Third Party Risk Management

Observations and Recommendations for Federal Banking Agencies

MAY 2026

CBA CONSUMER BANKERS ASSOCIATION | AFC American Fintech Council | cfes Coalition for Financial Ecosystem Standards | ICBA

Table of Contents

I. Introduction

In the nearly three years since the federal banking agencies (FBAs)[1] published their Interagency Guidance on Third Party Relationships,[2] depository institutions have continued to foster and rely on third party service provider relationships to deliver essential products, services, and financial technology solutions to consumers.

Recognizing the critical role played by service providers in our financial system, the Consumer Bankers Association (CBA), in collaboration with its members, has undertaken an assessment of the current state of third party risk management (TPRM) compliance and supervision in consumer banking. As part of this assessment, CBA reviewed existing TPRM guidance, met with members to hear and understand their perspectives, and hosted a roundtable with representatives from banks, leading technology providers including generative artificial intelligence and cloud service providers, industry associations, and current and former representatives of federal banking agencies to discuss the future of TPRM in financial services (the "Roundtable").

This project has culminated in several recommendations jointly proposed by CBA, the American Fintech Council, the Coalition for Financial Ecosystem Standards, and the Independent Community Bankers of America (collectively, the "Authors").[3]

---

[1] References to the federal banking agencies in this report include the Office of the Comptroller of the Currency (OCC), the Federal Deposit Insurance Corporation (FDIC), and the Board of Governors of the Federal Reserve System (Federal Reserve).

[2] Federal Reserve, FDIC, and OCC, Interagency Guidance on Third Party Relationships, 88 Fed. Reg. 37920 (June 9, 2023).

[3] A description of each of the Authors is available in Appendix A. Participation in the Roundtable by a person or entity other than the Authors should not be construed as endorsement of anything in this report.

The Roundtable included current and former senior representatives from multiple federal banking agencies, as well as senior representatives from:

Alliance for Innovative Regulation (who co-facilitated the event with Consumer Bankers Association)

Anthropic, PBC

American Fintech Council

Capital One Financial Corporation

Coalition for Financial Ecosystem Standards

Circle Internet Group, Inc.

City National Bank of Florida

Fiserv, Inc.

FS Vector

Gattaca Horizons

Independent Community Bankers of America

JPMorgan Chase

Mercury Technologies

Orrick, Herrington & Sutcliffe LLP

PNC Financial Services Group, Inc.

SoFi Technologies

Unit

Important Disclaimer: The Roundtable was held under Chatham House Rules. Under this structure, CBA invited participants to share their thoughts freely and noted that their comments would not be attributed to them or their employers. This was to allow participants to share information and insights without fear of attribution. This format enabled candid discussion of concerns, uncertainties, and potential solutions.

This report summarizes the Authors' observations and recommendations and invites further dialogue with the federal banking agencies to ensure that the core principles of TPRM continue to be applied consistently and fairly to banks and their service providers, such as fintechs, even as service providers proliferate and increase their market power and complexity.

II. Executive Summary

The 2023 Interagency Guidance on Third Party Relationships (Interagency Guidance) remains a strong foundation for risk-based oversight of service providers in banking (e.g., fintech companies, vendors, cloud service providers).[4] The Authors generally support the principles-based structure of the guidance and do not believe large-scale revisions to the framework are necessary at this time. In particular, the Authors continue to value the guidance's recognition that not all relationships present the same level of risk and therefore should not be subject to the same level of oversight, diligence, or monitoring.

At the same time, Roundtable discussions revealed a growing disconnect between the assumptions underlying the current supervisory framework and the operational realities of today's banking and technology environment.

When many foundational TPRM expectations were first developed, banks managed a smaller number of vendors, technology stacks changed more slowly, and it was generally possible to conduct relatively comprehensive ex ante diligence before deploying a service provider relationship. That environment – and the resulting risk landscape – is rapidly changing. Banks today operate within a highly interconnected ecosystem of cloud providers, fintech partners, AI developers, data aggregators, and subcontractors whose relationships evolve continuously and often with limited visibility to the bank itself. Modern vendor ecosystems are increasingly characterized by concentration, interdependence, and technological complexity — particularly as banks become structurally dependent on a small number of hyperscale cloud providers, emerging AI infrastructure providers, and the emergence of software-as-a-service as the default format in which software is delivered.

As a result, the central challenge in TPRM is no longer simply obtaining comprehensive information about a vendor before onboarding. Rather, it is determining how to identify material risks in an environment of imperfect information, monitor those risks continuously as technologies and relationships evolve, and ensure that banks can contain operational disruption and customer harm when failures occur.

Importantly, the Authors generally do not view these challenges as evidence that the Interagency Guidance itself is fundamentally flawed. To the contrary, Roundtable participants repeatedly emphasized that the principles-based nature of the guidance remains one of its greatest strengths. The primary concerns raised by Roundtable participants instead related to the application of the guidance during supervisory activities, the practical limitations banks face in dealing with dominant service providers

---

[4] Recognizing the diversity and evolution of banks' relationships with third parties in conducting both consumer-facing banking functions as well as enterprise activities, we broadly construe the term "third party" to encompass contract-based bank-fintech, vendor, and other service provider relationships for the purpose of this report.

and complex subcontractor chains, and the need for supervisory expectations to evolve alongside changes in technology and market structure.

Specifically, Roundtable participants observed that:

- Examiners across agencies, regions, and examination teams often appear to apply third party risk management expectations inconsistently with respect to issues of comparable risk or complexity; at the same time, examiners appear to treat principles-based guidance as a static checklist rather than a risk-calibrated supervisory framework;

- Banks frequently lack sufficient bargaining power to obtain desired diligence information, audit rights, or contractual protections from large and market-dominant service providers, particularly in concentrated sectors such as cloud computing and artificial intelligence infrastructure;

- Existing guidance does not provide sufficient clarity regarding the limits of banks' responsibility for subcontractor and "nth-party" oversight, particularly where banks lack direct privity or operational visibility;

- The increasing speed and complexity of technological change has made traditional point-in-time validation models less effective as a standalone mechanism for managing risk, increasing the importance of a collective move towards a more efficient and robust due diligence approach and maturation of continuous monitoring capabilities; and

- Emerging technologies and digital solutions offer significant opportunities to improve due diligence, monitoring, supervisory consistency, and supply-chain mapping — but technological tools are not substitutes for clear regulatory policy, calibrated supervisory expectations, or sound governance.

Taken together, these observations reflect a more fundamental shift in what effective third party risk management requires. The existing framework must increasingly orient around resiliency, materiality, and continuous risk management, rather than assumptions of complete ex ante visibility into every vendor relationship and subcontractor dependency. In practice, this means supervisory expectations should eventually evolve to a point at which examiners would place greater emphasis on whether banks can identify material risks, monitor them dynamically, implement effective controls and "circuit breakers," and maintain operational continuity when disruptions occur — rather than on whether banks can produce exhaustive pre-deployment documentation for increasingly complex and opaque vendor ecosystems.

Accordingly, the Authors recommend that the federal banking agencies:

- Preserve the Interagency Guidance's principles-based structure and maintain sufficiently detailed expectations regarding diligence, governance, and contracting practices;

- Reinforce through examiner training, supervisory calibration, and appeals processes that third party risk management reviews should remain risk-based, materiality-focused, and tailored to the nature of the relationship being examined;

- Recognize and accommodate the practical limitations banks face when dealing with concentrated or market-dominant vendors, including hyperscale cloud and AI providers, and avoid criticizing banks for failing to obtain information that is not commercially available;

- Clarify that banks are responsible for assessing the adequacy of their direct third party's own subcontractor risk management programs and ensuring that risk-management expectations appropriately cascade downstream, but are not expected to directly supervise every fourth- or nth-party relationship;

- Encourage the responsible use of AI and related technologies to support third party risk management functions and supervisory consistency, while making clear that AI-assisted processes remain subject to proportionate governance and human oversight expectations; and

- Support public-private standards-setting and certification initiatives that could help streamline vendor due diligence and improve consistency across institutions and regulators.

These recommendations are not intended to weaken third party risk management expectations or reduce accountability for banks and third parties. Rather, they are intended to align supervisory expectations with the realities of the modern banking environment and to ensure that regulatory attention remains focused on the risks most likely to threaten consumers, operational resiliency, and the safety and soundness of the banking system.

III. Current State of Third Party Risk Management in Banking

A. Banks and third parties rely on the Interagency Guidance to effectively offer modern banking services

Roundtable participants reported that they find the Interagency Guidance to be a practical and flexible framework for managing third party-related risks, and that they rely on it in designing, implementing, and updating their own third party risk management programs.[5] Banks appreciated regulators' recognition in the guidance that "[n]ot all relationships present the same level of risk, and therefore not all relationships require the same level or type of oversight or risk management."[6] They generally agreed that the core principle of the Interagency Guidance – that service provider oversight should be risk-based and tailored to the complexity and criticality of the relationship – is pragmatic and necessary in today's banking environment, where many banking activities involve one or more providers.

Some Roundtable participants also expressed that the Interagency Guidance contrasts favorably with third party risk management frameworks adopted by regulators outside of the United States. For example, the European Union's Digital Operational Resilience Act (DORA),[7] which establishes guidelines for managing risks presented by information and communication technology (ICT) providers, and guidelines issued by the Monetary Authority of Singapore (MAS)[8] were cited as overly proscriptive with respect to financial institutions' third party risk management responsibilities, particularly with regard to the oversight of subcontractors (*i.e.*, "fourth parties"). Participants felt that the Interagency Guidance strikes the right balance between (i) setting out clear principles for third party risk management and (ii) explicitly permitting banks to make risk-based decisions to engage third parties, even where there may be a mismatch in information sharing or bargaining power.

Roundtable participants also noted that the effectiveness of the Interagency Guidance depends not only on how banks implement it, but on how their service providers understand and respond to regulators' expectations. Roundtable participants observed that many fintechs and smaller technology vendors struggle not merely with the burden

---

[5] Roundtable participants noted that the approach to third party risk management presented in the Interagency Guidance is echoed in other informal guidance that banks also leverage in overseeing third parties, such as the 2024 Guide for Community Banks on TPRM and the portion of the 2021 Interagency Statement on Model Risk Management relating to third party models.

[6] Interagency Guidance, 88 Fed. Reg. at 37922.

[7] Regulation (EU) 2022/2554 (Jan. 2023).

[8] *See e.g.* MAS, Key Resources on Third Party Risk Management, *available at* https://www.mas.gov.sg/regulation/third-party-risk-management.

of compliance, but with a more fundamental challenge: they lack familiarity with the supervisory framework that governs their bank customers' oversight obligations in the first place. Unlike larger, more established service providers that have developed internal compliance infrastructure over years of bank engagements, newer market entrants may be unprepared to respond meaningfully to due diligence requests, provide adequate audit access, or engage constructively on contractual terms — not out of resistance, but out of genuine unfamiliarity with what banks are legally and regulatorily required to ask. This dynamic can be just as frustrating for banks as outright non-cooperation from a dominant vendor, and it points to a gap that the Interagency Guidance, directed as it is to banking organizations rather than their counterparties, is structurally unable to close on its own.

Banks reported that the "strength" and level of detail in the Interagency Guidance has proven useful in negotiations with providers at onboarding and throughout the relationship. Specifically, banks seeking information regarding a third party's financial condition, legal and regulatory compliance, information security and incident reporting practices, and other key policies, procedures, and activities can point to the Interagency Guidance as a source of authority for requiring submission of this information during initial diligence or periodic reviews. Roundtable participants expressed concern about potentially losing leverage with third parties if this specificity were to be curtailed or removed altogether from the Interagency Guidance. One Roundtable participant cited recent revisions to the federal banking agencies' model risk management guidance — and in particular, the decision to carve out generative and agentic AI from that guidance's scope — as reflective of the types of changes that could be damaging to the effectiveness a third party risk management program, which relies heavily on the Interagency Guidance in its current form.

B. Inconsistent application of the Interagency Guidance during examinations

While Roundtable participants generally found that the Interagency Guidance sets appropriate regulatory expectations for effective third party risk management, some banks shared they had observed and/or experienced inconsistency in the *application* of the principles therein. Specifically, participants have been subject to different levels of rigidity in applying the Interagency Guidance during supervisory activity, depending on the agency, region, or even examiner-in-charge (EIC) directing the examination. The result is that in some examinations, participants have sensed that EICs and supervisory staff view the Interagency Guidance as establishing firm compliance requirements against which all relationships will be measured, instead of setting the "scope of the supervisory review depend[ing] on the degree of risk and the complexity associated with the banking organization's activities and relationships."[9]

Roundtable participants recognize that risk-based supervision is inherently institution-specific, and that consequently there is often some level of inconsistency between

[9] Interagency Guidance, 88 Fed. Reg. at 37936.

examination approaches and findings for different entities. Still, participants generally shared the view that, where possible, relationships posing similar types and levels of risk should be held to similar standards for third party risk management. Roundtable participants observed that differing interpretations and applications of the Interagency Guidance may be the result of examiner training taking place on a regional, rather than centralized, basis – or a lack of a practical accountability mechanism to mitigate the risk that examiners feel structural or personal pressure to err towards conservatism.

C. Banks seek clarity regarding the limits of their responsibility to directly supervise "Nth-Party" relationships

The Interagency Guidance makes clear that "the use of third parties does not diminish or remove banking organizations' responsibilities to ensure that activities are performed" in a safe, sound, and compliant manner.[10] Banks generally understand and accept this responsibility, though Roundtable participants noted that there are limits to what banks can reasonably accomplish when it comes to collecting and assessing information at onboarding and on an ongoing basis from providers, particularly with respect to their subcontractors and other "nth" parties. Banks take this into consideration when performing risk assessments, recognizing that there will be relationships for which there are information gaps, slow or incomplete vendor responses, or limited negotiating power at onboarding or during ongoing monitoring.

The Interagency Guidance helpfully recognizes there will be instances where banks are in an unequal bargaining position with key service providers, or where direct oversight of subcontractors is not practical or possible, and contemplates that institutions will engage in risk-based decisions with respect to their management of these relationships. Nevertheless, the guidance leaves open the possibility that where a subcontractor is integral to a third party's activities on behalf of a bank, a bank may need to engage in more extensive monitoring activities to compensate for more limited ability to negotiate specific business practice or contractual changes with vendors, ex ante.

In light of the increasing prevalence of "nth parties" in nearly every engagement, Roundtable participants generally expressed consensus that the expectation of banks' direct oversight should be limited to parties with which they were in direct privity. In doing so, participants generally agreed that federal banking agencies could and should expect banks to perform diligence on and monitor their direct third parties' own subcontractor risk management programs, ensuring that such expectations "cascade" to fourth parties and so-forth – but that regulatory expectations should not extend to such fourth parties and beyond. Roundtable participants noted that, in some cases, banks would face legal hurdles in even asking to review contracts between third and fourth parties. Accordingly, Roundtable participants noted an opportunity to clarify these expectations in any revised third party risk management guidance.

---

[10] *Id.* at 37920.

D. Technology and artificial intelligence should be embraced in third party risk management — but are not a substitute for sound policy

Roundtable participants expressed genuine enthusiasm for AI's potential to address many of the challenges described in this report — and that enthusiasm was not unfounded. AI tools are already being deployed by banks for due diligence processing, vendor questionnaire analysis, risk scoring, and ongoing monitoring, and participants noted that regulators have generally been receptive to this trend. Some participants went further, suggesting that AI could eventually help map nth-party supply chains (assuming the data is made available and is a high-quality, representative data set). AI could help identify patterns of examiner inconsistency across institutions. And AI could be incorporated with other new technologies to enable the kind of continuous monitoring (as part of efforts to affect a broader shift in the third party risk management operating model) that existing point-in-time validation frameworks cannot practically achieve. The Authors share this optimism and our recommendations in Section IV.D reflect it.

At the same time, a note of caution emerged from the Roundtable that the Authors believe deserves equal weight: AI is a resource enhancement tool — a powerful one — but it is not a policy answer. Participants observed, with some concern, a tendency in the broader industry conversation to treat "AI will figure this out" as a response to hard questions about regulatory clarity, supervisory expectations, and the allocation of responsibilities among banks, vendors, and regulators. That tendency is understandable given AI's genuine capabilities, but it risks substituting technological optimism for the deliberate policy choices that only the federal banking agencies can make. A community bank should not be expected to deploy AI to compensate for the absence of clear guidance on nth-party oversight. A regulator should not defer difficult questions about examiner consistency to an algorithm. The near-term regulatory clarity that banks need cannot wait for AI to mature into a solution. These themes informed our recommendations in Section IV.D and the paradigm shift discussion in Section III.E that follows.

E. A Shifting Paradigm: From ex ante validation to real-time risk management

A cross-cutting theme emerged from the Roundtable that deserves explicit recognition before turning to recommendations: the existing third party risk management framework — and the supervisory expectations that have grown up around it — was designed for a world that is now rapidly changing.

When the foundational principles of risk management were developed, banks maintained relationships with a manageable number of vendors, operated relatively stable technology stacks, and could reasonably aspire to understand what their service providers were doing before deploying them. Pre-deployment due diligence, point-in-time validation, and comprehensive ex ante documentation were demanding but achievable standards. The guidance that emerged from that era reflects those assumptions.

That world has given way to something fundamentally different. Banks today maintain relationships with hundreds or thousands of vendors, many of whom are themselves dependent on subcontractors that change frequently and with limited notice. For example, AI models — increasingly integrated into banking operations — are updated continuously, may behave differently across contexts, and resist the kind of static validation that works for more deterministic systems. The speed of technological change means that contracted services may undergo more frequent and rapid changes, and the related risks may as a result materialize in a more rapid or differing manner. And the opacity inherent in many modern AI systems means that even a vendor acting in complete good faith may be unable to provide the kind of comprehensive developmental information that the existing due diligence and oversight framework contemplates.

The result is a widening gap between what the guidance envisions and what currently is operationally achievable — a gap that manifests as both over-examination in some areas (examiners demanding documentation that simply does not exist) and under-examination in others (missing real risks because they emerge post-deployment rather than being visible at onboarding). Neither outcome serves the goal of sound risk management as banks work to evolve their risk management practices, which importantly requires collaboration with vendors to establish new oversight capabilities to better accommodate the changing landscape.

Roundtable participants converged on a different paradigm — one that accepts the limits of ex ante knowledge, at present, and invests instead in the infrastructure for real-time risk management to address the changing nature of the service landscape and dependencies.

This reorientation has three practical components:

- Materiality-Focused Scoping: Due diligence should focus on identifying the most critical risks and the infrastructure needed to manage them, rather than seeking exhaustive advance knowledge of a vendor's entire internal system.

- Continuous Monitoring: Industry collaboration is needed to progress real-time monitoring capabilities and work with vendors to implement this evolution. These capabilities make it much more operationally feasible to track vendor performance more proactively, identify potential issues or vulnerabilities, and better identify changes in service risks. Collaboration is key to affecting this change.

- "Circuit Breaker" measures: The ultimate measure of a sound system is its ability to catch and contain problems before they become catastrophic. Banks should be evaluated on their "circuit breakers"—the specific controls, contractual rights, and business continuity capabilities that allow them to detect degradation, isolate systems, and switch to alternate providers or manual backups (where technically and operationally feasible) during a failure. Where such measures are limited by vendor cooperation or refusal, especially for critical third-parties, the federal

banking agencies should take direct actions to address these obstacles on behalf of the sector.

The Authors do not raise this as an argument to lower standards. We do, however, believe that at every level of the supervisory and regulatory relationship, all parties should be clear-eyed about the new operating environment and focus supervisory attention on the risk management capabilities that matter most. In the Roundtable, participants raised writer Atul Gawande's insights about complex systems: in domains where failure cannot be prevented entirely, the measure of a sound system is not whether it eliminates all risk but whether it is designed to catch and contain problems before they become catastrophic. A bank that cannot produce a complete vendor validation report but has robust real-time monitoring, tested circuit breakers, and a documented remediation playbook is managing risk more effectively than one that has voluminous pre-deployment documentation but no plan for what happens when something goes wrong. Robust real-time monitoring tools are still relatively nascent, however; we encourage the federal banking agencies to appreciate the journey to develop and integrate these capabilities across the sector and supplier ecosystem will take time to achieve and to calibrate their supervisory expectations accordingly.

The near-term recommendations in Section IV are informed by this paradigm shift — orienting due diligence, examiner training, and vendor accountability around materiality and real-time risk rather than documentation completeness. The broader supervisory modernization steps that this paradigm ultimately requires — continuous monitoring, circuit breakers, and updated examination standards — are addressed in Section V, where the Authors treat them as longer-horizon goals that will require sustained collaboration between the federal banking agencies, banks, and their service providers

IV. Recommendations

The Roundtable led the Authors to develop the following recommendations for consideration by the federal banking agencies.

F. Federal banking agencies should maintain robust Interagency Guidance on third party risk management, while enhancing examiner training regarding its application

As noted above, the Interagency Guidance is widely recognized by banks of varying sizes and complexity as a useful framework for managing risks. The Authors recommend that to the extent the federal banking agencies are considering updating the Interagency Guidance, the revised guidance should preserve the level of detail available in the current version regarding the elements of effective third party risk management. In particular, the sections of the Interagency Guidance on due diligence, contract negotiation, and governance have become important, practical guidelines that risk departments rely on when designing and implementing oversight functions. And as discussed below in Section IV.B, these sections of the Interagency Guidance are also useful references for banks when negotiating with third parties regarding contract terms and information collection for diligence and monitoring.

However, while banks view the Interagency Guidance itself favorably, they are concerned about the negative impacts that can result from an overly rigid application of the guidance in connection with federal banking agencies' supervisory activities. Examiners may interpret the guidance as a checklist of mandatory requirements; this has led some banks to feel they must devote equal resources to low-risk vendors and critical service providers alike, undermining the risk-based approach espoused by the guidance and potentially creating inefficiencies that disproportionately impact community and mid-sized institutions. For example, a community bank onboarding a vendor for a non-critical, ancillary service should not be required to conduct similar levels of due diligence, contract negotiation, and ongoing monitoring as it would for a core systems provider.

The Authors recommend that the federal banking agencies take concrete steps internally to reinforce with their supervisory teams the principles-based, risk-driven nature of the Interagency Guidance. This could be accomplished by providing centralized "case-study" style examiner training that explains how principles-based reviews differ from applying a checklist, and provides illustrative examples of how an examiner should assess aspects of a bank's third party risk management performance using the Interagency Guidance. Examiners should be encouraged to focus on actual or likely risk outcomes associated with relationships when determining the adequacy of third party risk management activities, and to consider the bank's own assessment of the level of risk presented by the vendor and/or the outsourced services, in addition to the examiners' own views.

In developing such training, the Authors encourage the federal banking agencies to think carefully about the role of checklists in the examination process. Checklists are not

inherently problematic. As Atul Gawande's influential work on the subject demonstrates, well-designed checklists serve as memory aids that help experts apply consistent judgment under pressure, not as substitutes for that judgment.[11] The problem arises when checklists become static and universal: applied identically regardless of institution size, vendor criticality, or risk profile, they transform a principles-based framework into a box-checking exercise and create exactly the kind of "foolish consistency" that undermines sound supervision. The goal should be dynamic checklists — ones that are calibrated to the nature and materiality of the relationship being examined, that prompt examiners to ask the right questions for a given risk context rather than the same questions for every vendor, and that are updated as the technology and risk landscape evolves. A community bank onboarding a payroll vendor and a large regional bank deploying a foundation model for credit decisioning should not be evaluated against the same checklist. Training examiners to build and apply checklists dynamically, and to treat them as pattern-recognition tools rather than scorecards, could go a long way toward addressing the inconsistency that Roundtable participants have observed.

Much of what the Authors are recommending in this section ultimately depends less on guidance text than on culture change — and culture change requires both leadership commitment and accountability mechanisms that outlast any particular administration. On the substance, Roundtable participants have been encouraged by concrete steps the federal banking agencies have taken to reorient their supervisory programs around material financial risks. The OCC and FDIC jointly proposed a rule in October 2025 that would define "unsafe or unsound practice" and revise the framework for issuing MRAs, with FDIC Acting Chair Travis Hill stating explicitly that examiners must prioritize material risks rather than "a litany of process-related items that are unrelated to a bank's current or future financial condition."[12] The Federal Reserve similarly announced in late 2025 that it was reshaping its supervision and regulation division to focus on banks' material risks rather than process-related errors that do not affect safety and soundness,[13] and the OCC has moved to eliminate mandatory policy-based examination

---

[11] Atul Gawande, *The Checklist Manifesto: How to Get Things Right* (Metropolitan Books 2009).

[12] Statement by Acting Chairman Travis Hill on Proposal Regarding Unsafe or Unsound Practices, Matters Requiring Attention (Oct. 7, 2025). https://www.fdic.gov/statement-acting-chairman-travis-hill-proposal-regarding-unsafe-or-unsound-practices-matters.pdf

[13] Press Release, Bd. of Governors of the Fed. Rsrv. Sys., *Federal Reserve Board Releases Information Regarding Enhancements to Bank Supervision* (Nov. 18, 2025). https://www.federalreserve.gov/newsevents/pressreleases/bcreg20251118a.htm ("Our supervisory approach is not about narrowing our focus—it is about sharpening it," said Vice Chair for Supervision Michelle W. Bowman. "By anchoring our work in material financial risks, we strengthen the banking system's foundation while upholding transparency, accountability, and fairness. This is not about what we are leaving behind—it is about building a more effective supervisory framework that truly promotes safety and soundness across our financial system, which is the Federal Reserve's core supervisory responsibility.")

requirements for community banks beginning January 2026.[14] These are meaningful commitments. Encouragingly, agency leadership appears to be reinforcing this message directly with examination staff, including through regional outreach by agency heads, signaling that the emphasis on materiality is a genuine institutional priority, not merely aspirational language that field staff can interpret as they see fit.

Accountability mechanisms are equally important. The Authors have been encouraged by recent steps the federal banking agencies have taken to create more structured opportunities for banks to challenge examination findings that appear inconsistent with the risk-based framework the Interagency Guidance envisions. Most notably, the OCC has proposed a formal supervisory appeals process that would include independent board members, and the FDIC has undertaken similar efforts to strengthen its appeals framework. CBA has submitted letters in support of both efforts, underscoring that the availability of a credible, independent appeals process is itself a check on examiner overreach — not because banks will always appeal, but because the existence of the mechanism creates appropriate incentives for examiners to ground their findings in the guidance rather than personal or regional interpretations of it.[15]

Accountability mechanisms and training programs are necessary but not sufficient responses to examiner inconsistency, because they address behavior without addressing the underlying incentive structure that produces it. The root of the problem is a classic agency problem: an examiner who applies third party risk management expectations too broadly, demands documentation that does not exist, or treats principles-based guidance as a mandatory checklist faces essentially no institutional consequence for doing so. An examiner who applies the guidance too leniently and misses a material risk faces significant professional exposure. That asymmetry is not a character flaw; it is a rational response to the incentive environment, and it will persist regardless of how many training sessions are conducted or how clearly the guidance is written. The Authors do not presume to tell the federal banking agencies how to structure their internal personnel systems. But we would observe that the commitments described above will remain aspirational unless they are reinforced by internal recognition and evaluation practices that reward proportionate, risk-calibrated supervision rather than simply thorough supervision. An examiner who correctly identifies that a low-risk vendor relationship does not warrant exhaustive documentation review, and says so clearly in an examination, should be recognized as exercising sound judgment — not second-guessed for what they did not examine. Building that culture requires agency

---

[14] Office of the Comptroller of the Currency, OCC Bulletin 2025-24, *Examinations: Frequency and Scope for Community Banks* (Oct. 6, 2025). https://www.occ.treas.gov/news-issuances/bulletins/2025/bulletin-2025-24.html.

[15] Consumer Bankers Ass'n, Comment Letter on the Office of the Comptroller of the Currency's Notice of Proposed Rulemaking on the Bank Appeals Process (Apr. 20, 2026), https://consumerbankers.com/wp-content/uploads/2026/04/OCC-Appeal-Process-Docket-ID-OCC-2026-0001-Final-CBA-.pdf.

leadership to be as explicit internally about what good risk-calibrated supervision looks like as they have been externally about why it matters.

Beyond formal appeals, however, banks need a lower-friction option for engaging with examination teams before a finding becomes an adversarial dispute. A formal appeals process is a remedy; what banks also need is a pressure valve. Federal banking agencies should consider establishing a portal mechanism or other formal escalation channel(s) for banks to seek guidance or raise concerns when faced with inconsistent supervisory interpretations of the Interagency Guidance. While Roundtable participants cited recent changes to FBA supervisory appeals processes as offering a potential avenue for challenging examiner overreach in third party risk management-related findings, banks generally supported also offering a portal mechanism as a way of engaging with examination teams outside of a formal administrative process – ideally allowing the parties to avoid the need for a bank to file an appeal. However, Roundtable participants underscored that in order for the portal to be useful, federal banking agencies would need to provide the industry assurance that issues reported through the portal would not be used to support regulatory criticism or negative examination findings. Finally, interagency calibration reviews may also be a useful exercise to ensure alignment among supervisory teams, regardless of the applicable FBA.

G. Federal banking agencies' expectations should reflect the reality of bargaining power dynamics in third party relationships

A challenge faced by banks of all sizes – but especially smaller and mid-sized banks – is the mismatch in bargaining power between banks and large or market-dominant service providers. These third parties often possess significant market leverage, making it difficult for banks to negotiate contract terms and obtain due diligence information at onboarding. This dynamic can also make it difficult for banks to secure data for ongoing monitoring (beyond information that the third party itself deems sufficient for oversight purposes).

The Interagency Guidance acknowledges these challenges, noting that banks may encounter practical limitations in obtaining desired information from third parties.[16] However, the guidance stops short of offering actionable solutions for banks facing such market power mismatches. In practice, banks may be unable to obtain developmental information, testing results, or performance data from large vendors, particularly those providing core banking, payment processing, cloud services, or consumer reporting data. In such an event, banks should not be criticized or penalized for failing to obtain

[16] Interagency Guidance, 88 Fed. Reg. at 37929 ("In some instances, a banking organization may not be able to obtain the desired due diligence information from a third party. . . . While the methods and scope of due diligence may differ, it is important for the banking organization to identify and document any limitations of its due diligence, understand the risks from such limitations, and consider alternatives as to how to mitigate the risks.").

information that is not commercially obtainable and we encourage regulators to weigh in on model risk management issues in their exams of service providers.

Additionally, the adoption of artificial intelligence within the banking sector is fundamentally dependent on relationships. Whether a large-scale institution or a community bank, nearly all financial institutions now rely on a remarkably small number of vendors, primarily a handful of hyperscale cloud service providers and an emerging cohort of foundation model developers, to provide the computing infrastructure and AI capabilities necessary for modern banking operations. This concentration is not incidental; it reflects the economics of frontier AI development and cloud infrastructure, which require capital investment at a scale that forecloses meaningful competition from all but a few global technology firms. The result is a structural dependency that is unlike anything the existing third party risk management framework was designed to manage: banks cannot credibly threaten to take their business elsewhere, alternative providers often do not exist, and the leverage that underlies the entire due diligence negotiation is effectively absent.[17] Obtaining meaningful risk information from these vendors (e.g., developmental data, model performance metrics, incident response protocols, subcontractor maps) is not merely a compliance exercise; it is a prerequisite for understanding whether the systems that now run large portions of the U.S. banking system are safe and sound. The pace of AI development makes this more urgent, not less, and the third party risk management framework needs to reckon explicitly with the asymmetry that concentration creates.

To address these concerns, regulators should ensure that guidance on third party risk management practices, including the Interagency Guidance, continues to include specific language regarding oversight and risk management expectations for banks during onboarding, contracting, and ongoing monitoring. Roundtable participants reported that being able to direct vendors to these provisions of the Interagency Guidance gives them leverage to push back on providers – including AI companies and other large technology providers – that resist responding to reasonable third party risk management-related requests or requirements. Some banks expressed concern that revisions to the Interagency Guidance to make it higher-level, similar to recent changes to the interagency guidance on model risk management, would make it more challenging to push for transparency and disclosure from key vendors.

The Authors additionally recommend that the federal banking agencies consider accepting reports from banks regarding instances where a vendor refuses to provide information that the bank has deemed necessary for effective third party risk management. Opening this line of communication – either through a portal (as discussed above) or another mechanism – would allow agencies to identify patterns of

---

[17] U.S. Dep't of the Treasury, *The Financial Services Sector's Adoption of Cloud Services* (2023). https://home.treasury.gov/system/files/136/Treasury-Cloud-Report.pdf.

non-cooperation by service providers, and could even inform the federal banking agencies' decisions regarding which entities to prioritize for direct oversight under the Bank Service Company Act (if applicable, depending on the services provided). Knowledge among service providers that this mechanism is available to banks could also incentivize third parties to adhere to the principles-based guidance described in the preceding paragraph.

Finally, the federal banking agencies should ensure examiners at all levels, and across regions, recognize and accommodate the practical limitations faced by banks in their due diligence efforts, particularly where services are being provided by a large company that faces limited competition in its market. In alignment with the Interagency Guidance, when full information about a service provider is not available, banks should be permitted to use alternative sources, implement compensating controls, or, depending on the circumstances, accept an appropriate level of residual risk, with the input and visibility of senior management. Supervisory expectations should reflect the realities of the marketplace, acknowledging that banks may not always have access to the ideal set of data or documentation.[18] By promoting transparency and accountability among large service providers, regulators can help level the playing field and ensure that all banks, regardless of their size or resources, are able to engage with third parties and effectively manage the associated risks.

H. Federal banking agencies should clarify expectations that banks are not expected to directly manage "Nth-Parties"

It is increasingly common for banks' relationships with third parties to involve subcontractors (*i.e.*, "nth party" providers). While banks are responsible for managing risks associated with their direct vendors, in many cases it is neither practical nor feasible for banks to oversee and monitor an entire supply chain – in other words, the "third parties" of the bank's third parties. The Interagency Guidance appears to recognize this reality in discussing subcontractor relationships but does not provide specific expectations for how banks should approach subcontractor and fourth- (or "nth") party risks.

The Authors recommend that the federal banking agencies confirm that a bank's third party risk management obligations extend only as far as their third parties – the parties with whom they are in contractual privity.

Depending on the risk and materiality of those relationships, banks may assess, confirm, and monitor the adequacy of their direct vendors' own subcontractor risk management programs. But banks cannot be expected to directly vet, monitor, or audit their third parties' subcontractors with which the banks do not have a direct relationship. This key

[18] If a reporting mechanism, as suggested in the preceding paragraph, is adopted, bank feedback regarding third parties could also be an important consideration for examination teams in assessing a bank's compliance management and TPRM activities.

principle should be reiterated with supervisory staff to ensure consistent application during examinations.

I. Technology and artificial intelligence should be embraced

To realize the potential of AI described in Section III.D, the federal banking agencies must provide a regulatory environment that encourages adoption while maintaining sound oversight. The Authors offer the following specific recommendations to integrate AI into the third party risk management framework:

Affirmative encouragement of AI service providers. The Authors recommend that the federal banking agencies explicitly confirm that AI-assisted processes — including AI-assisted due diligence review, vendor questionnaire analysis, risk scoring, and ongoing monitoring — satisfy supervisory expectations when implemented under appropriate governance frameworks that preserve human oversight of material decisions. This matters especially for community banks, which have been more hesitant to adopt AI for risk management in part because of uncertainty about whether examiners will accept AI-assisted outputs as adequate documentation of third party risk management compliance. While this encouragement could be included in revised guidance, less formal affirmative statements like speeches or bulletins from the federal banking agencies could still help close that gap and encourage responsible adoption across institutions of all sizes.[19]

Proportionate governance expectations for AI-assisted TPRM tools. As AI becomes more deeply embedded in banks' TPRM programs, a practical concern arises: examiners may scrutinize the AI tools themselves as relationships requiring their own comprehensive due diligence, potentially creating a recursive compliance burden. Updated guidance should clarify that governance expectations for AI-assisted third party risk management tools are proportionate to the materiality of the decisions they support — consistent with the risk-based approach the Interagency Guidance applies to all relationships. A bank using an AI tool to process vendor questionnaires should not face the same diligence requirements for that tool as it would for a core banking system provider.

---

[19] The same AI tools that banks are deploying for third party risk management could, in principle, be used by the federal banking agencies themselves — to evaluate whether examination findings are being applied consistently across institutions, regions, and agencies, and to flag outlier findings for supervisory review. Roundtable participants noted that this application is technically feasible today: given access to examination data, AI systems could identify patterns of inconsistency that would be invisible to any individual examiner or supervisory office. The Authors encourage the federal banking agencies to explore this application seriously, including assessing whether existing appropriations and technology infrastructure support it. This is precisely the kind of use case where AI functions as a resource multiplier for regulators facing real capacity constraints — not a replacement for examiner judgment, but a check on whether that judgment is being applied evenly.

Automation of the "Common App": Regulators should support the use of AI to ingest vendor control documentation (e.g., audit reports and security certifications), discussed further below.

J. Regulators should support standards-setting and certification efforts

One of the most concrete near-term opportunities within a standards-setting framework is the development of a standardized due diligence protocol — a "common app" for vendor assessments that establishes a consistent set of information requirements applicable across institutions and regulators. Today, banks of all sizes submit materially similar information requests to the same vendors, creating redundant burden for both parties without producing meaningfully differentiated risk insight. A shared baseline protocol, developed through public-private collaboration and recognized by the federal banking agencies as satisfying foundational due diligence documentation requirements, would eliminate that redundancy and allow banks to focus institution-specific diligence on questions that actually vary by use case and risk profile.

V. Longer-Term Considerations

The recommendations set forth in Section IV are intended to be actionable in the near term, requiring no statutory change and minimal rulemaking. However, the Roundtable discussions surfaced a set of structural challenges that will require more sustained attention from regulators and the industry alike — and that the Authors suggest merit continued study even if regulatory solutions remain years away.

K. Supporting the evolution of continuous monitoring capabilities

The paradigm shift described in Section III.E may, over time, contribute to broader changes in how banks, service providers, and the federal banking agencies approach risk management. As vendor ecosystems become increasingly interconnected and technologically dynamic, industry participants and regulators alike may need to explore new approaches to monitoring and oversight. The Authors encourage the federal banking agencies to be active partners in that evolution by recognizing and supporting industry efforts to develop more advanced monitoring capabilities, engaging with service providers regarding the infrastructure needed to support those capabilities, and calibrating supervisory expectations in a manner that recognizes both the promise and the current limitations of emerging tools and methodologies.

Over time, federal banking agencies may wish to support broader adoption of continuous monitoring capabilities that allow banks to track vendor performance, financial condition, operational resiliency, and risk indicators on a more dynamic basis. As these capabilities continue to mature, supervisory approaches may increasingly recognize the value of effective ongoing monitoring programs alongside traditional point-in-time review processes. The Authors recognize, however, that many of these capabilities remain relatively nascent and will require sustained collaboration among banks, service providers, technology firms, standards-setting bodies, and regulators before they can be implemented consistently and effectively across the sector.

Supervisory expectations should continue evolving alongside changes in technology, service-provider ecosystems, and operational risk-management capabilities, while remaining grounded in the core objectives of operational resiliency, consumer protection, and safety and soundness.

L. The Bank Service Company Act as a tool for vendor accountability

The Bank Service Company Act (BSCA) grants the federal banking agencies authority to examine and, in some circumstances, take supervisory action against companies that provide services to banks. In principle, this authority could be a meaningful complement to banks' own third party risk management efforts — particularly with respect to large, market-dominant service providers that resist banks' reasonable requests for diligence information or audit access. Roundtable participants observed that the federal banking agencies could, over time, use patterns of bank-reported non-cooperation to inform decisions about which service providers to prioritize for direct examination under the

BSCA. The existence of such a mechanism, even if rarely invoked, could itself create incentives for vendors to engage more constructively with banks' third party risk management requirements.

That said, participants were clear-eyed about the BSCA's limitations as a near-term solution. Examiner capacity constraints, jurisdictional questions about which vendors fall within the BSCA's scope, and the practical complexity of examining large technology companies under a bank-centric supervisory framework all present meaningful obstacles. At the same time, the Authors would observe that many of these obstacles are, at their core, questions of prioritization rather than legal authority — and that legal questions that do exist, such as whether federal banking agencies could issue an MRA directly to a non-bank service provider, are not obviously insurmountable. More to the point: the more than 4,000 banking organizations subject to third party risk management requirements face analogous prioritization and resourcing challenges every day, with far fewer economies of scale and considerably less bargaining power than the agencies themselves bring to the table. The federal banking agencies are not without tools here; the question is whether deploying them more assertively against large, non-cooperative service providers is treated as a priority.

Given the strength of the feedback we heard from Roundtable participants, the Authors do not recommend immediate reliance on the BSCA. We do, however, encourage the federal banking agencies to study how BSCA authority could be modernized or more systematically deployed — and to consider whether the Act's scope is adequate to cover the full range of technology providers that now sit at the center of banks' operational infrastructure. This will become increasingly important in the near future as AI developers, most of which will be highly-concentrated, become increasingly critical service providers to the banking sector.

There is, however, a dimension of BSCA authority that deserves more immediate attention and that does not require resolving the harder questions above: its potential function as a carrot rather than a stick. The mere existence of a credible supervisory backstop — communicated clearly and consistently by the federal banking agencies to the vendor community — could itself reshape vendor behavior without a single examination ever being opened. Vendors that understand BSCA authority is available, and that patterns of non-cooperation with banks' reasonable third party risk management requests could attract regulatory attention, have a commercial and reputational incentive to engage constructively with due diligence requirements, audit access requests, and contractual negotiations. This is, in some respects, how the Interagency Guidance itself already functions: banks report that pointing vendors to specific provisions gives them leverage they would not otherwise have. BSCA authority could operate the same way at a higher level — not as a regulatory hammer held over vendors, but as a signal that the federal banking agencies stand behind banks' third party risk management expectations and that market-dominant vendors cannot simply ignore them. Realizing this potential requires little more than deliberate communication: agency leadership making clear, in published guidance or supervisory statements, that BSCA oversight of service providers is a tool the federal banking

agencies are prepared to use when vendor non-cooperation becomes a pattern. The market-signaling value of that posture should not be underestimated, particularly given the concentrated nature of the vendor ecosystem the report describes.

It bears noting that the universe of relevant actors here is not large: there are a handful of hyperscale cloud service providers and a similarly small number of foundation model vendors whose services underpin a significant share of the U.S. banking system's technology stack. The supervisory challenge, while real, is not one of scale.

If the federal banking agencies conclude that existing legal authority is genuinely inadequate to address the risks posed by these concentrated dependencies, the Authors encourage them to say so plainly — and to bring that assessment to Congress, where the case for modernizing the BSCA's scope to reflect the realities of twenty-first century banking infrastructure would seem straightforward to make.

M. Confidential Supervisory Information and information-sharing challenges in modern third party risk management

Roundtable participants noted that existing confidentiality requirements and information-sharing frameworks can create practical challenges in certain risk management contexts, particularly where banks and service providers are attempting to exchange sufficient information to support effective diligence and risk assessment. Participants also observed that these questions may become more complex as banking organizations continue to rely on increasingly interconnected technology ecosystems and concentrated service-provider relationships.

While the Authors do not offer specific recommendations on these issues at this time, participants generally agreed that further dialogue among regulators, banks, and service providers regarding information-sharing frameworks and supervisory coordination could be beneficial as the third party risk management landscape continues to evolve.[20]

[20] Industry commentary has discussed the need for regulators to engage on this issue. See, e.g., AFC and ICBA Letter to Financial Banking Regulators on Confidential Supervisory Information Reform (Jan. 13, 2026), https://fintechcouncil.org/advocacy/afc-and-ibca-letter-on-confidential-supervisory-information-reform; Nat Weber, Ian P. Moloney, and Dan Swislow, Regulators and Fintechs Need to Talk, Open Banker (March 31, 2026) https://openbanker.beehiiv.com/p/needtotalk.

VI. Conclusion

CBA began this project with a straightforward goal: to give the federal banking agencies an honest, member-grounded assessment of how the existing TPRM framework is working in practice, and where it needs to evolve. What emerged from that process — through member conversations, the Roundtable's discussions, subsequent conversations with the other Authors, and the iterative work of translating practitioner experience into policy recommendations — was a document that changed substantially from where it began.

Early drafts focused primarily on the familiar pain points: examiner inconsistency, power imbalances with dominant vendors, and the need for clearer nth-party guidance. Those issues remain central to this report, and the recommendations in Section IV address them directly. But the Roundtable surfaced something more fundamental — a growing recognition among banks, technology providers, and former regulators alike that the existing TPRM framework is operating on assumptions about transparency, validation, and supervisory oversight that the modern vendor ecosystem can no longer support. The shift from ex ante validation to real-time risk management, the circuit breaker paradigm, and the longer-term questions about BSCA authority and CSI sharing were not part of our original outline. They emerged from the conversation.

The Authors recognize that not all of the recommendations in this report will be acted on quickly, and that the longer-term considerations in Section V may take years to fully realize, and in some cases will depend as much on industry and vendor progress as on regulatory action.

We are not under the illusion that a white paper changes policy on its own. But we hope this report gives the federal banking agencies a clear picture of where the current framework is creating friction, a set of actionable near-term recommendations they can act on without statutory change, and a candid articulation of the structural questions that will need to be addressed as the banking system's dependence on a concentrated set of technology providers continues to deepen.

The Interagency Guidance remains a strong foundation. The challenge now is building supervisory expectations on top of that foundation that reflect the world banks are actually operating in — one where perfect information is rarely available, where technology changes faster than guidance can keep pace, and where the most important question is increasingly not whether a bank validated everything before going live, but whether it is prepared to manage risk in real time and limit harm when things go wrong.

The Authors look forward to continuing this conversation with the federal banking agencies, and to working collaboratively toward a third party risk management framework that is honest, durable, and fit for the environment it governs.

Appendix A

The **Consumer Bankers Association** is a member-driven trade association, and the only national financial trade group focused exclusively on retail banking—banking services geared toward consumers and small businesses. As the recognized voice on retail banking issues, CBA provides leadership, education, research, and federal representation for its members. CBA members operate in all 50 states. They include the nation's largest bank holding companies as well as regional and super-community banks. Eighty-five percent of CBA's members are financial institutions holding more than $10 billion in assets.

A standards-based organization, the **American Fintech Council** is the largest and most diverse trade association representing financial technology (fintech) companies and innovative banks. On behalf of over 150 member companies and partners, AFC promotes a transparent, inclusive, and customer-centric financial system by supporting responsible innovation in financial services and encouraging sound public policy. AFC members foster competition in consumer finance and pioneer products to better serve underserved consumer segments and geographies.

The **Coalition for Financial Ecosystem Standards** is an industry-led initiative housed within FS Vector, a financial services regulatory strategy and advisory firm. CFES develops operating standards and risk management frameworks for innovators within the financial services, including fintechs and sponsor banks. CFES also advances policy positions supporting a more modern supervisory and examination framework that reflects the increasingly technology-driven nature of banking infrastructure.

The **Independent Community Bankers of America®** has one mission: to create and promote an environment where community banks flourish. We power the potential of the nation's community banks through effective advocacy, education, and innovation. As local and trusted sources of credit, America's community banks leverage their relationship-based business model and innovative offerings to channel deposits into the neighborhoods they serve, creating jobs, fostering economic prosperity, and fueling their customers' financial goals and dreams.