

Regulatory Alert

Regulatory Insights for Financial Services

September 2026

Third-Party Risk Management: Proposed Guidance; Joint Statement

KPMG Regulatory Insights

- **Tailoring and Prioritization:** Proposal aims for banking organizations to tailor TPRM based on risk assessments and to prioritize higher-risk relationships.
- **Experience-Driven:** Proposed approach based on “supervisory experience” and “stakeholder feedback” that finds the existing guidance does not provide sufficient focus on tailoring risk management, incentivizes process-driven approaches over risk-focused practices, and discourages new and innovative third-party relationships.
- **Community Bank Considerations:** Additional supplemental guidance is directed toward the reliance of many community banks on third parties, especially with regard to higher-risk relationships such as with core service providers; notably, the agencies signal potentially heightened scrutiny of core service providers.

The Federal Deposit Insurance Corporation (FDIC), the Federal Reserve Board (FRB), the National Credit Union Administration (NCUA), and the Office of the Comptroller of the Currency (OCC) (collectively, the agencies) have released three separate issuances related to third-party risk management (TPRM), including a:

- Joint Proposal on TPRM Guidance (for all banking organizations)
- FRB Proposal for a Community Bank TPRM Guide
- Joint Statement on Community Bank Engagement with Core Service Providers

The agencies state the proposed guidance will assist banking organizations to prioritize TPRM by emphasizing risk identification and assessment as the foundation of a risk-based approach – enabling organizations to focus on material financial risks, compliance with laws and regulations, and resource allocation.

The agencies request comments on the proposed TPRM guidance on or before November 16, 2026. Additionally, the FRB seeks comment on its proposed Community Bank Guide by November 16, 2026.

Proposed TPRM Guidance

The proposed guidance reflects the agencies' supervisory experience and lessons learned from examining financial institutions' third-party risk management practices. It is intended to assist banks and credit unions to better align and tailor their TPRM practices to the “reasonably assessed” risks specific to each of their third-party relationships. The proposed guidance presents four risk management components that banking organizations may consider when managing third-party risk:

- Risk Identification and Assessment.
- Risk Oversight.
- Residual Risk Acceptance.
- Governance.

Risk Identification and Assessment

The agencies emphasize risk identification and assessment as the foundation of a risk-based approach – which would enable banking organizations and examiners to focus on material financial risks, compliance with laws and regulations, and resource allocation. Elements of risk identification and assessment include:

Third-Party Relationship Identification. For purposes of the proposed guidance, a third-party relationship would be defined as “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.” The agencies note that the use of subcontractors alone does not typically create an independent third-party relationship or create a presumption of direct banking organization oversight of any subcontractors.

When identifying and categorizing third-party relationships, banking organizations may choose to maintain an inventory of third-party relationships, potentially mapping individual subcomponents of a higher-risk third-party relationship to various banking organization business units, reporting lines, or other accountability mechanisms.

Risk Identification. Risks presented by third-party relationships are varied and may change over time or may not be immediately apparent. The agencies note that although a banking organization is not expected to identify all possible risks, it should identify the most relevant risks as a part of effective third-party risk management. Involving relevant staff, such as subject matter experts, in the risk identification process may improve identification of the most salient risks.

Risk Assessment. 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. The agencies state there are multiple ways to conduct risk assessment and that they will give “due consideration to a banking organization’s ‘reasonable judgement’” regarding risk assessments.

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 factors such as:

- Changes in reliance on the third party.
- Any new or existing identified concerns with the third party.
- A change in the level(s) and type(s) of services provided by the third party.

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. Priority is given to oversight of higher-risk relationships. A banking organization may tailor its oversight in a manner commensurate with its size, complexity, and risk profile, as well as with the nature of the third-party relationship. Elements of risk oversight include:

Due Diligence and Third-Party Selection. 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. Depending on the circumstances, due diligence may include assessing the third party’s:

- Financial condition.
- Business experience and key personnel.
- Staffing capabilities and qualifications.
- Legal and regulatory compliance.
- Insurance coverage.
- Information security and cybersecurity capabilities and track record.

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.

Contract negotiation. The proposed guidance would state that effective TPRM 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, including higher-risk relationships.

A banking organization may maintain an inventory of, and periodically review, third-party contracts to confirm 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.

Ongoing monitoring. 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. Higher-risk relationships may also involve additional staffing with the necessary expertise, authority, and accountability to perform a wide range of ongoing monitoring activities. Because both the types and levels of risks banking organizations face may change over the lifetime of a third-party relationship, a banking organization may later 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.

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. The agencies will give due consideration to an organization's "reasonable determinations" that an alternative third party can provide the services as contracted for and within the banking organization's risk appetite and tolerances.

Cross-Cutting Oversight Topics. The agencies recognize that banking organizations can leverage alternate arrangements to manage third-party risk, including participating in co-ventures and consortia for joint due diligence or developing standard contracts, using standard-setting and certification organizations for assessments, and hiring consultants to supplement expertise. Other approaches to mitigate certain third-party risks might include negotiating contract terms regarding the use of subcontractors or limitations on liability such as through insurance or guarantees and adding operational resilience through alternate back-up providers and data storage.

Residual Risk Acceptance

The proposed guidance notes that the agencies do not expect banking organizations to eliminate third-party risk and that 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. Banking organizations would determine whether risks remaining after mitigation are acceptable within their risk appetite and tolerances.

Governance

Banking organizations may consider adopting governance practices to support their TPRM practices, including practices that address:

- Roles and responsibilities.
- Risk appetite and risk tolerances related to risks from third-party relationships.
- Identification and assessment of third-party relationship risks and prioritization of risk management in relation to the assessed risk levels of such relationships.
- Reporting to senior management and the board.
- Documentation of key elements of risk management for third-party relationships
- A process for conducting periodic independent reviews to assess the effectiveness of TPRM practices.

Potential Impact

If finalized, the proposed guidance would replace the current *Interagency Guidance on Third-Party Relationships: Risk Management* (referred to as the 2023 interagency guidance) and related supplemental TPRM resources. Notably, the proposal does not set forth enforceable standards or prescriptive requirements. Accordingly, non-compliance will not result in supervisory action against a banking organization.

FRB Community Bank Guide

The FRB separately proposed supplemental guidance for "traditional community banking organizations" (TCBOs) to support their third-party risk management efforts. For this purpose, TCBOs would be defined as "banking organizations with less than \$30 billion in assets that focus on serving their local communities."

The proposal – referred to as the Community Bank Guide – would cover:

- **Overarching TPRM considerations**, including these areas of "highest priority:"
 - Operational resilience.
 - System and information security.
 - Compliance with rules and regulations.
 - Financial resilience.
- **Vendor-by-vendor TPRM considerations**, including how the overarching considerations apply and additional risk management considerations specific to these types of third parties:
 - Core service providers.
 - Information technology infrastructure providers.
 - Cybersecurity providers.
 - Payment processing and digital banking providers.
 - Loan management system providers.
 - Card issuing and processing providers.
 - Bank Secrecy Act/Anti-Money Laundering and financial crime platform providers.
 - Fraud prevention and detection providers.

The FRB is seeking comment on all aspects of the Community Bank Guide and, in particular, whether it would be useful to "traditional community banking organizations," and whether it would provide the appropriate level of detail, such that it will serve as a useful resource for those organizations without establishing de facto supervisory standards.

Interagency Statement on Core Service Providers

The FDIC, FRB and OCC jointly released a [statement](#) outlining how the agencies will approach risk-based supervision of core service providers that support community banking organizations (CBOs). The agencies state that core service providers represent the most material, complex, and highest-risk third-party relationships for CBOs.

The agencies will consider factors related to core provider practices in three categories when determining how to allocate supervisory resources, including the nature, extent, and frequency of supervisory activities; the contents of examination reports provided to core providers' clients; and whether to add a core provider to the agencies' service provider examination program:

- **Transparency**, including an assessment of the core service provider's: i) willingness to provide relevant and timely due diligence information; ii) use of and compliance with measurable performance standards that the CBO can monitor and enforce; and iii) transparency and timely disclosure of operational issues and security incidents.
- **Contract features**, including a core provider's business practices and use of contract terms that make it difficult for CBOs to manage their core provider relationships in a manner that aligns with the CBO's business needs, such as by seeking an alternative core provider or supplementary services. Examples include: i) opaque pricing or billing practices; ii) extended "back-billing" windows; and iii)

limitations on the ability of unaffiliated service providers to integrate with the core platform.

- **Technology**, including an assessment of the core provider's technology investments and capabilities such as: i) the number and severity of computer security incidents; ii) management of end-of-support and end-of-life assets that enable client CBOs to transition to updated platforms, and iii) demonstrated operational resilience capabilities.

The agencies reiterate that outsourcing to third parties does not reduce a CBO's own responsibility for safety, soundness, and legal compliance. They state they monitor services that core providers deliver to CBOs to identify issues related to safety and soundness or violations of law. When such issues are identified, they may bring appropriate actions against core providers and/or the CBO pursuant to their statutory authorities.

In addition, the agencies state they may "have a reasonable basis to treat certain core providers as 'institution-affiliated parties' (IAPs) under the Federal Deposit Insurance Act — specifically, as 'persons...who participate[] in the conduct of the affairs of an insured depository institution.'" They conclude that because core service providers are integral to carrying out the business of banking and the functions of CBOs, they may be held liable for the practices or violations of a CBO as an IAP.

For more information, please contact [Laura Byerly](#) or [Joey Gyengo](#).

Contact



Laura Byerly
Managing Director
Regulatory Insights
lbyerly@kpmg.com



Brian Hart
Principal
Risk, Regulatory and Compliance
bhart@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Learn about us:



kpmg.com

© 2026 KPMG LLP, a Delaware limited liability partnership, and its subsidiaries are part of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.