third party's services to the banking organization to assess the third party's performance and effectiveness; (4) reviews of public filings or reports of examination arising from the agencies' standard supervisory processes for certain large third parties' provision of services, if applicable;[17] and (5) reviews of customer complaints.

[16] Banking organizations and bank service providers have incident notification obligations under the agencies' Computer Security Incident Notification Rule, which may also inform ongoing monitoring. *See* 12 CFR part 53 (OCC); 12 CFR 225, subpart N (Board); 12 CFR 304, subpart C (FDIC). *See also*, 12 CFR 748.1 for the NCUA's Cyber Incident Report Rule.

[17] *See* 12 U.S.C. 1464(d)(7)(D) and 1867(c)(1). These reports of examination are not tailored to any individual banking organization's circumstances or risk management needs and may be based on targeted rather than comprehensive examinations. These reports are the property of the agencies and are not intended as a proxy or substitute for any banking organization's responsibilities to undertake effective risk management and reliance on such reports without performing independent due diligence would be inconsistent with sound risk management principles.

Banking organizations may choose to conduct ongoing monitoring on a periodic or continuous basis based on the banking organization's assessment of the risk, complexity, and nature of the third-party relationship. For example, in the case of higher-risk third-party relationships, a banking organization may determine that effective risk oversight requires it to conduct more comprehensive or frequent monitoring. Higher-risk relationships may also involve additional staffing with the necessary expertise, authority, and accountability to perform a wide range of ongoing monitoring activities. For lower-risk relationships, a banking organization may determine that relatively less extensive, less detailed, or less frequent reporting, and commensurately reduced staffing needs, are necessary to support its risk oversight.

Banking organizations can tailor monitoring to their needs, abilities, risk determinations, and negotiating power, all of which can vary between larger or more complex banking organizations and community banks or among third-party relationships. For example, whether on-site visits to a third party or audits of a third party's control practices are practical may depend on the circumstances.

Because both the types and levels of risks a banking organization faces may change over the lifetime of a third-party relationship, a banking organization may later find it useful to adapt or alter its ongoing monitoring practices accordingly, including by expanding or contracting the scope, level of detail, or frequency of information collected or produced for monitoring.

iv. Termination

A banking organization may terminate a third-party relationship for various reasons, such as expiration or breach of contract; the third party's failure to comply with applicable laws or regulations; concerns regarding a third party's performance of the

activity more generally; or a desire to seek an alternate third party, bring the activity in-house, or discontinue the activity. When this occurs, management typically seeks to terminate relationships in an efficient manner, and management's ability to do so may depend on previously negotiated contract provisions. For example, a banking organization may determine that a lower-risk third-party relationship presents relatively few concerns, and it may be easy and cost-effective to seamlessly switch to an alternative third party, if necessary. As the complexity and materiality of a third-party relationship increases, a banking organization may benefit from advanced planning and ultimately determine that potential beneficial factors associated with a termination—*e.g.*, in-house or alternative third-party options with the potential for long-term cost reductions or improvements to the banking organization's products, services, and operations; better access to or control over data; or use of innovative technology—either do or do not outweigh the potential negative factors—*e.g.*, costs and fees associated with termination,[18] extended transition timespans, operational complications, the likelihood of service or data access disruptions, data retention and destruction issues, and handling of joint intellectual property.

In any case, a banking organization's assessment as to the preferability of terminating a contract with one third party and transitioning services to another typically draws on numerous factors relevant to the organization's business and strategy and the agencies will give due consideration to the organization's reasonable determinations that

[18] Termination cost considerations typically include whether alternative providers may be willing to buy out the remaining term of the contract or otherwise defer the banking organization's termination-related costs.

an alternative third party can provide the services as contracted for and within the banking organization's risk appetite and tolerances.

v. Cross-Cutting Oversight Topics

The preceding discussion provides a high-level overview of tailoring third-party relationship oversight to a banking organization's size, complexity, and risk profile and the nature and assessed risk levels of its third-party relationships. However, banking organizations may benefit from considering third-party risk management on a holistic, rather than a siloed, stage-by-stage basis, since effectively managing any given risk may be a multi-factored process. Understanding how risks and mitigating factors may cut across or implicate different oversight stages and where certain risk management strategies may be complementary or redundant may help banking organizations more effectively tailor and prioritize their risk management practices.

The following highlights certain examples that may help illuminate such an approach.

Subcontractors

While a banking organization typically does not have a direct business arrangement with a third party's subcontractors, their use may nonetheless heighten risks related to the third-party relationship as it may lessen the banking organization's control of activities. Since subcontractors may be considered in connection with the primary third-party relationship, the extent to which a banking organization exercises risk oversight related thereto may depend on the nature and risks of the third-party relationship. A banking organization may be able to exercise effective risk oversight related to a third party's use of subcontractors by, for example, negotiating and monitoring compliance with contractual terms governing the use and oversight of

subcontractors (including specifying whether service level agreements apply to subcontractor activity) or by assessing, confirming, and monitoring the adequacy of its third party's own third-party risk management programs. The banking organization remains responsible for complying with applicable laws and regulations, and operating in a safe and sound manner, regardless of a third party's use of subcontractors.

Use of Co-ventures, Consortia, Standard-Setting Organizations, Consultants, and Other Third Parties that Provide Risk Management Services

The agencies recognize that banking organizations can leverage new arrangements to manage third-party risk, including:

- Participating in a co-venture or consortium that collaborates on an aspect of third-party risk management, such as performing due diligence or developing standard contracts, or use of services from standard-setting and certification organizations that provide risk management and compliance standards for third parties engaging with banking organizations and issue certifications that assess that a third party meets the standards.
- Considering the results from services provided by consultants, auditors, or law firms for risk management and compliance purposes.

Such arrangements could, among other things, create new efficiencies, provide banking organizations additional leverage in conducting due diligence on, negotiating with, or monitoring third parties, and facilitate access to new technologies and strategic expertise.[19] The use of such arrangements could inform a banking organization's risk

[19] Any collaborative activities among banking organizations must comply with antitrust laws. Refer to the Federal Trade Commission and U.S. Department of Justice's "Antitrust Guidelines for Collaborations Among Competitors" (Apr. 2000), available at https://www.ftc.gov/sites/default/files/documents/public_events/joint-venture-hearings-antitrust-guidelines-collaboration-among-competitors/ftcdojguidelines-2.pdf.

assessment and enhance a banking organization's ability to oversee its third-party relationships. For example, review of credible summaries of technical data or proprietary information, as well as certifications or results of assessments provided by such arrangements, may be adequate for a banking organization's due diligence needs, depending on facts and circumstances. However, it is important for effective risk management to be based on the banking organization's own specific circumstances and performance criteria for the activity.

In addition, effective third-party risk management may also involve relying on third-party technologies or processes to supplement or assist the banking organization's own risk oversight activities. This may allow community banks, in particular, to benefit from advanced technology and industry expertise otherwise unavailable. However, reliance on third parties for risk management purposes can itself involve risks, which a banking organization can address based on its individual circumstances.

Insurance, Indemnification, and Other Limitations on Liability

Depending on risk exposure, negotiating for credible indemnification provisions, limitations on banking organization liability, insurance, or guarantees from the third party's parent or other entity may serve to effectively mitigate risks arising from the third-party relationship, which may lower the risk associated with the relationship. Such a conclusion may be based upon, for example, due diligence regarding the ability of the relevant party to meet any obligations, negotiating terms of the coverage as relevant to the specific risks of the third-party relationship, maintaining the coverage and confirming its ongoing sufficiency, and considering whether the banking organization has the

capacity to cover any costs associated with pursuing, filing, disputing, or litigating a claim.

Operational Resilience Planning

Effective risk oversight, particularly for higher-risk relationships, may include due diligence, contract negotiations, and ongoing monitoring sufficient to demonstrate resilience and assess assurances, including, for example, contractual obligations related to review of a third party's operational resilience plan, the existence of alternative back-up providers that can provide an easy transition of services, the practice of maintaining critical data backed up at a physically and logically separated site, or other relevant considerations. In certain circumstances, even if a higher-risk third party suffers a disruption event, cyberattack, or otherwise is unable to provide business-as-usual services, if a banking organization has sufficient demonstration of its own or of the third party's ability to quickly and effectively resume operations and preserve relevant data, the harms from any such event may be significantly mitigated. This may in turn inform the risk associated with the third-party relationship.

3. Residual Risk Acceptance

Residual risk is the risk remaining after the banking organization applies mitigating measures. The agencies do not expect banking organizations to eliminate third-party risk. Some residual risk is unavoidable, as discussed above. In some cases, the materiality of the risk does not justify the oversight required to significantly mitigate it. In other cases, a banking organization may lack the means to significantly mitigate a risk, such as when it lacks bargaining power to conduct sufficient due diligence, negotiate customized contract terms, or engage in in-depth ongoing monitoring, or where the banking organization has limited alternative options. Managing third-party risk includes

determining when and to what extent elements of risk oversight may not be practicable and whether residual risks may be acceptable according to a banking organization's risk appetite and tolerances, while still conducting activities in a safe and sound manner, and when and to what extent a banking organization can make this determination based on limited information. Even in cases where the banking organization cannot significantly mitigate a risk, the third-party relationship may still be beneficial and necessary for the banking organization to operate effectively and competitively in a rapidly evolving marketplace. Risk acceptance is ultimately a fact- and circumstance-specific consideration, commensurate with a banking organization's size, complexity, and risk profile and with the nature of its third-party relationships.

4. Governance

In order to support its overall third-party risk management practices, banking organizations may consider adopting governance practices that: (1) establish clear roles and responsibilities, (2) establish an appropriate risk appetite and appropriate risk tolerances related to risks from third-party relationships, (3) help ensure that the banking organization is able to identify and assess its third-party relationship risks and prioritize risk management in relation to the assessed risk levels of such relationships and the banking organization's risk appetite and tolerances, (4) establish appropriate reporting to senior management and the board, (5) document key elements of risk management for third-party relationships, and (6) establish a process for conducting periodic independent reviews to assess the effectiveness of the banking organization's third-party risk management practices.

However, there is no one right way for a banking organization to structure such practices, and a banking organization's size, complexity, and risk profile and the nature

of its third-party relationships will ultimately drive any relevant governance decisions. The agencies will give due consideration to a banking organization's reasonable governance considerations when reviewing those practices.

Jonathan V. Gould,
Comptroller of the Currency.

By order of the Board of Governors of the Federal Reserve System.
Benjamin W. McDonough,
Secretary of the Board.

Federal Deposit Insurance Corporation.
Dated at Washington, DC, on September 10, 2026.
Jennifer M. Jones,
Deputy Executive Secretary.

By the National Credit Union Administration Board on September 10, 2026.
Melane Conyers-Ausbrooks,
Secretary of the Board.