
**Board of Governors of the Federal Reserve System
Federal Deposit Insurance Corporation Office of
the Comptroller of the Currency**

June 7, 2023

Interagency Guidance on Third-Party Relationships: Risk Management Guidance

The Board, FDIC, and OCC (collectively, the agencies) are issuing final guidance on managing risks associated with third-party relationships. The final guidance offers the agencies' views on sound risk management principles for banking organizations when developing and implementing risk management practices for all stages in the life cycle of third-party relationships. The final guidance states that sound third-party risk management takes into account the level of risk, complexity, and size of the banking organization and the nature of the third-party relationship. The agencies are issuing this joint guidance to promote consistency in supervisory approaches; it replaces each agency's existing general guidance on this topic and is directed to all banking organizations supervised by the agencies.

A. OVERVIEW

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) (collectively, the agencies) have issued this guidance to provide sound risk management principles supervised banking organizations' can leverage when developing and implementing risk management practices to assess and manage risks associated with third-party relationships.²

Whether activities are performed internally or via a third party, banking organizations are required to operate in a safe and sound manner¹ and in compliance with applicable laws and regulations. A banking organization's use of third parties does not diminish its responsibility to meet these requirements to the same extent as if its activities were performed by the banking organization in-house. To operate in a safe and sound manner, a banking organization

B. Risk Management Components

1. Risk Identification and Assessment

i. Third-Party Relationship Identification

ii. Risk Identification

iii. Risk Assessment

2. Risk Oversight

i. Due Diligence and Third Party Selection

ii. Contract Negotiation

iii. Ongoing Monitoring

iv. Termination

v. Cross-Cutting Oversight Topics

3. Residual Risk Acceptance

4. Governance

A. Overview

Banking organizations⁷ routinely rely on third parties for a range of products, services, and other activities. These third-party relationships come in a variety of forms and involve services related to many aspects of a banking organization's business. The degree of discretion granted to a third party can vary significantly in different types of relationships.

Banking organizations of all sizes rely on third-party relationships to operate effectively and meet evolving customer expectations. Community and mid-size banking organizations, which play an outsized role in lending and are vital to the strength of the U.S. economy, may be particularly reliant on such relationships to remain competitive in a rapidly evolving marketplace. Third-party relationships benefit banking organizations by allowing access to or facilitating technological advances; strategic business

For a description of the banking organizations supervised by each agency, refer to the definition of "appropriate Federal banking agency" in section 3(q) of the Federal Deposit Insurance Act (12 U.S.C. 1813(q)). ~~This~~ For purposes of this proposed guidance ~~is relevant to all~~, banking organizations also include insured credit unions as defined in the Federal Credit Union Act (12 U.S.C. 1752(7)). Use of this guidance may also be relevant to any other entity supervised by the agencies. innovations; new or improved products, services, and delivery channels and engagement with new or expanded markets; and operational efficiencies.

At the same time, use of third parties may introduce new risks or amplify existing risks to banking organizations and their customers.

A banking organization has ultimate responsibility to establish and maintain sound risk management practices and comply with applicable laws and regulations. A banking organization's use of third parties does not diminish its responsibility to meet these requirements to the same extent as if the activities were performed by the banking organization internally, including where the third-party relationship involves affiliates, service providers that are themselves highly-regulated entities, or subcontractors, or where elements of the banking organization's risk management practices are performed by a third party. The proposed guidance provides sound risk management principles to assist banking organizations in identifying, assessing, and managing risks associated with third-party relationships.⁸

Third-Party Relationships

For purposes of this guidance, a third-party relationship is a business arrangement between a banking organization and an entity or individual for the provision of one or more products, services, and other activities that support the banking organization.⁹ The use of subcontractors alone does not typically create an independent third-party

s Banking organizations' third-party relationships may raise additional consumer compliance considerations that may be relevant to, but that are not directly addressed in, this proposed guidance.

⁹ The agencies have observed that third-party relationships typically involve written agreements. Where a banking organization lacks a written agreement with a third party, or where no clear consideration underlies an activity, that activity is unlikely to constitute a third-party relationship. What would be the advantages and disadvantages of a banking organization applying the proposed guidance only to third parties that are subject to a written agreement with the banking organization to which it provides services? Would this approach, or an alternative, help clarify the scope of the proposed guidance and, if so, how? —

relationship or create a presumption of direct banking organization oversight of any subcontractors.

These third-party relationships vary widely in form and in the degree of operational functions outsourced to the third party. Some third parties provide services central to the banking organization's operations. These include core processing service providers that provide

comprehensive back-end applications and infrastructure that support the operation and essential functions of one or more of a banking organization's business lines; firms that provide other services that support a banking organization's essential operating functions, such as cloud processing, cloud storage, and compliance tools; and fintechs that partner with banking organizations to provide access to financial services. Other third-party relationships involve varying levels of interaction with a banking organization's operations. These include third parties that provide assistance with business-line- or product-specific activities (e.g., software or data providers); perform administrative or clerical tasks (e.g., operators of call centers or recordkeeping services); offer professional support services (e.g., auditors, lawyers, or consultants); and maintain office support services (e.g., physical security providers).

Principles-Based Approach

Each banking organization is responsible for operating in a safe and sound manner and adopting risk management practices that are best suited to managing the specific risks that it faces, commensurate with the banking organization's size, complexity, and risk profile and with the nature of its third-party relationships (including the risk and complexity of those relationships and type of activities performed by the third party). Not all third-party relationships present the same level of risk, and a similar relationship at different banking organizations may present different risks. Accordingly,

there is no one-size-fits-all approach to effective risk management. Banking organizations are experienced in determining, and are ultimately responsible for establishing, third-party risk management practices that are appropriate for the banking organization, consistent with safe and sound banking practices and in compliance with applicable laws and regulations. The agencies will give due consideration to a banking organization's reasonable decisions in matters of third-party risk management supervision.

Non-Enforceable Guidance

This proposed guidance does not set forth enforceable standards or prescriptive requirements;^{1°} accordingly, non-compliance with this guidance will not result in supervisory action against a banking organization. Any supervisory criticism will be specific to a banking organization's operations, financial condition, or other relevant factors, consistent with the applicable legal standards. Deviation from or inconsistency with this proposed guidance or any examples herein, including where an examiner believes that deviation or inconsistency is contrary to best practices, will not alone be a basis for supervisory action. However, the agencies may take action for violations of laws or regulations, unsafe or unsound practices, or other material risks that result from insufficient management of third-party risk (consistent with applicable rules and guidance on agency enforcement and supervisory standards).

B. Risk Management Components

The proposed guidance presents four components that banking organizations may consider when managing third-party risk: (1) identifying and assessing applicable risks;

~~Supervisory guidance does not have the force and effect of law and does not impose any new requirements on banking organizations.~~^{1°} See 12 CFR Part 4, Subpart F, Appendix A (OCC); 12 CFR [Part 262](#), ~~E~~- Appendix A (~~FRB~~Board); 12 CFR [Part 302](#), Appendix A (FDIC); 12 CFR Part 791, Subpart D (NCUA).

(2) overseeing risks proportionate to their significance; (3) making informed decisions about residual risks and risk acceptance; and (4) establishing appropriate governance practices.

1. Risk Identification and Assessment

i. Third-Party Relationship Identification

~~See 12 U.S.C. 1831p-1. The agencies implemented section 1831p-1 by regulation through the "Interagency Guidelines Establishing Standards for Safety and Soundness." See 12 CFR part 30, appendix A (OCC), 12 CFR part 208, appendix D-1 (Board); and 12 CFR part 364, appendix A (FDIC).~~

~~References to applicable laws and regulations throughout this guidance include but are not limited to those designed to protect consumers (such as fair lending laws and prohibitions against unfair, deceptive or abusive acts or practices) and those addressing financial crimes.~~

establishes risk management practices to effectively manage the risks arising from its activities, including from third-party relationships

This guidance addresses any business arrangement⁶ between a banking organization and another entity, by contract or otherwise. A third-party relationship may exist despite a lack of a contract or remuneration. Third-party relationships can include, but are not limited to, outsourced services, use of independent consultants, referral arrangements, merchant payment processing services, services provided by affiliates and subsidiaries, and joint ventures. Some banking organizations may form third-party relationships with new or novel structures and features—such as those observed in relationships with some financial technology (fintech) companies. The respective roles and responsibilities of a banking organization and a third party may differ, based on the specific circumstances of the relationship. Where the third-party relationship involves the provision of products or services to, or other interaction with, customers, the banking organization and the third party may have varying degrees of interaction with those customers.

The use of third parties can offer banking organizations significant benefits, such as access to new technologies, human capital, delivery channels, products, services, and markets. However, the use of third parties can reduce a banking organization's direct control over activities and may introduce new risks or increase existing risks, such as operational, compliance, and strategic risks. Increased risk often arises from greater operational or technological complexity, newer or, different types of relationships, or potential inferior performance by the third party. A banking organization can be exposed to adverse impacts, including substantial financial loss and operational disruption, if it fails to appropriately manage the risks associated with third-party relationships. Therefore, it is important for a banking organization to identify, assess, monitor, and control risks related to third-party relationships

The principles set forth in this guidance can support effective third-party risk management for all types of third-party relationships, regardless of how they may be structured. It is important for a banking organization to understand how the arrangement with a particular third party is structured so that the banking organization may assess the types and levels of risks posed and determine how to manage the third-party relationship accordingly;

B. RISK MANAGEMENT

Not all relationships present the same level of risk, and therefore not all relationships require the same level or type of oversight or, risk management. As part of sound risk management, a banking organization analyzes the risks associated with each third-party relationship and tailors risk management practices, commensurate with the banking organization's size, complexity, and risk profile and with the nature of the third-party relationship. Maintaining a complete inventory of its third-party relationships and periodically conducting risk assessments for each third-party relationship supports a banking organization's

⁶ This guidance is relevant for all third-party relationships, including situations in which a supervised banking organization provides services to another supervised banking organization.

⁶ The term "business arrangement" is meant to be interpreted broadly and is synonymous with the term "third-party relationship."

determination of whether risks have changed over time and to update risk management practices accordingly.

As part of sound risk management, banking organizations engage in more comprehensive and rigorous oversight and management of third-party relationships that support higher risk activities, including critical activities. Characteristics of critical activities may include those activities that could:

- cause a banking organization to face significant risk if the third party fails to meet expectations;
- have significant customer impacts; or
- have a significant impact on a banking organization's financial condition or operations.

It is up to each banking organization to identify its critical activities and third-party relationships that support these critical activities. Notably, an activity that is critical for one banking organization may not be critical for another. Some banking organizations may assign a criticality or risk level to each third-party relationship, whereas others identify critical activities and those third parties that support such activities. Regardless of a banking organization's approach, a key element of effective risk management is applying a sound methodology to designate which activities and third-party relationships receive more comprehensive oversight.

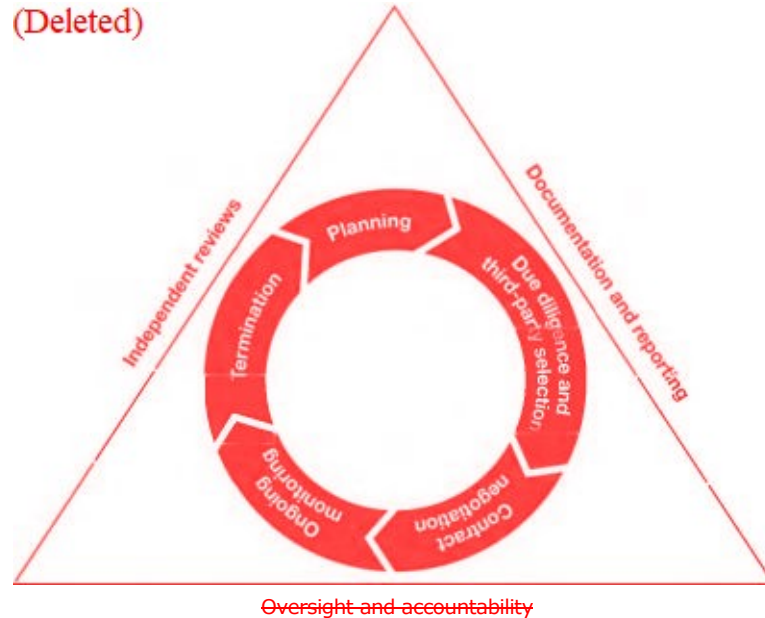
C. THIRD-PARTY RELATIONSHIP LIFE CYCLE

Effective Sound third-party risk management ~~generally follows a continuous life cycle for~~ commonly begins with identifying and categorizing third-party relationships. ~~The stages of the risk management life cycle. Maintaining an inventory~~ of third-party relationships ~~are shown in Figure 1 and detailed below. The degree to which the examples of considerations discussed in this guidance are relevant to each~~ may be useful for managing third-party risks. For example, a large or complex banking organization ~~is based on specific facts and circumstances and these examples may not apply to all of a banking organization's~~ with multiple higher-risk third-party relationships.

may benefit from a periodically updated and detailed inventory that maps individual subcomponents of a third-party relationship to various banking organization business units, reporting lines, or other accountability mechanisms, while a community bank may benefit from a simpler or streamlined format that ~~It is important to involve staff with the requisite knowledge and skills in each stage of the risk management life cycle. A banking organization may involve experts across disciplines, such as compliance, risk, or technology, as well as legal counsel, and may engage external support when helpful to supplement the qualifications and technical expertise of in-house staff.¹~~

¹ When a banking organization uses a third-party assessment service or utility, it has a business arrangement with that entity. Therefore, the arrangement should be incorporated into the banking organization's third-party risk management processes.

Figure 1: Stages of the Risk-Management Life Cycle



Source: Board, FDIC, and OCC

I. Planning

As part of sound risk management, effective planning allows a banking organization to evaluate and consider how to manage risks before entering into a third-party relationship. Certain third parties, such as those that support a banking organization's higher-risk activities, including critical activities, typically warrant a greater degree of planning and consideration. For example, when critical activities are involved, plans may be presented to and approved by a banking organization's board of directors (or a designated board committee). allows its management to quickly assess relevant third-party relationships at a higher level. Banking organizations may decide not to maintain extensive inventories of relationships posing limited risk, such as those related to administrative or clerical tasks, professional support services (including auditing and legal advice), or office support services (including physical security).

ii. Risk Identification

After identifying its prospective or existing third-party relationships, a banking organization generally identifies relevant risks. Risks presented by third-party relationships are varied and may change over time or may not be immediately apparent. For example, a core service

provider, given the extent of its services, is likely to touch on many components of a banking organization's operational risk, in addition to other risks. A facilities maintenance third party, by contrast, may implicate only a relatively limited range of risks, such as physical access risk. A banking organization typically has the experience and relevant information for identifying the most salient risks, especially where relevant staff members, such as subject-matter experts, are included in the risk identification process. It is unlikely that a banking organization could identify all possible risks and it is not expected to do so; however, identifying the most relevant risks is generally part of effective third-party risk management.

iii. Risk Assessment

Not all third-party relationships present the same level of risk, and there is not only one way to properly conduct risk assessments. Risk assessments commonly take into account both the magnitude of harm the third-party relationship could cause the banking organization or its customers and the likelihood that the harm will occur. A banking organization's higher-risk third-party relationships could include those (1) that, if disrupted, subjected to attack, conducted in breach of the terms of any applicable contract, or otherwise performed in a manner in which non-business-as-usual circumstances prevail, could cause the banking organization to incur an actual non-trivial violation of law or regulation, pose material harm to the financial condition of the banking organization, or result in a significant disruption to the banking organization's operations or customers; and (2) where there is a material likelihood that such legal or regulatory violation, financial harm, or operational disruption may occur under current or reasonably foreseeable conditions.

While certain third-party relationships, such as core processing service provider relationships, are likely to be assessed by most banking organizations as higher risk,¹¹ other relationships may be assessed as higher risk by one banking organization but not by another.¹²

Some banking organizations may conduct a risk assessment for an overall third-party relationship, considering all activities conducted by the third party, while other banking organizations may conduct the assessment on a per-activity basis.¹³

Certain third-party relationships may be less likely to be assessed as higher risk. For example, many banking organizations contract with affiliated entities that operate within an enterprise-wide risk management framework to perform various services. Use of such affiliate arrangements can help a banking organization and its related entities more efficiently organize operations and maximize efficiencies. Such services, when conducted within an organization-wide enterprise risk management framework with which the banking organization is familiar, may be lower-risk and can enable the banking organization to rely on alternative oversight mechanics such as staff overlaps.

Additionally, certain third parties may themselves be entities that are heavily regulated and supervised by one or more state or federal regulators. As such, in certain

¹¹ As risk assessments are typically tailored to an individual banking organization's circumstances, a banking organization may determine, for example, that a core bank processor that provides services for only a limited portion of the banking organization's business represents a relatively lower-risk relationship compared to a core bank processor that provides services for the majority of a banking organization's business, depending on the relevant factors.

¹² Relatedly, many third parties may connect to a banking organization's information technology systems and networks, including through application programming interfaces, vendor portals, or other means. These access points may be exploited; however, a third party with access to a banking organization's systems or networks that do not hold critical data and are appropriately segmented is not necessarily higher risk, and banking organizations may, for example, be able to manage any related risks primarily through safe and sound cybersecurity risk management rather than through extensive third-party risk management.

¹³ The agencies have also observed, for example, that banking organizations will commonly take the overall third-party relationship into account in circumstances where the bank is exposed to concentration risk from a third party due to relying on the third party for extensive services.

circumstances, a banking organization may consider a third party's regulatory status and

regulatory obligations as part of its risk assessment. However, supervisory and regulatory

schemes may differ materially between entity types and with regard to applicable legal

requirements, regulatory or supervisory authority, the nature of the activity, or other factors, and

thus the mere presence of a regulatory scheme may not necessarily serve to mitigate risks relevant to a banking organization.¹⁴ Further, even regulated entities could nevertheless operate in a less than satisfactory condition, which could increase the risk they pose to the banking organization.

A banking organization may obtain further information that warrants adjusting its initial risk assessment after it performs due diligence and engages in contractual negotiations. Additionally, changing circumstances, an expanded or a renegotiated contract, or a banking organization's experience overseeing a third-party relationship, among other factors, may be indicators that a third-party relationship's risk has changed since the banking organization's initial assessment and may benefit from being reassessed. The decision of whether and how frequently to re-assess a banking organization's risks related to a third-party relationship may take into account additional factors such as changes in reliance on the third party, any new or existing identified concerns with the third party, or a change in the level(s) and type(s) of services provided by the third party.

Banking organizations typically have extensive experience assessing risks as part of their business. As such, examiners will give due consideration to a banking

¹⁴ No supervisory or regulatory agency is responsible for a banking organization's third-party risk management. Banking organizations should not rely on the existence of any agency supervision or regulation as a substitute for managing third-party risk or as a proxy for whether such third parties provide services in a safe and sound manner.

organization's reasonable judgment regarding the banking organization's risk assessments.¹⁵

2. Risk Oversight

Effective risk management involves overseeing third-party relationships in a manner proportionate to the risks they present and consistent with the banking organization's risk appetite and tolerances. Banking organizations typically prioritize oversight of higher-risk third-party

relationships and establish more rigorous oversight practices for such relationships. A banking organization may tailor its oversight in a manner commensurate with the banking organization's size, complexity, and risk profile, as well as with the nature of the third-party relationship. For example, the level of oversight appropriate for a banking organization with multiple business lines, operating subsidiaries, and a diversified customer base may not be appropriate for a banking organization with a less complex business model. Risk management practices that do not prioritize and tailor according to risk could increase the magnitude and likelihood of harm arising from higher-risk relationships due to inappropriate levels of attention and oversight.

The following discusses oversight at a high level. The examples provided are illustrative only, may not be relevant to all banking organizations or relationships, and are not comprehensive.

i. Due Diligence and Third Party Selection

~~Depending on the degree of risk and complexity of the third-party relationship, a banking organization typically considers the following factors, among others, in planning~~

~~Understanding the strategic purpose of the business arrangement and how the arrangement aligns with a banking organization's overall strategic goals, objectives, risk appetite, risk profile, and broader corporate policies;~~

- ~~▪ Identifying and assessing the benefits and the risks associated with the business arrangement and determining how to appropriately manage the identified risks;~~
- ~~▪ Considering the nature of the business arrangement, such, as volume of activity, use of subcontractor(s), technology needed, interaction with customers, and use of foreign-based third parties;¹~~

~~The term "foreign-based third-party" refers to third parties whose servicing operations are located in a foreign country and subject to the law and jurisdiction of that country. Accordingly, this term does not include a U.S.-based~~

- ~~▪ Evaluating the estimated costs, including estimated direct contractual costs and indirect costs expended to augment or alter banking organization staffing, systems, processes, and technology;~~
- ~~▪ Evaluating how the third-party relationship could affect banking organization employees, including dual employees,¹ and what transition steps are needed for the banking organization to manage the impacts when activities currently conducted internally are outsourced;~~

- Assessing a potential third party's impact on customers, including access to or use of those customers' information, third-party interaction with customers, potential for consumer harm, and handling of customer complaints and inquiries;
- Understanding potential information security implications, including access to the banking organization's systems and to its confidential information;
- Understanding potential physical security implications, including access to the banking organization's facilities;
- Determining how the banking organization will select, assess, and oversee the third party, including monitoring the third party's compliance with applicable laws, regulations, and contractual provisions, and requiring remediation of compliance issues that may arise;
- 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 over time 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.

2. *Due Diligence and Third-Party Selection*

Conducting due diligence on third parties before selecting and entering into third-party relationships is an important part of sound risk management. It provides management with the information needed about potential third parties to determine if a relationship would help achieve a banking organization's strategic and financial goals. The due diligence process also provides the banking organization with the information needed to evaluate whether it can appropriately identify, monitor, and control risks associated with the particular third-party relationship. Due diligence includes assessing the third party's ability to: perform the activity as expected, adhere to a banking organization's policies related to the activity, comply with all applicable laws and

subsidiary of a foreign firm because its servicing operations are subject to U.S. laws. This term does include U.S. third parties to the extent that their actual servicing operations are located in or subcontracted to entities domiciled in a foreign country and subject to the law and jurisdiction of that country.

^aDual employees are employed by both the banking organization and the third party.

regulations, and conduct the activity in a safe and sound manner Relying solely on experience with or prior knowledge of a third party is not an adequate proxy for performing appropriate due diligence, as due diligence should be tailored to the specific activity to be performed by the third party.

The scope and degree of due diligence should be commensurate with the level of risk and complexity of the third-party relationship. More comprehensive due diligence is particularly important when a third party supports higher-risk activities, including critical activities. 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.

~~In some instances, a banking organization may not be able to obtain the desired due diligence information from a third party. For example, the third party may not have a long operational history, may not allow on-site visits, or may not share (or be permitted to share) information that a banking organization requests. While the methods and scope of due diligence may differ, it is important for the banking organization to identify and document any limitations of its due diligence, understand the risks from such limitations, and consider alternatives as to how to mitigate the risks. In such situations, a banking organization may, for example, obtain alternative information to assess the third party, implement additional controls on or monitoring of the third party to address the information limitation, or consider using a different third party.~~

~~A banking organization may use the services of industry utilities or consortiums, consult with other organizations,¹⁰ or engage in joint efforts to supplement its due diligence. As the activity to be performed by the third party may present a different level of risk to each banking organization, it is important to evaluate the conclusions from such supplemental efforts based on the banking organization's own specific circumstances and performance criteria for the activity. Effective risk management processes include evaluating the capabilities of any external party conducting the supplemental efforts, understanding how such supplemental efforts relate to the banking organization's planned use of the third party, and assessing the risks of relying on the supplemental efforts. Use of such external parties to conduct supplemental due diligence does not abrogate the responsibility of the banking organization to manage third-party relationships in a safe and sound manner and consistent with applicable laws and regulations.~~

~~Depending on the degree of risk and complexity of the third-party relationship, a banking organization typically considers the following factors, among others, as part of due diligence:~~

~~*a. Strategies and Goals*~~

~~A review of the third party's overall business strategy and goals helps the banking organization to understand: (1) how the third party's current and proposed strategic business arrangements (such as mergers, acquisitions, and partnerships) may affect the activity, and (2) the third party's service philosophies, quality initiatives, and employment policies and practices (including its diversity policies and practices). Such information may assist a banking~~

¹⁰ 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" (April 2000), available at https://www.ftc.gov/sites/default/files/documents/public_events/joint-ynaue-hearings-antitrust-guidelines-collaboration-among-competitors/ftcdoiguidelines-2.pdf.

Due diligence is the process by which a banking organization ~~to determine whether the~~
~~third party can~~assesses a third party's ability to perform the activity ~~in a manner that is~~
~~consistent with~~as expected, adhere to the banking organization's ~~broader corporate policies and~~
~~practices.~~

¹⁵ To what extent would it be helpful for the guidance to include a list of characteristics that generally indicate that a third-party relationship is high risk, and if so, what characteristics should be included?
policies, comply with applicable laws and regulations, and conduct the activity in a safe and
sound manner. As with all third-party oversight, the amount of due diligence that is warranted
depends on the risk presented by the third-party relationship and the banking organization's
individual business needs. In the case of lower-risk third-party relationships, a banking
organization may be more comfortable with relying either on less-detailed due diligence
information or on public or alternative sources, as compared to its higher-risk relationships.
Depending on the circumstances, this relatively less-detailed level of due diligence may be
sufficient for the banking organization to determine that the third party is likely able to perform
the services being contracted for (including, for example, that the third party has sufficient
staffing and capabilities) and that further due diligence may not provide appreciable benefits to
the banking organization.

Depending on the circumstances, due diligence may involve assessing a third party's
financial condition; business experience and key personnel; staffing capabilities and
qualifications, including training relevant to the banking organization's business; legal and
regulatory compliance; insurance coverage; and information security and cybersecurity
capabilities and track record, as applicable. Due diligence may also evaluate the effectiveness
of the third party's relevant risk management practices and capabilities, including policies,

procedures, and internal controls and whether there is an alignment with the banking organization's own applicable policies, procedures, controls, strategies, and expectations.

In some cases, a banking organization may not be able to obtain certain due diligence information from a third party. For example, a third party may not have a long operational history, may not permit on-site visits, or may not share (or is not permitted to share) information that the banking organization requests, but a banking organization may determine that other factors offset or compensate for those limitations. A banking organization may also have limited negotiating power with some third parties, which may amplify these difficulties. Even when unable to meet all of its due diligence objectives, a banking organization may still collect sufficient information, including from supplemental sources, to be able to determine that engaging with the third party is within the banking organization's risk appetite and tolerances. Outside information sources may be relied upon in certain contexts, including, for example, information or feedback obtained through banking organizations or trade groups, review of available public sources, or, in the case of a third party with a limited operational history, the overall qualifications and experience of management and employees of the third party in performing the services that would be provided. Similarly, external industry experts familiar with the third party, the relevant industry, or with market standard terms and practices may also supplement or help a banking organization conduct due diligence. However, where the third party is unable or unwilling to provide information or other cooperation reasonably necessary for the banking organization to conduct due diligence, ongoing monitoring and risk assessments, the alternative sources described above may not be sufficient to allow the banking organization to engage with the third party within its risk appetite and tolerances.

b. Legal and Regulatory Compliance

A review of any legal and regulatory compliance considerations associated with engaging a third party allows a banking organization to evaluate whether it can appropriately mitigate risks associated with the third-party relationship. This may include (1) evaluating the third party's ownership structure (including identifying any beneficial ownership, whether public or private, foreign, or domestic ownership) and whether the third party has the necessary legal authority to perform the activity, such as any necessary licenses or corporate powers; (2) determining whether the third party itself or any owners are subject to sanctions by the Office of Foreign Assets Control; (3) determining whether the third party has the expertise, processes, and controls to enable the banking organization to remain in compliance with applicable domestic and international laws and regulations; (4) considering the third party's responsiveness to any compliance issues (including violations of law or regulatory actions) with applicable supervisory agencies and self-regulatory organizations, as appropriate; and (5) considering whether the third party has identified, and articulated a process to mitigate, areas of potential consumer harm.

c. Financial Condition

An assessment of a third party's financial condition through review of available financial information, including audited financial statements, annual reports, and filings with the U.S. Securities and Exchange Commission (SEC), among others, helps a banking organization evaluate whether the third party has the financial capability and stability to perform the activity. Where relevant and available, a banking organization may consider other types of information such as access to funds, expected growth, earnings, pending litigation, unfunded liabilities, reports from debt rating agencies, and other factors that may affect the third party's overall financial condition.

d. Business Experience

An evaluation of a third party's: (1) depth of resources (including staffing); (2) previous experience in performing the activity; and (3) history of addressing customer complaints or litigation and subsequent outcomes, helps to inform a banking organization's assessment of the third party's ability to perform the activity effectively. Another consideration may include whether there have been significant changes in the activities offered or in its business model. Likewise, a review of the third party's websites, marketing materials, and other information related to banking products or services may help determine if statements and assertions accurately represent the activities and capabilities of the third party.

e. Qualifications and Backgrounds of Key Personnel and Other Human Resources Considerations

An evaluation of the qualifications and experience of a third party's principals and other key personnel related to the activity to be performed provides insight into the capabilities of the third party to successfully perform the activities. An important consideration is whether the third party and the banking organization, as appropriate, periodically conduct background checks on

the third party's key personnel and contractors who may have access to information technology systems or confidential information. Another important consideration is whether there are procedures in place for identifying and removing the third party's employees who do not meet minimum suitability requirements or are otherwise barred from working in the financial services sector. Another consideration is whether the third party has training to ensure that its employees understand their duties and responsibilities and are knowledgeable about applicable laws and regulations as well as other factors that could affect performance or pose risk to the banking organization. Finally, an evaluation of the third party's succession and redundancy planning for key personnel, and of the third party's processes for holding employees accountable for compliance with policies and procedures, provides valuable information to the banking organization.

f. Risk Management

Appropriate due diligence includes an evaluation of the effectiveness of a third party's overall risk management, including policies, processes, and internal controls, and alignment with applicable policies and expectations of the banking organization surrounding the activity. This would include an assessment of the third party's governance processes, such as the establishment of clear roles, responsibilities, and segregation of duties pertaining to the activity. It is also important to consider whether the third party's controls and operations are subject to effective audit assessments, including independent testing and objective reporting of results and findings. Banking organizations also gain important insight by evaluating processes for escalating, remediating, and holding management accountable for concerns identified during audits, internal compliance reviews, or other independent tests, if available. When relevant and available, a banking organization may consider reviewing System and Organization Control (SOC) reports and any conformity assessment or certification by independent third parties related to relevant domestic or international standards." In such cases, the banking organization may also consider whether the scope and the results of the SOC reports, certifications, or assessments are relevant to the activity to be performed or suggest that additional scrutiny of the third party or any of its contractors may be appropriate.

g. Information Security

Understanding potential information security implications, including access to a banking organization's systems and information, can help a banking organization decide whether or not to engage with a third party. Due diligence in this area typically involves assessing the third party's information security program, including its consistency with the banking organization's information security program, such as its approach to protecting the confidentiality, integrity, and availability of the banking organization's data. It may also involve determining whether there are any gaps that present risk to the banking organization or its customers and considering the extent to which the third party applies controls to limit access to the banking organization's data and transactions, such as multifactor authentication, end-to-end encryption, and secure source code management. It also aids a banking organization when determining whether the third party keeps informed of, and has sufficient experience in identifying, assessing, and

¹¹ For example, those of the National Institute of Standards and Technology, Accredited Standards Committee X9, and the International Standards Organization.

mitigating, known and emerging threats and vulnerabilities. As applicable, assessing the third party's data, infrastructure, and application security programs, including the software development life cycle and results of vulnerability and penetration tests, can provide valuable information regarding information technology system vulnerabilities. Finally, due diligence can help a banking organization evaluate the third party's implementation of effective and sustainable corrective actions to address any deficiencies discovered during testing.

h. Management of Information Systems

It is important to review and understand the third party's business processes and information systems that will be used to support the activity. When technology is a major component of the third party relationship, an effective practice is to review both the banking organization's and the third party's information systems to identify gaps in service-level expectations, business process and management, and interoperability issues. It is also important to review the third party's processes for maintaining timely and accurate inventories of its technology and its contractor(s). A banking organization also benefits from understanding the third party's measures for assessing the performance of its information systems.

i. Operational Resilience

An assessment of a third party's operational resilience practices supports a banking organization's evaluation of a third party's ability to effectively operate through and recover from any disruption or incidents, both internal and external.¹² Such an assessment is particularly important where the impact of such disruption could have an adverse effect on the banking organization or its customers, including when the third party interacts with customers. It is important to assess options to employ if the third party's ability to perform the activity is impaired and to determine whether the third party maintains appropriate operational resilience and cybersecurity practices, including disaster recovery and business continuity plans that specify the time frame to resume activities and recover data. To gain additional insight into a third party's resilience capabilities, a banking organization may review (1) the results of operational resilience and business continuity testing and performance during actual disruptions; (2) the third party's telecommunications redundancy and resilience plans; and (3) 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. Other considerations related to operational resilience include (1) dependency on a single provider for multiple activities; and (2) interoperability or potential end-of-life issues with the software programming language, computer platform, or data storage technologies used by the third party.

j. Incident Reporting and Management Processes

Review and consideration of a third party's incident reporting and management processes is helpful to determine whether there are clearly documented processes, timelines, and accountability for identifying, reporting, investigating, and escalating incidents. Such review

¹³. Disruptive events could include technology-based failures, human error, cyber incidents, pandemic outbreaks, and natural disasters.

assists in confirming that the third party's escalation and notification processes meet the banking organization's expectations and regulatory requirements.¹³

k. Physical Security

It is important to evaluate whether the third party has sufficient physical and environmental controls to protect the safety and security of people (such as employees and customers), its facilities, technology systems, and data, as applicable. This would typically include a review of the third party's employee on- and off-boarding procedures to ensure that physical access rights are managed appropriately.

l. Reliance on Subcontractors¹⁴

An evaluation of the volume and types of subcontracted activities and the degree to which the third party relies on subcontractors helps inform whether such subcontracting arrangements pose additional or heightened risk to a banking organization. This typically includes an assessment of the third party's ability to identify, manage, and mitigate risks associated with subcontracting, including how the third party selects and oversees its subcontractors and ensures that its subcontractors implement effective controls. Other important considerations include whether additional risk is presented by the geographic location of a subcontractor or dependency on a single provider for multiple activities.

m. Insurance Coverage

An evaluation of whether the third party has existing insurance coverage helps a banking organization determine the extent to which potential losses are mitigated, including losses posed by the third party to the banking organization or that might prevent the third party from fulfilling its obligations to the banking organization. Such losses may be attributable to dishonest or negligent acts; fire, floods, or other natural disasters; loss of data; and other matters. Examples of insurance coverage may include fidelity bond; liability; property hazard and casualty; and areas that may not be covered under a general commercial policy, such as cybersecurity or intellectual property.

n. Contractual Arrangements with Other Parties

A third party's commitments to other parties may introduce potential legal, financial, or operational implications to the banking organization. Therefore, it is important to obtain and evaluate information regarding the third party's legally binding arrangements with subcontractors or other parties to determine whether such arrangements may create or transfer risks to the banking organization or its customers.

¹⁴ See, e.g., *15 C.F.R. § 1.101*.

¹³. For example, regulatory requirements regarding incident notification include the FBAs' "Computer Security Incident Notification Rule." See 12 CFR part 53 (OCC); 12 CFR 225, subpart N (Board); 12 CFR 304, subpart C (FDIC).

¹⁴. Third parties may enlist the help of suppliers, service providers, or other organizations, which this guidance collectively refers to as subcontractors.

3ii. Contract Negotiation

When evaluating whether to enter into a relationship with a third party, a banking organization typically determines whether a written contract is needed, and if the proposed contract can meet the banking organization's business goals and risk management needs. After such determination, a banking organization typically negotiates contract provisions that will facilitate effective risk management and oversight and that specify the expectations and obligations of both the banking organization and the third party. A banking organization may tailor the level of detail and comprehensiveness of such contract provisions based on the risk and complexity posed by the particular third-party relationship.

While third parties may initially offer a standard contract, a banking organization may seek to request modifications, additional contract provisions, or addendums to satisfy its needs. In difficult contract negotiations, including when a banking organization has limited negotiating power, it is important for the banking organization to understand any resulting limitations and consequent risks. Possible actions that a banking organization might take in such circumstances include determining whether the contract can still meet the banking organization's needs, whether the contract would result in increased risk to the banking organization, and whether residual risks are acceptable. If the contract is unacceptable for the banking organization, it may consider other approaches, such as employing other third parties or conducting the activity in-house. In certain circumstances, banking organizations may gain an advantage by negotiating contracts as a group with other organizations.

Effective third-party risk management generally involves negotiating contract provisions designed to facilitate effective risk management, oversight, and performance, in line both with the banking organization's risk identification and assessment and with the results of its due diligence, and that specify the expectations and obligations of both the banking organization and the third party.

There are no generally applicable expected contract terms for third-party relationships—even for higher-risk relationships—and banking organizations typically tailor their contract negotiations and provisions to their individual needs and circumstances, commensurate with the banking organization's size, complexity, and risk profile and the nature of its third-party

relationships. As such, the presence or absence of a specific contractual term that an examiner may believe to be contrary to best practices would not alone be a sufficient basis for an examiner to communicate an adverse finding related to a banking organization's third-party risk management practices.

Depending on the circumstances, the terms of the contract may allocate responsibility between the parties. A service level agreement can define performance measures, which can assist banking organizations in evaluating a third party's performance and compliance with applicable laws and regulations. Other items that may be relevant for a banking organization to consider during contract negotiations include, depending on the circumstances, confidentiality and information security, and, as discussed below, use of subcontractors, operational resilience plans, and termination provisions.

Third parties often offer standard contracts. Banking organizations can assess whether these standard terms adequately address their specific circumstances and risks. For example, banking organizations may determine that they need to request modifications, additional contract provisions, or activity-specific addenda to strengthen oversight for areas that pose higher risk to the banking organization. For lower-risk relationships, a banking organization may determine that standard form contracts are sufficient. Alternatively, a banking organization may focus negotiations on a narrow subset of contractual provisions most relevant to the risks presented by the third-party relationship and that could provide the banking organization sufficient comfort that the services provided through the third-party relationship will be conducted in a manner that meets its needs and that is within its risk appetite and tolerances.

~~It is important that~~ When a banking organization ~~understand the benefits and risks associated with engaging third parties and particularly before executing contracts involving higher risk activities, including critical activities. As part of its oversight responsibilities, the board of directors should be aware of and, as appropriate, may approve or delegate approval of contracts involving higher risk activities. Legal counsel review may also be warranted prior to~~ finalization, has limited negotiating power relative to a third party, it may be unable to negotiate all of its desired contractual provisions. The banking organization may still reasonably proceed with the relationship if, for example, the banking organization has a reasonable understanding of the risks relevant to the third-party relationship and any residual risks are in line with the banking organization's risk appetite and tolerances, especially if there are limited alternative options. In certain circumstances, banking organizations may also be able to gain an advantage by negotiating contracts as a group with other organizations, as discussed below.

~~Periodic reviews of executed~~ Maintaining an inventory of and periodically reviewing third party contracts ~~allow~~ may assist a banking organization ~~to confirm~~ in confirming that existing provisions continue to address pertinent ~~risk controls and legal protections~~ risks. If new risks are identified, a banking organization may consider ~~renegotiating a contract~~ whether it is appropriate to renegotiate or terminate a third-party relationship.

~~Depending on the degree of risk and complexity of the third party relationship, a banking organization typically considers the following factors, among others, during contract negotiations:~~

~~a. Nature and Scope of Arrangement~~

~~In negotiating a contract, it is helpful for a banking organization to clearly identify the rights and responsibilities of each party. This typically includes specifying the nature and scope of the business arrangement. Additional considerations may also include, as applicable, a description of (1) ancillary services such as software or other technology support, maintenance,~~

and customer service; (2) the activities the third party will perform; and (3) the terms governing the use of the banking organization's information, facilities, personnel, systems, intellectual property, and equipment, as well as access to and use of the banking organization's or customers' information. If dual employees will be used, it may also be helpful to specify their responsibilities and reporting lines. It is also important for a banking organization to understand how changes in business and other circumstances may give rise to the third party's rights to terminate or renegotiate the contract.

b. Performance Measures or Benchmarks

For certain relationships, clearly defined performance measures can assist a banking organization in evaluating the performance of a third party. In particular, a service level agreement between the banking organization and the third party can help specify the measures surrounding the expectations and responsibilities for both parties, including conformance with policies and procedures and compliance with applicable laws and regulations. Such measures can be used to monitor performance, penalize poor performance, or reward outstanding performance. It is important to negotiate performance measures that do not incentivize imprudent performance or behavior, such as encouraging processing volume or speed without regard for accuracy, compliance requirements, or adverse effects on the banking organization or customers.

e. Responsibilities for Providing, Receiving, and Retaining Information

It is important to consider contract provisions that specify the third party's obligation for retention and provision of timely, accurate, and comprehensive information to allow the banking organization to monitor risks and performance and to comply with applicable laws and regulations. Such provisions typically address:

- The banking organization's ability to access its data in an appropriate and timely manner;
- The banking organization's access to, or use of, the third party's data and any supporting documentation, in connection with the business arrangement;
- The banking organization's access to, or use of, its own or the third party's data and how such data and supporting documentation may be shared with regulators in a timely manner as part of the supervisory process;
- Whether the third party is permitted to resell, assign, or permit access to customer data, or the banking organization's data, metadata, and systems, to other entities;
- Notification to the banking organization whenever compliance lapses, enforcement actions, regulatory proceedings, or other events pose a significant risk to the banking organization or customers;

- Notification to the banking organization of significant strategic or operational changes, such as mergers, acquisitions, divestitures, use of subcontractors, key personnel changes, or other business initiatives that could affect the activities involved; and
- Specification of the type and frequency of reports to be received from the third party, as appropriate. This may include performance reports, financial reports, security reports, and control assessments.

d. The Right to Audit and Require Remediation

To help ensure that a banking organization has the ability to monitor the performance of a third party, a contract often establishes the banking organization's right to audit and provides for remediation when issues are identified. Generally, a contract includes provisions for periodic, independent audits of the third party and its relevant subcontractors, consistent with the risk and complexity of the third party relationship. Therefore, it would be appropriate to consider whether contract provisions describe 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, or other financial and operational reviews). Such contract provisions may also 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

A banking organization is responsible for conducting its activities in compliance with applicable laws and regulations, including those activities involving third parties. The use of third parties does not abrogate these responsibilities. Therefore, it is important for a contract to specify the obligations of the third party and the banking organization to comply with applicable laws and regulations. It is also important for the contract to provide the banking organization with the right to monitor and be informed about the third party's compliance with applicable laws and regulations, and to require timely remediation if issues arise. Contracts may also reflect considerations of relevant guidance and self-regulatory standards, where applicable.

f. Costs and Compensation

Contracts that clearly describe all costs and compensation arrangements help reduce misunderstandings and disputes over billing and help ensure that all compensation arrangements are consistent with sound banking practices and applicable laws and regulations. Contracts commonly describe compensation and fees, including cost schedules, calculations for base services, and any fees based on volume of activity and for special requests. Contracts also may specify the conditions under which the cost structure may be changed, including limits on any cost increases. During negotiations, a banking organization should confirm that a contract does not include incentives that promote inappropriate risk taking by the banking organization or the third party. A banking organization should also consider whether the contract includes burdensome upfront or termination fees, or provisions that may require the banking organization to reimburse the third party. Appropriate provisions indicate which party is responsible for payment of legal, audit, and examination fees associated with the activities involved. Another

consideration is outlining cost and responsibility for purchasing and maintaining hardware and software, where applicable.

g. Ownership and License

In order to prevent disputes between the parties regarding the ownership and licensing of a banking organization's property, it is common for a contract to state the extent to which 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, and copyrighted material. Provisions that indicate whether any data generated by the third party become the banking organization's property help avert misunderstandings. It is also important to include appropriate warranties on the part of the third party related to its acquisition of licenses or subscriptions for use of any intellectual property developed by other third parties. When the banking organization purchases software, it is important to consider a provision to 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

With respect to contracts with third parties, there may be increased risks related to the sensitivity of non-public information or access to infrastructure. Effective contracts typically prohibit the use and disclosure of banking organization and customer 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 personally identifiable information, contract provisions are important to ensure that the third party implements and maintains appropriate security measures to comply with applicable laws and regulations.

Another important provision is one that specifies when and how the third party will disclose, in a timely manner, information security breaches or unauthorized intrusions. Considerations may include the types of data stored by the third party, legal obligations for the banking organization to disclose the breach to its regulators or customers, the potential for consumer harm, or other factors. Such provisions typically stipulate that the data intrusion notification to the banking organization include estimates of the effects on the banking organization and its customers and specify corrective action to be taken by the third party. They also 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. Typically, such provisions 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

Both internal and external factors or incidents (for example, natural disasters or cyber incidents) may affect a banking organization or a third party and thereby disrupt the third party's performance of the activity. Consequently, an effective contract provides for continuation of the activity in the event of problems affecting the third party's operations, including degradations or interruptions in delivery. As such, it is important for the contract to address the third party's

responsibility for appropriate controls to support operational resilience of the services, such as protecting and storing programs, backing up datasets, addressing cybersecurity issues, and maintaining current and sound business resumption and business continuity plans.

To help ensure maintenance of operations, 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. Contracts may also stipulate whether and how often the banking organization and the third party will jointly test business continuity plans. Another consideration is whether the contract provides for the transfer of 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.

j. Indemnification and Limits on Liability

Incorporating indemnification provisions into a contract may reduce the potential for a banking organization to be held liable for claims and be reimbursed for damages arising from a third party's misconduct, including negligence and violations of laws and regulations. As such, it is important to consider whether indemnification clauses specify the extent to which the banking organization will be held liable for claims or be reimbursed for damages based on the failure of the third party or its subcontractor to perform, including failure of the third party to obtain any necessary intellectual property licenses. Such consideration typically includes an assessment of whether any limits on liability are in proportion to the amount of loss the banking organization might experience as a result of third party failures, or whether indemnification clauses require the banking organization to hold the third party harmless from liability.

k. Insurance

One way in which a banking organization can protect itself against losses caused by or related to a third party and the products and services provided through third party relationships is by including insurance requirements in a contract. These provisions typically require the third party to (1) maintain specified types and amounts of insurance (including, if appropriate, naming the banking organization as insured or additional insured); (2) notify the banking organization of material changes to coverage; and (3) provide evidence of coverage, as appropriate. The type and amount of insurance coverage should be commensurate with the risk of possible losses, including those caused by the third party to the banking organization or that might prevent the third party from fulfilling its obligations to the banking organization, and the activities performed.

l. Dispute Resolution

Disputes regarding a contract can delay or otherwise have an adverse impact upon the activities performed by a third party, which may negatively affect the banking organization. Therefore, a banking organization may want to consider whether the contract should establish a dispute resolution process 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. It is important to also

understand whether the contract contains provisions that may impact the banking organization's ability to resolve disputes in a satisfactory manner, such as provisions addressing arbitration or forum selection.

m. Customer Complaints

Where customer interaction is an important aspect of the third-party relationship, a banking organization may find it useful to include a contract provision to ensure that customer complaints and inquiries are handled properly. Effective contracts typically specify whether the banking organization or the third party is responsible for responding to customer complaints or inquiries. If it is the third party's responsibility, it is important to include provisions for the third party to receive and respond to customer complaints and inquiries in a timely manner and to provide the banking organization with sufficient, timely, and usable information to analyze customer complaint and inquiry activity and associated trends. If it is the banking organization's responsibility, it is important to include provisions for the banking organization to receive prompt notification from the third party of any complaints or inquiries received by the third party.

n. Subcontracting

Third-party relationships may involve subcontracting arrangements, which can result in risk due to the absence of a direct relationship between the banking organization and the subcontractor, further lessening the banking organization's direct control of activities. The impact on a banking organization's ability to assess and control risks may be especially important if the banking organization uses third parties for higher-risk activities, including critical activities. For this reason, a banking organization may want to address when and how the third party should notify the banking organization of its use or intent to use a subcontractor and whether specific subcontractors are prohibited by the banking organization. Another important consideration is whether the contract should prohibit assignment, transfer, or subcontracting of the third party's obligations to another entity without the banking organization's consent. Where subcontracting is integral to the activity being performed for the banking organization, it is important to consider more detailed contractual obligations, such as reporting on the subcontractor's conformance with performance measures, periodic audit results, and compliance with laws and regulations. Where appropriate, a banking organization may consider including a provision that states 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. It may also be appropriate to reserve the right to terminate the contract without penalty if the third party's subcontracting arrangements do not comply with contractual obligations.

o. Foreign-Based Third Parties

In contracts with foreign-based third parties, it is important to consider choice of law and jurisdictional provisions that provide dispute adjudication under the laws of a single jurisdiction, whether in the United States or elsewhere. When engaging with foreign-based third parties, or where contracts include a choice of law provision that includes a jurisdiction other than the United States, it is important to understand that such contracts and covenants may be subject to

~~the interpretation of foreign courts relying on laws in those jurisdictions. It may be warranted to seek legal advice on the enforceability of the proposed contract with a foreign-based third party and other legal ramifications, including privacy laws and cross-border flow of information.~~

~~*p. Default and Termination*~~

~~Contracts can protect the ability of the banking organization to change third parties when appropriate without undue restrictions, limitations, or cost. An effective contract stipulates what constitutes default, identifies remedies, allows opportunities to cure defaults, and establishes the circumstances and responsibilities for termination. Therefore, it is important to consider including contractual provisions that:~~

- ~~• Provide termination and notification requirements with reasonable time frames to allow for the orderly transition of the activity, when desired or necessary, without prohibitive expense;~~
- ~~• Provide for the timely return or destruction of the banking organization's data, information, and other resources;~~
- ~~• Assign all costs and obligations associated with transition and termination; and~~
- ~~• Enable the banking organization to terminate the relationship with reasonable notice and without penalty, if formally directed by the banking organization's primary federal banking regulator.~~

~~*q. Regulatory Supervision*~~

~~For relevant third-party relationships, it is important for contracts to stipulate that the performance of activities by third parties for the banking organization is subject to regulatory examination and oversight, including appropriate retention of, and access to, all relevant documentation and other materials.¹ This can help ensure that a third party is aware of its role and potential liability in its relationship with a banking organization.~~

4iii. Ongoing Monitoring

Ongoing monitoring is the process by which banking organizations assess and monitor third-party performance and changes in the risks posed by third-party relationships. It also includes any associated reporting to the board and senior management, as appropriate, in line with the banking organization's size, complexity, and risk profile, as well as the nature of its third-party relationships. Ongoing monitoring

~~Ongoing monitoring enables~~may enable a banking organization to: (1) confirm the quality ~~and sustainability~~ of a third party's controls and its ability to meet contractual obligations and

perform as expected; (2) ~~escalate~~identify significant issues or concerns, such as material or repeat audit findings, deterioration in financial condition, security breaches, data loss, service interruptions, compliance ~~lapses~~issues, customer complaints, changes to insurance coverage, or other indicators of increased risk; and (3) respond to such significant issues or concerns when identified.

~~Effective third-party risk management includes ongoing monitoring throughout the duration of a third-party relationship, commensurate with the level of risk and complexity of the relationship and the activity performed by the third party. Ongoing monitoring may be conducted on a periodic or continuous basis, and more comprehensive or frequent monitoring is appropriate when a third-party relationship supports higher-risk activities, including critical activities. Because both the level and types of risks may change over the lifetime of third-party relationships, banking organizations may adapt their ongoing monitoring practices accordingly, including changes to the frequency or type of information used in monitoring.~~

¹⁶ See 12 U.S.C. 1464(d)(7)(D) and 1867(e)(1).

~~Typical~~Examples of monitoring activities may include: (1) ~~review of~~reviews of updates to information utilized in due diligence and reports or data regarding the third party's performance and the effectiveness of its controls, including audits conducted by the third party (or an independent entity hired by the third party);¹⁶ (2) periodic visits and meetings with third-party representatives to discuss performance and operational issues; ~~and~~ (3) ~~regular~~periodic testing of the banking organization's controls that manage risks from its third-party relationships and, particularly when supporting higher-risk activities, including critical activities. In certain circumstances, ~~based on risk, a banking organization may also perform direct~~periodic testing of the third party's ~~own controls. To gain efficiencies or leverage specialized expertise, banking organizations may engage external resources, refer to conformity assessments or certifications, or collaborate when performing ongoing monitoring.~~¹⁶ To support effective monitoring, a services to the banking organization ~~dedicates sufficient staffing with the necessary expertise, authority, and accountability to perform a range of ongoing monitoring activities, such as those described~~

~~above.~~ to assess the third party's performance and effectiveness; (4) reviews of public filings or reports of examination arising from the agencies' standard supervisory processes for certain large third parties' provision of services, if applicable;¹⁷ and (5) reviews of customer complaints.

¹⁶ Banking organizations and bank service providers have incident notification obligations under the agencies' Computer Security Incident Notification Rule, which may also inform ongoing monitoring. See 12 CFR part 53 (OCC); 12 CFR 225, subpart N (Board); 12 CFR 304, subpart C (FDIC). See also, 12 CFR 748.1 for the NCUA's Cyber Incident Report Rule.

¹⁷ See 12 U.S.C. 1464(d)(7)(D) and 1867(c)(1). These reports of examination are not tailored to any individual banking organization's circumstances or risk management needs and may be based on targeted rather than comprehensive examinations. These reports are the property of the agencies and are not intended as a proxy or substitute for any banking organization's responsibilities to undertake effective risk management and reliance on such reports without performing independent due diligence would be inconsistent with sound risk management principles.

Banking organizations may choose to conduct ongoing monitoring on a periodic or continuous basis based on the banking organization's assessment of the risk, complexity, and nature of the third-party relationship. For example, in the case of higher-risk third-party relationships, a banking organization may determine that effective risk oversight requires it to conduct more comprehensive or frequent monitoring. Higher-risk relationships may also involve additional staffing with the necessary expertise, authority, and accountability to perform a wide range of ongoing monitoring activities. For lower-risk relationships, a banking organization may determine that relatively less extensive, less detailed, or less frequent reporting, and commensurately reduced staffing needs, are necessary to support its risk oversight.

Banking organizations can tailor monitoring to their needs, abilities, risk determinations, and negotiating power, all of which can vary between larger or more complex banking organizations and community banks or among third-party relationships.

For example, whether on-site visits to a third party or audits of a third party's control practices are practical may depend on the circumstances.

Because both the types and levels of risks a banking organization faces may change over the lifetime of a third-party relationship, a banking organization may later find it useful to adapt or alter its ongoing monitoring practices accordingly, including by expanding or contracting the scope, level of detail, or frequency of information collected or produced for monitoring.

~~Depending on the degree of risk and complexity of the third-party relationship, a banking organization typically considers the following factors, among others, as part of ongoing monitoring:~~

- ~~• The overall effectiveness of the third-party relationship, including its consistency with the banking organization's strategic goals, business objectives, risk appetite, risk profile, and broader corporate policies;~~
- ~~• Changes to the third party's business strategy and its agreements with other entities that may pose new or increased risks or impact the third party's ability to meet contractual obligations;~~
- ~~• Changes in the third party's financial condition, including its financial obligations to others;~~
- ~~• Changes to, or lapses in, the third party's insurance coverage;~~
- ~~• Relevant audits, testing results, and other reports that address whether the third party remains capable of managing risks and meeting contractual obligations and regulatory requirements;~~
- ~~• The third party's ongoing compliance with applicable laws and regulations and its performance as measured against contractual obligations;~~
- ~~• Changes in the third party's key personnel involved in the activity;~~
- ~~• The third party's reliance on, exposure to, and use of subcontractors, the location of subcontractors (and any related data), and the third party's own risk management processes for monitoring subcontractors;~~
- ~~• Training provided to employees of the banking organization and the third party;~~

¹⁶ Refer to important considerations discussed in "Due Diligence and Third-Party Selection" of this guidance when a banking organization chooses to engage external resources to supplement its third-party risk management.

- The third party's response to changing threats, new vulnerabilities, and incidents impacting the activity, including any resulting adjustments to the third party's operations or controls;
- The third party's ability to maintain the confidentiality, availability, and integrity of the banking organization's systems, information, and data, as well as customer data, where applicable;
- The third party's response to incidents, business continuity and resumption plans, and testing results to evaluate the third party's ability to respond to and recover from service disruptions or degradations;
- Factors and conditions external to the third party that could affect its performance and financial and operational standing, such as changing laws, regulations, and economic conditions; and
- The volume, nature, and trends of customer inquiries and complaints, the adequacy of the third party's responses (if responsible for handling customer inquiries or complaints), and any resulting remediation.

5.iv. Termination

A banking organization may terminate a third-party relationship for various reasons, such as expiration or breach of ~~the contract;~~ the third party's failure to comply with applicable laws or regulations; concerns regarding a third party's performance of the activity more generally; or a desire to seek an alternate third party, bring the activity in-house, or discontinue the activity. When this occurs, ~~it is important for~~ management typically seeks to terminate relationships in an efficient manner, ~~whether the activities are transitioned to another third party, brought in-house, or discontinued.~~ Depending on the degree of risk and complexity of the third-party relationship, a banking organization typically considers the following factors, among others, to facilitate termination: and management's ability to do so may depend on previously negotiated contract provisions. For example, a banking organization may determine that a lower-risk third-party relationship presents relatively few concerns, and it may be easy and cost-effective to seamlessly switch to an alternative third party, if necessary. As the

complexity and materiality of a third-party relationship increases, a banking organization may benefit from advanced planning and ultimately determine that potential beneficial factors associated with a termination—e.g., in-house or alternative third-party options with the potential for long-term cost reductions or improvements to the banking organization's products, services, and operations; better access to or control over data; or use of innovative technology—either do or do not outweigh the potential negative factors—e.g., costs and fees associated with termination,¹⁸ extended transition timespans, operational complications, the likelihood of service or data access disruptions, data retention and destruction issues, and handling of joint intellectual property.

In any case, a banking organization's assessment as to the preferability of terminating a contract with one third party and transitioning services to another typically draws on numerous factors relevant to the organization's business and strategy and the agencies will give due consideration to the organization's reasonable determinations that

¹⁸ Termination cost considerations typically include whether alternative providers may be willing to buy out the remaining term of the contract or otherwise defer the banking organization's termination-related costs, an alternative third party can provide the services as contracted for and within the banking organization's risk appetite and tolerances.

- ~~• Options for an effective transition of services, such as potential alternate third parties to perform the activity;~~
- ~~• Relevant capabilities, resources, and the time frame required to transition the activity to another third party or bring in-house while still managing legal, regulatory, customer, and other impacts that might arise;~~

- ~~Costs and fees associated with termination;~~
- ~~Managing risks associated with data retention and destruction, information system connections and access control, or other control concerns that require additional risk management and monitoring after the end of the third-party relationship;~~
- ~~Handling of joint intellectual property; and~~
- ~~Managing risks to the banking organization, including any impact on customers, if the termination happens as a result of the third party's inability to meet expectations.~~

~~D. GOVERNANCE~~

~~There are a variety of ways for banking organizations to structure their third-party risk management processes. Some banking organizations disperse accountability for their third-party risk management processes among their business lines." Other banking organizations may centralize the processes under their compliance, information, security, procurement, or risk management functions. Regardless of how a banking organization structures its process, the following practices are typically considered throughout the third-party risk management life cycle," commensurate with risk and complexity.~~

~~4v. Cross-Cutting Oversight and Accountability Topics~~

~~The preceding discussion provides a high-level overview of tailoring third-party relationship oversight to a banking organization's size, complexity, and risk profile and the nature and assessed risk levels of its third-party relationships. However, banking organizations may benefit from considering third-party risk management on a holistic, rather than a siloed, stage-by-stage basis, since effectively managing any given risk may be a multi-factored process. Understanding how risks and mitigating factors may cut across or implicate different oversight stages and where certain risk management strategies may be complementary or redundant may help banking organizations more effectively tailor and prioritize their risk management practices.~~

~~The following highlights certain examples that may help illuminate such an approach.~~

~~Subcontractors~~

While a banking organization typically does not have a direct business arrangement with a third party's subcontractors, their use may nonetheless heighten risks related to the third-party relationship as it may lessen the banking organization's control of activities. Since subcontractors may be considered in connection with the primary third-party relationship, the extent to which a banking organization exercises risk oversight related thereto may depend on the nature and risks of the third-party relationship. A banking organization may be able to exercise effective risk oversight related to a third party's use of subcontractors by, for example, negotiating and monitoring compliance with contractual terms governing the use and oversight of subcontractors (including specifying whether service level agreements apply to subcontractor activity) or by assessing, confirming, and monitoring the adequacy of its third party's own third-party risk management programs. The banking organization remains responsible for complying with applicable laws and regulations, and operating in a safe and sound manner, regardless of a third party's use of subcontractors.

Use of Co-ventures, Consortia, Standard-Setting Organizations, Consultants, and Other Third Parties that Provide Risk Management Services

The agencies recognize that banking organizations can leverage new arrangements to manage third-party risk, including:

- Participating in a co-venture or consortium that collaborates on an aspect of third-party risk management, such as performing due diligence or developing standard contracts, or use of services from standard-setting and certification organizations that provide risk management and compliance standards for third parties engaging with

banking organizations and issue certifications that assess that a third party meets the standards.

~~Proper oversight and accountability are important aspects of third-party risk management because they help enable a banking organization to minimize adverse financial, operational, or other consequences. A banking organization's board of directors has ultimate responsibility for providing oversight for third-party risk management and holding management accountable. The board also provides clear guidance regarding acceptable risk appetite, approves appropriate policies, and ensures that appropriate procedures and practices have been established. A banking organization's management is responsible for developing and implementing third-party risk management policies, procedures, and practices, commensurate with the banking organization's risk appetite and the level of risk and complexity of its third-party relationships.~~

~~In carrying out its responsibilities, the board of directors (or a designated, board committee) typically considers the following factors, among others:~~

- ~~• Whether third-party relationships are managed in a manner consistent with the banking organization's strategic goals and risk appetite and in compliance with applicable laws and regulations;~~

~~Whether there is appropriate periodic reporting on the banking organization's third-party relationships, such as the results of management's planning, due diligence, contract negotiation, and ongoing monitoring activities; and~~

- ~~• Whether management has taken appropriate actions to remedy significant deterioration in performance or address changing risks or material issues identified, including through ongoing monitoring and independent reviews.~~

~~When carrying out its responsibilities, management typically performs the following activities, among others~~

¹⁷-Each applicable business line can provide valuable input into the third-party risk management process, for example, by completing risk assessments, reviewing due diligence information, and evaluating the controls over the third-party relationship.

¹⁸-Refer to Figure 1: Stages of the Risk Management Life Cycle.

- ~~• Integrating third-party risk management with the banking organization's overall risk management processes;~~
- ~~• Directing planning, due diligence, and ongoing monitoring activities;~~
 - ~~• Reporting periodically to the board (or designated committee), as appropriate, on~~

~~third-party~~Considering the results from services provided by consultants, auditors, or law firms for risk management activities; and compliance purposes.

Such arrangements could, among other things, create new efficiencies, provide banking organizations additional leverage in conducting due diligence on, negotiating with, or monitoring third parties, and facilitate access to new technologies and strategic expertise.¹⁹ The use of such arrangements could inform a banking organization's risk

¹⁹ Any collaborative activities among banking organizations must comply with antitrust laws. Refer to the Federal Trade Commission and U.S. Department of Justice's "Antitrust Guidelines for Collaborations Among Competitors" (Apr. 2000), available at https://www.ftc.gov/sites/default/files/documents/public_events/joint-venture-hearings-antitrust-guidelines-collaboration-among-competitors/ftcdojguidelines-2.pdf.

assessment and enhance a banking organization's ability to oversee its third-party relationships. For example, review of credible summaries of technical data or proprietary information, as well as certifications or results of assessments provided by such arrangements, may be adequate for a banking organization's due diligence needs, depending on facts and circumstances. However, it is important for effective risk management to be based on the banking organization's own specific circumstances and performance criteria for the activity.

In addition, effective third-party risk management may also involve relying on third-party technologies or processes to supplement or assist the banking organization's own risk oversight activities. This may allow community banks, in particular, to benefit from advanced technology and industry expertise otherwise unavailable. However, reliance on third parties for risk management purposes can itself involve risks, which a banking organization can address based on its individual circumstances.

Insurance, Indemnification, and Other Limitations on Liability

Depending on risk exposure, negotiating for credible indemnification provisions, limitations on banking organization liability, insurance, or guarantees from the third party's parent

or other entity may serve to effectively mitigate risks arising from the third-party relationship, which may lower the risk associated with the relationship. Such a conclusion may be based upon, for example, due diligence regarding the ability of the relevant party to meet any obligations, negotiating terms of the coverage as relevant to the specific risks of the third-party relationship, maintaining the coverage and confirming its ongoing sufficiency, and considering whether the banking organization has the capacity to cover any costs associated with pursuing, filing, disputing, or litigating a claim.

Operational Resilience Planning

Effective risk oversight, particularly for higher-risk relationships, may include due diligence, contract negotiations, and ongoing monitoring sufficient to demonstrate resilience and assess assurances, including, for example, contractual obligations related to review of a third party's operational resilience plan, the existence of alternative back-up providers that can provide an easy transition of services, the practice of maintaining critical data backed up at a physically and logically separated site, or other relevant considerations. In certain circumstances, even if a higher-risk third party suffers a disruption event, cyberattack, or otherwise is unable to provide business-as-usual services, if a banking organization has sufficient demonstration of its own or of the third party's ability to quickly and effectively resume operations and preserve relevant data, the harms from any such event may be significantly mitigated. This may in turn inform the risk associated with the third-party relationship.

- ~~Providing that contracts with third parties are appropriately reviewed, approved, and executed;~~

- Establishing appropriate organizational structures and staffing (level and expertise) to support the banking organization's third-party risk management processes;
- Implementing and maintaining an appropriate system of internal controls to manage risks associated with third-party relationships;
- Assessing whether the banking organization's compliance management system is appropriate to the nature, size, complexity, and scope of its third-party relationships;
- Determining whether the banking organization has appropriate access to data and information from its third parties;
- Escalating significant issues to the board and monitoring any resulting remediation, including actions taken by the third party; and
- Terminating business arrangements with third parties when they do not meet expectations or no longer align with the banking organization's strategic goals, objectives, or risk appetite.

2. *Independent Reviews*

It is important for a banking organization to conduct periodic independent reviews to assess the adequacy of its third-party risk management processes. Such reviews typically consider the following factors, among others:

- Whether the third-party relationships align with the banking organization's business strategy, and with internal policies, procedures, and standards;
- Whether risks of third-party relationships are identified, measured, monitored, and controlled;
- Whether the banking organization's processes and controls are designed and operating adequately;
- Whether appropriate staffing and expertise are engaged to perform risk management activities throughout the third-party risk management life cycle, including involving multiple disciplines across the banking organization, as appropriate; and
- Whether conflicts of interest or appearances of conflicts of interest are avoided or eliminated when selecting or overseeing third parties.

A banking organization may use the results of independent reviews to determine whether and how to adjust its third-party risk management process, including its policies, reporting, resources, expertise, and controls. It is important that management respond promptly and thoroughly to issues or concerns identified and escalate them to the board, as appropriate.

3. ~~Documentation and Reporting~~ Residual Risk Acceptance

Residual risk is the risk remaining after the banking organization applies mitigating measures. The agencies do not expect banking organizations to eliminate third-party risk. Some residual risk is unavoidable, as discussed above. In some cases, the materiality of the risk does not justify the oversight required to significantly mitigate it. In other cases, a banking organization may lack the means to significantly mitigate a risk, such as when it lacks bargaining power to conduct sufficient due diligence, negotiate customized contract terms, or engage in in-depth ongoing monitoring, or where the banking organization has limited alternative options. Managing third-party risk includes

~~It is important that a banking organization properly document and report on its third-party risk management process and specific third-party relationships throughout their life cycle. Documentation and reporting, key elements that assist those within or outside the banking organization who conduct control activities, will vary among banking organizations depending on the risk and complexity of their third-party relationships. Examples of processes that support effective documentation and internal reporting that the agencies have observed include, but are not limited to:~~

- ~~• A current inventory of all third-party relationships (and, as appropriate to the risk presented, related subcontractors) that clearly identifies those relationships associated with higher risk activities, including critical activities;~~
- ~~• Planning and risk assessments related to the use of third parties;~~
- ~~• Due diligence results and recommendations;~~
- ~~• Executed contracts;~~
- ~~• Remediation plans and related reports addressing the quality and sustainability of the third party's controls;~~
- ~~• Risk and performance reports required and received from the third party as part of ongoing monitoring;~~
- ~~• If applicable, reports related to customer complaint and inquiry monitoring, and any subsequent remediation reports;~~

- ~~Reports from third parties of service disruptions, security breaches, or other events that pose, or may pose, a material risk to the banking organization;~~
- ~~Results of independent reviews; and~~
- ~~Periodic reporting to the board (including, as applicable, dependency on a single provider for multiple activities).~~

~~E. SUPERVISORY REVIEWS OF THIRD-PARTY RELATIONSHIPS~~

~~The concepts discussed in this guidance are relevant for all third-party relationships and are provided to banking organizations to assist in the tailoring and implementation of risk management practices~~determining when and to what extent elements of risk oversight may not be practicable and whether residual risks may be acceptable according to a banking organization's risk appetite and tolerances, while still conducting activities in a safe and sound manner, and when and to what extent a banking organization can make this determination based on limited information. Even in cases where the banking organization cannot significantly mitigate a risk, the third-party relationship may still be beneficial and necessary for the banking organization to operate effectively and competitively in a rapidly evolving marketplace. Risk acceptance is ultimately a fact- and circumstance-specific consideration, commensurate to eachwith a banking organization's size, complexity, and risk profile, and with the nature of its third-party relationships~~Each agency will review its supervised banking organizations' risk management of third-party relationships as part of its standard supervisory processes. Supervisory reviews will evaluate risks and the effectiveness of risk management to determine whether activities are conducted in a safe and sound manner and in compliance with applicable laws and regulations.~~

4. Governance

In ~~their evaluations of a banking organization's~~order to support its overall third-party risk management, ~~examiners consider that~~ practices, banking organizations ~~engage in a diverse~~

~~set of third-party relationships, that not all third-party risk relationships present the same risks, and that banking organizations accordingly tailor their practices to the risks presented. Thus, the scope of the supervisory review depends on the degree of risk and the complexity associated with~~ may consider adopting governance practices that: (1) establish clear roles and responsibilities, (2) establish an appropriate risk appetite and appropriate risk tolerances related to risks from third-party relationships, (3) help ensure that the banking organization is able to identify and assess its third-party relationship risks and prioritize risk management in relation to the assessed risk levels of such relationships and the banking organization's activities and risk appetite and tolerances, (4) establish appropriate reporting to senior management and the board, (5) document key elements of risk management for third-party relationships. When reviewing, and (6) establish a process for conducting periodic independent reviews to assess the effectiveness of the banking organization's third-party risk management processes, examiners typically conduct the following activities, among others: practices.

- ~~▪ Assess the ability of the banking organization's management to oversee and manage the banking organization's third-party relationships;~~
- ~~▪ Assess the impact of third-party relationships on the banking organization's risk profile and key aspects of financial and operational performance, including compliance with applicable laws and regulations;~~

~~Perform transaction testing or review results of testing to evaluate the activities performed by the third party and assess compliance with applicable laws and regulations;~~

~~Highlight and discuss any material risks and deficiencies in the banking organization's risk management process with senior management and the board of directors as appropriate;~~

~~Review the banking organization's plans for appropriate and sustainable remediation of any deficiencies, particularly those associated with the oversight of third parties that involve critical activities; and~~

- ~~Consider supervisory findings when assigning the components of the applicable rating system and highlight any material risks and deficiencies in the Report of Examination.~~

~~When circumstances warrant, an agency may use its legal authority to examine functions or operations that a third party performs on a banking organization's behalf. Such examinations may evaluate the third party's ability to fulfill its obligations in a safe and sound manner and comply with applicable laws and regulations, including those designed to protect customers and to provide fair access to financial services. The agencies may pursue corrective measures, including enforcement actions, when necessary to address violations of laws and regulations or unsafe or unsound banking practices by the banking organization or its third party.~~

However, there is no one right way for a banking organization to structure such practices, and a banking organization's size, complexity, and risk profile and the nature of its third-party relationships will ultimately drive any relevant governance decisions.

The agencies will give due consideration to a banking organization's reasonable governance considerations when reviewing those practices.

Jonathan V. Gould,
Comptroller of the Currency.

By order of the Board of Governors of the Federal Reserve System.
Benjamin W. McDonough,
Secretary of the Board.

Federal Deposit Insurance Corporation.
Dated at Washington, DC, on September 10, 2026.
Jennifer M. Jones,
Deputy Executive Secretary.

By the National Credit Union Administration Board on September 10, 2026.
Melane Conyers-Ausbrooks,
Secretary of the Board.