

# DIGITALTRADE4.EU, RIHO VEDLER

## Proposal and Comment Information

**Title:** Proposed Third-Party Risk Management Guide for Traditional Community Banking Organizations, OP-1880

**Comment ID:** FR-2026-0030-01-C10

## Submitter Information

**Organization Name:** DigitalTrade4.EU

**Organization Type:** Foreign

**Name:** Riho Vedler

**Submitted Date:** 10/02/2026

This response proposes a simple, proportionate way for community banks to manage risks arising from third-party data, system outputs, and analytical services. It recommends an optional dependency check focused on what the bank relies on, how it verifies that the information is accurate and current, and what fallback action is available if it cannot be trusted. The approach is designed to build on existing reconciliation, continuity, vendor-risk, and contract-management processes without creating new mandatory frameworks, reporting requirements, or AI-specific standards.

## Practical Dependency Checks, Reconciliation and Critical Analytical Inputs

# Response to Proposed Third-Party Risk Management Guide for Traditional Community Banking Organizations

DigitalTrade4.EU

Contact: Riho Vedler | [secretariat@digitaltrade4.eu](mailto:secretariat@digitaltrade4.eu) | October 2026 | Docket No. OP-1880 | v3

**Abstract.** DigitalTrade4.EU provides technical observations on the Federal Reserve Board's proposed Third-Party Risk Management Guide for Traditional Community Banking Organizations. The response focuses on a narrow implementation opportunity already visible in the Guide's examples for core providers, payment processing, loan systems, BSA/AML platforms and fraud tools: a TCBO may rely on a third-party result, feed or status that is technically available but stale, incomplete, misconfigured or otherwise unsafe to use. The response proposes an optional, low-burden dependency check that can be embedded in existing vendor, business-impact, continuity, reconciliation or risk records rather than maintained as a new form. Four plain-language questions are sufficient for a small bank: what matters, what must be right, how will the bank know, and what will it do if the answer is uncertain? Seven more detailed prompts are offered only as an optional expansion for higher-impact relationships. Daily reconciliation and exception handling are emphasized as practical detection and recovery controls. AI or analytics are addressed only when their outputs become material inputs to a banking decision or control. The approach is intended to improve usability without creating a new taxonomy, data-governance framework, required data fields or de facto supervisory standard.

**KEY WORDS.** community banking; third-party risk management; operational resilience; reconciliation; dependency check; core-provider contracts; AI and analytical services.

## 1. Introduction

The Federal Reserve Board's proposed Community Bank Guide is intended to help traditional community banking organizations (TCBOs) operationalize the companion all-bank third-party risk management principles through concrete examples. The Board asks whether the Guide is useful, whether its level of detail is appropriately calibrated so that it does not become a de facto supervisory standard, what clarifications would improve the overarching risk considerations in Section IV.B, whether vendor categories should be adjusted, and how the Guide could better support contract negotiations. The proposed Guide defines TCBOs as banking organizations with less than \$30 billion in assets that focus on their local communities and organizes its practical examples around operational resilience, system and information security, compliance, financial resilience and eight common vendor categories.<sup>1</sup>

This response is deliberately selective. It addresses the Board's questions about usefulness, calibration, overarching risk considerations, vendor categories and contract support. It does not

take a position on the \$30 billion threshold, the definition of a TCBO, or whether deposit placement networks should be added as a separate category. Consumer compliance allocation is likewise outside the scope of this response. The objective is to add a small implementation tool where the Guide already identifies material integration, data, monitoring and transition risks.

The central observation is simple: for some higher-impact relationships, a TCBO's operational risk is not fully described by the vendor name or by whether the service is online. The bank may rely on a transaction status, sanctions-screening result, fraud alert, credit-decision input, reconciliation output or other external result. If that result is stale, incomplete, incorrectly mapped or materially changed, the bank may need to pause, reconcile or use a fallback even though the provider remains available. The proposed dependency check is therefore a plain operational aid, not a technical mapping exercise and not a new set of required records.

## 2. Direct Responses to the Board's Request for Comment

*Usefulness and level of detail* - The proposed Guide is structured as a practical resource rather than a rule. One additional example could improve usability without increasing prescriptiveness: where a third-party result or feed is material to an essential operation or risk-control step, a TCBO may record only the few facts needed to understand the dependency, detect a problem and use a fallback. This can be a note in an existing vendor, BIA/BCP, continuity or reconciliation record; no separate template should be expected.<sup>1</sup>

*Overarching considerations in Section IV.B* - Operational resilience, system and information security, and compliance can each be affected when a material third-party result is wrong even though the service remains available. A short cross-cutting example could ask whether the information is current, complete, correctly mapped and fit for the bank's immediate use, using ordinary reconciliation and exception handling where those controls already exist.<sup>1</sup>

*Vendor categories* - The existing categories are broad enough to capture most information-intensive dependencies described in this response. A separate AI, data or analytics vendor category is not necessary. The relevant question is the function performed and the consequence of output failure. Analytics may be embedded in loan-management, BSA/AML, fraud, cybersecurity, payment or core-provider services.<sup>1</sup>

*Contract negotiations* - The Guide could add a short list of optional review topics for higher-impact relationships: timely notice of material interface, processing-rule or service changes; reasonable access to bank data and material alert, exception or decision history; transition assistance; and clarity on integration restrictions, deconversion costs and testing support. These should be framed as discussion topics, not model clauses.<sup>1,3</sup>

*Proportionality* - No additional check is needed for every endpoint, dataset, advisory tool or low-risk vendor. The approach is useful only where an error could materially interrupt operations, defeat a compliance or fraud control, impair reconciliation, or leave the bank unable to explain an important prior decision. Where existing controls already answer the relevant questions, nothing new should be created.

## 3. Optional Minimum Dependency Check

The proposed check is not a prescribed seven-field form. At the simplest level, a TCBO can ask four questions: (1) what banking function or control matters; (2) what result, feed or status must be right; (3) how the bank knows that it is right; and (4) what the bank does if it is not. For a higher-impact relationship, the same four questions can be expanded into seven optional

prompts - function, source/input, relied-upon output, condition for use, owner, failure mode and fallback. A TCBO need use only the prompts that add value to its existing records.

*Small-TCBO implementation* - A very small bank should be able to apply the check with only a few lines. One row in an existing vendor record, BIA/BCP worksheet, continuity plan or reconciliation procedure can be sufficient. The companion OP-1881 proposal itself recognizes that a community bank may benefit from a simpler or streamlined inventory format. The example below deliberately uses only three relationships and three practical columns.<sup>2</sup>

| Relationship / function                            | Routine check already available to the TCBO                                | If the check fails                                                                                         |
|----------------------------------------------------|----------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|
| <b>Core provider / daily posting</b>               | Daily reconciliation and exception review confirm ledger/interface results | Investigate exceptions; hold affected processing or use the continuity process until reconciled.           |
| <b>BSA/AML service / sanctions screening</b>       | Confirm timely list/rule updates and review alert exceptions               | Use an approved manual or secondary check; hold affected items if current screening cannot be established. |
| <b>Payment processor / time-sensitive payments</b> | Reconcile transaction status between processor, core and control systems   | Use an alternate rail or manual process where feasible; resolve mismatches before normal resumption.       |

*Boundary* - This is not a data-governance, data-lineage, model-governance or AI-governance tool. It is a simple operational dependency check. It should not create an expectation that a TCBO maintain a separate artefact, populate all seven prompts, map every subcontractor, or recreate technical records held by a large provider.

| Optional prompt - not a required field | Plain-language question                                               | Illustrative example                                                                        |
|----------------------------------------|-----------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| <b>Function</b>                        | What important operation or control depends on the service?           | Posting/reconciliation; sanctions screening; loan booking; fraud control.                   |
| <b>Source or input</b>                 | What material feed, list, rule or record does the provider depend on? | Core ledger state; transaction feed; sanctions update; underwriting parameters.             |
| <b>Result used by the bank</b>         | What does the TCBO actually rely on?                                  | Transaction status; alert; screening result; risk score; exception.                         |
| <b>Condition for use</b>               | What must be true before the result is safe to use?                   | Current update; complete feed; correct mapping; expected configuration; resolved exception. |
| <b>Owner</b>                           | Who at the TCBO is accountable for using or accepting the result?     | Operations; compliance; fraud; lending; information security; business line.                |
| <b>Likely failure</b>                  | What can go wrong without a complete outage?                          | Stale update; missing field; mapping error; configuration change; wrong context.            |
| <b>Fallback or hold</b>                | What will the bank do until the result can be trusted again?          | Manual review; alternate provider/rail; source check; transaction hold; reconciliation.     |

*Suggested non-prescriptive wording* - Where a TCBO materially relies on a third-party result or feed for an essential operation or risk-control step, it may be useful to record, in existing documentation, enough information to understand the supported function, the condition for safe use, the responsible owner, how a problem would be detected and what fallback or hold is available. Additional source, version or failure-mode detail may be added when warranted by the risk of the relationship. No separate mapping document or minimum data set is implied.

#### 4. Applying the Check to Examples Already in OP-1880

The proposed Guide already contains the practical hooks needed for this approach. Core providers are described as the system-of-record and integration hub for payments, cards, lending and other applications; the Guide notes that integration failures can cause significant operational breakdowns and points to pre-go-live testing, monitoring after material changes and daily reconciliation. Payment-processing examples address feeds into compliance and fraud systems; loan-management examples address automated credit decisioning and risk scoring; and BSA/AML and fraud sections address rules, thresholds, list updates, false positives, multiple data sources and model calibration. The proposed check simply organizes those existing practices around the material result the bank uses.<sup>1</sup>

| Existing Guide context             | What may need to be right                                              | Routine bank check                                                         | Illustrative response if not                                                                          |
|------------------------------------|------------------------------------------------------------------------|----------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|
| <b>Core provider / integration</b> | Core record, interface mapping and connected application state         | Daily reconciliation, exception review and post-change checks              | Investigate and contain mismatches; hold affected processing if the state cannot be established.      |
| <b>Payment and digital banking</b> | Transaction status and feeds into compliance or fraud controls         | Reconcile processor status with the core and control systems               | Use an alternate rail or manual process where feasible; resolve exceptions before normal resumption.  |
| <b>Loan management</b>             | Borrower data, policy parameters and automated decision/scoring output | Implementation testing, sampling and exception review                      | Use manual underwriting or file review; correct configuration before relying on the automated result. |
| <b>BSA/AML platform</b>            | Customer/transaction data, sanctions updates, rules and thresholds     | Update verification, alert review and exception handling                   | Use an approved secondary/manual check; hold affected items; preserve investigation history.          |
| <b>Fraud prevention</b>            | Transaction/device data, intelligence feeds and analytical output      | Monitor alert quality, complaints and false-positive/false-negative trends | Manual review or controlled parameter/fallback action until performance is understood.                |

## 5. Operational Resilience: Availability, Reconciliation and Safe Resumption

The Guide's resilience examples primarily address disruption and recovery. A complementary but familiar scenario is a service that remains online while a result, feed or status cannot safely be used because it is stale, incomplete, incorrectly mapped or based on a delayed update. In community-bank terms, this should be framed through ordinary processing controls - especially reconciliation, exception handling and continuity procedures - rather than through a new technical label or risk category.

*Reconciliation as a first-line check* - For core and payment dependencies, routine reconciliation and exception handling may be the most practical way for a TCBO to detect that a third-party result no longer matches the bank's records or expected processing state. Reconciliation is not itself a backup provider or continuity solution, but it can detect mismatches, stop propagation and provide an objective gate for safe resumption. This is often more realistic for a small bank than performing deep technical audits of a large provider.

*Safe resumption* - Normal processing can resume when the TCBO has enough confidence that the affected records, feeds or rules are current and reconciled and that material exceptions have been resolved. Depending on the service, the bank may also confirm that downstream systems are receiving the expected information.

*Change-triggered testing* - Testing can focus on consequential changes to an interface, mapping, source, ruleset, model, provider or access path rather than every routine release. This preserves proportionality and directs limited TCBO resources to changes that can alter a material banking outcome.<sup>1</sup>

The agencies' Joint Statement on core providers reinforces the same practical direction from the provider side. It highlights transparency, measurable service levels, timely disclosure of operational and security issues, excessive limitations on integrations with unaffiliated providers, unsupported or undefined deconversion fees, technology investment and demonstrated operational resilience. For a TCBO, the proposed dependency check helps identify which interfaces, records and transition conditions are important enough to raise during monitoring and contract discussions.<sup>3</sup>

## 6. Analytical and AI Services When the Output Becomes a Critical Input

OP-1880 does not need a separate AI vendor category. The Guide already addresses functions in which third-party analytics can become consequential: automated credit decisioning or risk scoring in loan systems, behavioral analytics and identity verification in fraud tools, transaction-monitoring logic and thresholds in BSA/AML platforms, and real-time decision support embedded in payment or core services. The same optional dependency check can be used only when an analytical output becomes a material input in a banking decision or control.<sup>1</sup>

*AI is analytical, not authoritative* - An AI or machine-learning output can identify patterns, relationships, anomalies or risks, but it should not be treated as the authoritative source of the underlying customer, account, transaction, entitlement or regulatory state. Even accurate data can support a misleading conclusion when material context is missing or when the intended use, inputs, configuration, thresholds or model version change.

*Criticality test* - Additional attention is most relevant where the output can directly approve, reject, block, route or materially influence a transaction, credit action, fraud decision or

compliance workflow with limited independent review. An advisory output that is independently checked before material use can remain under ordinary controls.

*Controlled deployment and confidentiality* - Running an AI or large-language-model capability inside the institution's own isolated or controlled environment can reduce the need to send sensitive banking data to an external inference provider and can keep source data, logs and resulting intelligence under institutional access controls. Technical isolation does not, however, make the analysis authoritative, establish permission for secondary data use, cure weak provenance or guarantee a contextually reliable conclusion.

*Model-risk boundary* - The April 2026 interagency model-risk guidance is expected by the Federal Reserve to be most relevant to banking organizations with more than \$30 billion in assets, and it expressly excludes generative and agentic AI from its model definition. This response therefore does not propose importing that guidance into OP-1880 as a TCBO standard. The narrower cross-framework point is that materially relied-upon vendor analytical products still require the banking organization to understand their use, monitor performance and retain accountability under the risk-management framework that actually applies.<sup>5</sup>

## 7. Contracts, Transition and Continuity

The proposed Guide already treats transition as an operational issue, not merely a termination clause. Core conversion, cloud migration and card-provider transition examples address integration cost, data accuracy, parallel processing, network access and operational complexity. The BSA/AML section also identifies ownership and access to customer data, alert histories, investigation documentation and SAR filings as possible contract considerations. The Joint Statement adds a direct supervisory context by identifying deconversion fees, integration restrictions and provider transparency as issues that can limit a community bank's ability to manage risk.<sup>1,3</sup>

*Transition continuity* - For a material service, a replacement environment may need more than a bulk file transfer. Depending on the function, the TCBO may need open exceptions, decision or authorization history, relevant rules/configuration, transaction identifiers and mapping information needed to continue processing or explain selected prior actions. The level of detail should remain proportionate to the service.

*Illustrative contract review topics* - The Board asks how the Guide could better support contract negotiations. The following questions could be offered as optional discussion points for higher-impact relationships. They are not model clauses and would not all be relevant to every TCBO or vendor.<sup>1,3</sup>

| Review topic                  | Illustrative question for the TCBO                                                                                                                                                                            |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Material change notice</b> | Does the agreement provide timely notice, where reasonably practicable, of material changes to interfaces, processing logic, rules, configurations or critical service components that could affect the TCBO? |
| <b>Bank data and history</b>  | Can the TCBO obtain its customer/transaction data and material alert, exception or decision history in a usable form during the relationship and at exit, subject to applicable law and retention limits?     |
| <b>Transition assistance</b>  | Does the agreement describe reasonable cooperation, testing access and timing for migration, parallel operation or temporary fallback when the relationship ends or materially changes?                       |

|                                     |                                                                                                                                                                                      |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Integration and deconversion</b> | Are material integration restrictions, testing constraints, termination conditions and deconversion fees clear enough for the TCBO to assess exit and supplementary-service options? |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

*No standard clause set* - The appropriate terms depend on the service, risk, provider market, negotiating leverage and available alternatives. The Guide should make clear that these are prompts for consideration, not minimum contractual provisions and not a basis for criticism merely because a particular clause is absent.

## 8. Relationship to OP-1881 and Existing TCBO Records

OP-1881 is the direct companion framework and provides the relevant policy logic. It assesses risk by the magnitude and likelihood of harm, allows assessment at the relationship or activity level, and recognizes that a community bank may use a simpler or streamlined inventory. The optional dependency check follows that logic: it adds detail only when a specific third-party result can materially affect the banking function, rather than because the vendor belongs to a particular technology or data category.<sup>2</sup>

*Existing records first* - A TCBO should be able to place the few relevant prompts inside documentation it already uses - for example a vendor record, business-impact analysis, business-continuity plan, risk assessment, reconciliation procedure or change record. The proposal does not assume a separate dependency register, specialist data-lineage tooling or new reporting to the Board. If existing records already identify the material dependency, check and fallback, no additional artefact is needed.

## 9. Illustrative Optional Additions to the Guide

If the Board concludes that the dependency concept would make the Guide more useful, it could be incorporated through a few short examples rather than a new section, form or vendor category. Table 4 shows possible locations and limiting principles.

| Guide location                                          | Possible optional clarification                                                                                                                                                            | Limiting principle                                                    |
|---------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------|
| <b>Section IV.B - Operational Resilience</b>            | For a material third-party result, consider whether ordinary reconciliation or exception handling confirms that processing is safe to resume, and whether a fallback or hold is available. | Use existing controls; no new technical test or required record.      |
| <b>Section IV.B - System &amp; Information Security</b> | Where relevant, consider whether source/authenticity, data completeness and correct transaction or account mapping affect the safe use of the third-party result.                          | No separate data-governance or security framework.                    |
| <b>Section IV.B - Compliance</b>                        | For material compliance outputs, consider timeliness of required updates, input coverage, exception handling and accountable bank review.                                                  | The provider result does not replace the bank's legal responsibility. |

|                                              |                                                                                                                                                              |                                                                         |
|----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|
| <b>Section IV.C - Core / Payments</b>        | Use a simple small-bank example built around reconciliation, exception handling and a documented fallback after a consequential interface or mapping change. | A few notes in BIA/BCP, vendor or reconciliation records may be enough. |
| <b>Section IV.C - Loan / BSA-AML / Fraud</b> | When an automated or analytical output becomes a material input, consider intended use, material inputs, result, bank review and fallback.                   | No separate AI vendor category or AI-specific supervisory standard.     |
| <b>Contract negotiation examples</b>         | Offer optional review questions on material-change notice, bank data/history access, transition assistance, integration constraints and deconversion costs.  | Discussion prompts only; not model clauses or minimum provisions.       |

## 10. Scope, Proportionality and Conclusion

The proposed clarification is intentionally small. It should not create a new TPRM risk category, universal source inventory, regulatory definition of critical data, data- or model-governance framework, mandatory AI regime, requirement to map every subcontractor, or expectation that TCBOs recreate technical documentation held by large providers. A small institution should be able to reuse existing vendor, BIA/BCP, continuity and reconciliation records and add only the few facts needed for a material relationship.

The value of the proposed check is practical rather than theoretical. At its simplest it asks four questions: what matters, what must be right, how the bank will know, and what it will do if the answer is uncertain. Daily reconciliation and exception handling provide a familiar control for many core and payment dependencies; BIA/BCP and vendor records provide familiar places to record the answer; and the Joint Statement supplies concrete contract and transition issues for core-provider relationships. This approach is consistent with OP-1881's focus on magnitude and likelihood of harm rather than vendor category and can improve the Guide's usefulness without turning an illustrative example into a new supervisory checklist.<sup>1,2,3</sup>

## Notes and References

1. Board of Governors of the Federal Reserve System. "Proposed Third-Party Risk Management Guide for Traditional Community Banking Organizations." Docket No. OP-1880, 91 Fed. Reg. 58438 (15 September 2026). Federal Reserve comment period closes 16 November 2026.
2. 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." Docket No. OP-1881, 91 Fed. Reg. 58536 (15 September 2026).
3. Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, and Office of the Comptroller of the Currency. "Joint Statement on Community Banks' Engagement with Core Service Providers." 11 September 2026.
4. Board of Governors of the Federal Reserve System. Staff memorandum concerning the proposed All-Bank Third-Party Risk Management Guidance and Proposed Traditional CBO Guide. September 2026.
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.