ANONYMOUS

Proposal and Comment Information

Title: Proposed Third-Party Risk Management Guidance, OP-1881

Comment ID: FR-2026-0031-01-C66

Submitter Information

Name: Anonymous

Submitted Date: 11/16/2026

The document includes a consolidated public comment regarding the third-party risk management guide for:
- FDIC-2026-1750-0001
- FRS-2026-4028-0001
- FRS-2026-4027-0001
- OCC-2026-0793-0001
- NCUA-2026-1684-0001

Third-Party Risk Management Interagency Guidance and Community Bank Guide

Agency / proceeding	Docket number
FDIC	**FDIC-2026-1750-0001**
Federal Reserve — interagency guidance	**FRS-2026-4028-0001**
OCC	**OCC-2026-0793-0001**
NCUA	**NCUA-2026-1684-0001**
Federal Reserve — community bank guide	**FRS-2026-4027-0001**

To the Federal Deposit Insurance Corporation, the Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency, and the National Credit Union Administration:

I respectfully submits this consolidated comment on the proposed Interagency Third-Party Risk Management Guidance, published at 91 Fed. Reg. 58536 (September 15, 2026), and the Federal Reserve Board's proposed Third-Party Risk Management Guide for Traditional Community Banking Organizations, published at 91 Fed. Reg. 58438 (September 15, 2026). This comment is intended to address the five docket records listed above. The two proposals are related but distinct: the interagency guidance is the general framework, while the Federal Reserve community-bank guide is a supplementary resource for a narrower group of Federal Reserve-supervised institutions. [1] [2] Requested action: adopt a principles-based framework with explicit statutory floors and operational safeguards

I. EXECUTIVE SUMMARY

The proposed move toward more tailored, principles-based third-party risk management is capable of producing meaningful benefits. A bank or credit union should not be required to apply identical controls to every vendor, and supervision should not reward paperwork for its own sake. Risk assessments should account for the institution's size, complexity, resources, the service performed, the sensitivity of information involved, the degree of operational dependence, and the potential effect on customers and members.

But flexibility must not become a reason to leave material risks unexamined or to treat management's stated risk appetite as a substitute for binding law. The central concern is the combined effect of several features of the proposals: the invitation to consider whether the framework should apply only to vendors with direct written agreements; the absence of a presumption of direct bank oversight of subcontractors; the absence of generally applicable contract expectations even for higher-risk relationships; and the fact-specific acceptance of residual risk where bargaining power or alternatives are limited. [1]

The proposed community-bank guide raises additional issues. It is designed for traditional community banking organizations with less than $30 billion in assets that focus on their local communities; it is not intended for institutions with more complex relationship profiles, including certain bank-fintech distribution arrangements; and consumer compliance is outside the guide's scope. The Board also specifically asks whether deposit placement networks should be added as a vendor category. [2]

The comment therefore supports risk-based tailoring, but requests that the agencies revise and supplement the proposals to:

1. Preserve a functional definition of material third-party relationships that does not turn solely on direct contractual privity or the form of a written agreement.
2. Require risk-proportionate visibility and control over material subcontractors and critical supply-chain dependencies.
3. State expressly that residual risk cannot be accepted where doing so would violate applicable law or regulation, or result in unsafe or unsound operations.
4. Require institutions to consider minimum contractual subjects for material and critical services, including information security, regulatory access, incident reporting, subcontractors, resilience, data portability, and exit rights.
5. Identify reassessment triggers and minimum monitoring principles for material and critical vendors.
6. Supplement institution-level assessments with interagency monitoring of concentration among common critical providers.
7. Clarify the continuing application of privacy, consumer-protection, fair-lending, and other legal requirements to outsourced activities, where those laws apply.
8. Publish a document-by-document crosswalk explaining what replaces each rescinded or superseded supervisory resource.
9. Clarify that the community-bank guide is illustrative, does not create de facto supervisory standards, and does not limit consumer-compliance obligations.
10. Add specific guidance for deposit placement networks, complex fintech relationships, foreign service providers, and vendor-controlled automated decision systems.

II. THE TWO PROPOSALS SHOULD BE READ TOGETHER, BUT THEIR DISTINCT SCOPES MUST REMAIN CLEAR

The proposed interagency guidance would apply across the agencies' supervised populations, including insured credit unions, and would replace the 2023 Interagency Guidance on Third-Party Relationships: Risk Management and identified supplemental resources. The proposal describes risk identification, assessment, oversight, residual-risk acceptance, and governance as the principal components of the framework. [1]

The separate Federal Reserve guide is expressly a companion resource for traditional community banking organizations supervised by the Board. The Board defines that group as banking organizations with less than $30 billion in assets that focus on serving local communities. The guide excludes consumer compliance from its scope and is not intended for more complex business models or third-party relationship profiles, including certain fintech distribution arrangements. It also states that its suggestions are illustrative and nonbinding. [2]

A single comment can appropriately address both proposals, provided it does not conflate them. The interagency guidance should establish the common principles and statutory boundaries. The community-bank guide should explain how those principles may be operationalized by eligible Federal Reserve-supervised community banks without implying that the guide covers all community banks, all complex business models, or consumer compliance.

III. THE FINAL GUIDANCE MUST PRESERVE BINDING STATUTORY AND REGULATORY OBLIGATIONS

The proposed guidance is supervisory guidance, not a regulation. The agencies may revise nonbinding supervisory guidance and may tailor supervisory materials to different institutions and risks. The comment does not contend that every example in the 2023 guidance is a binding legal requirement, that every subcontractor must be directly supervised by a bank, or that the agencies lack authority to change their approach.

The relevant distinction is between nonbinding supervisory practices and independent legal duties. For insured depository institutions, 12 U.S.C. § 1831p-1 directs appropriate Federal banking agencies to prescribe operational

and managerial standards, including standards addressing internal controls and information systems. [4] The Gramm-Leach-Bliley Act establishes an affirmative and continuing obligation to respect customer privacy and protect the security and confidentiality of nonpublic personal information, and directs federal regulators to establish appropriate administrative, technical, and physical safeguards. 15 U.S.C. §§ 6801(b), 6805. [5]

Those statutory duties are implemented through agency-specific information-security requirements. Examples include the FDIC's 12 C.F.R. part 364, appendix B; the OCC's 12 C.F.R. part 30, appendix B; and the Federal Reserve's 12 C.F.R. part 208, appendix D-2. These standards address service-provider arrangements, including due diligence, contractual obligations to implement appropriate safeguards, and risk-based monitoring. [6] The precise requirements and supervisory jurisdiction differ by institution and charter; the final interagency guidance should identify those differences rather than imply a single identical legal framework for every bank and credit union.

For federally insured credit unions, 12 C.F.R. § 748.0 requires a written security program designed to protect the security and confidentiality of member records, protect against anticipated threats, and respond to unauthorized access. Section 748.1(c) requires reporting of qualifying cyber incidents to NCUA as soon as possible and no later than 72 hours after the credit union reasonably believes it has experienced a reportable incident, subject to the rule's terms. Appendix A to part 748 contains additional service-provider guidance; it should not be mischaracterized as an independently binding regulation, although the underlying rule remains binding. [7]

The Bank Service Company Act, 12 U.S.C. § 1867(c), subjects services within the statute's scope and performed for a depository institution by contract or otherwise to examination and regulation to the same extent as if performed by the institution itself. This is not universal direct examination authority over every fourth party. It is, however, a reason for the final guidance to preserve applicable examination rights and to ensure that contractual arrangements do not obstruct access to information needed by supervisors. [8]

Consumer financial laws also remain applicable where their statutory coverage and jurisdictional requirements are met. The Consumer Financial Protection Act defines "service provider" to include persons providing material services in connection with a covered person's consumer financial product or service, subject to statutory exceptions. 12 U.S.C. § 5481(26). Sections 1031 and 1036, codified at 12 U.S.C. §§ 5531 and 5536, address unfair, deceptive, or abusive acts or practices and other prohibited conduct by covered persons and service providers. [9] Other consumer statutes, including the Equal Credit Opportunity Act, Fair Credit Reporting Act, and Electronic Fund Transfer Act, apply according to their respective terms.

The agencies should state plainly that no risk appetite, contract limitation, vendor refusal, or supervisory tailoring decision excuses compliance with an applicable statute, regulation, order, or enforceable supervisory requirement. Outsourcing a task does not outsource the institution's own legal responsibility.

IV. SPECIFIC CONCERNS AND REQUESTED REVISIONS

A. Preserve functional coverage; do not make contractual form dispositive

The proposed interagency guidance defines a third-party relationship as a business arrangement with an entity or individual for products, services, or other activities that support the banking organization. A footnote observes that third-party relationships typically involve written agreements and asks whether the guidance should apply only to third parties subject to a written agreement directly with the banking organization. [1]

The agencies should not adopt a rule under which material risk falls outside the framework merely because the bank lacks direct contractual privity with the entity performing the activity. Modern service arrangements can include program managers, platform operators, data processors, cloud infrastructure, payment intermediaries, identity-verification providers, and further subcontractors. The institution may have a direct contract with one provider while the operational or information risk is created by another entity in the chain.

A functional approach would assess the service actually performed, access to customer or member information, access to systems, role in customer-facing products, ability to affect payment or account activity, degree of operational dependence, and likely impact of disruption or failure. The intensity of oversight may be tailored; the existence of material risk should not depend solely on the contract's drafting or the number of intermediaries.

Requested revision: Confirm that material activities and dependencies may be considered within the risk assessment whether performed by a direct contractor, affiliate, subcontractor, or other entity acting through the primary provider. Explain that direct contractual privity is not a prerequisite to identifying or managing a material risk.

B. Establish proportionate visibility into material subcontractors

The proposal states that subcontractors do not typically create an independent third-party relationship or a presumption of direct bank oversight. It also acknowledges that subcontractors may heighten risk by reducing the institution's control and suggests contractual requirements or review of the primary provider's own third-party risk management program as possible means of oversight. [1]

That approach is reasonable for ordinary low-risk suppliers but needs clearer direction for material subcontractors. A primary vendor may not have adequate visibility or leverage over a cloud infrastructure provider, payment-routing processor, data center, identity provider, or foreign-based subprocessor. A bank's review of the primary vendor's general program may not reveal a material dependency, a new processing location, a concentration point, or an incident affecting customer information.

The final guidance should require institutions to obtain, proportionate to the risk, identification of material subcontractors; notice of material additions, substitutions, or changes in location; confirmation of appropriate security and resilience controls; contractual flow-down of relevant confidentiality, security, incident-notification, and regulatory-cooperation obligations; and sufficient audit or assessment information to evaluate the chain. It should not require every institution to negotiate directly with every subcontractor. It should require the institution to have adequate information and control over the material risks created by that chain.

For credit unions, the final guidance should expressly connect subcontractor risk to the information-security program and the 72-hour cyber-incident reporting framework in 12 C.F.R. § 748.1(c), including the need for timely vendor-to-credit-union notification where third-party events may trigger reporting. [7]

C. Bound residual-risk acceptance by nonwaivable legal obligations

The proposal recognizes that residual risk is not always eliminated and that an institution may lack bargaining power, sufficient due-diligence access, customized contractual terms, or alternative providers. It states that a relationship may still be beneficial and necessary if residual risks are within the institution's risk appetite and the institution continues to operate safely and soundly. [1]

A risk-based framework should acknowledge unavoidable residual risk. But a management-approved risk appetite is not a legal waiver. An institution cannot accept a risk that results in noncompliance with an applicable information-security rule, unlawful consumer practice, violation of a regulatory order, or unsafe or unsound operation. A vendor's market power may explain why a control is difficult to obtain; it does not itself make a legally deficient arrangement permissible.

The final guidance should distinguish at least four categories: (1) ordinary residual risk that can be accepted through documented governance; (2) material unresolved risk requiring compensating controls, escalation, and periodic reassessment; (3) critical-service risk requiring time-limited remediation, enhanced monitoring, and a tested contingency or exit plan; and (4) risk that would cause violation of law or regulation or unsafe or unsound operations, which cannot be accepted merely because management approves it. Material and critical risk acceptance should be documented, approved at an appropriately senior level, and revisited when conditions change.

D. Preserve contract protections required by law and identify core subjects for critical services

The proposal states that there are no generally applicable expected contract terms, even for higher-risk relationships, and that an examiner's disagreement with a specific contractual term would not alone support an

adverse finding. It nevertheless identifies confidentiality, information security, subcontractor use, operational resilience, and termination as matters that may be relevant to contract negotiations. [1]

The final guidance should retain flexibility over contract form while clarifying that specific contract protections are required where binding rules require them or where they are necessary to manage a material or critical risk. For example, the FDIC and Federal Reserve information-security guidelines expressly address service-provider oversight and require appropriate contractual security measures for covered arrangements. [6]

For material and critical services, institutions should be directed to consider, as relevant to the service and applicable law, contractual provisions addressing:

- confidentiality, permitted uses of information, access controls, security safeguards, and secure data return or destruction;
- prompt notice of security incidents, service disruptions, material control failures, and events that may trigger regulatory reporting;
- institutional and regulatory access to relevant records, systems, personnel, audit reports, and information, subject to applicable law;
- identification and oversight of material subcontractors, notice of material changes, and appropriate flow-down obligations;
- service levels, data integrity, operational resilience, business continuity, disaster recovery, and testing;
- data portability, transition assistance, records retention, and orderly termination or replacement;
- cooperation with examinations, investigations, complaints, disputes, and legally required reporting.

The guidance should clarify that no confidentiality clause, vendor policy, or contract term can override lawful regulatory examination authority or prevent the institution from meeting its legal duties. A lack of bargaining power should be treated as a risk factor requiring compensating measures or an exit decision where appropriate, not as a blanket exception.

E. Provide monitoring triggers and minimum principles for changing risk

A point-in-time risk rating is not sufficient for a relationship whose risk can change rapidly. The final guidance should identify reassessment triggers for material providers, including a material cyber incident; repeated service outages; a change in ownership or financial condition; use of a new material subcontractor; a change in data location or processing; migration to a new platform or model; material changes in customer-facing activity; a significant increase in dependence; and adverse audit or control findings.

Monitoring frequency and depth may vary with risk, but institutions should document why a reduced monitoring approach remains adequate for a material provider. Critical services warrant monitoring that is responsive to the pace and severity of the risk rather than treating an annual review as automatically sufficient.

F. Address common-provider concentration at the system level

The proposal recognizes that a bank may face concentration risk when it depends extensively on one provider. [1] It should also address concentration that exists across institutions. A service provider may appear manageable to each institution when assessed alone but support hundreds of banks or credit unions. A single cyberattack, software update, insolvency, or service interruption may cause correlated disruption across the financial sector.

Institution-specific risk assessments cannot substitute for an interagency view of common critical dependencies. The agencies should describe how they will identify and monitor material concentration among core processors, cloud and data infrastructure, payment systems, identity and authentication providers, critical software, and shared subcontractors. The agencies should consider coordinated information sharing, cross-agency incident analysis, and appropriate communication to affected institutions. This request is for regulator-level monitoring; it does not assume that an existing statute mandates a particular new reporting inventory.

G. Integrate customer protection, privacy, and automated decision risks

The interagency proposal acknowledges that third-party arrangements may raise consumer-compliance considerations but does not directly address them. [1] The community-bank guide expressly places consumer compliance outside its scope. [2] Those scope statements should not be read to reduce or displace any applicable consumer-protection requirement.

Third parties may operate customer interfaces, process payments, service loans, determine fraud flags, support credit underwriting, calculate fees, resolve complaints, or produce account and credit data. Errors can cause customers to lose access to funds, receive inaccurate information, incur unauthorized fees, face erroneous account restrictions, or receive credit decisions inconsistent with applicable law. When a provider's system or personnel perform these functions, the institution still needs controls sufficient to meet its own obligations. A third party may also be directly subject to consumer-protection requirements if it meets the statutory definition of a service provider or covered person. [9]

The final framework should call for proportionate oversight of consumer-impacting services, including accuracy testing, complaint and dispute trend monitoring, escalation of recurring errors, assessment of data use and retention, review of automated decision systems where relevant, and vendor cooperation with investigations. For automated systems used in credit, fraud, identity, or account-management decisions, the institution should have sufficient access to testing results and change information to evaluate performance, error rates, and compliance with applicable law. This is not a request to impose one model-governance checklist on every vendor; it is a request to ensure that institutions can demonstrate meaningful oversight when vendor systems materially affect customers.

H. Preserve a complete supervisory crosswalk for rescinded or superseded materials

The interagency proposal states that final guidance would replace the 2023 interagency guidance and supplemental third-party risk management resources. It identifies OCC Bulletin 2002-16 on foreign-based service providers; the July 25, 2024 joint statement on banks' arrangements with third parties to deliver deposit products; and the 2024 community-bank third-party risk management guide. It also invites comment on whether additional guidance, interpretive letters, or resources should be rescinded. [1]

These resources address different risks. Foreign service-provider guidance addresses access to critical information and the ability of the OCC to supervise operations when data or processing are located abroad. The 2024 bank-fintech statement describes risks in arrangements used to deliver bank deposit products and services. The 2024 community-bank guide provides practical context for smaller institutions. [13] [14] [15]

The agencies should publish a document-by-document crosswalk identifying each resource to be rescinded, the specific subject matter it addresses, the replacement provision, any topic not carried forward, and the agency responsible for future interpretation. The agencies should retain or replace specialized material where the new general guidance does not address the same risk with sufficient specificity. The final guidance should also identify how foreign law, data location, government access, insolvency, information access, and supervisory cooperation are to be addressed in foreign-based arrangements.

I. Improve the community-bank guide without creating a de facto checklist

The Federal Reserve guide expressly says it is not enforceable, that noncompliance with the guide alone will not result in supervisory criticism, and that its examples are illustrative. [2] Those statements should be retained prominently in the final document and reflected in examination practice. Institutions should not be criticized merely for choosing a different method that effectively manages the same risk. Conversely, the guide should not be treated as a substitute for binding regulations or institution-specific supervisory requirements.

The guide should explain more fully how its scope interacts with the all-bank framework for community banks that have complex fintech distribution arrangements or other nontraditional vendor profiles. It should clarify that excluded business models remain subject to the all-bank guidance and all applicable laws and regulations, and that

the guide's exclusion of consumer compliance is a subject-matter limitation only—not a consumer-law exemption. [2]

The Board specifically asks whether deposit placement networks should be added as a vendor category. [2] They should. The guide should address, as relevant, account allocation and recordkeeping, reconciliation and data accuracy, intermediary insolvency, customer access to funds, concentration, pass-through deposit insurance representations, disclosure and complaint handling, and continuity and transition if the network or an intermediary fails. The guide should also cross-reference the July 2024 joint statement concerning bank deposit products and third-party arrangements. [14]

J. Explain the policy change and address reliance interests

The agencies explain that the 2023 guidance has, in their view, been interpreted too broadly, has encouraged process-driven compliance, has been difficult to tailor, and may have discouraged some innovative third-party relationships. [1] Those are legitimate policy considerations for the agencies to evaluate. But the final decision should also explain how the agencies assessed the consequences of replacing the earlier framework, including the rescission of specialized resources and any reliance interests created by long-standing supervisory materials.

The Administrative Procedure Act requires agency action to be reasoned and not arbitrary or capricious. 5 U.S.C. § 706(2)(A). The Supreme Court has explained that an agency changing policy must acknowledge the change and provide a reasoned explanation, including consideration of relevant reliance interests where they exist. Motor Vehicle Manufacturers Ass'n v. State Farm Mutual Automobile Insurance Co., 463 U.S. 29, 43 (1983); FCC v. Fox Television Stations, Inc., 556 U.S. 502, 515–16 (2009); Encino Motorcars, LLC v. Navarro, 579 U.S. 211, 221–22 (2016).

This comment does not claim that the proposals are automatically unlawful because they are nonbinding guidance or because they replace prior guidance. Nor does it claim that every policy change requires a more extensive explanation than the APA demands. It requests a reasoned account of the practical safeguards that will remain, the risks that may be less visible under the new framework, the treatment of specialized resources, and how the agencies will keep guidance nonbinding in practice. The D.C. Circuit has cautioned that an agency document nominally labeled guidance can raise concerns when it operates as a binding norm in practice. Appalachian Power Co. v. EPA, 208 F.3d 1015, 1020–23 (D.C. Cir. 2000).

V. AGENCY-SPECIFIC LEGAL DIFFERENCES SHOULD BE ACKNOWLEDGED IN THE COMMON FINAL FRAMEWORK

The agencies share an interest in safe, sound, and resilient financial institutions, but they do not administer identical statutes or regulations. The final guidance should therefore include a concise agency-by-agency crosswalk rather than implying that every provision has the same legal basis for every supervised entity.

For FDIC-supervised institutions, the crosswalk should identify the relationship between the guidance, 12 U.S.C. § 1831p-1, 15 U.S.C. §§ 6801 and 6805, and 12 C.F.R. part 364, appendix B. For Federal Reserve-supervised institutions, it should identify the relevant Federal Reserve information-security standards and supervisory authorities, including 12 C.F.R. part 208, appendix D-2, as applicable. For OCC-supervised institutions, it should identify 12 C.F.R. part 30, appendix B, the scope of Bank Service Company Act examination authority, and the status of foreign-provider guidance. For federally insured credit unions, it should separately identify the Federal Credit Union Act authorities, 12 C.F.R. part 748, the 72-hour cyber-incident rule, and the status of NCUA Appendix A guidance. [4] [6] [7] [8] [10]

The final joint document should also state which agency is responsible for interpreting and applying each component to its supervised population, how differences in agency regulations are to be respected, and how institutions can obtain clarification when the same service arrangement spans multiple charter types or regulators.

VI. REQUESTED CHANGES TO THE FINAL GUIDANCE AND COMMUNITY-BANK GUIDE

For the reasons above, the agencies should:

1. Retain a functional definition of third-party relationships and reject a categorical limitation to direct written agreements.

2. Require risk-based identification and oversight of material subcontractors, with appropriate notice, flow-down obligations, and access to sufficient audit and security information.

3. State that no institution may accept residual risk that would cause a violation of applicable law or regulation, or an unsafe or unsound practice.

4. Identify core contractual subjects to consider for material and critical services, while allowing institutions to tailor the exact wording and controls to the risk.

5. Establish material-provider reassessment triggers and explain what constitutes adequate ongoing monitoring for critical services.

6. Describe an interagency approach to monitoring concentration in shared critical service providers and common subcontractor dependencies.

7. Clarify that the consumer-compliance exclusions in the proposals do not limit applicable consumer, privacy, fair-lending, or data-protection laws.

8. Include expectations for material vendor-managed automated systems where they affect credit, payments, fraud, identity, account access, or consumer communications.

9. Publish a document-by-document rescission and replacement crosswalk for the 2023 guidance and all supplemental resources, including the foreign-service-provider material, 2024 bank-fintech deposit statement, and 2024 community-bank guide.

10. Add a dedicated deposit-placement-network section to the community-bank guide and clarify the treatment of complex fintech business models.

11. Preserve clear language that the community-bank guide is illustrative and nonbinding, and ensure examiners do not use it as a de facto checklist.

12. Publish an agency-specific legal crosswalk for FDIC, Federal Reserve, OCC, and NCUA authorities and regulations.

VII. QUESTIONS THE AGENCIES SHOULD ANSWER IN THE FINAL RECORD

1. Will material third-party risk be assessed when the service performer lacks a direct written agreement with the bank or credit union? If not, how will indirect dependencies be identified?

2. What information about material subcontractors must the institution obtain, and what should it do when the primary vendor cannot or will not provide it?

3. What criteria distinguish acceptable residual risk from risk that is inconsistent with binding legal requirements or safe-and-sound operations?

4. How should institutions ensure that confidentiality or standard-form contract clauses do not impede legally required examination, audit, incident reporting, or data access?

5. What minimum reassessment triggers should apply to critical providers, including material cyber incidents, ownership changes, subcontractor changes, and service disruptions?

6. How will the agencies identify common dependencies and concentration among critical providers that serve multiple supervised institutions?

7. Which protections from each rescinded resource will be retained, and where will the final guidance address foreign providers, bank-fintech deposit arrangements, and community-bank-specific risks?

8. How will the agencies prevent the community-bank guide from becoming a de facto supervisory checklist while ensuring that its scope exclusions are not misunderstood as exemptions from law?

9. Will the community-bank guide include deposit placement networks, and how will it address allocation records, reconciliations, pass-through insurance representations, intermediary failure, and access to funds?

10. What agency-specific statutes and regulations govern the final guidance for each regulated population, including insured credit unions?

VIII. CONCLUSION

A tailored, principles-based approach can be appropriate and beneficial. The agencies should not seek to eliminate all risk, impose identical controls on every vendor, or turn nonbinding examples into mandatory checklists. But flexibility must remain bounded by binding law and supported by adequate information, meaningful monitoring, and credible contingency arrangements for material and critical services.

The final framework should make clear that an institution may choose how to manage risk, but may not choose whether to comply with applicable law. It should preserve functional oversight of material service arrangements, require proportionate visibility into subcontractors, distinguish manageable residual risk from legally impermissible risk, preserve appropriate contractual and examination protections, and address shared critical-provider concentration. The community-bank guide should add practical detail for its intended audience without creating de facto standards or obscuring obligations that remain applicable outside its scope.

The requested revisions would preserve the benefits of tailoring while making the framework more transparent, legally precise, and effective in protecting depositors, credit union members, borrowers, customers, and the resilience of the financial system.

Reference

The citations below are consolidated for this comment. Statutes and regulations should be read together with the agency-specific jurisdictional rules applicable to the institution and activity at issue.

[1] Proposed Third-Party Risk Management Guidance, 91 Fed. Reg. 58536–58544 (Sept. 15, 2026), Federal Register Document No. 2026-18859 (including the definition and scope of third-party relationships, subcontractors, contract negotiation, residual risk acceptance, and proposed replacement of prior resources). Official source

[2] Proposed Third-Party Risk Management Guide for Traditional Community Banking Organizations, 91 Fed. Reg. 58438–58446 (Sept. 15, 2026), Federal Register Document No. 2026-18852. Official source

[3] Board of Governors of the Federal Reserve System, Agencies Extend Comment Period for Proposed Third-Party Risk Management Guidance (Nov. 13, 2026) (extending both comment periods to Dec. 16, 2026). Official source

[4] 12 U.S.C. § 1831p-1 (standards for safety and soundness; applies to insured depository institutions under the statute and should not be treated as the parallel statutory source for NCUA credit-union duties). Official source

[5] 15 U.S.C. §§ 6801(b), 6805 (Gramm-Leach-Bliley Act safeguards and enforcement). Official source

[6] 12 C.F.R. pt. 364, app. B (FDIC); 12 C.F.R. pt. 30, app. B (OCC); 12 C.F.R. pt. 208, app. D-2, and pt. 225, app. F (Federal Reserve), Interagency Guidelines Establishing Information Security Standards, including oversight of service-provider arrangements. FDIC eCFR | OCC eCFR | Federal Reserve, Part 225 | Federal Reserve, Part 208

[7] 12 C.F.R. §§ 748.0, 748.1(c), and app. A to pt. 748 (NCUA security program and cyber-incident reporting; Appendix A supplies service-provider guidance and should not be characterized as an independently binding regulation). Official source

[8] 12 U.S.C. § 1867(c) (Bank Service Company Act; examination authority for services within the scope of the Act performed for a depository institution by contract or otherwise). Official source

[9] 12 U.S.C. §§ 5481(26), 5531, 5536 (Consumer Financial Protection Act definitions and prohibitions applicable to covered persons and service providers, subject to statutory scope and exceptions). Official source

[10] 12 U.S.C. §§ 1786, 1789 (Federal Credit Union Act supervisory, enforcement, and administrative authorities). Official source

[11] 12 U.S.C. § 1818 (enforcement authority of appropriate federal banking agencies, as applicable). Official source

[12] Interagency Guidance on Third-Party Relationships: Risk Management, 88 Fed. Reg. 37920 (June 9, 2023). Official source

[13] Office of the Comptroller of the Currency, OCC Bulletin 2002-16, Bank Use of Foreign-Based Third-Party Service Providers: Risk Management Guidance (May 15, 2002). Official source

[14] Board of Governors of the Federal Reserve System, SR 24-5 (July 25, 2024), Joint Statement on Banks' Arrangements with Third Parties to Deliver Bank Deposit Products and Services; see also FDIC FIL-45-2024. Official source

[15] Office of the Comptroller of the Currency, OCC Bulletin 2024-11; Federal Reserve SR 24-2 / CA 24-1; FDIC FIL-19-2024, Third-Party Risk Management: A Guide for Community Banks (May 3, 2024). Official source

[16] 15 U.S.C. §§ 1691 et seq. (Equal Credit Opportunity Act); 15 U.S.C. §§ 1681 et seq. (Fair Credit Reporting Act); 15 U.S.C. §§ 1693 et seq. (Electronic Fund Transfer Act), where applicable. Official source

[17] 5 U.S.C. § 706(2)(A) (judicial review of agency action under the arbitrary-and-capricious standard). Official source

[18] Motor Vehicle Manufacturers Ass'n v. State Farm Mutual Automobile Insurance Co., 463 U.S. 29, 43 (1983) (reasoned decisionmaking and consideration of relevant factors). Official source

[19] FCC v. Fox Television Stations, Inc., 556 U.S. 502, 515–16 (2009) (agency policy change and reasoned explanation). Official source

[20] Encino Motorcars, LLC v. Navarro, 579 U.S. 211, 221–22 (2016) (unexplained inconsistency and reliance interests). Official source

[21] Appalachian Power Co. v. EPA, 208 F.3d 1015, 1020–23 (D.C. Cir. 2000) (guidance that operates as a binding norm in practice). Official source

Filing note: This is one consolidated comment addressing both proposals and all five docket records listed on the first page.