# US Federal Banking Agencies Propose Revised Third-Party Risk Management Guidance

Skadden

**September 17, 2026**

If you have any questions regarding the matters discussed in this memorandum, please contact the following attorneys or call your regular Skadden contact.


**Mark Chorazak**
Partner / New York
212.735.3488
mark.chorazak@skadden.com

**Monica Freas**
Partner / New York
212.735.2832
monica.freas@skadden.com

**Michael P. Reed**
Partner / New York
212.735.3443
michael.reed@skadden.com



This memorandum is provided by Skadden, Arps, Slate, Meagher & Flom LLP and its affiliates for educational and informational purposes only and is not intended and should not be construed as legal advice. This memorandum is considered advertising under applicable state laws.



One Manhattan West
New York, NY 10001
212.735.3000


## Executive Summary

- **What's new:** The U.S. federal banking agencies have issued proposed interagency guidance that would rescind and replace 2023 guidance for banks' relationships with third-party service providers. The Federal Reserve Board also proposed a companion guide for traditional community banks and, together with the OCC and FDIC, issued a joint statement on community bank engagement with core service providers.
- **Why it matters:** The proposal moves away from prior prescriptive guidance in favor of a more flexible approach that would allow institutions to focus on the magnitude and likelihood of the risks actually posed by each third-party relationship, with deference given to the institution's own risk assessments.
- **What to do next:** The proposal has not yet replaced existing guidance. However, institutions can begin to consider how they might reevaluate their current vendor risk classifications. Any changes to existing third-party risk frameworks should follow a supported assessment of harm, likelihood and available mitigants. Comments on the proposed guidance are due on November 16, 2026.

On September 11, 2026, the Office of the Comptroller of the Currency (OCC), Board of Governors of the Federal Reserve System (Federal Reserve Board), Federal Deposit Insurance Corporation (FDIC) and National Credit Union Administration (collectively, the "agencies") jointly issued proposed interagency guidance on third-party risk management (TPRM) that would rescind and replace the "Interagency Guidance on Third-Party Relationships: Risk Management" published on June 9, 2023 (2023 Guidance).

In the proposal, the agencies acknowledged that the 2023 Guidance "frequently has been interpreted in an overly broad manner and with an insufficient focus on tailoring its risk management principles."

Specifically, the agencies identified a number of deficiencies:

- The guidance's overly detailed examples and idealized factual scenarios effectively created de facto checklists, leading banking organizations to adopt an "overly-process-driven" approach rather than exercise tailored, risk-based judgment.
- The use of "should" throughout the 2023 Guidance failed to convey the importance of tailoring risk management practices to the specific risk profile of each third-party relationship.
- The framework's focus on "critical activities," rather than on the magnitude and likelihood of potential harm, did not provide a sufficiently nuanced basis for assessing risk.
- The 2023 Guidance was interpreted as discouraging banking organizations from entering into arrangements with newer and innovative third-party providers, and implied "an impossible goal of risk elimination, rather than risk management."

Separately, the Federal Reserve Board issued a proposed companion guide specifically tailored to traditional community banking organizations.

Finally, the OCC, Federal Reserve Board and FDIC issued a strongly worded joint statement addressing community banks' engagement with core service providers. This joint statement underscores agency officials' recent comments regarding their concern



© Skadden, Arps, Slate, Meagher & Flom LLP. All rights reserved.

about the potential adverse impacts that the core providers have on community banks given the highly concentrated market of core service providers.

Comments on the proposed interagency guidance and community bank guide are due on November 16, 2026. Though the proposal has not yet replaced existing guidance, institutions can begin to consider how they might reevaluate their current vendor risk classifications. Any changes to existing third-party risk frameworks should follow a supported assessment of harm, likelihood and available mitigants. Residual risks should be understood and explanations for risk acceptance strengthened.

Institutions should also consider whether outside or shared assessments may provide efficiencies, after taking into account both attendant risks and benefits.

## Key Features of the Proposed Interagency Guidance

### Risk Assessments Drive the Scope of Oversight

The proposed guidance is intended to assist institutions in the prioritization of third-party risk management based on material financial risks, compliance with laws and regulations, and resource allocation. The issuance is part of a larger overall effort by the federal banking agencies to refocus supervision and examination on material financial risk. (See our September 10, 2026, client alert "OCC and FDIC Finalize Standards for Unsafe or Unsound Practices and MRAs.")

Under the proposal, risk identification and assessment is reoriented toward the magnitude and likelihood of harm arising from the relationship.

### Lower-Risk Relationships May Receive Simpler Reviews

The proposal describes practical ways to tailor oversight, such as use of streamlined vendor inventories for relationships posing limited risk. Lower-risk relationships could also warrant less detailed due diligence, reliance on public or alternative information, standard contracts and less frequent monitoring.

Examples of lower-risk vendors discussed in the proposal include vendor services for certain administrative or clerical tasks (*e.g.*, operators of call centers or recordkeeping services), professionals (*e.g.*, auditors, lawyers, consultants) and office support services (*e.g.*, physical security providers).

Higher-risk relationships could warrant more comprehensive reviews and additional staff expertise.

For institutions using uniform annual reviews or extensive questionnaires across most vendors, the proposal would support reassessing whether those practices direct resources to the most significant exposures.

### Incomplete Due Diligence and Limited Bargaining Power Would Not Automatically Preclude Engagement

The proposal recognizes that a bank may be unable to obtain every requested document, conduct an on-site visit or negotiate every desired contract term. A provider's limited operating history also would not automatically prevent a relationship.

Supplemental information, including personnel experience, public sources, peer feedback and outside expertise, could help the bank reach a supported decision as part of its due diligence.

### Institutions May Rely on Shared Assessments and Outside Reviews for Vendors

The proposal expressly recognizes co-ventures, consortia, standard-setting and certification organizations, and assessments performed by consultants, auditors or law firms. Depending on the circumstances, credible summaries of technical or proprietary information, certifications and assessment results could also satisfy a bank's due diligence needs.

This language is particularly relevant to institutions that outsource individual vendor reviews or use a common assessment across multiple banks. In practice, institutions should consider assessing the review's scope, currency, assessor qualifications and coverage gaps, and determine what supplemental work may be required. A certification would not itself transfer the bank's accountability or establish a safe harbor. Reliance on an outside risk management provider also creates risks that the institution should evaluate.

### Affiliate Services May Be Lower-Risk

The proposal provides that contracts with affiliates of the banking institution that operate under an enterprisewide risk management framework to perform services may be lower-risk, and alternative oversight of the affiliate could be addressed by other means, including by overlapping staff.

# US Federal Banking Agencies Propose Revised Third-Party Risk Management Guidance

### Contract Negotiation Would Be More Flexible

The guidance states there are no generally expected contract terms for third-party relationships, even for higher-risk relationships. Supervisors would expect institutions to tailor their contract negotiations and provisions to their individual needs and circumstances, commensurate with the institution's size, complexity and risk profile as well as the nature of the third-party relationship.

### Ongoing Monitoring Would Be Tailored

Ongoing monitoring of activities is emphasized in the guidance, which states that these activities should be proportionate to the risk. It includes reviewing due diligence updates and performance data, conducting periodic visits and meetings with third-party representatives, testing the organization's own controls over third-party risks, reviewing public filings or supervisory examination reports for certain large service providers, and analyzing customer complaints.

The guidance contemplates that shared assessments and use of vendors can be leveraged for ongoing monitoring, in addition to due diligence and negotiation.

The frequency, scope and depth of ongoing monitoring should be tailored to the risk, complexity and nature of each third-party relationship, as well as to the institution's own size and capabilities.

Higher-risk relationships may warrant more comprehensive or frequent monitoring and dedicated staffing with appropriate expertise, while lower-risk relationships may require relatively less extensive oversight and reduced staffing.

### Reasonable Bank Judgments Would Receive Due Consideration

The proposal repeatedly states that agencies or examiners would give due consideration to reasonable bank decisions, including risk assessments, governance choices and provider transitions. According to the agencies, "banking organizations typically have extensive experience assessing risks as part of their business," and therefore, "examiners will give due consideration to a banking organization's reasonable judgment regarding the banking organization's risk assessments."

The proposal also expressly states that departures from the guidance or its examples, even if an examiner considers them inconsistent with best practices, would not alone support supervisory action.

### Governance Practices Would Generally Follow Traditional Principles

The proposed guidance reiterates traditional governance principles and encourages adopting governance practices that:

- Establish clear roles and responsibilities.
- Set appropriate risk appetites and tolerances.
- Help ensure that the banking organization is able to identify and assess its third-party relationship risks and prioritize risk management in relation to risk levels as well as the banking organization's risk assessments.
- Determine appropriate reporting to senior management and the board.
- Document key elements of risk management for third-party relationships.
- Create a process for conducting periodic independent reviews to assess the effectiveness of the institution's third-party risk management practices.

However, the guidance avoids being prescriptive and reiterates that "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."

## Joint Statement on Community Banks' Engagement With Core Service Providers

In addition to the proposed interagency guidance, the OCC, Federal Reserve Board and FDIC issued a joint statement specifically addressing the relationship between community banking organizations (CBOs) and their core processing service providers — entities that provide critical systems, applications and infrastructure for transaction processing, account management, payments, compliance, online banking and related functions.

The joint statement acknowledges that the core provider market is highly concentrated, with a small number of large providers serving the majority of community banks. This market structure, the agencies contend, limits CBOs' negotiating power and creates challenges in obtaining due diligence information, negotiating favorable contract terms and conducting ongoing monitoring.

# US Federal Banking Agencies Propose Revised Third-Party Risk Management Guidance

To address these concerns, the agencies identified three supervisory factors they will consider when making resource allocation decisions with respect to core service providers:

- **Transparency.** The agencies will consider a core provider's willingness to furnish due diligence information, the presence of contractual provisions that limit comparison shopping, the transparency and enforceability of service-level agreements, the timeliness of disclosures regarding operational issues and security incidents, and the complexity of billing practices.
- **Contract features.** The agencies will evaluate practices that make it difficult for CBOs to manage their core provider relationships, including opaque pricing and billing, "back billing" windows, unsupported deconversion fees (particularly where the core provider has breached the contract) and excessive limitations on the integration of services from unaffiliated providers.
- **Technology.** The agencies will assess the number and severity of computer security incidents, management of end-of-support and end-of-life technology assets, and demonstrated operational resilience.

### Enforcement Implications

The joint statement includes a noteworthy discussion of enforcement authority. The agencies suggest that core providers may qualify as "institution-affiliated parties" under the Federal Deposit Insurance Act, on the basis that they "participate in the conduct of the affairs of an insured depository institution."

They contend that because core providers undertake the most central operational aspects of banking for CBOs, core providers "may be held liable for the practices or violations of a CBO as an institution-affiliated party."

This view represents a potentially significant expansion of the agencies' enforcement reach with respect to third-party service providers.

## Federal Reserve Board's Proposed Community Bank Guide

The Federal Reserve Board separately issued a proposed companion guide for traditional community banking organizations, defined as banking organizations with less than $30 billion in total consolidated assets that focus primarily on serving local communities.

The guide is intended as a practical supplement to the proposed interagency guidance applicable to all banking organizations and is expressly not intended for complex bank-fintech partnerships.

The community bank guide is organized around four overarching risk management considerations:

1. Operational resilience
2. System and information security
3. Compliance with rules and regulations
4. Financial resilience

The guide then addresses these considerations across eight common vendor categories: (1) core providers, (2) information technology (IT) infrastructure providers, (3) cybersecurity providers, (4) payment processing and digital banking providers, (5) loan management system providers, (6) card issuing and processing providers, (7) Bank Secrecy Act/Anti-Money Laundering and financial crime platform providers, and (8) fraud prevention and detection providers.

Federal Reserve Board Governor Lisa D. Cook issued a statement supporting the proposals, endorsing the "fresh look" at third-party risk management and emphasizing the importance of a principles-based, risk-focused approach that enables innovation.

Board Governor Michael S. Barr dissented, expressing concern that the proposals would "reduce safe and sound operations, increase financial and other risk, create undue confusion, and leave gaps in supervisory coverage."