Deloitte.

Together makes progress



Third-party risk management: Proposed interagency guidance

September 2026

Center *for*
Regulatory Strategy US

Proposed guidance reflects a more principles, risk-based approach to third-party management

Executive summary

The Federal Deposit Insurance Corporation (FDIC), Federal Reserve Board of Governors (FRB), Office of the Comptroller of the Currency (OCC), and National Credit Union Administration (NCUA) jointly issued proposed Third-Party Risk Management Guidance[1] that would rescind and replace the 2023 Interagency Guidance on Third-Party Relationships: Risk Management and the supplemental TPRM resources.[2] The latest proposal includes the NCUA, unlike the 2023 guidance. If finalized, it would extend its applicability to credit unions within the NCUA's scope.

For those institutions wishing to provide input on the proposal, comments are due November 16, 2026.

The agencies observed that the 2023 guidance was often interpreted by firms as a one-size-fits-all approach to third-party risk management (TPRM). The proposal would replace relatively prescriptive guidance with a more risk-based approach to TPRM considering the firm's size and complexity, the individual third-party relationship, and the risks associated with each relationship. Nevertheless, the proposed guidance would continue to reinforce accountability of firms to identify, assess, and appropriately manage their third-party relationships.

The proposal

The proposed guidance is intended to promote consistency and innovation across the banking industry. It replaces the 2023 guidance's five-stage life cycle with a risk-based approach to scaling practices to the institution's size, complexity, risk profile, and each relationship's assessed risk.

Why the Agencies are acting

The agencies note in the proposal that the 2023 guidance was interpreted broadly, without enough focus on tailoring risk management to the risks associated with each third party. Many firms implemented uniform, process-heavy, checklist-based programs providing the same amount of resources to low- and medium-risk relationships as they did to their highest-risk relationships. The proposed guidance is intended to address the following concerns:

1. One-size-fits-all checklist: Firms applying a single uniform process to their TPRM programs, agnostic of the type of third party (e.g., core providers, fintechs, contractors, or facilities maintenance vendors).
2. Heightened rigor applied too broadly: Firms applying heightened risk management practices to a wide range of third parties, irrespective of the services provided by the third parties and associated risks.
3. Interpreting guidance as prescriptive requirements: Firms not tailoring risk management and instead applying the principles across all third-party relationships, resulting in process-driven approaches that did not always prioritize higher-risk relationships or direct risk management resources to the areas where they were most needed.
4. Hesitation to switch providers: Firms less likely to onboard newer, innovative third parties because they may have presented elevated risks. As a result, some firms may have maintained third-party relationships that may no longer be the most appropriate option.

A refined risk-based approach

The proposed guidance provides firms with a risk-based approach to identify, address, and manage risks associated with third parties. It emphasizes tailoring the approach for each third party to allow firms to focus on higher-risk third parties. The guidance is structured across four components that institutions may consider when managing third-party risk.

1. Risk identification and assessment

Sound TPRM begins with identifying and categorizing third-party relationships and thereafter conducting risk assessments. Risks presented by third parties vary with many factors that should be taken into consideration, including type of third-party entity, nature of services being provided, and the third party's regulatory oversight. The guidance emphasizes the importance for firms to have risk management programs with robust capabilities to identify, categorize, and inventory third-party relationships and that are commensurate with the size of the organization, services provided by the third party, and the magnitude and likelihood of potential harm.

2. Risk oversight and monitoring

The guidance stresses the importance of ensuring proper oversight of third-party risk and ongoing monitoring consistent with the firm's risk appetite and tolerances. This should include due diligence of the third party's financial condition, capabilities, and compliance. The guidance recognizes that banks may have limited leverage in negotiating with large or sole-source providers and notes that there are no universally required contract terms.

3. Residual risk acceptance

The guidance acknowledges that not all third-party risks will be mitigated. Firms should be aware of any residual risks while continuing to operate in a safe and sound manner. Even when a risk cannot be significantly reduced, the relationship may still be beneficial and necessary for the institution to operate effectively and remain competitive.

4. Governance

Firms should have strong risk management processes supported by a governance structure that establishes clear roles and responsibilities for identifying, assessing, monitoring, and reporting third-party risks. The guidance notes that there is not a one-size-fits-all approach and the nature of a firm's third-party relationships will ultimately drive any relevant governance decisions.

Implications for third-party risk management

The proposal offers an opportunity for firms to evaluate their TPRM capabilities and consider ways to improve efficiency by prioritizing higher-risk relationships tailored to the institution's size, complexity, risk profile, and the actual risk of each relationship.

The proposal emphasizes that firms should:

1. Calibrate risk management frameworks and oversight capabilities based on the risk of the third-party relationship.
2. Collaborate with the procurement function to establish standard contract templates for lower-risk relationships and focus negotiations on provisions tied to material risks.
3. Assess the level of review and challenge from the internal audit function.

Spotlight topic: Artificial intelligence

Although not addressed specifically in the proposal, firms should recognize that artificial intelligence (AI) is increasingly embedded in the processes and platforms their third parties use to deliver services, in addition to direct usage by institutions. As AI models move beyond peripheral functions into the critical core of service delivery, including underwriting, transaction monitoring, and decision support, the risk profile of the underlying relationship changes. A vendor that once performed a discrete, well-understood function may now rely on a model whose behavior evolves over time, whose decision logic is difficult to fully explain, and whose failure modes are less predictable than those of traditional software. This concern may be more pronounced for firms relying on frontier or rapidly evolving models, where outputs may be harder to predict.

This shift requires an agile TRPM program capable of evaluating not just the third party, but the AI models it deploys on the firm's behalf. Firms should assess model governance practices, the transparency and stability of model outputs, and the third party's ability to demonstrate ongoing performance monitoring. Equally important is contingency planning. Firms should confirm that processes ported to AI models remain reversible, meaning the organization retains the documentation, institutional knowledge, and operational capability to re-onboard a process internally or transition it to an alternate provider if the model underperforms, behaves unpredictably, or the relationship is terminated. Building this reversibility into the TRPM program, rather than treating AI adoption as a one-way transition, gives firms a practical mitigant against the heightened risks these technologies introduce.

Actions to take now

Firms may consider the following enhancements to align their TPRM frameworks and capabilities to a risk-based structure:

1. Recalibrate relationship-risk tiering: Reassess whether current tiers distinguish relationships based on the magnitude and material likelihood of regulatory violations, material financial harm, or significant operational or customer disruption.
2. Streamline inventories and documentation: Use more detailed relationship mapping where it informs accountability, concentration, or risk decisions for higher-risk providers; reduce documentation for lower-risk administrative, professional, or office-support relationships where extensive records add limited value.
3. Translate risk tiers into differentiated oversight: Define how the depth of due diligence, contracting, monitoring, testing, and exit planning changes by assessed risk. This can help demonstrate that more intensive controls and specialized resources are directed to relationships presenting the greatest potential harm.
4. Formalize residual-risk decisions: Establish a clear process to document when information, contractual protections, or monitoring options are limited; identify compensating measures; and determine whether the remaining risk is within approved appetite and tolerances. These decisions can be calibrated with your firm's overall risk acceptance processes.

5. Reassess contracts through a risk-based lens: Focus negotiation and renewal efforts on provisions that address the relationship's most material risks, including performance, data access, resilience, subcontracting, and termination, rather than pursuing a uniform set of terms. Standard-form agreements may be appropriate for lower-risk relationships.
6. Make monitoring responsive to events: Supplement periodic reviews with triggers for reassessment, such as expanded reliance, material service changes, adverse performance, cyber incidents, financial deterioration, or recurring audit findings. Escalation and reporting should focus on significant issues and the resulting residual-risk position.
7. Validate resilience for higher-risk providers: For relationships whose disruption could materially affect operations or customers, assess whether the firm and provider can resume services and preserve critical data. Use the results to refine recovery expectations, backup arrangements, transition options, and the relationship's risk rating.
8. Clarify governance and independent challenge: Refresh roles across the business, risk, procurement, compliance, and internal audit functions so accountability reflects the relationship's risk. Periodic independent review can test whether the program is effectively prioritizing material risks rather than merely completing required process steps.
9. Monitor third-party deployment of emerging technologies: Track where third parties embed AI and other emerging technologies into critical or customer-facing processes, since their behavior can evolve less predictably than traditional software, particularly for frontier models. Confirm reversibility is built in, so the firm can re-onboard or transition a process if performance degrades or the relationship ends.

Questions firms should ask themselves

TPRM functions should assess their programs against the proposed guidance and ask themselves the following:

- Does the risk management framework take into consideration inherent and residual risk of third-party relationships or does it overemphasize for low-to-medium-risk third parties?
- Are resources allocated appropriately to monitor and mitigate the highest risk areas?
- Are roles and responsibilities calibrated across first line functions and second line oversight?
- Can TPRM demonstrate operational resilience for higher-risk relationships including recovery time objectives, alternative back-up providers, and tested transition plans in case of a disruption of services?
- Do internal audit and the board provide effective independent review and challenge of TPRM?

Toward tailored, risk-based TPRM

The proposal offers an opportunity for firms to move beyond uniform, process-heavy oversight and toward a more tailored approach that concentrates governance, diligence, monitoring, and resilience resources on those relationships that present the greatest potential for material harm. Firms that can evidence this linkage may be better positioned to support both sound risk management and responsible innovation.

Endnotes

1. Office of the Comptroller of the Currency (OCC), Federal Reserve Board of Governors (FRB), Federal Deposit Insurance Corporation (FDIC), National Credit Union Administration, "Proposed Third-Party Risk Management Guidance," *Federal Register*, September 15, 2026.

2. FRB, FDIC, OCC, "SR 23-4: Interagency Guidance on Third-Party Relationships: Risk Management," June 7, 2023.

Contact us

Jennifer Burns
Managing Director
Deloitte & Touche LLP
jennburns@deloitte.com

Suzanne Denton
Managing Director
Deloitte & Touche LLP
sudenton@deloitte.com

Sean Hodgkinson
Principal
Deloitte & Touche LLP
seahodgkinson@deloitte.com

Brian Adams
Senior Manager
Deloitte & Touche LLP
briadams@deloitte.com

Megan Jones
Manager
Deloitte & Touche LLP
meganjones2@deloitte.com

Deloitte Center for Regulatory Strategy, US

Irena Gecas-McCarthy
FSI Director, Deloitte Center for Regulatory Strategy, US
Principal
Deloitte & Touche LLP
igecasmccarthy@deloitte.com

Lananh Nguyen
Co-Director, Deloitte Center for Regulatory Strategy, US
Managing Director
Deloitte Services LP
lananhnguyen@deloitte.com

Aaron Salerno
Manager
Deloitte Services LP
asalerno@deloitte.com

Kyle Cooke
Manager
Deloitte Services LP
kycooke@deloitte.com

Special thanks to Deloitte team members *Vignesh Sethumadhavan Venkatesh* and *Shruthi Kundar* for their contributions.

Deloitte.

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

About Deloitte

As used in this publication, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2026 Deloitte Development LLC. All rights reserved.