Third-Party Risk Management, Compliance Standards

Cite
FRB, OCC, FDIC; Final Interagency Guidance on Third-Party Relationships: Risk Management

Recommended Distribution
Risk Management, Corporate Development, Corporate Planning, Policy, Legal, Government Relations

Website
https://www.occ.gov/news-issuances/news-releases/2023/nr-ia-2023-53a.pdf

Impact Assessment

- Standards once covering only vendors are now significantly toughened and applied to all third-party relationships, customers included.
- Dramatically expanding the de facto regulatory perimeter, new indirect risk-management/compliance standards reach beyond all tech vendors to all interconnections, including providers of credit-risk mitigation or liquidity, consultants/advisers, secondary-market participants, fintech partnerships, bigtech platforms, affiliates/subs, and parent companies.
- This will enhance safety and soundness and reduce contagion risk, but also create new obstacles to innovative product offerings, digitalization, and corporate expansion.
- "Rent-a-bank" relationships or banks that ride on tech-platform companies face additional challenges consummating relationships and ensuring ongoing compliance.
- Banks are allowed to collaborate with other banks to gain market strength, negotiating with service providers such as cloud services. However, such cooperation could lead to collusion assertions by third parties or antitrust enforcers.
- Although issued as guidance, violations of new standards could result in enforcement actions not just at banks, but also at nonbanks, some of which may reduce or even eliminate their willingness to do business with certain or even all banks.

Overview

After frequently citing third-party relationships and outsourcing as worrisome risks,[1] the banking agencies have now finalized guidance first

[1] See **SYSTEMIC96**, *Client* Report, May 9, 2023.

proposed in 2021 to govern them.[2] The new standards are what the agencies describe as principles-based guidance on life-cycle management of third-party relationships, but the sum total of the steps banks are to take and the scale of relationships covered at banks of all sizes may result in a significant reduction of reliance on third parties for strategic services and/or "partnerships" akin to those with fintech companies common to smaller national banks. Conversely, nonbanks now at greater legal and reputational risk may reduce their exposure to banks or even cease providing services to some or all regulated companies. At the least, banks will face a significant set of new compliance and legal obligations dealing with nonbanks that will add cost and complexity to these interconnections. Although the final guidance is less prescriptive than the proposal due to clear delineation of many specifics as only illustrative, much in it remains prescriptive and subject to enforcement under other agency rules.

Impact

This guidance replaces each agency's existing vendor risk-management requirements, each of which differs in substance and application. It thus limits regulatory arbitrage as well as raises standards uniformly across the sector addressing not only a wider range of activities than most had previously contemplated, but also covering emerging technologies and activities that might otherwise pose risk to banks, consumers, the financial system, or even the economy.

In the past, the banking agencies principally focused third-party risk-management efforts on vendors of critical technology services.[3] The general thrust of these standards was to address information security in hopes of ensuring that bank and customer information was secure even if processed by a third party. However, in 2020, the OCC issued frequently-asked questions (FAQs) that broadened the agency's reach to alternative-data, cloud services, payment providers, consultants, data aggregators, and any entity with which the bank has a contractual or other service relationship.[4] The final guidance is in many places phrased more broadly than the FAQs, encompassing for example also the consumer-reporting firms now exempt from the reach of indirect bank-regulatory requirements and entities with which a bank has a "relationship" even if not contractual or otherwise subject to direct compensation.

This expanded scope is particularly germane to the Fed's liberalized approach to determining when direct or indirect "control" exists over a third-party, triggering requirements to form a bank holding company. Although the thrust of this rule addresses direct investment, it also captures "business relationships" that could create indirect control. A finding of indirect control could trigger the guidance's risk-management requirements, thus creating strategic challenges as well as enhanced risk mitigation regardless of the extent to which the business relationship is deemed permissible under the Bank Holding Company Act.

Indeed, the guidance would go farther and address not only entities brought within this new, broad definition of third parties, but also entities – affiliates and

2 See *Financial Services Management*, **VENDOR9**, July 21, 2021.

3 See *Client Reports* in the **VENDOR** series.

4 See **VENDOR8**, *Financial Services Management*, March 18, 2020.

parent holding companies – previously considered "second" parties or even the equivalent of an insured depository. The scope of this expansive coverage could be very far-reaching. For example, it covers the parent holding companies of industrial banks or the other entities addressed to some extent in controversial 2020 FDIC standards for non-traditional parent companies,[5] expanding the FDIC's reach through the insured depository to key aspects (e.g., information security, consumer protection) beyond the scope of its prior focus on source-of-strength capacity. Reaching to parent companies and affiliates could also lead to more de facto combined safety-and-soundness standards based on home-country parent companies and the branches and agencies affiliated with insured depositories controlled by foreign banking organizations.[6]

The agencies clearly intend this forceful approach not only because of concerns about some of the risks highlighted in the "rent-a-bank" discussion with relation to fintech partnerships[7] and the CFPB's new approach to third-party risk related to UDAAP,[8] but also FSOC's heightened concern that inter-connections between banks and nonbanks pose systemic risk. [9] Even customer relationships will now need to be undertaken with due diligence and additional risk mitigation akin in some respects to standards the FSOC considered in 2016 for bank/asset-management interconnections.[10]

Although this guidance does not have the express force of rule, it packs a considerable punch and may well lead banks to reconsider third-party relationship concentrations, indirect risk exposures, and the other hazards this guidance requires boards and senior management to address. The many, many specific details in the "life cycle" standards are now clearly described as only "illustrative," not "prescriptive." However, the guidance also makes it clear that failure to adhere to the full scope of all of the principles detailed for monitoring, review, revision, and termination up to and including by the board and senior management could be deemed a violation of other binding safety-and-soundness, resolution, or other prudential regulations.

Importantly, this guidance also expands the scope of the agencies' authority to examine third-party providers, asserting power not only to do so, but also to issue enforcement orders governing bank relationships with any sanctioned third party – a longstanding power albeit rarely used – also to direct enforcement power over the nonbank. Further, this power is asserted now not only with regard to safety and soundness, but also consumer protection. As a result, the banking agencies will become partners with the CFPB in selected cases, going beyond the new enforcement strategy recently announced by the OCC[11] to reach directly to nonbanks otherwise exempt from a range of federal standards.

---

5 See **ILC15**, *Financial Services Management*, December 21, 2020.

6 See *Financial Services Management*, **SIFI34**, October 23, 2019.

7 See *Financial Services Management*, **FINTECH20**, August 3, 2018.

8 See *Financial Services Management*, **FAIRLEND11**, June 1, 2022.

9 See *Financial Services Management*, **SYSTEMIC95**, April 26, 2023.

10 See **ASSETMANAGEMENT2**, *Client Report*, April 18, 2016.

11 See *Financial Services Management*, **SUPERVISION2**, May 30, 2023.

Although the guidance is at pains to assure banks that third-party relationships are not discouraged, banks may nonetheless be forced to be more self-reliant, developing business strategies that do not depend on third parties for customer access and/or critical services. The extent to which banks are in fact able to do so will depend at least in part on whether banks that cannot take advantage – opponents would say arbitrage – third-party offerings can succeed given the costly rules that often led them to turn to third parties in the first place. Indeed, many of these companies only began to offer financial services because banks left key markets, failed to innovate in part because of compliance costs, or otherwise could not effectively compete.

These standards could also bring critical payment and cloud-service infrastructure closer to the regulatory perimeter. This would address a range of concerns from FSOC, [12] Congress, and many banks related to the concentrated number of cloud-service providers increasingly proving a vital form of core financial infrastructure. The same is true of the risks posed by concentrated payment-service providers with direct access to bank transaction accounts or key interfaces with bank payment processing as well as the increasing dependence banks have on tech-platform companies handling payments or other product offerings.

As noted below, the failure of the final guidance to include express tailoring standards beyond those related to risk or provide some form of small-bank exemption led one member of the Federal Reserve Board to oppose finalization. The guidance does make clear that all third-party relationships do not require the same degree of risk management, with the final guidance also providing what the agencies believe to be sufficient flexibility for banks to judge their own risks commensurate with their own size and complexity. The final standards are also said to be simplified and streamlined to assist community banks, with additional guidance on these issues to be provided in the future.

What's Next

The final guidance was released on June 6, the same date it was declared final following approval by the FDIC, OCC, and a 6-1 vote of the Board of Governors of the Federal Reserve System. In her dissent, Gov. Bowman argued that the guidance does not sufficiently differentiate standards for smaller banks or make clear when promised compliance assistance will actually be forthcoming.

These standards are now effective.

Analysis

A. Definitions

"Business arrangements" covered by the guidance need not be material, high-risk, formal via a written agreement, or long-term. The final rule omits the proposal's exclusion for customer relationships, a move to reduce ambiguity

12 See **FSOC28**, *Client Report*, December 19, 2022.

that expands the scope of the guidance if a bank has any arrangements in which a customer also works with the bank (e.g., by providing mortgage servicing as well as receiving warehouse funding).

Covered third-party relationships also need not be material. These are any business arrangements between a banking organization and another entity by contract or otherwise. An exchange of money is not necessary to create such a relationship, including those for:

- outsourced services;
- independent consultants;
- referral arrangements;
- merchant-payment processing services;
- services provided by affiliates and subsidiaries; and
- joint ventures.

"Critical activities" are revised from the proposal to focus on illustrative, risk-based characteristics such as how much risk is presented to the bank in the absence of certain services and risks to customers or the bank's financial condition. Banks are to assess criticality based on their own criteria. Standards governing critical third-party activities for this guidance do not override, compensate for, or otherwise affect standards related to critical services with regard to resolution, operational-risk management, or other purposes.

B. Risk Management Life Cycle

As with the proposal, the final guidance stipulates that appropriate third-party risk management must be conducted over a relationship's life cycle. The guidance contains illustrative examples of aspects of each stage of the life cycle, stipulating that it consists of:

- planning involving relevant governance based on risk tolerance. The guidance lays out steps for effective planning;
- due diligence and third-party selection, with higher standards applied for critical services. Where asymmetric market power or other factors impede due diligence, banks are to document these limits, understand the risks they present, and determine how best to mitigate them. Industry consortia are one way to meet this information gap although antitrust restrictions would still apply. Even when consortia or other methods are used to supplement due diligence, the bank must conduct its own risk assessment and consider the third-party providing assistance as a third party otherwise subject to this guidance. Appropriate due-diligence criteria are also detailed;
- financial condition determined by review of relevant documents and other detailed methods;
- business experience judged by staffing, prior experience, litigation, and other factors;

- human capital based on an array of relevant factors that include a party's corporate culture;
- risk management based on the third party's policies, procedures, governance, and results;
- information security;
- information-system management;
- operational resilience, with particular attention given to relationships where a third-party contacts customers;
- incident reporting and management;
- physical security;
- insurance coverage;
- the need for a written contract and subsequent terms and conditions;
- contractual arrangements with other parties that may add legal or other risks;
- performance review and management;
- the need for contracts, with the guidance laying out key terms and conditions such as how ongoing performance management is to be ensured and conducted. Regardless of a contract, banks are responsible for ensuring that activities conducted on their behalf comply with all the law and rule applicable to the bank. Indemnification should also be considered and secured where desired. Dispute-resolution protocols are also to be assured with particular attention to deals with foreign-domiciled third parties or U.S. entities that rely on key services that are domiciled offshore (e.g., servicing);
- ongoing monitoring, with the guidance here detailing ways to do so and what to watch along with continuing documentation and reporting;
- proper oversight and accountability, with the bank's board participating in this where appropriate based on risk tolerance and strategic objectives. Management responsibilities are also detailed; and
- independent reviews of the overall risk-management process.

C. Request for Comment

The guidance also details how supervisors are to assess performance with all the factors outlined above, reiterating that the agencies may also examine third-party providers. The guidance also asserts that the agencies can address failings via enforcement actions or other penalties not only on the bank, but also third parties.