THE CHANGE HIVE, YEMI OLUSEUN

Proposal and Comment Information

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

Comment ID: FR-2026-0031-01-C71

Submitter Information

Organization Name: The Change Hive

Organization Type: Company

Name: Yemi Oluseun

Submitted Date: 11/21/2026

To: Board of Governors of the Federal Reserve System
Re: Proposed Third-Party Risk Management Guidance | OP-1881 | 91 FR 58536

I am submitting my comments on the Proposed Third-Party Risk Management Guidance (91 FR 58536).

Drawing on my experience in banking vendor management, finance and treasury transformation, and M&A integration, my response offers four recommendations to strengthen risk-based supplier oversight, operational resilience and organisational continuity.

These cover identifying higher-risk relationships, testing service continuity, managing supplier concentration through proportionate diversity and redundancy, and strengthening accountability and reassessment.

Please see my attached submission for the full recommendations and supporting rationale.

Yemi Oluseun
Founder, The Change Hive
www.thechangehive.co

Third-Party Risk Management Guidance: Comment from Yemi Oluseun

Risk-based supplier oversight, operational resilience and continuity of essential banking services

Submitted by: Yemi Oluseun, Founder, The Change Hive (London, UK)

To: Office of the Comptroller of the Currency; Federal Reserve Board; Federal Deposit Insurance Corporation; National Credit Union Administration

References: OCC-2026-0793 | Federal Reserve OP-1881 | FDIC RIN 3064-ZA58 | NCUA-2026-1684

Re: Proposed Third-Party Risk Management Guidance, 91 FR 58536 (15 September 2026)

Date: 21 November 2026

Summary

I support the agencies' plan to match third-party oversight to the risk each relationship creates. Banking organizations, including insured credit unions, remain responsible for their services when a supplier fails. The final guidance should help each institution identify higher-risk relationships and show how its operating model can keep essential services running or restore them after disruption.

I draw on banking vendor management, finance and treasury transformation, and M&A integration experience. I recommend four additions: an illustrative list of high-risk indicators; a clear test of service continuity; clearer triggers for reassessment and ownership; and one worked example.

1. Footnote 15: give institutions a short list of high-risk indicators

Footnote 15 asks whether a list of high-risk characteristics would help and what it should include. I believe it would help, especially smaller institutions, as long as the list guides judgement rather than setting an automatic rating.

I suggest four groups of indicators:

- **People:** The service depends on knowledge or decision rights held by a few people, creating key-person risk and knowledge concentration within the institution or supplier.
- **Processes:** An outage could disrupt essential finance and treasury processes, payment processing, settlement, liquidity management or access to customer funds.
- **Technology:** The supplier operates or hosts systems the institution cannot readily replace, including shared infrastructure and systems run through subcontractors.
- **Data:** The supplier holds or can access sensitive customer, financial or business data, even if it does not support a live service.

These indicators should prompt closer review. The final risk rating should reflect the likelihood and scale of harm, the institution's dependence on the supplier, available alternatives and its ability to recover.

Contract value is not the same as operational risk. In banking vendor management, I worked on a large managed-services contract that mainly supported technology development, testing and change work rather than day-to-day production. A much smaller supplier that supports live payments could pose a greater risk. The key question is: what would stop if this supplier failed?

2. Test whether essential services can continue

The proposal already discusses third parties' operational resilience plans and alternative backup providers. The final guidance could make the outcome clearer: for higher-risk relationships, can the institution keep an essential service running, or restore it within its tolerance for disruption?

For higher-risk relationships, institutions should assess potential financial losses, legal and regulatory consequences, and harm to customers. They should know how long a service could be unavailable, what recovery would cost and how quickly they could replace the supplier. For treasury and CFO-office processes, an outage may also affect cash visibility, liquidity decisions, settlement and financial reporting.

Supplier selection can help. For important services, a proportionate request for proposal (RFP) or market comparison lets the institution compare cost, financial strength, security, recovery arrangements and exit options. It also shows which alternatives exist. If a competitive process is not practical, the institution should record why it chose the supplier and how it will manage the risk.

Using one provider can cut cost and complexity, but may also create a single point of failure. Institutions should weigh those savings against supplier concentration risk and the cost of losing an essential service.

Where the potential harm is high, diversity and redundancy may be worth the cost. Institutions should test whether their recovery routes are truly independent. Two suppliers offer little extra protection if both depend on the same cloud platform, data centre or subcontractor.

Insurance and indemnities may cover some financial losses, within their limits. They cannot restore a payment service. For higher-risk relationships, scenario tests should use clear pass-or-fail measures: how quickly the service returns, whether staff can access records and make decisions, and whether customers can reach their money. Where relevant, tests should cover the end-to-end business process, including people, controls, data, technology and subcontractors.

The aim is to match the cost of resilience to the harm that failure could cause. Checks and tests should reflect each relationship's risk.

3. Review risk when things change, with one clear business owner

A supplier's risk can change long before its next planned review. The final guidance could name useful triggers: contract renewal, a wider scope of work, a supplier incident, growing reliance on one provider, loss of key staff, operating model transformation, or a merger, acquisition, carve-out or separation.

M&A integration, carve-outs and separations are clear examples. Inherited contracts, shared systems and transitional service agreements can quickly change supplier dependencies and decision rights. A risk rating made before the transaction may no longer fit on Day 1.

Each higher-risk relationship should have a business owner who understands the end-to-end service and its dependencies. To support organisational continuity, the institution should also test whether key knowledge and decision-making authority remain available when that owner or a supplier contact is absent. Procurement and third-party risk teams should support due diligence, contracts and monitoring. The institution should review risk at suitable intervals and accept any remaining risk through its established governance process.

4. Show how the four parts of the guidance work together

One short example could help institutions apply the guidance without adding another checklist. Consider a digital bank that uses an outside payments processor:

1. **Risk Identification and Assessment:** An outage could stop payments and leave customers unable to use their money.
2. **Risk Oversight:** The bank compares providers, checks for shared points of failure and tests how quickly payments can be restored.
3. **Residual Risk Acceptance:** The bank decides, through its governance process, whether any remaining exposure is acceptable.
4. **Governance:** A named business owner tracks incidents, changes in reliance and test results, and reports concerns when needed.

This connects the proposal's four risk-management components to one service that customers depend on.

Closing

The real test of third-party oversight comes on the day a supplier fails. Good oversight means the institution knows what it relies on, has workable alternatives where needed and can keep serving customers when things go wrong.

I would welcome the opportunity to discuss these recommendations with agency staff.

Yemi Oluseun
Founder, The Change Hive

www.thechangehive.co

About the author

Yemi Oluseun founded The Change Hive, a London advisory practice covering finance and treasury transformation, payments, CFO-office operating models and M&A integration, carve-outs and separations. At the International Fund for Agricultural Development (IFAD), she built and led a treasury transformation office across finance, technology and external providers. Her research on organisational continuity and organisational knowing examines how teams keep access to critical knowledge and decision-making authority.