

DIGITALTRADE4.EU, RIHO VEDLER

Proposal and Comment Information

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

Comment ID: FR-2026-0031-01-C12

Submitter Information

Organization Name: DigitalTrade4.EU

Organization Type: Foreign

Name: Riho Vedler

Submitted Date: 10/02/2026

This response supports a principles-based, proportionate approach to third-party risk management and focuses on higher-risk relationships where banks rely on external information or analytical outputs. It recommends assessing material upstream dependencies, monitoring whether outputs remain current and usable, ensuring safe fallback and transition options, and treating AI as an analytical tool rather than an authoritative source—without creating new mandatory inventories, risk categories, or AI-specific requirements.

MATERIAL INFORMATION DEPENDENCIES, OPERATIONAL
RESILIENCE AND USABLE OUTPUTS

Response to Proposed Third-Party Risk Management Guidance

DigitalTrade4.EU

Contact: Riho Vedler | secretariat@digitaltrade4.eu | October 2026 | Docket No. OP-1881 | v4

Abstract. DigitalTrade4.EU comments on the proposed interagency Third-Party Risk Management Guidance, focusing on higher-risk relationships in which a banking organization materially relies on information or analytical outputs supplied through a third party. The response supports the proposal's principles-based, risk-focused direction and addresses the written-agreement scope question and the request for characteristics of higher-risk relationships. It recommends keeping direct TPRM obligations relationship-based while allowing material upstream dependencies to inform risk assessment; distinguishing authoritative source information from assurance and analytical outputs; and using current-state validity, safe fallback, transition usability and reconstructability as optional implementation examples. The response also explains how these concepts fit the agencies' Community Bank Guide, Joint Statement on core providers and current model-risk guidance without creating a new risk category, universal inventory, mandatory technology or AI-specific TPRM regime.

KEY WORDS. third-party risk management; operational resilience; material information dependency; source traceability; exit and transition; AI and analytical services.

1. Introduction

The OCC, Board of Governors of the Federal Reserve System, FDIC and NCUA propose to replace the 2023 interagency third-party risk management guidance with a more streamlined framework centered on risk identification, assessment, proportionate oversight, residual-risk acceptance and governance. The proposal is explicitly non-binding and seeks to focus resources on the magnitude and likelihood of harm rather than on checklist-style treatment of broad categories of third parties.^{1,2}

This response addresses a narrow implementation question within that framework: how to assess a higher-risk relationship when a material banking function relies on an external information or analytical output that can remain technically available while becoming stale, superseded, misapplied or otherwise unfit for the bank's purpose. The issue is operational rather than technological. It concerns the bank's ability to understand what it relies on, detect meaningful change, use a safe fallback and explain important prior decisions.

The recommendations below stay within ordinary TPRM concepts. They offer optional U.S.-anchored examples for higher-risk relationships and do not create a new risk category, provider class, universal inventory, technology mandate or AI-specific regime.

2. Executive Summary and Direct Responses

The response recommends four limited clarifications, all subordinate to the proposal's existing magnitude-and-likelihood test, tailoring and residual-risk judgment.

Key recommendations—For higher-risk information-intensive relationships:

1. Keep direct TPRM obligations tied to the bank's actual third-party relationship, while allowing material upstream dependencies to inform the risk assessment of that relationship.
2. Where useful, identify the material banking function, critical source or upstream input, relied-upon output, principal failure modes and tested fallback using existing risk records.
3. Allow external assurance to reduce duplication while preserving the distinction between the underlying state, the assurance or analytical output, and the bank's accountable decision.
4. Use material-change, reachable-but-unusable, safe-resumption, transition and analytical-service examples to make oversight more testable without creating universal or AI-specific controls.

Written-agreement scope question—Advantages: a written-agreement boundary improves administrability and clarifies which relationships receive direct lifecycle oversight. Disadvantage: if treated as a limit on risk visibility, it can obscure a material upstream dependency. Suggested clarification: a non-contractual upstream source need not become a separately managed third party merely because the direct provider relies on it, but may be considered when it materially affects harm, substitutability, compliance, continuity or data access.

High-risk characteristics question (Federal Register note 15)—A short, expressly non-exclusive list could be useful if it remains subordinate to the proposal's magnitude-and-likelihood test. Four practical indicators are: (1) critical-path reliance, where an output feeds a material process with limited independent validation; (2) ability of the provider or a critical upstream dependency to change, gate or invalidate material state; (3) time sensitivity or weak fallback, where an error quickly makes the output unusable; and (4) reconstructability risk, where loss of source, version, status or decision context would prevent explanation of a material prior action.

Tailoring and residual-risk acceptance—DigitalTrade4.EU supports the proposal's recognition that residual risk cannot always be eliminated. Where current status, source authority, change controls or workable fallback remain uncertain in a higher-risk relationship, that uncertainty can be considered explicitly in the bank's residual-risk decision rather than converted into a mandatory control requirement.

3. Relationship Risk and Material Information Dependencies

The proposed guidance assesses risk by both magnitude of harm and likelihood of occurrence, and it allows assessment at the overall relationship or activity level. For information-intensive services, this can include whether the bank's material function depends on a particular output, not only whether the provider itself is generally available or financially sound.¹

Provider relationship and relied-upon output—A vendor may be financially sound, contractually compliant and technically available while a particular output becomes stale, incorrectly attributed, superseded or bound to the wrong context. If the bank materially relies on that output, the resulting risk is part of the relationship's operational or compliance profile.

Minimal functional mapping—For a higher-risk relationship, an existing inventory or risk record may be supplemented, where useful, with the material banking function, critical source

or upstream input, relied-upon output, principal failure modes and fallback. The depth should remain proportionate to the relationship risk.

4. Upstream Dependencies Without Scope Expansion

The written-agreement boundary can remain useful for identifying the relationship to which direct TPRM practices apply. It should not, however, prevent a bank from considering a material upstream dependency as a fact about the risk of its direct provider and the service being delivered.

Direct-scope boundary—A relationship-based approach avoids turning every public register, standards body, communications network, data source or remote software component into a separately managed third party. That administrability benefit should be preserved.

Dependency visibility—A direct provider may nevertheless rely on a registry, status service, cloud component, model provider, trust service or other source whose failure can materially alter the service. The bank can understand that dependency and its failure mode without having a direct contract with, or unrestricted access to, the upstream entity.

5. Due Diligence, External Assurance and Source-to-Decision Traceability

The proposed guidance allows supplemental information sources when direct due-diligence information is incomplete and recognizes consortia, certifications, auditors and other external assurance mechanisms. These can improve efficiency, especially where a bank cannot obtain every underlying technical detail.¹

Assurance can be reusable without becoming authoritative—A certification, SOC report, network attestation or consortium assessment can support the bank's risk decision, but it does not necessarily establish that the underlying customer, transaction, identity or status information was current and correct at the moment of reliance.

Source-to-decision distinction—Where material, the bank may distinguish the underlying source information, evidence that a check or verification occurred, a derived score or analytical result, and the bank's own decision. This is especially useful when the provider exposes only a summarized outcome.

Risk-based traceability—For higher-risk outputs, due diligence can focus on source authority, current status, material changes, correction or revocation handling, and whether the bank can explain the basis of its reliance. Lower-risk services need not carry the same documentation depth.

6. Ongoing Monitoring and Material Change

The proposed guidance permits monitoring to be periodic or continuous depending on risk and recognizes that monitoring may change as the relationship evolves. For information-dependent services, the practical question is whether the output continues to mean what the bank expects it to mean.¹

Change triggers—Examples that may justify reassessment include material changes to an authoritative source, interface or schema; status or validation semantics; subcontractors or critical feeds; model or ruleset versions; or the bank's own use of the output. The trigger should be consequence-based, not release-count based.

No universal retesting rule—Not every software release, data refresh or model update warrants bank-level retesting. A useful screen is whether the change can materially alter availability, integrity, compliance coverage, transaction meaning or the bank's ability to reconstruct a relied-upon decision.

Output monitoring—Monitoring can include existing operational indicators such as exceptions, reconciliation failures, false-positive or false-negative trends, unexplained changes in alert volumes, update latency, version changes and disagreement between a source and a derived service. These are examples of indicators of output or data-state problems that can complement uptime, incident and financial-condition monitoring without creating a separate monitoring regime.

7. Operational Resilience: Availability and Trusted Operational Usability

The proposed guidance treats operational resilience as a cross-cutting topic and discusses resilience plans, alternative providers, separated backups and the ability to resume operations. For information-intensive relationships, the same principle can distinguish restoration of connectivity from restoration of an operationally usable state.¹

Reachable-but-unusable failure—A provider can remain online while the bank cannot safely rely on the output. Examples include a sanctions-screening service that is behind the current list or a payment interface that still responds while mapped status information is incomplete or wrong.

Mini-case: sanctions screening—A U.S. sanctions-screening platform remains technically available but has not ingested a material list update within the expected window. Proportionate controls can focus on update latency, escalation and a defined hold or alternative screening path when current-state assurance is unavailable.

Mini-case: payment-processing integration—After an interface or mapping change, the processor remains online but the transaction-status data supplied to the bank's core, fraud or compliance systems is incomplete or misinterpreted. The relevant control is whether the bank detects the mismatch, contains propagation and can reconcile or route time-sensitive activity safely.

Agency examples—The TCBO Guide describes core systems as integration hubs for BSA/AML, fraud, payments, cards and loan systems; recommends pre-go-live testing, monitoring after material changes and routine reconciliation; and notes that instant-payment channels can require higher-frequency data exchange. The Joint Statement similarly emphasizes provider transparency, measurable service levels, incident disclosure, integration constraints and operational resilience. These examples support current-state and interface-integrity testing without adding a new OP-1881 requirement.^{3,4}

Mini-case: card-provider transition—An outgoing processor exports records, but authorization, fraud, dispute or exception states do not map cleanly into the replacement platform. The bank has data but may still lack usable continuity for open cases or selected prior decisions.

Safe resumption—For a higher-risk dependency, the bank can define the minimum trusted state required before normal reliance resumes, such as confirmation of source status, successful reconciliation, current rules or lists, and resolution of material exceptions. A tested fallback may be an alternative provider, authoritative-source check, controlled degraded service, manual review or a temporary hold.

Prospective and retrospective resilience—The bank needs both a way to continue or safely pause new activity and, where material, enough retained context to explain selected prior decisions after an incident. The latter should remain subject to ordinary legal and retention requirements.

8. Termination, Substitution and Evidence Continuity

The proposed guidance recognizes that termination and transition can involve costs, operational complications, data-access disruption and limited alternatives. For information-intensive services, the same analysis can include whether the replacement environment can continue the function and interpret the relevant state.¹

Data export versus usable continuity—A file export does not necessarily show that an alternative provider can establish current state, interpret status semantics, preserve transaction binding or reproduce the audit context needed for earlier decisions. The TCBO Guide's card-transition and cloud-migration examples similarly focus on status accuracy, data integrity and continuity, not only transfer of raw files.

Operational transition record—Where material, transition planning may preserve the meanings attached to status fields, open exceptions, decision or authorization history, relevant model or ruleset versions and identifiers linking migrated records to prior activity. The purpose is usable continuity, not indefinite replication of every historical field.

Substitutability—Provider diversity does not always equal dependency diversity. Two providers may rely on the same registry, network, cloud component or other upstream source. That common dependency can matter when assessing fallback quality, concentration and transition time.

Contract implications—Where proportionate, contracts may address notice of material source or interface changes, access to relevant status and audit information, incident and correction handling, and transition assistance. These remain examples, not a standard clause set.

9. Subcontractors, Analytical Services and AI

The proposed guidance recognizes that subcontractors can heighten risk and that oversight can be exercised through the direct provider's contract and third-party risk management. The same principle can apply to material data, trust and analytical chains.¹

Subcontractor and source chains—A bank need not maintain a complete nth-party inventory. For a higher-risk output, it may instead identify the specific upstream dependencies whose failure, change or loss of authority would materially affect the service.

AI is analytical, not authoritative—A third-party AI or machine-learning service should be treated as an analytical tool, not as a substitute for the authoritative source record or the bank's accountable decision. Even accurate data can support misleading conclusions when context is missing, the use case changes, or relevant inputs, retrieval sources or thresholds shift. Where an output is materially relied upon, useful TPRM facts include intended use, material inputs, version or change controls, monitoring, exceptions and the bank control that accepts, challenges or overrides the result.

Coordination with current model-risk guidance and controlled deployment—For Board-, OCC- and FDIC-supervised banking organizations, the April 17, 2026 revised model-risk guidance (SR-26-2 for the Board) is the current interagency reference. It applies a tailored approach to covered models and vendor products, while expressly excluding generative and agentic AI and directing institutions to use broader risk-management and governance practices for tools outside its scope. OP-1881 can therefore complement, rather than duplicate, model-risk governance. Running an AI or LLM in isolated or institution-controlled infrastructure can reduce external data exposure, but it does not make the analysis authoritative, justify secondary use of data, cure weak provenance or guarantee contextually reliable conclusions. Third-party software, updates, retrieval sources or support can still be assessed under OP-1881 according to their actual role and materiality.⁵

Silent change and context risk—Model, configuration, retrieval or upstream-data changes can alter output meaning without causing an outage. This is another form of reachable-but-

unusable risk. The proportionate response is ordinary change governance, input and version traceability, monitoring, exception handling, confidentiality and reconstructability where the output is on a material banking path.

10. Illustrative Clarifications and Limiting Principles

Table 1 summarizes the proposed implementation clarifications. They are illustrative, non-exclusive and intended to preserve tailoring, residual-risk judgment and resource prioritization.

Table 1. Information-dependency clarifications within a risk-based TPRM framework.

Guidance area	Illustrative clarification	Limiting principle
Risk inventory / assessment	For a higher-risk relationship, identify the material banking function, critical source or upstream input, relied-upon output, principal failure modes and fallback, in addition to the provider relationship.	Use existing inventories and add fields only where output failure could materially affect the bank; do not create a universal data-source inventory.
High-risk characteristics	If the agencies include examples under note 15, use a short non-exclusive list centered on critical-path reliance, ability to change or gate material state, time-sensitivity/fallback constraints, and loss of reconstructability.	Use the list only to illustrate the existing magnitude-and-likelihood test; it should not become a vendor-category checklist.
Scope / written agreements	Keep direct TPRM obligations tied to the bank's business relationship while allowing the risk assessment of that relationship to consider material upstream dependencies that affect service risk.	Identifying an upstream dependency does not by itself create a direct contractual, audit or due-diligence duty toward that entity.
Due diligence / assurance	Allow certifications, consortium due diligence and external assessments to support risk decisions while distinguishing assurance evidence from the underlying customer, transaction, identity, status or account information and from the bank's final decision.	Traceability depth depends on functional materiality; external assurance remains an input to the bank's own risk judgment.
Ongoing monitoring	Use material changes in source systems, status semantics, interfaces, critical subcontractors, access models or model/configuration versions as possible triggers for proportionate review.	No blanket retesting after every release or data update; focus on changes that can materially alter risk or reliance.
Operational resilience	For higher-risk dependencies, test at least where relevant both outage and reachable-but-unusable failure, and define the minimum trusted state needed for safe resumption.	Do not create a new recovery-time objective; use the bank's existing continuity framework and risk appetite.
Termination / substitution	Test both prospective continuity and usable transition of material status, exception and audit information needed to continue the service or reconstruct selected prior decisions.	A raw data export need not be treated as sufficient, but transition scope remains tied to materiality and applicable retention requirements.

Analytical services / AI	For materially relied-upon third-party analytics, understand intended use, material inputs, version/change controls, output and exception state, monitoring, accountable acceptance, and where relevant data-hosting or retrieval arrangements.	Do not treat AI as an authoritative source or create an AI-specific TPRM regime. Coordinate with applicable model-risk guidance where it applies; generative/agentive AI remain outside SR-26-2's scope.
---------------------------------	---	--

11. Scope, Proportionality and Evidence Boundaries

These observations remain within the proposed guidance's principles-based and tailored structure. They do not support a new standalone risk category, a universal repository or inventory, a mandatory trust index, mandatory VTE implementation, or a blanket classification of data, identity, trust, AI or analytical providers as higher risk. The relevant screen is the materiality of the banking function and the consequence of failure or unusability.

Legal validity and regulatory effect also remain governed by applicable U.S. law, the banking organization's obligations, payment or network rules and the facts of the activity. Technical verification, a credential, a model output or a provider certification cannot itself create legal authority, eliminate a bank's compliance responsibility or determine the legal effect of a transaction. Likewise, dependency discoverability should not be treated as a basis for unrestricted access to source data.

This response does not address consumer-compliance allocation, prudential capital treatment, competition policy or the supervisory threshold for enforcement. The proposed guidance notes that consumer-compliance considerations may be relevant but are not directly addressed. Those topics involve separate legal and policy questions outside the evidentiary and operational focus of this draft.¹

12. Conclusion

OP-1881 shifts third-party risk management toward relationship-specific assessment, prioritization and risk acceptance. For information-intensive relationships, one practical question is whether a provider is not only available but supplying an output that remains current, attributable, correctly applied and fit for the banking purpose at the time of use.

That question can be incorporated without expanding the definition of third party or imposing uniform controls. Material upstream dependencies can be treated as facts about the direct relationship; external assurance can support but not replace the bank's judgment; monitoring can focus on consequential change; resilience can test both outage and unusable-state scenarios; transition can test usable continuity; and third-party AI or analytics can remain subject to the same function- and consequence-based logic. The common limiting principle is proportionality.

Notes and References

1. Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, and National Credit Union Administration. "Proposed Third-Party Risk Management Guidance." 91 Fed. Reg. 58536 (15 September 2026), Docket No. OP-1881

/ OCC-2026-0793 / FDIC RIN 3064-ZA58 / NCUA-2026-1684. Federal Reserve proposal page:
<https://www.federalreserve.gov/apps/proposals/FR-2026-0031-01/details>

2. Board of Governors of the Federal Reserve System staff. "Proposals to Update Third-Party Risk Management Guidance." Memorandum to the Board of Governors, 28 August 2026.
3. Board of Governors of the Federal Reserve System, FDIC and OCC. "Joint Statement on Community Banks' Engagement with Core Service Providers." 11 September 2026.
4. Board of Governors of the Federal Reserve System. "Proposed Third-Party Risk Management Guide for Traditional Community Banking Organizations." 91 Fed. Reg. 58438 (15 September 2026), Docket No. OP-1880.
5. Board of Governors of the Federal Reserve System, Office of the Comptroller of the Currency, and Federal Deposit Insurance Corporation. "Supervisory Guidance on Model Risk Management." Interagency guidance issued 17 April 2026; Board issuance SR-26-2.