NEW PROPOSED RISK MANAGEMENT GUIDANCE

Date: 24 September 2026

US Policy and Regulatory Alert

By: Linda C. Odom, John ReVeal

The federal bank regulators and the National Credit Union Administration have proposed new Third-Party Risk Management Guidance (TPRM Guidance) that would replace the 2023 Interagency Guidance on Third Party Relationships: Risk Management (2023 Guidance) and all supplemental third-party risk management resources. The Federal Reserve has separately proposed Third-Party Risk Management Guidance for Traditional Community Banking Organizations (TCBO Guide).

The TPRM Guidance describes a number of perceived weaknesses with the 2023 Guidance, including that it has been "interpreted in an overly broad manner and with an insufficient focus on tailoring its risk management principles." The agencies note that banking organizations have "struggled to understand (i) which of the extensive list of considerations apply to specific contexts," such as core providers versus facilities maintenance vendors, "and (ii) how to tailor their approach in practice…." (The TPRM Guidance refers to "banking organizations" collectively as including credit unions as well as banks.) They further note that the expectations set forth in the 2023 Guidance "for more comprehensive and rigorous oversight of third-party relationships supporting 'critical activities' … 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." The agencies also say that the 2023 Guidance has been read "to discourage arrangements with newer and innovative third parties because it indicates they may present elevated risks."

Of perhaps most importance, the regulators recognize that the 2023 Guidance has been interpreted as establishing prescriptive requirements rather than conveying the importance of tailoring risk management to the actual risks faced by banks based on their size, complexity, and risk profile. We have noted in our practice that some regulators expect financial institutions to have fully addressed all 2023 Guidance items rather than focusing on whether their programs are properly tailored for their business and the actual risks.

It is important to note that by its terms the TPRM Guidance specifically "does not set forth enforceable standards or prescriptive requirements." Deviation from the TPRM Guidance would not "alone be a basis for supervisory action." However, the agencies still "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."

The TPRM Guidance provides four "components" that banking organizations may consider when managing third-party risk: "(1) identifying and assessing applicable risks; (2) overseeing risks proportionate to their significance; (3) making informed decisions about residual risks and risk acceptance; and (4) establishing appropriate governance practices."

©2005-2026 K&L Gates LLP. All Rights Reserved.

RISK IDENTIFICATION AND ASSESSMENT

Although the agencies emphasize that “non-compliance” with the TPRM Guidance will not itself result in supervisory action, they may take action for “material risks that result from insufficient management of third-party risk.” Therefore, as with any guidance or regulation that allows a risk-based approach, identifying and assessing the applicable risks of each third-party relationship is an institution's most important task. That assessment should then guide all of the institution's management of the relationship to minimize material risks.

The TPRM Guidance recognizes that the risks presented by third-party relationships are varied. As an example, the regulators note that a core processor service provider “is likely to touch on many components of a banking organization's operational risk,” while a facilities maintenance third party “may implicate only a relatively limited range of risks, such as physical access risks.” The TPRM Guidance notes that 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,” thereby suggesting that including the subject-matter experts would be prudent.

The TPRM Guidance states that “there is not only one way to properly conduct risk assessments,” but that those 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.” It explains that higher risk 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.” This is similar to what the 2023 Guidance refers to as “critical activities” that justify more comprehensive and rigorous oversight but with the favorable addition of taking into account the material likelihood of the negative consequences.

RISK OVERSIGHT

The largest portion of the TPRM Guidance is devoted to “risk oversight,” primarily because the agencies include five distinct subjects in this component.

Initially, “[e]ffective 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.” The TPRM Guidance encourages organizations to prioritize and tailor their oversight in a manner commensurate with their “size, complexity, and risk profile, as well as with the nature of the third-party relationship.” It notes that 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 risk oversight subject, “Due Diligence and Third Party Selection,” describes the process by which an organization “assesses a third party's ability to perform the activity as expected, adhere to the banking organization's policies, comply with applicable laws and regulations, and conduct the activity in a safe and sound manner.” The amount of due diligence that is warranted “depends on the risk presented” by the relationship and

©2005-2026 K&L Gates LLP. All Rights Reserved.

the organization's “individual business needs.” 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.”

The TPRM Guidance recognizes that an institution may not be able to obtain certain due diligence information from a third party and that these difficulties may be amplified when the institution has limited negotiating power. It suggests that, in these cases, the institution may be able to obtain sufficient information about vendor performance from outside sources, such as “feedback obtained through banking organizations or trade groups, [or] review of available public sources.” In addition, “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, the TPRM Guidance notes these alternative sources may not always be “sufficient to allow the banking organization to engage with the third party within its risk appetite and tolerances.”

The TPRM Guidance addresses “Contract Negotiation” in much less detail and with much less specificity than the 2023 Guidance. It states that there “are no generally applicable expected contract terms for third-party relationships—even for higher-risk relationships.” This is a significant departure from the 2023 Guidance recommending “clearly defined performance measures” for certain relationships and, in particular, a service-level agreement. The TPRM Guidance also recognizes that a banking organization might have limited negotiating power relative to a third party, but it may still reasonably proceed with the relations “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.”

The “Ongoing Monitoring” portion of this risk oversight component also is less detailed than the 2023 Guidance, but it is similar in many respects. Like the 2023 Guidance, it indicates that ongoing monitoring may be conducted on a periodic or continuous basis. However, rather than stating that more comprehensive or frequent monitoring “is appropriate” when a third-party relationship supports higher-risk activities, as is stated in the 2023 Guidance, the TPRM Guidance states that an organization “may determine that effective risk oversight requires” this more comprehensive or frequent monitoring.

Finally, the TPRM Guidance appears to be less prescriptive on contract termination issues than the 2023 Guidance, particularly with respect to contractual provisions. It recognizes that there may be many reasons for an organization to terminate a contract with one third party and transition to another. It states that the agencies “will give due consideration to the 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.”

The TCBO Guide is intended to service as a “companion document” to the TPRM Guidance. It is proposed to be for banking organizations with less than US$30 billion in assets “that focus on serving their local communities,” but the Federal Reserve solicits comment on how the Federal Reserve could further clarify the characteristics of traditional community banking organizations (TCBOs). Like the TPRM Guidance, the TCBO Guide “does not set forth enforceable standards or prescriptive requirements,” but supervisory action may result from any violations of law or unsafe or unsound practices stemming from insufficient management of third-party risk.

©2005-2026 K&L Gates LLP. All Rights Reserved.

The stated goal of the TCBO Guide is to assist TCBOs supervised by the Federal Reserve in understanding and conducting third-party risk management. It “would not be relevant” to non-TCBOs “because it would be specifically tailored to the unique characteristics and risk profiles of TCBOs.” The TCBO Guide is similarly not intended for “community banking organizations with more complex business models or third-party relationship profiles, such as bank-fintech partnerships.” Instead, it describes “overarching third-party risk management considerations” with respect to operational and financial resilience, system and information security, and compliance with rules and regulations. It then explains how these considerations apply for the third-party relationships most common to TCBOs, including core providers, information technology and infrastructure providers, cybersecurity providers, payment processing and digital banking providers, and loan management system providers.

The TPRM Guidance and the TCBO Guide both improve on the 2023 Guidance by not being prescriptive, allowing a risk-based approach, and recognizing that the magnitude and likelihood of harm arising from a third-party relationship are important considerations in determining risks and developing risk-based vendor management policies. With these materials, banking organizations are allowed a more flexible approach to entering into and monitoring their third-party relationships. If there are any potential drawbacks in these materials, it might be that they do not provide detailed parameters or directions for banking organizations when making their risk assessments.

Comments on both the TPRM Guidance and the TCBO Guide must be received on or before 16 November 2026.

KEY CONTACTS



LINDA C. ODOM
PARTNER

WASHINGTON, DC, NASHVILLE
+1.202.778.9363
LINDA.ODOM@KLGATES.COM



JOHN REVEAL
PARTNER

WASHINGTON, DC
+1.202.778.9055
JOHN.REVEAL@KLGATES.COM

This publication/newsletter is for informational purposes and does not contain or convey legal advice. The information herein should not be used or relied upon in regard to any particular facts or circumstances without first consulting a lawyer. Any views expressed herein are those of the author(s) and not necessarily those of the law firm's clients.

©2005-2026 K&L Gates LLP. All Rights Reserved.