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

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[1] 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 manner[3] and in compliance with applicable laws and regulations.[4] 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

[1] 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 guidance is relevant to all banking organizations supervised by the agencies.

[2] Supervisory guidance does not have the force and effect of law and does not impose any new requirements on banking organizations. See 12 CFR Part 4, Subpart F, Appendix A (OCC); 12 CFR 262, Appendix A (FRB) 12 CFR 302, Appendix A (FDIC).

[3] *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).

[4] 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.[5]

This guidance addresses any business arrangement[6] 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

[5] 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.

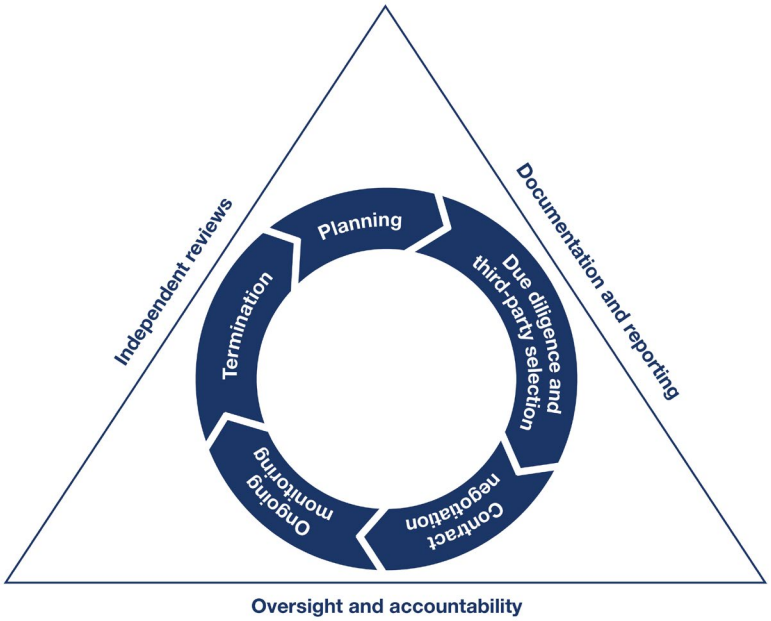
C. THIRD-PARTY RELATIONSHIP LIFE CYCLE

Effective third-party risk management generally follows a continuous life cycle for third-party relationships. The stages of the risk management life cycle 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 banking organization is based on specific facts and circumstances and these examples may not apply to all of a banking organization's third-party relationships.

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.[7]

[7] 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

1. 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).

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;[8]

[8] 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,[9] 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.

[9] Dual 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-venture-hearings-antitrust-guidelines-collaboration-among-competitors/ftcdojguidelines-2.pdf.

organization to determine whether the third party can perform the activity in a manner that is consistent with the banking organization's broader corporate policies and practices.

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.[11] 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

[12] 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 Subcontractors[14]

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.

---

[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.

*3. **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.

It is important that 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.

Periodic reviews of executed contracts allow a banking organization to confirm that existing provisions continue to address pertinent risk controls and legal protections. If new risks are identified, a banking organization may consider renegotiating a contract.

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.

c. 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.[15] This can help ensure that a third party is aware of its role and potential liability in its relationship with a banking organization.

*4. **Ongoing Monitoring***

Ongoing monitoring enables a banking organization to: (1) confirm the quality and sustainability of a third party's controls and ability to meet contractual obligations; (2) escalate significant issues or concerns, such as material or repeat audit findings, deterioration in financial condition, security breaches, data loss, service interruptions, compliance lapses, 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.

[15] *See* 12 U.S.C. 1464(d)(7)(D) and 1867(c)(1).

Typical monitoring activities include: (1) review of reports regarding the third party's performance and the effectiveness of its controls; (2) periodic visits and meetings with third-party representatives to discuss performance and operational issues; and (3) regular testing of the banking organization's controls that manage risks from its third-party relationships, particularly when supporting higher-risk activities, including critical activities. In certain circumstances, based on risk, a banking organization may also perform direct 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 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.

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. **Termination***

A banking organization may terminate a relationship for various reasons, such as expiration or breach of the contract, the third party's failure to comply with applicable laws or regulations, 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 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:

- 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.[17] 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,[18] commensurate with risk and complexity.

1. Oversight and Accountability

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 risk management activities;

- 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

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 commensurate to each banking organization's size, complexity, risk profile, and 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.

In their evaluations of a banking organization's third-party risk management, examiners consider that 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 the banking organization's activities and third-party relationships. When reviewing third-party risk management processes, examiners typically conduct the following activities, among others:

- 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.