FEDERAL RESERVE SYSTEM
[Docket No. OP-1752]

FEDERAL DEPOSIT INSURANCE CORPORATION
RIN 3064-ZA26

DEPARTMENT OF THE TREASURY
Office of the Comptroller of the Currency
[Docket ID OCC-2021-0011]

Proposed Interagency Guidance on Third-Party Relationships: Risk Management

AGENCY: The Board of Governors of the Federal Reserve System (Board), the Federal Deposit Insurance Corporation (FDIC), and the Office of the Comptroller of the Currency (OCC).

ACTION: Proposed interagency guidance and request for comment.

SUMMARY: The Board, FDIC, and OCC (together, the agencies) invite comment on proposed guidance on managing risks associated with third-party relationships. The proposed guidance would offer a framework based on sound risk management principles for banking organizations to consider in developing risk management practices for all stages in the life cycle of third-party relationships that takes into account the level of risk, complexity, and size of the banking organization and the nature of the third-party relationship. The proposed guidance sets forth considerations with respect to the management of risks arising from third-party relationships. The proposed guidance would replace each agency's existing guidance on this topic and would be directed to all banking organizations supervised by the agencies.

DATES: Comments must be received no later than [INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: Interested parties are encouraged to submit written comments to any or all agencies listed below. The agencies will share comments with each other.

Comments should be directed to:

Board: When submitting comments, please consider submitting your comments by e-mail or fax because paper mail in the Washington, DC area and at the Board may be subject to delay. You may submit comments, identified by Docket No. OP-1752, by any of the following methods:

- **Agency Website**: http://www.federalreserve.gov. Follow the instructions for submitting comments at http://www.federalreserve.gov/generalinfo/foia/RevisedRegs.cfm.
- **E-mail**: *regs.comments@federalreserve.gov*. Include docket number in the subject line of the message.
- **FAX**: (202) 452-3819 or (202) 452-3102.
- **Mail**: Ann E. Misback, Secretary, Board of Governors of the Federal Reserve System, 20th Street and Constitution Avenue, NW, Washington, DC 20551.

All public comments will be made available on the Board's website at:

http://www.federalreserve.gov/generalinfo/foia/RevisedRegs.cfm as submitted, unless modified for technical reasons or to remove personally identifiable information at the commenter's request. Accordingly, comments will not be edited to remove any identifying or contact information. Public comments also may be viewed electronically or in paper in Room 146, 1709 New York Avenue, NW, Washington, DC 20006, between 9:00 a.m. and 5:00 p.m. on weekdays.

FDIC: You may submit comments, identified by FDIC RIN 3064-ZA026, by any of the following methods:

- **Agency Website**: *https://www.fdic.gov/resources/regulations/federal-register-publications/*. Follow instructions for submitting comments on the agency website.

- **Mail**: James P. Sheesley, Assistant Executive Secretary, Attention: Comments-RIN 3064-ZA26, Legal ESS, Federal Deposit Insurance Corporation, 550 17th Street NW, Washington, DC 20429.

- **Hand Delivery/Courier**: Comments may be hand-delivered to the guard station at the rear of the 550 17th Street NW building (located on F Street) on business days between 7:00 a.m. and 5:00 p.m.

- **Email**: *comments@FDIC.gov*. Comments submitted must include "FDIC RIN 3064-ZA26" on the subject line of the message.

- **Federal eRulemaking Portal**: *http://www.regulations.gov*. Follow the instructions for submitting comments.

- **Public Inspection**: All comments received will be posted without change to *https://www.fdic.gov/resources/regulations/federal-register-publications/*, including any personal information provided.

***OCC*:**

Commenters are encouraged to submit comments through the Federal eRulemaking Portal. Please use the title "Proposed Interagency Guidance on Third-Party Relationships: Risk Management" to facilitate the organization and distribution of the comments. You may submit comments by any of the following methods:

- *Federal eRulemaking Portal – Regulations.gov:*

Go to *https://regulations.gov/*. Enter "Docket ID OCC-2021-0011" in the Search Box and click "Search." Public comments can be submitted via the "Comment" box below the displayed document information or by clicking on the document title and then clicking the "Comment" box on the top-left side of the screen. For help with submitting effective comments please click on "Commenter's Checklist." For assistance with the *Regulations.gov* site, please call (877) 378-5457 (toll free) or (703) 454-9859 Monday-Friday, 9am-5pm ET or e-mail *regulations@erulemakinghelpdesk.com*.

- *Mail:* Chief Counsel's Office, Attention: Comment Processing, Office of the Comptroller of the Currency, 400 7th Street, SW., suite 3E-218, Washington, DC 20219.
- *Hand Delivery/Courier:* 400 7th Street, SW., suite 3E-218, Washington, DC 20219.

Instructions: You must include "OCC" as the agency name and "Docket ID OCC-2021-0011" in your comment. In general, the OCC will enter all comments received into the docket and publish the comments on the *Regulations.gov* website without change, including any business or personal information provided such as name and address information, e-mail addresses, or phone numbers. Comments received, including attachments and other supporting materials, are part of the public record and subject to public disclosure. Do not include any information in your comment or supporting materials that you consider confidential or inappropriate for public disclosure.

You may review comments and other related materials that pertain to this action by the following method:

- *Viewing Comments Electronically – Regulations.gov:* Go to *https://regulations.gov/*. Enter "Docket ID OCC-2021-0011" in the Search Box and click

"Search." Click on the "Documents" tab and then the document's title. After clicking the document's title, click the "Browse Comments" tab. Comments can be viewed and filtered by clicking on the "Sort By" drop-down on the right side of the screen or the "Refine Results" options on the left side of the screen. Supporting materials can be viewed by clicking on the "Documents" tab and filtered by clicking on the "Sort By" drop-down on the right side of the screen or the "Refine Documents Results" options on the left side of the screen." For assistance with the *Regulations.gov* site, please call (877) 378-5457 (toll free) or (703) 454-9859 Monday-Friday, 9am-5pm ET or e-mail *regulations@erulemakinghelpdesk.com*.

The docket may be viewed after the close of the comment period in the same manner as during the comment period.

FOR FURTHER INFORMATION CONTACT:

Board: Nida Davis, Associate Director, (202) 872-4981; Timothy Geishecker, Lead Financial Institution and Policy Analyst, (202) 475-6353, Division of Supervision and Regulation; Jeremy Hochberg, Managing Counsel, (202) 452-6496; Matthew Dukes, Counsel, (202) 973-5096, Division of Consumer and Community Affairs; Claudia Von Pervieux, Senior Counsel, (202) 452-2552; Evans Muzere, Counsel, (202) 452-2621; Alyssa O'Connor, Senior Attorney, (202) 452-3886, Legal Division, Board of Governors of the Federal Reserve System, 20th and C Streets NW, Washington, DC 20551. For users of Telecommunications Device for the Deaf (TDD) (202) 263-4869.

FDIC: Thomas F. Lyons, Corporate Expert in Examination Policy, TLyons@fdic.gov, (202) 898-6850); Judy E. Gross, Senior Policy Analyst, JuGross@fdic.gov, (202) 898-7047, Policy & Program Development, Division of Risk Management Supervision; Paul Robin, Chief,

probin@fdic.gov, (202) 898-6818, Supervisory Policy Section, Division of Depositor and Consumer Protection; Marguerite Sagatelian, Senior Special Counsel, msagatelian@fdic.gov, (202) 898-6690, Supervision, Legislation & Enforcement Branch, Legal Division, Federal Deposit Insurance Corporation; 550 17th Street NW, Washington, DC 20429.

OCC: Kevin Greenfield, Deputy Comptroller for Operational Risk Division, Lazaro Barreiro, Director for Governance and Operational Risk Policy, Emily Doran, Governance and Operational Risk Policy Analyst, Stuart Hoffman, Governance and Operational Risk Policy Analyst, Operational Risk Policy Division, (202) 649-6550; or Tad Thompson, Counsel or Eden Gray, Assistant Director, Chief Counsel's Office, (202) 649-5490, Office of the Comptroller of the Currency, 400 7th Street SW, Washington, DC 20219.

SUPPLEMENTARY INFORMATION:

Table of Contents

I. Introduction

Banking organizations routinely rely on third parties for a range of products, services, and activities (herein activities). These may include core bank processing, information technology services, accounting, compliance, human resources, and loan servicing. A banking organization may also establish third-party relationships to offer products and services to improve customers' access to and the functionality of banking services, such as mobile payments, credit-scoring systems, and customer point-of-sale payments.

In other instances, a banking organization may make its banking services available to customers through the third party's platform. Competition, advances in technology, and innovation in the banking industry contribute to banking organizations' increasing use of third parties to perform business functions, deliver support services, facilitate providing new products and services, or facilitate providing existing products and services in new ways.

The use of third parties can offer banking organizations significant advantages, such as quicker and more efficient access to new technologies, human capital, delivery channels, products, services, and markets. To address these developments, many banking organizations,

including smaller and less complex banking organizations, have adopted risk management practices commensurate with the level of risk and complexity of their third-party relationships. Whether a banking organization conducts activities directly or through a third party, the banking organization must conduct the activities in a safe and sound manner and consistent with applicable laws and regulations, including those designed to protect consumers.

The use of third parties by banking organizations does not remove the need for sound risk management. On the contrary, the use of third parties may present elevated risks to banking organizations and their customers. Banking organizations' expanded use of third parties, especially those with new or innovative technologies, may also add complexity, including in managing consumer compliance risks, and otherwise heighten risk management considerations. A prudent banking organization appropriately manages its third-party relationships, including addressing consumer protection, information security, and other operational risks. The proposed supervisory guidance[1] is intended to assist banking organizations in identifying and addressing these risks and in complying with applicable statutes and regulations.[2]

The Board, FDIC, and OCC each have issued guidance for their respective supervised banking organizations addressing third-party relationships and appropriate risk management practices: the Board's 2013 guidance,[3] the FDIC's 2008 guidance,[4] and the OCC's 2013

---

[1] Supervisory guidance outlines the agencies' supervisory practices or priorities and articulates the agencies' general views regarding appropriate practices for a given subject area. The agencies have each adopted regulations setting forth Statements Clarifying the Role of Supervisory Guidance as guidance. *See* 12 CFR part 4, Appendix A to Subpart F (OCC); 12 CFR part 262, Appendix A (Board); 12 CFR part 302, Appendix A (FDIC).

[2] These include the Interagency Guidelines Establishing Standards for Safety and Soundness, and the Interagency Guidelines Establishing Information Security Standards, which were adopted pursuant to the procedures of section 39 of the Federal Deposit Insurance Act and section 505 of the Graham Leach Bliley Act, respectively.

[3] SR Letter 13-19 / CA Letter 13-21, "Guidance on Managing Outsourcing Risk" (December 5, 2013, updated February 26, 2021).

[4] FIL-44-2008, "Guidance for Managing Third-Party Risk" (June 6, 2008).

guidance and its 2020 FAQs.[5] The agencies seek to promote consistency in their third-party risk management guidance and to clearly articulate risk-based principles on third-party risk management. Accordingly, the agencies are jointly seeking comment on the proposed guidance.

The proposed guidance is based on the OCC's existing third-party risk management guidance from 2013 and includes changes to reflect the extension of the scope of applicability to banking organizations supervised by all three federal banking agencies. The agencies are including the OCC's 2020 FAQs, released in March 2020, as an exhibit, separate from the proposed guidance. The OCC issued the 2020 FAQs to clarify the OCC's 2013 third-party risk management guidance and discuss evolving industry topics. The agencies seek public comment on the extent to which the concepts discussed in the OCC's 2020 FAQs should be incorporated into the final version of the guidance. More specifically, the agencies seek public comment on whether: (1) any of those concepts should be incorporated into the final guidance; and (2) there are additional concepts that would be helpful to include.

II. Overview of Proposed Guidance on Third-Party Relationships

The proposed guidance provides a framework based on sound risk management principles that banking organizations may use to address the risks associated with third-party relationships. The proposed guidance describes third-party relationships as business arrangements between a banking organization and another entity, by contract or otherwise. The proposed guidance stresses the importance of a banking organization appropriately managing and evaluating the risks associated with each third-party relationship. The proposed guidance

[5] OCC Bulletin 2013-29, "Third-Party Relationships: Risk Management Guidance" and OCC Bulletin 2020-10, "Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29" The OCC also issued foreign-based third-party guidance, OCC Bulletin 2002-16, "Bank Use of Foreign-Based Third-Party Service Providers: Risk Management Guidance," which supplements this proposed guidance.

states that a banking organization's use of third parties does not diminish its responsibility to perform an activity in a safe and sound manner and in compliance with applicable laws and regulations. The proposed guidance indicates that banking organizations should adopt third-party risk management processes that are commensurate with the identified level of risk and complexity from the third-party relationships, and with the organizational structure of each banking organization. The proposed guidance is intended for all third-party relationships and is especially important for relationships that a banking organization relies on to a significant extent, relationships that entail greater risk and complexity, and relationships that involve critical activities as described in the proposed guidance.

The proposed guidance describes the third-party risk management life cycle and identifies principles applicable to each stage of the life cycle, including: (1) developing a plan that outlines the banking organization's strategy, identifies the inherent risks of the activity with the third party, and details how the banking organization will identify, assess, select, and oversee the third party; (2) performing proper due diligence in selecting a third party; (3) negotiating written contracts that articulate the rights and responsibilities of all parties; (4) having the board of directors and management oversee the banking organization's risk management processes, maintaining documentation and reporting for oversight accountability, and engaging in independent reviews; (5) conducting ongoing monitoring of the third party's activities and performance; and (6) developing contingency plans for terminating the relationship in an effective manner.

III. Request for Comment

The agencies invite comment on all aspects of the proposed guidance and the OCC's 2020 FAQs, including responses to the following questions.

A. General

1. *To what extent does the guidance provide sufficient utility, relevance, comprehensiveness, and clarity for banking organizations with different risk profiles and organizational structures? In what areas should the level of detail be increased or reduced? In particular, to what extent is the level of detail in the guidance's examples helpful for banking organizations as they design and evaluate their third-party risk-management practices?*

2. *What other aspects of third-party relationships, if any, should the guidance consider?*

B. Scope

As noted above, a third-party relationship is "any business arrangement between a banking organization and another entity, by contract or otherwise." The term "business arrangement" is meant to be interpreted broadly to enable banking organizations to identify all third-party relationships for which the proposed guidance is relevant. Neither a written contract nor a monetary exchange is necessary to establish a business arrangement. While determinations of business arrangements may vary depending on the facts and circumstances, third-party business arrangements generally exclude a banking organization's customers. The proposed guidance provides examples of third-party relationships, including use of independent consultants, networking arrangements, merchant payment processing services, services provided by affiliates and subsidiaries, joint ventures, and other business arrangements in which a banking organization has an ongoing relationship or may have responsibility for the associated records. The proposed guidance also describes additional risk management considerations when a banking organization entertains the use of foreign-based third parties.

3. *In what ways, if any, could the proposed description of third-party relationships be clearer?*
4. *To what extent does the discussion of "business arrangement" in the proposed guidance provide sufficient clarity to permit banking organizations to identify those arrangements for which the guidance is appropriate? What change or additional clarification, if any, would be helpful?*
5. *What changes or additional clarification, if any, would be helpful regarding the risks associated with engaging with foreign-based third parties?*

C. Tailored Approach to Third-Party Risk Management

This guidance offers a framework based on sound risk management principles that banking organizations may use in developing practices appropriate for all stages in the risk management life cycle of a third-party relationship based on the level of risk, complexity, and size of the banking organization and the nature of the third-party relationship. Some smaller and less complex banking organizations have expressed concern that they are expected to institute third-party risk management practices that they perceive to be more appropriate for larger and more complex banking organizations. The proposed guidance is intended to provide principles that are useful for a banking organization of any size or complexity and uses the concept of critical activities to help banking organizations scale the nature of their risk management activities. Banking organizations, including smaller and less complex banking organizations, should adopt risk management practices commensurate with the level of risk and complexity of their third-party relationships and the risk and complexity of the banking organization's operations.

6. *How could the proposed guidance better help a banking organization appropriately scale its third-party risk management practices?*
7. *In what ways, if any, could the proposed guidance be revised to better address challenges a banking organization may face in negotiating some third-party contracts?*
8. *In what ways could the proposed description of critical activities be clarified or improved?*

D. Third-Party Relationships

Banking organizations are engaging in different types of relationships[6] with third parties, including technology companies, to serve a range of purposes. Some banking organizations have business arrangements with third parties to offer competitive and innovative financial products and services that otherwise would be difficult, cost-prohibitive, or time-consuming to develop in-house. Other banking organizations have relationships with third parties to enhance their operational and compliance infrastructure, including for areas such as fraud detection, anti-money laundering, and customer service. The agencies recognize the prevalence of the range of relationships between banking organizations and third parties.

9. *What additional information, if any, could the proposed guidance provide for banking organizations to consider when managing risks related to different types of business arrangements with third parties?*
10. *What revisions to the proposed guidance, if any, would better assist banking organizations in assessing third-party risk as technologies evolve?*

[6] These relationships could include partnerships, joint ventures, or other types of formal legal structures or informal arrangements.

Third parties and banking organizations enter into a wide variety of business arrangements, including ones in which the banking organizations make parts of their information systems available to a third party that will directly engage with the end customer. These business arrangements may involve unique or additional risks relative to traditional third-party business arrangements.

11. *What additional information, if any, could the proposed guidance provide to banking organizations in managing the risk associated with third-party platforms that directly engage with end customers?*
12. *What risk management practices do banking organizations find most effective in managing business arrangements in which a third party engages in activities for which there are regulatory compliance requirements? How could the guidance further assist banking organizations in appropriately managing the compliance risks of these business arrangements?*

E. Due Diligence and Collaborative Arrangements

The proposed guidance notes that banking organizations may collaborate when they use the same third party, which can improve risk management and lower the costs among such banking organizations. For example, banking organizations may be able to collaborate when performing due diligence, negotiating contracts, and performing ongoing monitoring.[7] Collaboration may facilitate banking organizations' due diligence of particular third-party relationships by sharing expertise and resources. Third-party assessment service companies have

[7] Any collaborative activities among banks must comply with antitrust laws. Refer to the Federal Trade Commission and U.S. Department of Justice's "Antitrust Guidelines for Collaborations Among Competitors," https://www.ftc.gov/sites/default/files/documents/public_events/joint-venture-hearings-antitrust-guidelines-collaboration-among-competitors/ftcdojguidelines-2.pdf (April 2000).

been formed to help banking organizations with third-party risk management, including due diligence. Collaboration can also result in increased negotiating power and lower costs to banking organizations not only during contract negotiations but also for ongoing monitoring. Each banking organization, however, is ultimately accountable for managing the risks of its own third-party business arrangements.

13. *In what ways, if any, could the discussion of shared due diligence in the proposed guidance provide better clarity to banking organizations regarding third-party due diligence activities?*
14. *In what ways, if any, could the proposed guidance further address due diligence options, including those that may be more cost effective? In what ways, if any, could the proposed guidance provide better clarity to banking organizations conducting due diligence, including working with utilities, consortiums, or standard-setting organizations?*

F. Subcontractors

Third-party business arrangements may involve subcontracting arrangements, which can create a chain of service providers for a banking organization. The absence of a direct relationship with a subcontractor can affect the banking organization's ability to assess and control risks inherent in parts of the supply chain. In addition, the risks inherent in such a chain may be heightened when a banking organization uses third parties for critical activities.

The proposed guidance addresses due diligence and contract negotiations in dealing with a third party's subcontractors. Several sections of the proposed guidance, such as the sections titled "Management of Information Systems," "Reliance on Subcontractors," and "Conflicting Contractual Arrangements with Other Parties," detail possible procedures for handling subcontractors as part of due diligence and ongoing monitoring. Similarly, several sections of

the proposed guidance provide information on possible procedures for addressing the treatment of subcontractors in contract negotiation, including the sections on "Responsibilities for Providing, Receiving, and Retaining Information," "Confidentiality and Integrity," and "Subcontracting."

15. *How could the proposed guidance be enhanced to provide more clarity on conducting due diligence for subcontractor relationships? To what extent would changing the terms used in explaining matters involving subcontractors (for example, fourth parties) enhance the understandability and effectiveness of this proposed guidance? What other practices or principles regarding subcontractors should be addressed in the proposed guidance?*
16. *What factors should a banking organization consider in determining the types of subcontracting it is comfortable accepting in a third-party relationship? What additional factors are relevant when the relationship involves a critical activity?*

G. Information Security

The proposed guidance provides that a banking organization should, commensurate with its risk profile and consistent with safety and soundness principles and applicable laws and regulations, assess the information security program of third parties, including identifying, assessing, and mitigating known and emerging threats and vulnerabilities. Banking organizations with limited resources for security often depend on support from third parties or on security tools provided by third parties to assess information security risks.

17. *What additional information should the proposed guidance provide regarding a banking organization's assessment of a third party's information security and regarding information security risks involved with engaging a third party?*

H. OCC's 2020 FAQs

The agencies are seeking comment on the extent to which the concepts included in the OCC's 2020 FAQs should be incorporated into the final version of the guidance.

18. To what extent should the concepts discussed in the OCC's 2020 FAQs be incorporated into the guidance? What would be the best way to incorporate the concepts?

Paperwork Reduction Act

The Paperwork Reduction Act of 1995 (44 U.S.C. 3501-3521) (PRA) states that no agency may conduct or sponsor, nor is the respondent required to respond to, an information collection unless it displays a currently valid Office of Management and Budget (OMB) control number.

The proposed guidance does not revise any existing, or create any new, information collections pursuant to the PRA. Rather, any reporting, recordkeeping, or disclosure activities mentioned in the proposed guidance are usual and customary and should occur in the normal course of business as defined in the PRA.[8] Consequently, no submissions will be made to the OMB for review. The agencies request comment on the conclusion that the proposed guidance does not create a new or revise and existing information collections.

IV. Text of Proposed Guidance on Third-Party Relationships

A. SUMMARY

This guidance offers a framework based on sound risk management principles that banking organizations supervised by the Board of Governors of the Federal Reserve System (Board), the Federal Deposit Insurance Corporation (FDIC), and the Office of the Comptroller of the

[8] 5 CFR 1320.3(b)(2).

Currency (OCC) (together, the agencies)[9] may use when assessing and managing risks associated with third-party relationships. A third-party relationship is any business arrangement between a banking organization and another entity, by contract or otherwise.[10] A third-party relationship may exist despite a lack of a contract or remuneration. Third-party relationships can include relationships with entities such as vendors, financial technology (fintech) companies, affiliates, and the banking organization's holding company. While a determination of whether a banking organization's relationship constitutes a business arrangement may vary depending on the facts and circumstances, third-party business arrangements generally exclude a bank's customer relationships.

Use of third parties can reduce management's direct control of activities and may introduce new risks or increase existing risks, such as operational, compliance, reputation, strategic, and credit risks and the interrelationship of these risks. Increased risk often arises from greater complexity, ineffective risk management by a banking organization, and inferior performance by the third party.

Banking organizations should have effective risk management practices whether the banking organization performs an activity in-house or through a third party. A banking organization's use of third parties does not diminish the respective responsibilities of its board of directors to

[9] See the definition of "appropriate Federal banking agency" in section 3(q) of the Federal Deposit Insurance Act for a list of banking organizations supervised by each agency. 12 U.S.C. 1813(q).

[10] Third-party relationships include activities that involve outsourced products and services, use of independent consultants, networking arrangements, merchant payment processing services, services provided by affiliates and subsidiaries, joint ventures, and other business arrangements where a banking organization has an ongoing relationship or may have responsibility for the associated records. Affiliate relationships are also subject to sections 23A and 23B of the Federal Reserve Act (12 U.S.C. 371c and 12 U.S.C. 371c-1)) as implemented in Regulation W (12 CFR Part 223).

provide oversight of senior management to perform the activity in a safe and sound manner and in compliance with applicable laws and regulations, including those related to consumer protection.[11]

B. BACKGROUND

The agencies seek to promote consistent third-party risk management guidance, better address use of, and services provided by, third parties, and more clearly articulate risk-based principles on third-party relationship risk management. The use of third parties can offer banking organizations significant advantages, such as quicker and more efficient access to new technologies, human capital, delivery channels, products, services, and markets. As the banking industry becomes more complex and technologically driven, banking organizations are forming more numerous and more complex relationships with other entities to remain competitive, expand operations, and help meet customer needs. A banking organization can be exposed to substantial financial loss if it fails to manage appropriately the risks associated with third-party relationships. Additionally, a banking organization may be exposed to concentration risk if it is overly reliant on a particular third-party service provider.

Whether activities are performed internally or outsourced to a third party, a banking organization is responsible for ensuring that activities are performed in a safe and sound manner and in compliance with applicable laws and regulations. It is therefore important for a banking

[11] This guidance is relevant for all third-party relationships, including situations in which a supervised banking organization provides services to another supervised banking organization.

organization to identify, assess, monitor, and control the risks associated with the use of third parties and the criticality of services being provided.

C. RISK MANAGEMENT

A banking organization's third-party risk management program should be commensurate with its size, complexity, and risk profile as well as with the level of risk and number of the banking organization's third-party relationships.[12] Not all relationships present the same level of risk to a banking organization. As part of sound risk management, banking organizations engage in more comprehensive and rigorous oversight and management of third-party relationships that support "critical activities." "Critical activities" are significant bank functions[13] or other activities that:

- could cause a banking organization to face significant risk if the third party fails to meet expectations;
- could have significant customer impacts;
- require significant investment in resources to implement the third-party relationship and manage the risk; or
- could have a major impact on bank operations if the banking organization has to find an alternate third party or if the outsourced activity has to be brought in-house.

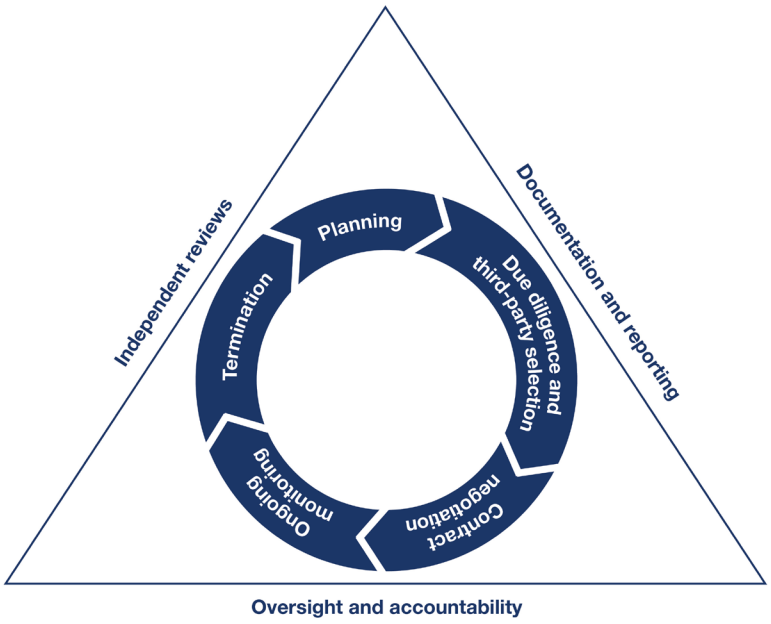
Third-Party Relationship Life Cycle

[12] These relationships could include partnerships, joint ventures, or other types of formal legal structures or informal arrangements.

[13] Significant bank functions include any business line of a banking organization, including associated operations, services, functions, and support, that upon failure would result in a material loss of revenue, profit, or franchise value.

Effective third-party risk management generally follows a continuous life cycle for all relationships and incorporates the following principles applicable to all stages of the life cycle:

Figure 1: Stages of the Risk Management Life Cycle



Source: Board, FDIC, and OCC

1. Planning

Before entering into a third-party relationship, banking organizations evaluate the types and nature of risks in the relationship and develop a plan to manage the relationship and its related risks. Certain third parties, particularly those providing critical services, typically warrant significantly greater planning and consideration. For example, when critical activities are involved, such plans may be presented to and approved by a banking organization's board of directors (or a designated board committee).

A banking organization typically considers the following factors, among others, in planning for a third-party relationship:

- Identifying and assessing the risks associated with the business arrangement and commensurate steps for appropriate risk management;
- Understanding the strategic purpose of the business arrangement and how the arrangement aligns with a banking organization's overall strategic goals, objectives, risk appetite, and broader corporate policies;
- Considering the complexity of the business arrangement, such as the volume of activity, potential for subcontractor(s), the technology needed, and the likely degree of foreign-based third-party activities;
- Evaluating whether the potential financial benefits outweigh the estimated costs (including estimated direct contractual costs as well as indirect costs to augment or alter banking organization processes, systems, or staffing to properly manage the third-party relationship or to adjust or terminate other existing contracts);
- Considering how the third-party relationship could affect other strategic banking organization initiatives, such as large technology projects, organizational changes, mergers, acquisitions, or divestitures;
- Evaluating how the third-party relationship could affect banking organization employees, including dual employees,[14] and what transition steps are needed for the banking

[14] Dual employees are employed by both the banking organization and the third party.

organization to manage the impacts when the activities currently conducted internally are outsourced;

- Assessing the nature of customer interaction with the third party and potential impact on the banking organization's customers—including access to or use of those customers' confidential information, joint marketing or franchising arrangements, and handling of customer complaints—and identifying possible steps needed to manage these impacts;
- Understanding potential information security implications including access to the banking organization's systems and to its confidential information;
- Describing how the banking organization will select, assess, and oversee the third party, including monitoring the third party's compliance with contractual provisions;
- Determining the banking organization's ability to provide adequate oversight and management of the proposed third-party relationship on an ongoing basis (including whether staffing levels and expertise, risk management and compliance management systems, organizational structure, policies and procedures, or internal control systems need to be adapted for the banking organization to effectively address the business arrangement); and
- Outlining the banking organization's contingency plans in the event the banking organization needs to transition the activity to another third party or bring it in-house.

As with all other phases of the third-party risk management life cycle, it is important for planning and assessment to be performed by those with the requisite knowledge and skills. A banking organization may involve experts across disciplines, such as compliance, risk, or

technology officers, legal counsel, and external support where helpful to supplement the qualifications and technical expertise of in-house staff.

2. Due Diligence and Third-Party Selection

Conducting due diligence on third parties before selecting and entering into contracts or relationships is an important risk management activity. Relying solely on experience with or prior knowledge of a third party is not an adequate proxy for performing appropriate due diligence.

The degree of due diligence should be commensurate with the level of risk and complexity of each third-party relationship. Due diligence will include assessing a third party's ability to perform the activity as expected, adhere to a banking organization's policies, comply with all applicable laws, regulations, and requirements, and operate in a safe and sound manner.

The due diligence process also provides management with the information needed to determine whether a relationship mitigates identified risks or poses additional risk. More extensive due diligence is particularly important when a third-party relationship is higher risk or where it involves critical activities. For some relationships, on-site visits may be useful to understand fully the third party's operations and capacity. If a banking organization uncovers information that warrants additional scrutiny, the banking organization should consider broadening the scope or assessment methods of the due diligence as needed. In some instances, a banking organization may not be able to obtain the desired due diligence information from the third party.

For example, the third party may not have a long operational history or demonstrated financial performance. In such situations, it is important to identify limitations, understand the risks, consider how to mitigate the risks, and determine whether the residual risks are acceptable.

In order to facilitate or supplement a banking organization's due diligence, a banking organization may use the services of industry utilities or consortiums, including development organizations, consult with other banking organizations,[15] or engage in joint efforts for performing due diligence to meet its established assessment criteria. Effective risk management processes include assessing the risks of outsourcing due diligence when relying on the services of other banking organizations, utilities, consortiums, or other similar arrangements and assessment standards. Use of such external services does not abrogate the responsibility of the board of directors to decide on matters related to third-party relationships involving critical activities or the responsibility of management to handle third-party relationships in a safe and sound manner and consistent with applicable laws and regulations.

A banking organization typically considers the following factors, among others, during due diligence of a third party:

a. Strategies and Goals

Review the third party's overall business strategy and goals to consider how the third party's current and proposed strategic business arrangements (such as mergers, acquisitions, divestitures,

[15] Any collaborative activities among banks must comply with antitrust laws. Refer to the Federal Trade Commission and U.S. Department of Justice's "Antitrust Guidelines for Collaborations Among Competitors," https://www.ftc.gov/sites/default/files/documents/public_events/joint-venture-hearings-antitrust-guidelines-collaboration-among-competitors/ftcdojguidelines-2.pdf (April 2000).

partnerships, joint ventures, or joint marketing initiatives) may affect the activity. Also consider reviewing the third party's service philosophies, quality initiatives, efficiency improvements, and employment policies and practices. Consider whether the selection of a third party is consistent with a banking organization's broader corporate policies and practices, including its diversity policies and practices.

b. Legal and Regulatory Compliance

Evaluate the third party's ownership structure (including any beneficial ownership, whether public or private, foreign or domestic ownership) and its legal and regulatory compliance capabilities. Determine whether the third party has the necessary licenses to operate and the expertise, processes, and controls to enable the banking organization to remain compliant with domestic and international laws and regulations.[16] Consider the third party's response to existing or recent regulatory compliance issues and its compliance status with applicable supervisory agencies and self-regulatory organizations, as appropriate. Consider whether the third party has identified, and articulated a process to mitigate, areas of potential consumer harm, particularly in which the third party will have direct contact with the bank's customers, develop customer-facing documents, or provide new, complex, or unique products.

c. Financial Condition

Assess the third party's financial condition, including reviews of the third party's audited financial statements, annual reports, filings with the U.S. Securities and Exchange Commission

[16] To the extent the activities performed by the third party are subject to specific laws and regulations (e.g., privacy, information security, Bank Secrecy Act/anti-money laundering (BSA/AML), or fiduciary requirements).

(SEC), and other available financial information. Alternative information may be beneficial for conducting an assessment, including when third parties have limited financial information. For example, the banking organization may consider expected growth, earnings, pending litigation, unfunded liabilities, or other factors that may affect the third party's overall financial stability. Depending on the significance of the third-party relationship or whether the banking organization has a financial exposure to the third party, the banking organization's analysis may be as comprehensive as if it were extending credit to the third party.

d. Business Experience

Evaluate the third party's depth of resources and any previous experience in meeting the banking organization's expectations. Assess the third party's degree of and its history of managing customer complaints or litigation. Determine how long the third party has been in business and whether there have been significant changes in the activities offered or in its business model. Check the third party's SEC or other regulatory filings. Review the third party's websites and other marketing materials related to the banking products or services to ensure that statements and assertions align with the banking organization's expectations and accurately represent the activities and capabilities of the third party. Determine whether and how the third party plans to use the banking organization's name in marketing efforts.

e. Fee Structure and Incentives

Evaluate the third party's fee structure and incentives to determine if the fee structure and incentives would create burdensome upfront or termination fees or result in inappropriate risk

taking by the third party or the banking organization. Consider whether any fees or incentives are subject to, and comply with, applicable law.

f. Qualifications and Backgrounds of Company Principals

Evaluate the qualifications and experience of the company's principals related to the services provided by the third party. Consider whether a third party periodically conducts thorough background checks on its senior management and employees, as well as on subcontractors, who may have access to critical systems or confidential information. Confirm that third parties have policies and procedures in place for identifying and removing employees who do not meet minimum background check requirements or are otherwise barred from working in the financial services sector.

g. Risk Management

Evaluate the effectiveness of the third party's own risk management, including policies, processes, and internal controls. Consider whether the third party's risk management processes align with applicable banking organization policies and expectations surrounding the activity. Assess the third party's change management processes, including to ensure that clear roles, responsibilities, and segregation of duties are in place. Where applicable, determine whether the third party's internal audit function independently and effectively tests and reports on the third party's internal controls. Evaluate processes for escalating, remediating, and holding management accountable for concerns identified during audits or other independent tests. If available, consider reviewing System and Organization Control (SOC) reports and whether these reports contain sufficient information to assess the third party's risk or whether additional

scrutiny is required through an assessment or audit by the banking organization or other third party at the banking organization's request. For example, consider whether or not SOC reports from the third party include within their coverage the internal controls and operations of subcontractors of the third party that support the delivery of services to the banking organization. Consider any conformity assessment or certification by independent third parties related to relevant domestic or international standards (for example, those of the National Institute of Standards and Technology (NIST), Accredited Standards Committee X9, Inc. (X9), and the International Standards Organization (ISO)).[17]

h. Information Security

Assess the third party's information security program. Consider the consistency of the third party's information security program with the banking organization's program, and whether there are gaps that present risk to the banking organization. Determine whether the third party has sufficient experience in identifying, assessing, and mitigating known and emerging threats and vulnerabilities. When technology supports service delivery, assess the third party's data, infrastructure, and application security programs, including the software development life cycle and results of vulnerability and penetration tests. Consider the extent to which the third party uses controls to limit access to the banking organization's data and transactions, such as multifactor authentication, end-to-end encryption, and secured source code management. Evaluate the third party's ability to implement effective and sustainable corrective actions to address deficiencies discovered during testing.

[17] Conformity assessment with domestic or international standards can be considered with respect to the other areas of consideration during due diligence mentioned above.

i. Management of Information Systems

Gain a clear understanding of the third party's business processes and technology that will be used to support the activity. When technology is a major component of the third-party relationship, review both the banking organization's and the third party's information systems to identify gaps in service-level expectations, technology, business process and management, or interoperability issues. Review the third party's processes for maintaining timely and accurate inventories of its technology and its subcontractor(s). Consider risks and benefits of different programing languages. Understand the third party's metrics for its information systems and confirm that they meet the banking organization's expectations

j. Operational Resilience

Assess the third party's ability to deliver operations through a disruption from any hazard with effective operational risk management combined with sufficient financial and operational resources to prepare, adapt, withstand, and recover from disruptions.[18] Assess options to employ if a third party's ability to deliver operations is impaired.

Determine whether the third party maintains an appropriate business continuity management program, including disaster recovery and business continuity plans that specify the time frame to resume activities and recover data. Confirm that the third party regularly tests its operational

[18] Disruptive events could include technology-based failures, human error, cyber incidents, pandemic outbreaks, and natural disasters. Additional information is available in the Interagency "Sound Practices to Strengthen Operational Resilience." The OCC issued Sound Practices as part of Bulletin 2020-94 on October 30, 2020; The Board issued Sound Practices with SR Letter 20-24 on November 2, 2020; and The FDIC issued Sound Practices as a FIL Letter on November 2, 2020.

resilience in an appropriate format and frequency. In order to assess the scope of operational resilience capabilities, banks may review the third party's telecommunications redundancy and resilience plans and preparations for known and emerging threats and vulnerabilities, such as wide-scale natural disasters, pandemics, distributed denial of service attacks, or other intentional or unintentional events. Consider risks related to technologies used by third parties, such as interoperability or potential end of life issues with software programming language, computer platform, or data storage technologies that may impact operational resilience. Banks may also gain additional insight into a third party's resilience capabilities by reviewing the results of business continuity testing results and performance during actual disruptions.

k. Incident Reporting and Management Programs

Review and consider the third party's incident reporting and management programs to ensure there are clearly documented processes, timelines, and accountability for identifying, reporting, investigating, and escalating incidents. Confirm that the third party's escalation and notification processes meet the banking organization's expectations and regulatory requirements.

l. Physical Security

Evaluate whether the third party has sufficient physical and environmental controls to protect the safety and security of its facilities, technology systems, data, and employees. Where sensitive banking organization data may be accessible, review employee on- and off-boarding procedures to ensure physical access rights are managed appropriately.

m. Human Resource Management

Review the third party's processes to train and hold employees accountable for compliance with policies and procedures. Review the third party's succession and redundancy planning for key management and support personnel. Review training programs to ensure that the third party's staff is knowledgeable about applicable laws, regulations, technology, risk, and other factors that may affect the quality of services and risk to the banking organization.

n. Reliance on Subcontractors

Evaluate the volume and types of subcontracted activities and consider any implications or risks associated with the subcontractors' geographic locations. Evaluate the third party's ability to identify, assess, monitor, and mitigate risks from its use of subcontractors and to provide that the same level of quality and controls exists no matter where the subcontractors' operations reside. Evaluate whether additional risks may arise from the third party's reliance on subcontractors and, as appropriate, conduct similar due diligence on the third party's critical subcontractors, such as when additional risk may arise due to concentration-related risk, when the third party outsources significant activities, or when subcontracting poses other material risks.

o. Insurance Coverage

Evaluate whether the third party has fidelity bond coverage to insure against losses attributable to, at a minimum, dishonest acts, liability coverage for losses attributable to negligent acts, and hazard insurance covering fire, loss of data, and protection of documents. Evaluate whether the third party has insurance coverage for areas that may not be covered under a general commercial

policy, such as its intellectual property rights and cybersecurity. The amounts of such coverage should be commensurate with the level of risk involved with the third party's operations and the type of activities to be provided.

p. Conflicting Contractual Arrangements with Other Parties

Obtain information regarding legally binding arrangements with subcontractors or other parties to determine whether the third party has indemnified itself, as such arrangements may transfer risks to the banking organization. Evaluate the potential legal and financial implications to the banking organization of these contracts between the third party and its subcontractors or other parties.

3. Contract Negotiation

Once a banking organization selects a third party, it negotiates a contract that clearly specifies the rights and responsibilities of each party to the contract. The banking organization seeks to add provisions to satisfy its needs. While third parties may initially offer a standard contract, banks may seek to request additional contract provisions or addendums upon request. In situations where it is difficult for a banking organization to negotiate contract terms, it is important for the banking organization to understand any resulting limitations, determine whether the contract can still meet the banking organization's needs, and determine whether the contract would result in increased risk to the banking organization. If the contract would not satisfy the banking organization's needs or would result in an unacceptable increase in risk, the

banking organization may wish to consider other third parties for the service. Banking organizations may also gain advantage by negotiating contracts as a group with other users.

The board (or a designated committee reporting to the board) should be aware of and approve contracts involving critical activities before their execution. Legal counsel review may be necessary for significant contracts prior to finalization. As part of sound risk management, a banking organization reviews existing contracts periodically, particularly those involving critical activities, to ensure they continue to address pertinent risk controls and legal protections. Where problems are identified, the banking organization should seek to renegotiate at the earliest opportunity. A material or significant contract with a third party typically prohibits assignment, transfer, or subcontracting by the third party of its obligations to another entity without the banking organization's consent.

A banking organization typically considers the following factors, among others, during contract negotiations with a third party:

a. Nature and Scope of Arrangement

A contract specifies the nature and scope of the business arrangement (for example, the frequency, content, and format of the activity) and includes, as applicable, such ancillary services as software or other technology support and maintenance, employee training, and customer service. A contract may also specify which activities the third party is to conduct, whether on or off the banking organization's premises, and describe the terms governing the use of the banking

organization's information, facilities, personnel, systems, and equipment, as well as access to and use of the banking organization's or customers' information. When dual employees will be used, the contract typically clearly articulates their responsibilities and reporting lines.

b. Performance Measures or Benchmarks

A service-level agreement between the banking organization and third party specifies measures surrounding the expectations and responsibilities for both parties, including conformance with regulatory standards or rules. Performance and risk measures can be used to motivate the third party's performance, penalize poor performance, or reward outstanding performance. Performance measures should not incentivize undesirable performance or behavior, such as encouraging processing volume or speed without regard for timeliness, accuracy, compliance requirements, or adverse effects on banking organization customers.

c. Responsibilities for Providing, Receiving, and Retaining Information

Confirm that the contract includes provisions that the third party provides and retains timely, accurate, and comprehensive information, such as records and reports, that allow banking organization management to monitor performance, service levels, and risks. Stipulate the frequency and type of reports needed.

Confirm that the contract sufficiently addresses:

- The ability of the institution to have unrestricted access to its data whether or not in the possession of the third party;
- The responsibilities and methods to address failures to adhere to the agreement including the ability of all parties to the agreement to exit the relationship;
- The banking organization's materiality thresholds and the third party's procedures for immediately notifying the banking organization whenever service disruptions, security breaches, compliance lapses, enforcement actions, regulatory proceedings, or other events pose a significant risk to the banking organization (for example, financial difficulty, catastrophic events, and significant incidents);
- Notification to the banking organization before making significant changes to the contracted activities, including acquisition, subcontracting, offshoring, management, or key personnel changes, or implementing new or revised policies, processes, and information technology;
- Notification to the banking organization of significant strategic business changes, such as mergers, acquisitions, joint ventures, divestitures, or other business activities that could affect the activities involved;
- The ability for the banking organization to access native data and to authorize and allow other third parties to access its data during the term of the contract;
- The ability of the third party to resell, assign, or permit access to the banking organization's data, metadata, and systems to other entities;
- Expectations for the third party to notify the banking organization of significant operational changes or when the third party experiences significant incidents; and

- Specification of the type and frequency of management information reports to be received from the third party, where appropriate. This may include routine reports, among others, on performance reports, audits, financial reports, security reports, and business resumption testing reports.

d. The Right to Audit and Require Remediation

The contract often establishes the banking organization's right to audit, monitor performance, and provide for remediation when issues are identified. Generally, a third-party contract includes provisions for periodic, independent, internal, or external audits of the third party, and relevant subcontractors, at intervals and scopes consistent with the banking organization's in-house functions to monitor performance with the contract. An effective contract provision includes the types and frequency of audit reports the banking organization is entitled to receive from the third party (for example, SOC reports, Payment Card Industry (PCI) compliance reports, and other financial and operational reviews). Contract provisions reserve the banking organization's right to conduct its own audits of the third party's activities or to engage an independent party to perform such audits.

e. Responsibility for Compliance with Applicable Laws and Regulations

Provide that the contract requires compliance with laws and regulations and considers relevant guidance and self-regulatory standards. These may include, among others: the Gramm-Leach-Bliley Act (including privacy and safeguarding of customer information); the Bank Secrecy Act

and Anti-Money Laundering (BSA/AML) laws; the Office of Foreign Assets Control (OFAC) regulations; and consumer protection laws and regulations, including with respect to fair lending and unfair, deceptive or abusive acts or practices. Confirm that the contract gives the banking organization the right to monitor the third party's compliance with applicable laws, regulations, and policies, conduct periodic reviews to verify adherence to expectations, and require remediation if issues arise.

f. Cost and Compensation

Contracts describe compensation, fees, and calculations for base services, as well as any fees based on volume of activity and for special requests. Confirm that the contracts do not include burdensome upfront fees or incentives that could result in inappropriate risk taking by the banking organization or third party. Indicate which party is responsible for payment of legal, audit, and examination fees associated with the activities involved. Consider outlining cost and responsibility for purchasing and maintaining hardware and software and specifying the conditions under which the cost structure may be changed, including limits on any cost increases.

g. Ownership and License

State whether and how the third party has the right to use the banking organization's information, technology, and intellectual property, such as the banking organization's name, logo, trademark, metadata, and copyrighted material. Indicate whether any records generated by the third party become the banking organization's property. Include appropriate warranties on the part of the

third party related to its acquisition of licenses or subscription for use of any intellectual property developed by other third parties. If the banking organization purchases software, establish escrow agreements to provide for the banking organization's access to source code and programs under certain conditions (for example, insolvency of the third party).

h. Confidentiality and Integrity

Prohibit the use and disclosure of the banking organization's information by a third party and its subcontractors, except as necessary to provide the contracted activities or comply with legal requirements. If the third party receives a banking organization's customers' personally identifiable information, the contract should ensure that the third party implements and maintains appropriate security measures to comply with privacy regulations and regulatory guidelines. Specify when and how the third party will disclose, in a timely manner, information security breaches that have resulted in unauthorized intrusions or access that may materially affect the banking organization or its customers. Stipulate that intrusion notifications of customer data include estimates of the effects on the banking organization and its customers and specify corrective action to be taken by the third party. Address the powers of each party to change security and risk management procedures and requirements and resolve any confidentiality and integrity issues arising out of shared use of facilities owned by the third party. Stipulate whether and how often the banking organization and the third party will jointly practice incident management exercises involving unauthorized intrusions or other breaches of confidentiality and integrity.

i. Operational Resilience and Business Continuity

Confirm that the contract provides for continuation of the business function in the event of problems affecting the third party's operations, including degradations or interruptions resulting from natural disasters, human error, or intentional attacks. Stipulate the third party's responsibility for backing up and otherwise protecting programs, data backup, periodic maintenance for cybersecurity issues that emerge over time, and maintaining current and sound business resumption and business continuity plans. Include provisions for transferring the banking organization's accounts, data, or activities to another third party without penalty in the event of the third party's bankruptcy, business failure, or business interruption.

Contracts often require the third party to provide the banking organization with operating procedures to be carried out in the event business continuity plans are implemented, including specific recovery time and recovery point objectives. In particular, it is important for the contract to contain service level agreements and related services that can support the needs of the banking organization. Stipulate whether and how often the banking organization and the third party will jointly test business continuity plans. In the event the third party is unable to provide services as agreed, the contract permits the banking organization to terminate the service without being assessed a termination penalty and provides access to data in order to transfer services to another provider for continuity of operations.

j. Indemnification

Consider including indemnification clauses that specify the extent to which the banking organization will be held liable for claims that cite failure of the third party to perform, including failure of the third party to obtain any necessary intellectual property licenses. Carefully assess indemnification clauses that require the banking organization to hold the third party harmless from liability.

k. Insurance

Consider whether the third party maintains adequate types and amounts of insurance (including, if appropriate, naming the banking organization as insured or additional insured), notifies the banking organization of material changes to coverage, and provides evidence of coverage where appropriate. Types of insurance coverage may include fidelity bond; cybersecurity; liability; property hazard and casualty; and intellectual property.

l. Dispute Resolution

Consider whether the contract should establish a dispute resolution process (arbitration, mediation, or other means) to resolve problems between the banking organization and the third party in an expeditious manner, and whether the third party should continue to provide activities to the banking organization during the dispute resolution period.

m. Limits on Liability

A contract may limit the third party's liability, in which case the banking organization may consider whether the proposed limit is in proportion to the amount of loss the banking organization might experience because of the third party's failure to perform or to comply with applicable laws, and whether the contract would subject the banking organization to undue risk of litigation.

n. Default and Termination

Confirm that the contract stipulates what constitutes default; identifies remedies and allows opportunities to cure defaults; and stipulates the circumstances and responsibilities for termination. Contracts can protect the ability of the banking organization to change providers when appropriate without undue restrictions, limitations, or cost. Determine whether the contract:

- Includes a provision that enables the banking organization to terminate the relationship in a timely manner without prohibitive expense;
- Includes termination and notification provisions with reasonable time frames to allow for the orderly conversion to another third party;
- Provides for the timely return or destruction of the banking organization's data and other resources;
- Provides for ongoing monitoring of the third party after the contract terms are satisfied, as necessary; and

- Clearly assigns all costs and obligations associated with transition and termination.

Additionally, effective contracts enable the banking organization to terminate the relationship upon reasonable notice and without penalty in the event that the banking organization's primary federal banking regulator formally directs the banking organization to terminate the relationship.

o. Customer Complaints

Specify whether the banking organization or third party is responsible for responding to customer complaints. If it is the third party's responsibility, include provisions in the contract that provide for the third party to receive and respond in a timely manner to customer complaints, and forward a copy of each complaint and response to the banking organization. The contract addresses the submission of sufficient, timely, and usable information to enable the banking organization to analyze customer complaint activity and trends for risk management purposes.

p. Subcontracting

Consider whether to allow the third party to use a subcontractor, and if so, address when and how the third party should notify or seek approval from the banking organization of its intent to use a subcontractor (for example, for certain activities or in certain locations) or whether specific subcontractors are prohibited by the banking organization. Detail contractual obligations, such as reporting on the subcontractor's conformance with performance measures, periodic audit

results, compliance with laws and regulations, and other contractual obligations. State the third party's liability for activities or actions by its subcontractors and which party is responsible for the costs and resources required for any additional monitoring and management of the subcontractors. Reserve the right to terminate the contract with the third party without penalty if the third party's subcontracting arrangements do not comply with the terms of the contract.

q. Foreign-Based Third Parties

Include in contracts with foreign-based third parties choice-of-law provisions and jurisdictional provisions that provide for adjudication of all disputes between the parties under the laws of a single jurisdiction. Understand that such contracts and covenants may be subject, however, to the interpretation of foreign courts relying on local laws. Seek legal advice to confirm the enforceability of all aspects of a proposed contract with a foreign-based third party and other legal ramifications of each such business arrangement, including privacy laws and cross-border flow of information.

r. Regulatory Supervision

For relevant third-party relationships, stipulate that the performance of activities by external parties for the banking organization is subject to regulatory examination oversight, including access to all work papers, drafts, and other materials.[19]

[19] The agencies generally have the authority to examine and to regulate banking-related functions or operations performed by third parties for a banking organization to the same extent as if they were performed by the banking organization itself. *See* 12 U.S.C. 1464(d)(7)(D) and 1867(c)(1).

4. Oversight and Accountability

The banking organization's board of directors (or a designated board committee) and management are responsible for overseeing the banking organization's overall risk management processes. Banking organization management is responsible for implementing third-party risk management. An effective board oversees risk management implementation and holds management accountable. Effective management teams should establish responsibility and accountability for managing third parties commensurate with the level of risk and complexity of the relationship.

a. Board of Directors

In overseeing the management of risks associated with third-party relationships, boards of directors (or directors) typically consider the following factors, among others:

- Confirming that risks related to third-party relationships are managed in a manner consistent with the banking organization's strategic goals and risk appetite;
- Approving the banking organization's policies that govern third-party risk management;
- Approving, or delegating to, an appropriate committee reporting to the board, approval of contracts with third parties that involve critical activities;
- Reviewing the results of management's ongoing monitoring of third-party relationships involving critical activities;

- Confirming that management takes appropriate actions to remedy significant deterioration in performance or address changing risks or material issues identified through ongoing monitoring; and
- Reviewing results of periodic independent reviews of the banking organization's third-party risk management process.

b. Management

When executing and implementing third-party relationship risk management strategies and policies, management typically considers:

- Developing and implementing the banking organization's third-party risk management process;
- Confirming that appropriate due diligence and ongoing monitoring is conducted on third parties and presenting results to the board when making recommendations to use third parties that involve critical activities;
- Reviewing and approving contracts with third parties;
- Providing appropriate organizational structures, management and staffing (level and expertise);
- Confirming that third parties comply with the banking organization's policies and reporting requirements;
- Providing that third parties be notified of significant operational issues at the banking organization that may affect the third party;

- Confirming that the banking organization has an appropriate system of internal controls and regularly tests the controls to manage risks associated with third-party relationships;
- Confirming that the banking organization's compliance management system is appropriate to the nature, size, complexity, and scope of its third-party business arrangements;
- Providing that third parties regularly test and implement agreed-upon remediation when issues arise;
- Escalating significant issues to the board;
- Terminating business arrangements with third parties that do not meet expectations or no longer align with the banking organization's strategic goals, objectives, or risk appetite; and
- Maintaining appropriate documentation throughout the life cycle.

c. Independent Reviews

Banking organizations typically conduct periodic independent reviews of the third-party risk management process, particularly when third parties perform critical activities. The banking organization's internal auditor or an independent third party may perform the reviews, and senior management confirms that the results are reported to the board. Reviews include assessing the adequacy of the banking organization's process for:

- Confirming third-party relationships align with the banking organization's business strategy;
- Identifying, measuring, monitoring, and controlling risks of third-party relationships;

- Understanding and monitoring concentration risks that may arise from relying on a single third party for multiple activities or from geographic concentrations of business;[20]
- Responding to material breaches, service disruptions, or other material issues;
- Involving multiple disciplines across the banking organization as appropriate during each phase of the third-party risk management life cycle;[21]
- Confirming appropriate staffing and expertise to perform risk assessment, due diligence, contract negotiation, and ongoing monitoring and management of third parties;
- Confirming oversight and accountability for managing third-party relationships (for example, whether roles and responsibilities are clearly defined and assigned and whether the individuals possess the requisite expertise, resources, and authority); and
- Confirming that conflicts of interest or appearances of conflicts of interest do not exist when selecting or overseeing third parties.

The results of independent reviews may be used to determine whether and how to adjust the banking organization's third-party risk management process, including policy, reporting, resources, expertise, and controls. It is important that management responds promptly and thoroughly to significant issues or concerns identified and escalates them to the board if the risk posed is approaching the banking organization's risk appetite limits.

[20] For example, more complex relationships could include foreign-based third parties and the use of subcontractors.

[21] In addition to the functional business units, this may include information technology, identity and access management, physical security, information security, business continuity, compliance, legal, risk management, and human resources.

d. Documentation and Reporting

It is important that banking organization management properly document and report on its third-party risk management process and specific business arrangements throughout their life cycle. Proper documentation and reporting facilitate the accountability, monitoring, and risk management associated with third parties, will vary among organizations depending on their size and complexity, and may include the following:

- A current inventory of all third-party relationships, which clearly identifies those relationships that involve critical activities and delineates the risks posed by those relationships across the banking organization;[22]
- Approved plans for the use of third-party relationships;
- Risk assessments;
- Due diligence results, findings, and recommendations;
- Analysis of costs associated with each activity or third-party relationship, including any indirect costs assumed by the banking organization;
- Executed contracts;
- Regular risk management and performance reports required and received from the third party, which may include reports on service level reporting, internal control testing, cybersecurity risk and vulnerabilities metrics, results of independent reviews and other ongoing monitoring activities; and

[22] Under Section 7(c) of the Bank Service Company Act, 12 U.S.C. 1867(c), banks are required to notify the appropriate federal banking agency of the existence of a servicing relationship. Federal savings associations are subject to similar requirements set forth in 12 U.S.C. 1464(d)(7)(D)(ii) and 1867(c)(2).

- Reports from third parties of service disruptions, security breaches, or other events that pose a significant risk to the banking organization.

5. Ongoing Monitoring

Ongoing monitoring is an essential component of third-party risk management, occurring throughout the duration of a third-party relationship. Ongoing monitoring occurs after the third-party relationship is established and often leverages processes similar to due diligence. The appropriate degree of ongoing monitoring is commensurate with the level of risk and complexity of the third-party relationship. More comprehensive monitoring is typically necessary when the third-party relationship is higher risk (for example, involving critical activities). Banking organizations periodically re-assess existing relationships to determine whether the nature of an activity subsequently becomes critical.

Because both the level and types of risks may change over the lifetime of third-party relationships, banking organizations adapt their ongoing monitoring practices accordingly. Management's monitoring may result in changes to the frequency and types of reports from the third party, including service-level agreement performance reports, audit reports, and control testing results.

As part of sound risk management, banking organizations dedicate sufficient staffing with the necessary expertise, authority, and accountability to perform ongoing monitoring, which may include periodic on-site visits and meetings with third-party representatives to discuss

performance and operational issues. Effective monitoring activities enable banking organizations to confirm the quality and sustainability of the third party's controls and ability to meet service-level agreements (for example, ongoing review of third-party performance metrics). Additionally, ongoing monitoring typically includes the regular testing of the banking organization's controls to manage risks from third-party relationships, particularly when critical activities are involved. Bank employees who directly manage third-party relationships escalate to senior management significant issues or concerns arising from ongoing monitoring, such as an increase in risk, material weaknesses and repeat audit findings, deterioration in financial condition, security breaches, data loss, service or system interruptions, or compliance lapses. In addition, based on the results of the ongoing monitoring and internal control testing, banking organizations respond to issues when identified, including escalating significant issues to the board.

A banking organization typically considers the following factors, among others, for ongoing monitoring of a third party:

- Evaluate the overall effectiveness of the third-party relationship and the consistency of the relationship with the banking organization's strategic goals;
- Assess changes to the third party's business strategy, legal risk, and its agreements with other entities that may pose conflicting interests, introduce risks, or impact the third party's ability to meet contractual obligations;
- Evaluate the third party's financial condition and changes in the third party's financial obligations to others;

- Review the adequacy of the third party's insurance coverage;
- Review relevant audits and other reports from the third party, and consider whether the results indicate an ability to meet contractual obligations and effectively manage risks;
- Monitor for compliance with applicable legal and regulatory requirements;
- Assess the effect of any changes in key third party personnel involved in the relationship with the banking organization;
- Monitor the third party's reliance on, exposure to, performance of, and use of subcontractors, as stipulated in contractual requirements, the location of subcontractors, and the ongoing monitoring and control testing of subcontractors;
- Determine the adequacy of any training provided to employees of the banking organization and the third party;
- Review processes for adjusting policies, procedures, and controls in response to changing threats and new vulnerabilities and material breaches or other serious incidents;
- Monitor the third party's ability to maintain the confidentiality and integrity of the banking organization's systems and information, including the banking organization's customers' data if received by the third party;
- Review the third party's business resumption contingency planning and testing and evaluate the third party's ability to respond to and recover from service disruptions or degradations and meet business resilience expectations; and
- Evaluate the volume, nature, and trends of consumer inquiries and complaints and assess the third party's ability to appropriately address and remediate inquiries and complaints.

6. Termination

A banking organization may terminate a relationship for various reasons specified in the contract, such as expiration of or dissatisfaction with the contract, a desire to seek an alternate third party, a desire to bring the activity in-house or discontinue the activity, or a breach of contract. When this occurs, it is important for management to terminate relationships in an efficient manner, whether the activities are transitioned to another third party, brought in-house, or discontinued. In the event of contract default or termination, a well-run banking organization should consider how to transition services in a timely manner to another third-party provider or bring the service in-house if there are no alternate third-party providers. In planning for termination, a banking organization typically considers the following factors, among others:

- Capabilities, resources, and the time frame required to transition the activity while still managing legal, regulatory, customer, and other impacts that might arise;
- Potential third-party service providers to which the services could be transitioned;
- Risks associated with data retention and destruction, information system connections and access control issues, or other control concerns that require additional risk management and monitoring during and after the end of the third-party relationship;
- Handling of joint intellectual property developed during the course of the business arrangement; and
- Risks to the banking organization if the termination happens as a result of the third party's inability to meet expectations.

D. SUPERVISORY REVIEWS OF THIRD-PARTY RELATIONSHIPS

A banking organization's failure to have an effective third-party risk management process that is commensurate with the level of risk, complexity of third-party relationships, and organizational structure of the banking organization may be an unsafe or unsound practice.

When reviewing third party risk management, examiners typically:

- Assess the banking organization's ability to oversee and manage its relationships;
- Highlight and discuss material risks and any deficiencies in the banking organization's risk management process with the board of directors and senior management;
- Carefully review the banking organization's plans for appropriate and sustainable remediation of such deficiencies, particularly those associated with the oversight of third parties that involve critical activities;
- Identify and report deficiencies in supervisory findings and reports of examination and recommend appropriate supervisory actions. These actions may include issuing Matters Requiring Attention, issuing Matters Requiring Board Attention, and recommending formal enforcement actions;
- Consider the findings when assigning the management component of the Federal Financial Institutions Examination Council's Uniform Financial Institutions Rating System. Serious deficiencies may result in management being deemed less than satisfactory; and
- Reflect the associated risks in the overall assessment of the banking organization's risk profile.

When circumstances warrant, the agencies may use their authorities to examine the functions or operations performed by a third party on the banking organization's behalf. Such examinations may evaluate safety and soundness risks, the financial and operational viability of the third party, the third party's ability to fulfill its contractual obligations and comply with applicable laws and regulations, including those related to consumer protection (including with respect to fair lending and unfair or deceptive acts or practices), and BSA/AML and OFAC laws and regulations. The agencies may pursue appropriate corrective measures, including enforcement actions, to address violations of law and regulations or unsafe or unsound banking practices by the banking organization or its third party.

[Separate Exhibit]

V. OCC's 2020 Frequently Asked Questions (FAQs) on Third-Party Relationships

The agencies are including the OCC's 2020 FAQs, released in March 2020, as an exhibit, separate from the proposed guidance. The OCC issued the 2020 FAQs to clarify the OCC's 2013 third-party risk management guidance. The agencies seek public comment on the extent to which the concepts discussed in the OCC's 2020 FAQs should be incorporated into the final version of the guidance. More specifically, the agencies seek public comment on whether: (1) any of these concepts should be incorporated into the final guidance; and (2) there are additional concepts that would be helpful to include.

Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29

Summary

The Office of the Comptroller of the Currency (OCC) issued frequently asked questions (FAQ) to supplement OCC Bulletin 2013-29, "Third-Party Relationships: Risk Management Guidance." These FAQs were intended to clarify the OCC's existing guidance and reflect evolving industry trends.

Note for Community Banks

This bulletin applies to community banks.[1]

Highlights

Topics addressed in the FAQs include

- the terms “third-party relationship” and “business arrangement.”
- when cloud computing providers are in a third-party relationship with a bank.
- when data aggregators are in a third-party relationship with a bank.
- risk management when the bank has limited negotiating power in contractual arrangements.
- critical activities and how a bank can determine the risks associated with third-party relationships.
- bank management’s responsibilities regarding a third party’s subcontractors.
- reliance on and use of third party-provided reports, certificates of compliance, and independent audits.
- risk management when third party has limited ability to provide the same level of due diligence-related information as larger or more established third parties.
- risk management when using a third-party model or when using a third party to assist with model risk management.
- use of third-party assessment services in managing third-party relationship risks.
- a board’s approval of contracts.
- risk management when obtaining alternative data from a third party.

Frequently Asked Questions

1. What is a third-party relationship? (originally FAQ No. 1 in OCC Bulletin 2017-21)

OCC Bulletin 2013-29 defines a third-party relationship as any business arrangement between the bank and another entity, by contract or otherwise.

Bank management should conduct in-depth due diligence and ongoing monitoring of each of the bank's third-party service providers that support critical activities. The OCC realizes that although banks may want in-depth information, they may not receive all the information they seek on each critical third-party service provider, particularly from new companies. When a bank does not receive all the information it seeks about third-party service providers that support the bank's critical activities, the OCC expects the bank's board of directors and management to

- develop appropriate alternative ways to analyze these critical third-party service providers.
- establish risk-mitigating controls.
- be prepared to address interruptions in delivery (for example, use multiple payment systems, generators for power, and multiple telecommunications lines in and out of critical sites).
- make risk-based decisions that these critical third-party service providers are the best service providers available to the bank despite the fact that the bank cannot acquire all the information it wants.

- retain appropriate documentation of all their efforts to obtain information and related decisions.
- ensure that contracts meet the bank's needs.

2. What is a "business arrangement?"

OCC Bulletin 2013-29 states that a third-party relationship is any business arrangement between a bank and another entity, by contract or otherwise. The term "business arrangement" is meant to be interpreted broadly and is synonymous with the term third-party relationship. A footnote in OCC Bulletin 2013-29 provides examples of business arrangements (third-party relationships), such as activities that involve outsourced products and services, use of independent consultants, networking arrangements, merchant payment processing, services provided by affiliates and subsidiaries, joint ventures, and other business arrangements in which the bank has an ongoing relationship or may have responsibility for the associated records. Neither a written contract nor a monetary exchange is necessary to establish a business arrangement; all that is necessary is an agreement between the bank and the third party. Business arrangements generally exclude bank customers.

Traditionally, banks use the terms "vendor" or "outsource" to describe business arrangements and often use these terms instead of third-party relationships. A "vendor" is typically an individual or company offering something for sale, and banks may "outsource" a bank function or task to another company. A bank's relationships with vendors or entities to which banks outsource bank functions or activities do not represent the only types of business arrangements.

Since the publication of OCC Bulletin 2013-29, business arrangements have expanded and become more varied and, in some cases, more complex. The OCC has received requests for clarification regarding business arrangements and how those arrangements relate to OCC Bulletin 2013-29. The following are some examples:

- **Referral arrangements:** A referral arrangement is a continuing agreement between a bank and another party (e.g., bank, corporate entity, or individual) in which the bank refers potential customers (or "leads") to the other party in exchange for some form of compensation. The compensation may also be non-financial such as cross-marketing. The bank has a business arrangement with the party receiving the bank's referral.
- **Appraisers and appraisal management companies:** Some banks maintain an approved panel or list of individual appraisers. When an appraisal is requested, the bank enters into an agreement with an individual appraiser. This establishes a business arrangement between the bank and the individual appraiser. Banks may also outsource the process of engaging real estate appraisers to appraisal management companies. In such an instance, a bank has a business arrangement with the appraisal management company that the bank uses.[2]
- **Professional service providers:** Service providers such as law firms, consultants, or audit firms often provide professional services to banks. A bank that receives these professional services has a business arrangement with the professional service provider.[3]
- **Maintenance, catering, and custodial service companies:** There are many companies that a bank or a line of business may need to provide a product or service

either to the bank or to the bank's customers. The bank has a business arrangement with each of these types of companies.[4]

3. Does a company that provides a bank with cloud computing have a third-party relationship with the bank? If so, what are the third-party risk management expectations?

Consistent with OCC Bulletin 2013-29, a bank that has a business arrangement with a cloud service provider has a third-party relationship with the cloud service provider. Third-party risk management for cloud computing services is fundamentally the same as for other third-party relationships. The level of due diligence and oversight should be commensurate with the risk associated with the activity or data using cloud computing. Bank management should keep in mind that specific technical controls in cloud computing may operate differently than in more traditional network environments.

When using cloud computing services, bank management should have a clear understanding of, and should document in the contract, the controls that the cloud service provider is responsible for managing and those controls that the bank is responsible for configuring and managing. Regardless of the division of control responsibilities between the cloud service provider and the bank, the bank is ultimately responsible for the effectiveness of the control environment.

A bank may have a third-party relationship with a third party that has subcontracted with a cloud service provider to house systems that support the third-party service provider. As with other third-party relationships, bank management should conduct due diligence to confirm that the third party can satisfactorily oversee and monitor the cloud service subcontractor.[5] In many

cases, independent reports, such as System and Organization Controls (SOC) reports, may be leveraged for this purpose.[6]

4. If a data aggregator[7] collects customer-permissioned data from a bank, does the data aggregator have a third-party relationship with the bank? If so, what are the third-party risk management expectations?

A data aggregator typically acts at the request of and on behalf of a bank's customer without the bank's involvement in the arrangement. Banks typically allow for the sharing of customer information, as authorized by the customer, with data aggregators to support customers' choice of financial services. Whether a bank has a business arrangement with the data aggregator depends on the level of formality of any arrangements that the bank has with the data aggregator for sharing customer-permissioned data.

A bank that has a business arrangement with a data aggregator has a third-party relationship, consistent with the existing guidance in OCC Bulletin 2013-29. Regardless of the structure of the business arrangement for sharing customer-permissioned data, the level of due diligence and ongoing monitoring should be commensurate with the risk to the bank. In many cases, banks may not receive a direct service or benefit from these arrangements. In these cases, the level of risk for banks is typically lower than with more traditional business arrangements. Banks still have a responsibility, however, to manage these relationships in a safe and sound manner with consumer protections.

Information security and the safeguarding of sensitive customer data should be a key focus for a bank's third-party risk management when a bank is contemplating or has a business arrangement

with a data aggregator. A security breach at the data aggregator could compromise numerous customer banking credentials and sensitive customer information, causing harm to the bank's customers and potentially causing reputation and security risk and financial liability for the bank.

If a bank is not receiving a direct service from a data aggregator and if there is no business arrangement, banks still have risk from sharing customer-permissioned data with a data aggregator. Bank management should perform due diligence to evaluate the business experience and reputation of the data aggregator to gain assurance that the data aggregator maintains controls to safeguard sensitive customer data.

The following are examples of different types of interactions that banks might have with data aggregators.

- **Agreements for banks' use of data aggregation services:**[8] A business arrangement exists when a bank contracts or partners with a data aggregator to use the data aggregator's services to offer or enhance a bank product or service. Due diligence, contract negotiation, and ongoing monitoring should be commensurate with the risk, similar to the bank's risk management of other third-party relationships.
- **Agreements for sharing customer-permissioned data:** Many banks are establishing bilateral agreements with data aggregators for sharing customer-permissioned data, typically through an application programming interface (API).[9] Banks typically establish these agreements to share sensitive customer data through an efficient and secure portal. These business arrangements, using APIs, may reduce the use of less effective methods, such as screen scraping, and can allow bank customers to better

define and manage the data they want to share with a data aggregator and limit access to unnecessary sensitive customer data.

When a bank establishes a contractual relationship with a data aggregator to share sensitive customer data (with the bank customer's permission), the bank has established a business arrangement as defined in OCC Bulletin 2013-29. In such an arrangement, the bank's customer authorizes the sharing of information and the bank typically is not receiving a direct service or financial benefit from the third party. As with other business arrangements, however, banks should gain a level of assurance that the data aggregator is managing sensitive bank customer information appropriately given the potential risk.

- **Screen scraping:** A common method for data aggregation is screen scraping, in which a data aggregator uses the customer's credentials (that the customer has provided) to access the bank's website as if it were the customer. The data aggregator typically uses automated scripts to capture various data, which is then provided to the customer or a financial technology (fintech) application that serves the customer or some other business. Relevant agreements concerning customer-permissioned information sharing are generally between the customer and the financial service provider or the data aggregator and do not involve a contractual relationship with the bank.

While screen-scraping activities typically do not meet the definition of business arrangement, banks should engage in appropriate risk management for this activity. Screen-scraping can pose operational and reputation risks. Banks should take steps to manage the safety and soundness of the sharing of customer-permissioned data with third parties. Banks' information security

monitoring systems, or those of their service providers, should identify large-scale screen scraping activities. When identified, banks should take appropriate steps to identify the source of these activities and conduct appropriate due diligence to gain reasonable assurance of controls for managing this process. These efforts may include research to confirm ownership and understand business practices of the firms; direct communication to learn security and governance practices; review of independent audit reports and assessments; and ongoing monitoring of data-sharing activities.

5. What type of due diligence and ongoing monitoring should be conducted when a bank enters into a contractual arrangement in which the bank has limited negotiating power?

Some companies do not allow banks to negotiate changes to their standard contract, do not share their business resumption and disaster recovery plans, do not allow site visits, or do not respond to a bank's due diligence questionnaire. In these situations, bank management is limited in its ability to conduct the type of due diligence, contract negotiation, and ongoing monitoring that it normally would, even if the third-party relationship involves or supports a bank's critical activities.

When a bank does not receive all the information it is seeking about a third party that supports the bank's critical activities, bank management should take appropriate actions to manage the risks in that arrangement. Such actions may include

- determining if the risk to the bank of having limited negotiating power is within the bank's risk appetite.

- determining appropriate alternative methods to analyze these critical third parties (e.g., use information posted on the third party's website).
- being prepared to address interruptions in delivery (e.g., use multiple payment systems, generators for power, and multiple telecom lines in and out of critical sites).
- performing sound analysis to support the decision that the specific third party is the most appropriate third party available to the bank.
- retaining appropriate documentation of efforts to obtain information and related decisions.
- confirming that contracts meet the bank's needs even if they are not customized contracts.

6. How should banks structure their third-party risk management process? (originally FAQ No. 3 in OCC Bulletin 2017-21)

There is no one way for banks to structure their third-party risk management process. OCC Bulletin 2013-29 notes that the OCC expects banks to adopt an effective third-party risk management process commensurate with the level of risk and complexity of their third-party relationships. Some banks have dispersed accountability for their third-party risk management process among their business lines. Other banks have centralized the management of the process under their compliance, information security, procurement, or risk management functions. No matter where accountability resides, each applicable business line can provide valuable input into the third-party risk management process, for example, by completing risk assessments, reviewing due diligence questionnaires and documents, and evaluating the controls over the third-party relationship. Personnel in control functions such as audit, risk management, and compliance

programs should be involved in the management of third-party relationships. However, a bank structures its third-party risk management process, the board is responsible for overseeing the development of an effective third-party risk management process commensurate with the level of risk and complexity of the third-party relationships. Periodic board reporting is essential to ensure that board responsibilities are fulfilled.

7. OCC Bulletin 2013-29 defines third-party relationships very broadly and reads like it can apply to lower-risk relationships. How can a bank reduce its oversight costs for lower-risk relationships? (originally FAQ No. 2 from OCC Bulletin 2017-21)

Not all third-party relationships present the same level of risk. The same relationship may present varying levels of risk across banks. Bank management should determine the risks associated with each third-party relationship and then determine how to adjust risk management practices for each relationship. The goal is for the bank's risk management practices for each relationship to be commensurate with the level of risk and complexity of the third-party relationship. This risk assessment should be periodically updated throughout the relationship. It should not be a one-time assessment conducted at the beginning of the relationship.

The OCC expects banks to perform due diligence and ongoing monitoring for all third-party relationships. The level of due diligence and ongoing monitoring, however, may differ for, and should be specific to, each third-party relationship. The level of due diligence and ongoing monitoring should be consistent with the level of risk and complexity posed by each third-party relationship. For critical activities, the OCC expects that due diligence and ongoing monitoring will be robust, comprehensive, and appropriately documented. Additionally, for activities that

bank management determines to be low risk, management should follow the bank's board-established policies and procedures for due diligence and ongoing monitoring.

8. OCC Bulletin 2013-29 states that the OCC expects more comprehensive and rigorous oversight and management of third-party relationships that involve critical activities. What third-party relationships involve critical activities?

OCC Bulletin 2013-29 indicates that critical activities include significant bank functions (e.g., payments, clearing, settlements, and custody) or significant shared services (e.g., information technology) or other activities that

- could cause a bank to face significant risk if the third party fails to meet expectations.
- could have significant customer impacts.
- require significant investment in resources to implement the third-party relationship and manage the risk.
- could have a major impact on bank operations if the bank needs to find an alternate third party or if the outsourced activity has to be brought in-house.

As part of ongoing monitoring, bank management should periodically assess existing third-party relationships to determine whether the nature of the activity performed constitutes a critical activity. Some banks assign a criticality or risk level to each third-party relationship, whereas others identify critical activities and those third parties associated with the critical activities. Either approach is consistent with the risk management principles in OCC Bulletin 2013-29. Not every relationship involving critical activities is necessarily a critical third-party relationship. Mere involvement in a critical activity does not necessarily make a third party a critical third

party. It is common for a bank to have several third-party relationships that support the same critical activity (e.g., a major bank project or initiative), but not all of these relationships are critical to the success of that particular activity. Regardless of a bank's approach, the bank should have a sound methodology for designating which third-party relationships receive more comprehensive and rigorous oversight and risk management.

9. How should bank management determine the risks associated with third-party relationships?

OCC Bulletin 2013-29 recognizes that not all third-party relationships present the same level of risk or criticality to a bank's operations. Risk does not depend on the size of the third-party relationship. For example, a large service provider delivering office supplies might be low risk; a small service provider in a foreign country that provides information technology services to a bank's call center might be considered high risk.

Some banks categorize their third-party relationships by similar risk characteristics and criticality (e.g., information technology service providers; portfolio managers; catering, maintenance, and groundkeeper providers; and security providers). Bank management then applies different standards for due diligence, contract negotiation, and ongoing monitoring based on the risk profile of the category. By differentiating its third-party service providers by category, risk profile, or criticality, the bank may be able to gain efficiencies in due diligence, contract negotiation, and ongoing monitoring.

Bank management should determine the risks associated with each third-party relationship or category of relationship. A bank's third-party risk management should be commensurate with

the level of risk and complexity of its third-party relationships; the higher the risk of the individual or category of relationships, the more robust the third-party risk management should be for that relationship or category of relationships. A bank's policies regarding the extent of due diligence, contract negotiation, and ongoing monitoring for third-party relationships should show differences that correspond to different levels of risk.

10. Is a fintech company arrangement considered a critical activity? (originally FAQ No. 7 from OCC Bulletin 2017-21)

A bank's relationship with a fintech company may or may not involve critical bank activities, depending on a number of factors. OCC Bulletin 2013-29 provides criteria that a bank's board and management may use to determine what critical activities are. It is up to each bank's board and management to identify the critical activities of the bank and the third-party relationships related to these critical activities. The board (or committees thereof) should approve the policies and procedures that address how critical activities are identified. Under OCC Bulletin 2013-29, critical activities can include significant bank functions (e.g., payments, clearing, settlements, and custody), significant shared services (e.g., information technology), or other activities that

- could cause the bank to face significant risk if a third party fails to meet expectations.
- could have significant bank customer impact.
- require significant investment in resources to implement third-party relationships and manage risks.
- could have major impact on bank operations if the bank has to find an alternative third party or if the outsourced activities have to be brought in-house.

The OCC expects banks to have more comprehensive and rigorous management of third-party relationships that involve critical activities.

11. What are a bank management's responsibilities regarding a third party's subcontractors?

Third parties often enlist the help of suppliers, service providers, or other organizations. OCC Bulletin 2013-29 refers to these entities as subcontractors, which are also referred to as fourth parties.

As part of due diligence and ongoing monitoring, bank management should determine whether a third party appropriately oversees and monitors its subcontractors. OCC Bulletin 2013-29 includes information about the types of activities bank management should conduct regarding how the bank's third parties oversee and monitor subcontractors.

Third parties can fail to manage their subcontractors with the same rigor that the bank would have applied if it had engaged the subcontractor directly. To demonstrate its oversight of its subcontractors, a third party may provide a bank with independent reports or certifications. For example, as explained in FAQ No. 23, a SOC 1, type 2, report may be particularly useful, as standards of the American Institute of Certified Public Accountants require the auditor to determine and report on the effectiveness of the client's internal controls over financial reporting and associated controls to monitor relevant subcontractors. In other words, the SOC 1 report may provide bank management useful information for purposes of evaluating whether the third party has effective oversight of its subcontractors.

During due diligence, bank management should evaluate the volume and types of subcontracted activities and the subcontractors' geographic locations. Bank management should determine the third party's ability to identify and control risks from its use of subcontractors and to determine if the subcontractor's quality of operations is satisfactory and if the subcontractor has sufficient controls no matter where the subcontractor's operations reside.

Contracts should stipulate when and how the third party will notify the bank of its intent to use a subcontractor as well as how the third party will report to the bank regarding a subcontractor's conformance with performance measures, periodic audit results, compliance with laws and regulations, and other contractual obligations of the third party.

Key areas of consideration for ongoing monitoring may include

- the nature and extent of changes to the third party's reliance on, exposure to, or performance of subcontractors.
- location of subcontractors and bank data.
- whether subcontractors provide services for critical activities.
- whether subcontractors have access to sensitive customer information.
- the third party's monitoring and control testing of subcontractors.

The bank's inventory of third-party relationships should identify the third parties that use subcontractors. This is particularly important for a bank's third-party relationships that support the bank's critical activities or for higher-risk third parties.

12. When multiple banks use the same third-party service providers, can they collaborate[10] to meet expectations for managing third-party relationships specified in OCC Bulletin 2013-29? (originally FAQ No. 4 from OCC Bulletin 2017-21)

If they are using the same service providers to secure or obtain like products or services, banks may collaborate[11] to meet certain expectations, such as performing the due diligence, contract negotiation, and ongoing monitoring responsibilities described in OCC Bulletin 2013-29. Like products and services may, however, present a different level of risk to each bank that uses those products or services, making collaboration a useful tool but insufficient to fully meet the bank's responsibilities under OCC Bulletin 2013-29. Collaboration can leverage resources by distributing costs across multiple banks. In addition, many banks that use like products and services from technology or other service providers may become members of user groups. Frequently, these user groups create the opportunity for banks, particularly community banks, to collaborate with their peers on innovative product ideas, enhancements to existing products or services, and customer service and relationship management issues with the service providers. Banks that use a customized product or service may not, however, be able to use collaboration to fully meet their due diligence, contract negotiation, or ongoing responsibilities.

Banks may take advantage of various tools designed to help them evaluate the controls of third-party service providers. In general, these types of tools offer standardized approaches to perform due diligence and ongoing monitoring of third-party service providers by having participating third parties complete common security, privacy, and business resiliency control assessment questionnaires. After third parties complete the questionnaires, the results can be shared with

numerous banks and other clients. Collaboration can result in increased negotiating power and lower costs to banks during the contract negotiation phase of the risk management life cycle.

Some community banks have joined an alliance to create a standardized contract with their common third-party service providers and improve negotiating power.

13. When collaborating to meet responsibilities for managing a relationship with a common third-party service provider, what are some of the responsibilities that each bank still needs to undertake individually to meet the expectations in OCC Bulletin 2013-29? (originally FAQ No. 5 from OCC Bulletin 2017-21)

While collaborative arrangements can assist banks with their responsibilities in the life cycle phases for third-party risk management, each individual bank should have its own effective third-party risk management process tailored to each bank's specific needs. Some individual bank-specific responsibilities include defining the requirements for planning and termination (e.g., plans to manage the third-party service provider relationship and development of contingency plans in response to termination of service), as well as

- integrating the use of product and delivery channels into the bank's strategic planning process and ensuring consistency with the bank's internal controls, corporate governance, business plan, and risk appetite.
- assessing the quantity of risk posed to the bank through the third-party service provider and the ability of the bank to monitor and control the risk.
- implementing information technology controls at the bank.

- ongoing benchmarking of service provider performance against the contract or service-level agreement.
- evaluating the third party's fee structure to determine if it creates incentives that encourage inappropriate risk taking.
- monitoring the third party's actions on behalf of the bank for compliance with applicable laws and regulations.
- monitoring the third party's disaster recovery and business continuity time frames for resuming activities and recovering data for consistency with the bank's disaster recovery and business continuity plans.

14. Can a bank rely on reports, certificates of compliance, and independent audits provided by entities with which it has a third-party relationship?

In conducting due diligence and ongoing monitoring, bank management may obtain and review various reports (e.g., reports of compliance with service-level agreements, reports of independent reviewers, certificates of compliance with International Organization for Standardization (ISO) standards,[12] or SOC reports).[13] The person reviewing the report, certificate, or audit should have enough experience and expertise to determine whether it sufficiently addresses the risks associated with the third-party relationship.

OCC Bulletin 2013-29 explains that bank management should consider whether reports contain sufficient information to assess the third party's controls or whether additional scrutiny is necessary through an audit by the bank or other third party at the bank's request. More specifically, management may consider the following:

- Whether the report, certificate, or scope of the audit is enough to determine if the third-party's control structure will meet the terms of the contract.
- Whether the report, certificate, or audit is consistent with widely recognized standards.

For some third-party relationships, such as those with cloud providers that distribute data across several physical locations, on-site audits could be inefficient and costly. The American Institute of Certified Public Accountants has developed cloud-specific SOC reports based on the framework advanced by the Cloud Security Alliance. When available, these reports can provide valuable information to the bank. The Principles for Financial Market Infrastructures are international standards for payment systems, central securities depositories, securities settlement systems, central counterparties, and trade repositories. One key objective of the Principles for Financial Market Infrastructures is to encourage clear and comprehensive disclosure by financial market utilities, which are often in third-party relationships with banks. Financial market utilities typically provide disclosures to explain how their businesses and operations reflect each of the applicable Principles for Financial Market Infrastructures. Banks that have third-party relationships with financial market utilities can rely on these disclosures. Banks can also rely on pooled audit reports, which are audits paid for by a group of banks that use the same company for similar products or services.

15. What collaboration opportunities exist to address cyber threats to banks as well as to their third-party relationships? (originally FAQ No. 6 from OCC Bulletin 2017-21)

Banks may engage with a number of information-sharing organizations to better understand cyber threats to their own institutions as well as to the third parties with whom they have

relationships. Banks participating in information-sharing forums have improved their ability to identify attack tactics and successfully mitigate cyber attacks on their systems. Banks may use the Financial Services Information Sharing and Analysis Center (FS-ISAC), the U.S. Computer Emergency Readiness Team (US-CERT), InfraGard, and other information-sharing organizations to monitor cyber threats and vulnerabilities and to enhance their risk management and internal controls. Banks also may use the FS-ISAC to share information with other banks.

16. Can a bank engage with a start-up fintech company with limited financial information? (originally FAQ No. 8 from OCC Bulletin 2017-21)

OCC Bulletin 2013-29 states that banks should consider the financial condition of their third parties during the due diligence stage of the life cycle before the banks have selected or entered into contracts or relationships with third parties. In assessing the financial condition of a start-up or less established fintech company, the bank may consider a company's access to funds, its funding sources, earnings, net cash flow, expected growth, projected borrowing capacity, and other factors that may affect the third party's overall financial stability. Assessing changes to the financial condition of third parties is an expectation of the ongoing monitoring stage of the life cycle. Because it may be receiving limited financial information, the bank should have appropriate contingency plans in case the start-up fintech company experiences a business interruption, fails, or declares bankruptcy and is unable to perform the agreed-upon activities or services.

Some banks have expressed confusion about whether third-party service providers need to meet a bank's credit underwriting guidelines. OCC Bulletin 2013-29 states that depending on the significance of the third-party relationship, a bank's analysis of a third party's financial condition

may be as comprehensive as if the bank were extending credit to the third-party service provider. This statement may have been misunderstood as meaning a bank may not enter into relationships with third parties that do not meet the bank's lending criteria. There is no such requirement or expectation in OCC Bulletin 2013-29.

17. Some third parties, such as fintechs, start-ups, and small businesses, are often limited in their ability to provide the same level of due diligence-related information as larger or more established third parties. What type of due diligence and ongoing monitoring should be applied to these companies?

OCC Bulletin 2013-29 states that banks should consider the financial condition of their third parties during due diligence and ongoing monitoring. When third parties, such as fintechs, start-ups, and small businesses, have limited due diligence information, the bank should consider alternative information sources. The bank may consider a company's access to funds, its funding sources, earnings, net cash flow, expected growth, projected borrowing capacity, and other factors that may affect the third party's overall financial stability. Assessing changes to the financial condition of third parties is an expectation of the ongoing monitoring component of the bank's risk management. When a bank can only obtain limited financial information, the bank should have contingency plans in case this third party experiences a business interruption, fails, or declares bankruptcy and is unable to perform the agreed-upon activities or services.

Bank management has the flexibility to apply different methods of due diligence and ongoing monitoring when a company may not have the same level of corporate infrastructure as larger or more established companies. During due diligence and before signing a contract, bank management should assess the risks posed by the relationship and understand the third party's

risk management and control environment. The scope of due diligence and the due diligence method should vary based on the level of risk of the third-party relationship. While due diligence methods may differ, it is important for management to conclude that the third party has a sufficient control environment for the risk involved in the arrangement.

18. How can a bank offer products or services to underbanked or underserved segments of the population through a third-party relationship with a fintech company? (originally FAQ No. 9 from OCC Bulletin 2017-21)

Banks have collaborated with fintech companies in several ways to help meet the banking needs of underbanked or underserved consumers. Banks may partner with fintech companies to offer savings, credit, financial planning, or payments in an effort to increase consumer access. In some instances, banks serve only as facilitators for the fintech companies' products or services with one of the products or services coming from the banks. For example, several banks have partnered with fintech companies to establish dedicated interactive kiosks or automated teller machines (ATM) with video services that enable the consumer to speak directly to a bank teller. Frequently, these interactive kiosks or ATMs are installed in retail stores, senior community centers, or other locations that do not have branches to serve the community. Some fintech companies offer other ways for banks to partner with them. For example, a bank's customers can link their savings accounts with the fintech company's application, which can offer incentives to the bank's customers to save for short-term emergencies or achieve specific savings goals.

In these examples, the fintech company is considered to have a third-party relationship with the bank that falls under the scope of OCC Bulletin 2013-29.

19. What should a bank consider when entering a marketplace lending arrangement with nonbank entities? (originally FAQ No. 10 from OCC Bulletin 2017-21)

When engaging in marketplace lending activities, a bank's board and management should understand the relationships among the bank, the marketplace lender, and the borrowers; fully understand the legal, strategic, reputation, operational, and other risks that these arrangements pose; and evaluate the marketplace lender's practices for compliance with applicable laws and regulations. As with any third-party relationship, management at banks involved with marketplace lenders should ensure the risk exposure is consistent with their boards' strategic goals, risk appetite, and safety and soundness objectives. In addition, boards should adopt appropriate policies, inclusive of concentration limitations, before beginning business relationships with marketplace lenders.

Banks should have the appropriate personnel, processes, and systems so that they can effectively monitor and control the risks inherent within the marketplace lending relationship. Risks include reputation, credit, concentrations, compliance, market, liquidity, and operational risks. For credit risk management, for example, banks should have adequate loan underwriting guidelines, and management should ensure that loans are underwritten to these guidelines. For compliance risk management, banks should not originate or support marketplace lenders that have inadequate compliance management processes and should monitor the marketplace lenders to ensure that they appropriately implement applicable consumer protection laws, regulations, and guidance. When banks enter into marketplace lending or servicing arrangements, the banks' customers may associate the marketplace lenders' products with those of the banks, thereby introducing reputation risk if the products underperform or harm customers. Also, operational risk can

increase quickly if the operational processes of the banks and the marketplace lenders do not include appropriate limits and controls, such as contractually agreed-to loan volume limits and proper underwriting.

To address these risks, banks' due diligence of marketplace lenders should include consulting with the banks' appropriate business units, such as credit, compliance, finance, audit, operations, accounting, legal, and information technology. Contracts or other governing documents should lay out the terms of service-level agreements and contractual obligations. Subsequent significant contractual changes should prompt reevaluation of bank policies, processes, and risk management practices.

20. Does OCC Bulletin 2013-29 apply when a bank engages a third party to provide bank customers the ability to make mobile payments using their bank accounts, including debit and credit cards? (originally FAQ No. 11 from OCC Bulletin 2017-21)

When using third-party service providers in mobile payment environments, banks are expected to act in a manner consistent with OCC Bulletin 2013-29. Banks often enter into business arrangements with third-party service providers to provide software and licenses in mobile payment environments. These third-party service providers also provide assistance to the banks and the banks' customers (for example, payment authentication, delivering payment account information to customers' mobile devices, assisting card networks in processing payment transactions, developing or managing mobile software (apps) or hardware, managing back-end servers, or deactivating stolen mobile phones).

Many bank customers expect to use transaction accounts and credit, debit, or prepaid cards issued by their banks in mobile payment environments. Because almost all banks issue debit cards and offer transaction accounts, banks frequently participate in mobile payment environments even if they do not issue credit cards. Banks should work with mobile payment providers to establish processes for authenticating enrollment of customers' account information that the customers provide to the mobile payment providers.

21. May a community bank outsource the development, maintenance, monitoring, and compliance responsibilities of its compliance management system? (originally FAQ No. 12 from OCC Bulletin 2017-21)

Banks may outsource some or all aspects of their compliance management systems to third parties, so long as banks monitor and ensure that third parties comply with current and subsequent changes to consumer laws and regulations. Some banks outsource maintenance or monitoring or use third parties to automate data collection and management processes (for example, to file compliance reports under the Bank Secrecy Act or for mortgage loan application processing or disclosures). The OCC expects all banks to develop and maintain an effective compliance management system and provide fair access to financial services, ensure fair treatment of customers, and comply with consumer protection laws and regulations. Strong compliance management systems include appropriate policies, procedures, practices, training, internal controls, and audit systems to manage and monitor compliance processes as well as a commitment of appropriate compliance resources.

22. How should bank management address third-party risk management when using a third-party model or a third party to assist with model risk management?

The principles in OCC Bulletin 2013-29 are relevant when a bank uses a third-party model or uses a third party to assist with model risk management, as are the principles in OCC Bulletin 2011-12, "Sound Practices for Model Risk Management: Supervisory Guidance on Model Risk Management." Accordingly, third-party models should be incorporated into the bank's third-party risk management and model risk management processes. Bank management should conduct appropriate due diligence on the third-party relationship and on the model itself.

If the bank lacks sufficient expertise in-house, a bank may decide to engage external resources (i.e., a third party) to help execute certain activities related to model risk management and the bank's ongoing third-party monitoring responsibilities. These activities could include model validation and review, compliance functions, or other activities in support of internal audit. Bank management should understand and evaluate the results of validation and risk control activities that are conducted by third parties. Bank management typically designates an internal party to

- verify that the agreed upon scope of work has been completed by the third party.
- evaluate and track identified issues and ensure they are addressed.
- make sure completed work is incorporated into the bank's model risk management and third-party risk management processes.

Bank management should conduct a risk-based review of each third-party model to determine whether it is working as intended and if the existing validation activities are sufficient. Banks should expect the third party to conduct ongoing performance monitoring and outcomes analysis of the model, disclose results to the bank, and make appropriate modifications and updates to the model over time, if applicable.

Many third-party models can be customized by a bank to meet its needs. A bank's customization choices should be documented and justified as part of the validation. If third parties provide input data or assumptions, the relevance and appropriateness of the data or assumptions should be validated. Bank management should periodically conduct an outcomes analysis of the third-party model's performance using the bank's own outcomes.

Many third parties provide banks with reports of independent certifications or validations of the third-party model. Validation reports provided by a third-party model provider should identify model aspects that were reviewed, highlighting potential deficiencies over a range of financial and economic conditions (as applicable), and determining whether adjustments or other compensating controls are warranted. Effective validation reports include clear executive summaries, with a statement of model purpose and a synopsis of model validation results, including major limitations and key assumptions. Validation reports should not be taken at face value. Bank management should understand any of the limitations experienced by the validator in assessing the processes and codes used in the models.

As part of the planning and termination phases of the third-party risk management life cycle, the bank should have a contingency plan for instances when the third-party model is no longer available or cannot be supported by the third party. Bank management should have as much knowledge in-house as possible, in case the third party or the bank terminates the contract, or if the third party is no longer in business.

23. Can banks obtain access to interagency technology service providers' (TSP) reports of examination? (originally FAQ No. 13 from OCC Bulletin 2017-21)

TSP reports of examination[14] are available only to banks that have contractual relationships with the TSPs at the time of the examination. Because the OCC's (and other federal banking regulators') statutory authority is to examine a TSP that enters into a contractual relationship with a regulated financial institution, the OCC (and other federal banking regulators) cannot provide a copy of a TSP's report of examination to financial institutions that are either considering outsourcing activities to the examined TSP or that enter into a contract after the date of examination.

Banks can request TSP reports of examination through the banks' respective OCC supervisory office. TSP reports of examination are provided on a request basis. The OCC may, however, proactively distribute TSP reports of examination in certain situations because of significant concerns or other findings to banks with contractual relationships with that particular TSP.

Although a bank may not share a TSP report of examination or the contents therein with other banks, a bank that has not contracted with a particular TSP may seek information from other banks with information or experience with a particular TSP as well as information from the TSP to meet the bank's due diligence responsibilities.

24. Can a bank rely on a third party's Service Organization Control (SOC) report, prepared in accordance with the American Institute of Certified Public Accountants Statement on Standards for Attestation Engagements No. 18 (SSAE 18)? (originally FAQ No. 14 from OCC Bulletin 2017-21).

In meeting its due diligence and ongoing monitoring responsibilities, a bank may review a third party's SOC 1 report prepared in accordance with SSAE 18 to evaluate the third party's client(s)'

internal controls over financial reporting, including policies, processes, and internal controls. If a third party uses subcontractors (also referred to as fourth parties), a bank may find the third party's SOC 1 type 2 report particularly useful, as SSAE 18 requires the auditor to determine and report on the effectiveness of controls the third party has implemented to monitor the controls of the subcontractor. In other words, the SOC 1 type 2 report will address the question as to whether the third party has effective oversight of its subcontractors. A bank should consider whether an SOC 1 type 2 report contains sufficient information and is sufficient in scope to assess the third party's risk environment or whether additional audit or review is required for the bank to properly assess the third party's control environment.

25. How may a bank use third-party assessment services (sometimes referred to as third-party utilities)?

Third-party assessment service companies have been formed to help banks with third-party risk management, including due diligence and ongoing monitoring. These companies offer banks a standardized questionnaire with responses from a variety of third parties (particularly information technology-related companies). The benefit of this arrangement is that the third party can provide the same information to many banks using a standardized questionnaire. Banks often pay a fee to the utility to receive the questionnaire. The utility may provide other services in addition to the questionnaire. This form of collaboration can help banks gain efficiencies in due diligence and ongoing monitoring. When a bank uses a third-party utility, it has a business arrangement with the utility, and the utility should be incorporated into the bank's third-party risk management process.

Bank management should understand how the information contained within the utility report covers the specific services that the bank has obtained from the third party and meets the bank's due diligence and ongoing monitoring needs. For example, in some cases a standardized questionnaire may not be enough if the third party is supporting a critical activity at the bank, as the information requested on the questionnaire may not be specific to the bank. In these circumstances, bank management may need additional information from the third party.

26. How does a bank's board of directors approve contracts with third parties that involve critical activities?

OCC Bulletin 2013-29 indicates that a bank's board should approve contracts with third parties that involve critical activities. This statement was not meant to imply that the board must read or be involved with the negotiation of each of these contracts. The board should receive sufficient information to understand the bank's strategy for use of third parties to support products, services, and operations and understand key dependencies, costs, and limitations that the bank has with these third parties. This allows the board to understand the benefits and risks associated with engaging third parties for critical services and knowingly approve the bank's contracts. The board may use executive summaries of contracts in their review and may delegate actual approval of contracts with third parties that involve critical activities to a board committee or senior management.

27. How should a bank handle third-party risk management when obtaining alternative data from a third party?

Banks may be using or contemplating using a broad range of alternative data in credit underwriting, fraud detection, marketing, pricing, servicing, and account management.[15] For the purpose of this FAQ, alternative data mean information not typically found in the consumer's credit files at the nationwide consumer reporting agencies or customarily provided by consumers as part of applications for credit.[16]

When contemplating a third-party relationship that may involve the use of alternative data by or on behalf of the bank, bank management should:[17]

- conduct due diligence on third parties before selecting and entering into contracts. The degree of due diligence should be commensurate with the risk to the bank from the third-party relationship.
- ensure that alternative data usage comports with safe and sound operations. Appropriate data controls include rigorous assessment of the quality and suitability of data to support prudent banking operations. Additionally, the OCC's model risk management guidance contains important principles, including those that may leverage alternative data.
- analyze relevant consumer protection laws and regulations to understand the opportunities, risks, and compliance requirements before using alternative data. Based on that analysis, data that present greater compliance risk warrant more robust compliance management. Robust compliance management includes appropriate testing, monitoring, and controls to ensure that compliance risks are understood and addressed.

- conduct ongoing monitoring on third parties in a manner and with a frequency commensurate with the risk to the bank from the third-party relationship.
- discuss its plans with an OCC portfolio manager, examiner-in-charge, or supervisory office if the use of alternative data from a third-party relationship constitutes a substantial deviation from the bank's existing business plans or material changes in the bank's use of alternative data.

[1] As used in this bulletin, "banks" refers collectively to national banks, federal savings associations, and federal branches and agencies of foreign banking organizations.

[2] For more information, refer to OCC Bulletin 2019-43, "Appraisals: Appraisal Management Company Registration Requirements."

[3] Refer to OCC Bulletin 2003-12, "Interagency Policy Statement on Internal Audit and Internal Audit Outsourcing: Revised Guidelines on Internal Audit and its Outsourcing."

[4] If a bank considers these activities to be low risk, management should refer to FAQ No. 7 in this bulletin for more information about the extent of due diligence, contract negotiation, and ongoing monitoring that should be conducted for third-party relationships that support or involve low-risk bank activities.

[5] Refer to FAQ No. 11 in this bulletin for more information about a third party's subcontractors.

[6] Refer to FAQ No. 14 in this bulletin for more information on bank reliance on reports, certificates of compliance, and independent audits provided by entities with which the bank has a third-party relationship.

[7] Data aggregators are entities that access, aggregate, share, or store consumer financial account and transaction data that they acquire through connections to financial services companies. Aggregators are often intermediaries between the financial technology (fintech) applications that consumers use to access their data and the sources of data at financial services companies. An aggregator may be a generic provider of data to consumer fintech application providers and other third parties, or the aggregator may be part of a company providing branded and direct services to consumers. Refer to U.S. Department of the Treasury report "A Financial System That Creates Economic Opportunities: Nonbank Financials, Fintech, and Innovation" for more information on data aggregators.

[8] Refer to OCC Bulletin 2001-12, "Bank-Provided Account Aggregation Services: Guidance to Banks" (national banks) for more information on direct relationships. While the OCC has not made OCC Bulletin 2001-12 applicable to federal savings associations, federal savings associations may nonetheless find the information in the bulletin relevant.

[9] An API refers to a set of protocols that links two or more systems to enable communication and data exchange between them. An API for a particular routine can easily be inserted into code that uses that API in the software. An example would be the Financial Data Exchange's "FDX API Standard."

[10] Refer to OCC News Release 2015-1, "Collaboration Can Facilitate Community Bank Competitiveness, OCC Says," January 13, 2015.

[11] Any collaborative activities among banks must comply with antitrust laws. Refer to the Federal Trade Commission and U.S. Department of Justice's "Antitrust Guidelines for Collaborations Among Competitors."

[12] Refer to ISO 22301:2012, "Societal Security – Business Continuity Management Systems – Requirements," for more information regarding the ISO's standards for business continuity management.

[13] For more information on types of audits and control reviews, refer to appendix B of the "Internal and External Audits" booklet of the *Comptroller's Handbook*.

[14] The OCC conducts examinations of services provided by significant TSPs based on authorities granted by the Bank Service Company Act, 12 U.S.C. 1867. These examinations typically are conducted in coordination with the Board of Governors of the Federal Reserve Board, Federal Deposit Insurance Corporation, and other banking agencies with similar authorities. The scope of examinations focuses on the services provided and key technology and operational controls communicated in the *FFIEC Information Technology Examination Handbook* and other regulatory guidance.

[15] Existing OCC and interagency guidance potentially applicable to alternative data includes "Policy Statement on Discrimination in Lending" (59 FR 18266 (April 15, 1994)); OCC Bulletin 1997-24, "Credit Scoring Models: Examination Guidance;" OCC Bulletin 2011-12, "Sound Practices for Model Risk Management: Supervisory Guidance on Model Risk Management;" OCC Bulletin 2013-29, "Third-Party Relationships: Risk Management;" and OCC Bulletin

2017-43, "New, Modified, or Expanded Bank Products and Services: Risk Management Principles."

[16] Refer to OCC Bulletin 2019-62, "Consumer Compliance: Interagency Statement on the Use of Alternative Data in Credit Underwriting," for more information about compliance risk management considerations regarding the use of alternative data. Also refer to Consumer Financial Protection Bureau (CFPB), "Request for Information Regarding Use of Alternative Data and Modeling Techniques in the Credit Process," 82 FR 11183 (February 21, 2017).

[17] The information in this list is consistent with the Interagency Policy Statement on the Use of Alternative Data in Credit Underwriting.

Michael J. Hsu,

Acting Comptroller of the Currency.

By order of the Board of Governors of the Federal Reserve System

Ann Misback,
Secretary of the Board.

Federal Deposit Insurance Corporation.
Dated at Washington, DC, on July 12, 2021.
James P. Sheesley,
Assistant Executive Secretary.