The Vendors Behind Your Vendors: Managing Fourth- and Nth-Party Risk

By Joe Terry

Your vendor management program covers your vendors. But what about the vendors your vendors rely on, or the ones behind those?

Most financial organizations have documented programs that give them a clear line of sight into their direct third-party relationships. But that visibility often stops at the edge of their vendor portfolios, and that's where the problem starts.

Fourth-party risk — the risk introduced when your vendors outsource critical functions to other vendors — is one of the most underestimated gaps in TPRM today. As vendor ecosystems grow more complex and reliant on artificial intelligence (AI), the problem compounds.

When a fourth-party failure disrupts operations, damages customers, or draws examiner scrutiny, the distance between your organization and the source of the problem isn't a defense. It's the gap that made it possible.

What Regulators Expect

Regulators — including the OCC, FDIC, FFIEC, and Federal Reserve — hold organizations responsible for activities conducted through their third parties, a position reinforced by the 2023 Interagency Guidance on Third-Party Relationships. That responsibility doesn't stop at your direct vendors. It extends to the functions they outsource.

If your vendor's vendor fails and your customers are impacted, regulators will want to know whether you had safeguards in place to prevent or detect it. "We didn't know" won't hold under scrutiny.

The goal isn't to audit your vendor's vendors directly — it's to verify that your vendor is doing it.

The Visibility Gap Is the Risk

Many financial organizations assume that if their direct vendor passes due diligence, the risk stops there. But a vendor can have strong security controls and a solid track record while still

relying on subcontractors with inadequate oversight or concentration risk that your organization has never mapped.

Take cloud infrastructure, for example. If your payment processor and loan origination platform depend on the same underlying infrastructure, you may be carrying concentration risk you've never formally identified because neither vendor surfaces it without being asked. If that underlying vendor goes down, your financial institution could experience significant outages. That kind of overlap is easy to miss when vendor relationships are managed in silos.

The same logic applies to AI. As vendors embed AI tools into their platforms, those models often rely on third-party data pipelines, open-source components, or external APIs. The AI your vendor uses may itself depend on a network of tools and data sources your organization has no visibility into. You approved the vendor. You didn't approve — or even evaluate — everything running underneath it.

What Good Fourth-Party Oversight Looks Like

Building fourth-party risk into your TPRM program doesn't require a complete overhaul; it starts with asking better questions in the right places.

Begin with your critical and high-risk vendors, where a subcontractor failure would have the most direct impact on your operations, customers, or regulatory standing. Due diligence for these relationships should go beyond the vendor's own controls to include how they manage their downstream partners — whether they maintain a vendor inventory, how they vet subcontractors handling your data, and how they monitor for changes in their own ecosystem.

SOC 2 reports are one of the most practical tools available. Under SSAE 18 standards, a vendor's SOC 2 should address its own vendor management program, including contract management, critical vendor identification, and monitoring practices. That section tells you whether your vendor is governing their downstream relationships or treating them as formalities.

Contracts are the other lever. If a vendor isn't contractually required to notify you of subcontractor changes, there's no mechanism to enforce it when it matters. Critical vendor contracts should explicitly require disclosure of material subcontracting arrangements, advance notice of changes, and your right to request information about vendor oversight practices. Without that language, you're relying on goodwill rather than obligation.

Where Financial Organizations Typically Fall Short

Too often, financial organizations under-invest in fourth-party oversight. They assume their resources are too limited, their vendor portfolios too large, or that their vendors are simply handling it. Spreadsheet-based programs only compound this problem. When your vendor inventory lives in a static document and due diligence runs through email, there's no systematic way to track subcontractor disclosures, flag concentration risk, or surface fourth-party exposure before it becomes an incident.

The organizations with the strongest TPRM programs treat fourth-party visibility as an ongoing process, not a point-in-time review. Subcontractor disclosure requirements belong in contracts. Fourth-party questions belong in due diligence questionnaires. And SOC reports deserve a genuine read — not just confirmation that one exists. Technology can help here too; a centralized vendor management platform makes it easier to track subcontractor relationships, monitor for changes, and maintain the kind of audit trail examiners expect.

The Bottom Line

Your third-party risk program is only as strong as your understanding of the ecosystem behind it. Regulators expect that understanding. The question isn't whether your vendors have vendors — they do. The question is whether you know enough about those relationships to manage the risk before it manages you.

About Ncontracts

Ncontracts provides integrated risk management, compliance, and third-party risk management solutions to over 5,500 organizations worldwide, including 4,500 U.S. financial institutions, mortgage companies, and fintechs. The flagship Ncontracts IRM suite combines AI-powered software with expert services, helping financial institutions streamline risk, compliance, and vendor management through an intuitive, cloud-based platform. Ncontracts' Venminder solution is trusted by enterprise financial companies and other large organizations to strategically manage third-party risk across the entire vendor lifecycle.

Visit http://www.ncontracts.com or follow the company on LinkedIn and X for more information.