Third-Party Risk Management

A Guide for Community Banks

MAY 2024

Board of Governors of the
Federal Reserve System

Federal Deposit Insurance
Corporation

Office of the Comptroller of
the Currency

Contents

Introduction

Community banks engage with third parties to compete in and respond to an evolving financial services landscape. Third-party relationships can offer community banks access to new technologies, risk-management tools, human capital, delivery channels, products, services, and markets. A community bank's reliance on third parties, however, reduces its direct operational control over activities[1] and may introduce new risks or increase existing risks, including, but not limited to, operational, compliance, financial, and strategic risks.

Due to the varied risks associated with third-party relationships, it is important for community banks to appropriately identify, assess, monitor, and control these risks as well as ensure that activities are performed in a safe and sound manner and in compliance with applicable laws and regulations.[2] These laws and regulations 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 (such as fraud and money laundering).

Engaging a third party does not diminish or remove a bank's responsibility to operate in a safe and sound manner and to comply with applicable legal and regulatory requirements, including consumer protection laws and regulations, just as if the bank were to perform the service or activity itself. A community bank may engage an external party to conduct aspects of its third-party risk management. However, the bank cannot abrogate its responsibility to employ effective risk-management practices, including when using a third party to conduct third-party risk management on behalf of the bank.

About This Guide

In June 2023, 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) issued the *Interagency Guidance on Third-Party Relationships: Risk Management* (TPRM Guidance).[3] The TPRM Guidance includes sound risk-management principles for banking

---

1 Banks routinely rely on third parties for a range of products, services, and other activities (collectively, activities).

2 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 C.F.R. pt. 30, appendix A (OCC), 12 C.F.R. pt. 208, appendix D–1 (Board); and 12 C.F.R. pt. 364, appendix A (FDIC).

3 The agencies issued Interagency Guidance on Third-Party Relationships: Risk Management, 88 Fed. Reg. 37,920 (June 6, 2023), https://www.federalregister.gov/documents/2023/06/09/2023-12340/interagency-guidance-on-third-party-relationships-risk-management. See also the Board, "Interagency Guidance on Third-Party Relationships: Risk Management," SR letter 23-4 (June 6, 2023), https://www.federalreserve.gov/supervisionreg/srletters/SR2304.htm; FDIC Financial Institution Letter, "Interagency Guidance on Third-Party Relationships: Risk Management," FIL 29-2023 (June 6, 2023), https://www.fdic.gov/news/financial-institution-letters/2023/fil23029.html; and OCC, "Third-Party Relationships: Interagency Guidance on Risk Management," OCC Bulletin 2023-17 (June 6, 2023), https://www.occ.gov/news-issuances/bulletins/2023/bulletin-2023-17.html. The principles and considerations in the TPRM Guidance are relevant to all banking organizations supervised by the agencies; however, since this guide is primarily directed at community banks, it refers to that subset of institutions.

organizations to consider when developing and implementing risk-management practices for all stages in the life cycle of third-party relationships.

This guide is intended to assist community banks when developing and implementing their third-party risk-management practices. This guide is not a substitute for the TPRM Guidance.[4] Rather, it is intended to be a resource for community banks to consider when managing the risk of third-party relationships. This guide is not a checklist and does not prescribe specific risk-management practices or establish any safe harbors for compliance with laws or regulations. While this guide is intended for use by community banks, other banks may find it useful. Some additional resources that can help support a bank's development and implementation of its risk-management program are listed in the appendix to this guide. The agencies underscore that supervisory guidance does not have the force and effect of law and does not impose any new requirements on banks.

Guide Contents

The guide provides potential considerations, resources, and examples through each stage of the third-party risk-management life cycle and is organized under the following topics:

- Risk Management. Discussion on risk considerations.
- Third-Party Relationship Life Cycle. The five stages of the life cycle are explained.
- Governance. Considerations for governance related to third-party risk.
- Appendix. Additional resources that can help support a bank's development and implementation of its third-party risk-management practices.

Excerpts from the TPRM Guidance are also highlighted within boxes in each section.

TPRM Guidance

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.

[4] Excerpts from the TPRM Guidance in the boxes highlight some key concepts.

Risk Management

Not all third-party relationships present the same level of risk, and therefore not all relationships require the same level of oversight. As part of sound risk management, community banks apply more rigorous risk-management practices throughout the third-party relationship life cycle for third parties that support higher-risk activities, including critical activities. A community bank may adjust and update its third-party risk-management practices commensurate with its size, complexity, and risk profile by periodically analyzing the risks associated with each third-party relationship. It is important to involve bank staff with the requisite knowledge and skills in each stage of the risk-management life cycle.

This guide includes considerations illustrating how a community bank may apply risk-management practices in different stages of the third-party relationship life cycle. An important initial step is identifying third-party relationships that support higher-risk activities, including critical activities. In determining whether an activity is higher risk, banks may assess various factors, such as if the third party has access to sensitive data (including customer data), processes transactions, or provides essential technology and business services.

TPRM Guidance

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:

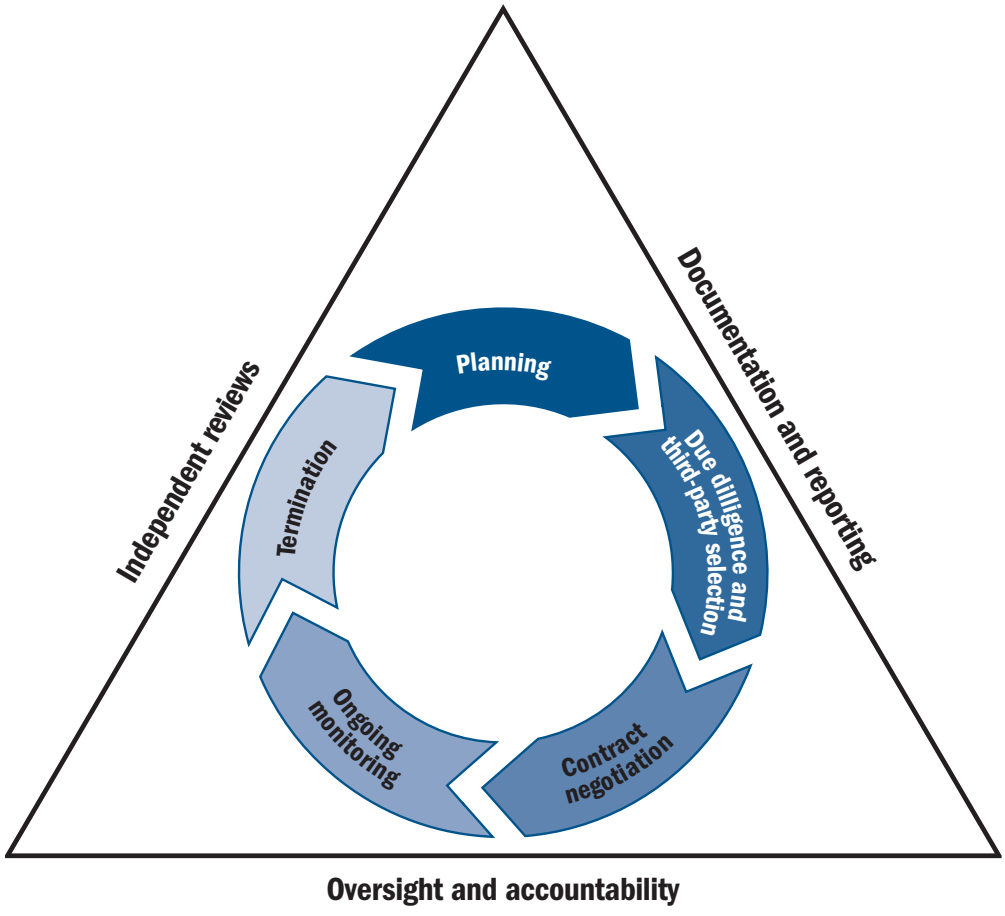
- cause a banking organization to face significant risk if the third party fails to meet expectations;
- have significant customer impacts; or
- have a significant impact on a banking organization's financial condition or operations.

Third-Party Relationship Life Cycle

Effective third-party risk management generally follows a continuous life cycle for third-party relationships. The five stages of the life cycle are set forth in figure 1, surrounded by the governance practices of Oversight and Accountability, Independent Reviews, and Documentation and Reporting.

For every stage, a community bank's level or type of oversight may vary, commensurate with its size, complexity, and risk profile as well as with the nature of the specific third-party relationship.

Figure 1. Stages of the risk-management life cycle



Planning

Careful planning enables a community bank to consider potential risks in the proposed third-party relationship. In addition, risk assessments are an important component of managing third-party relationships and help a bank evaluate the extent of risk-management resources and practices for effective oversight of the proposed third-party relationship throughout the subsequent stages of the third-party relationship life cycle.

TPRM Guidance

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.

Potential Considerations

- What are the underlying activities to be performed, and what are the bank and third party's prospective roles in the activities?
- What legal and compliance requirements will apply to the prospective third-party activities?
- What are the benefits of the relationship, and how would the relationship align with the bank's strategic plan?
- What risk-management and governance practices (including internal controls) will be necessary to manage and mitigate the potential risks?
- What are the financial implications of entering into and maintaining the business arrangement?
- What are the direct contractual costs and indirect costs to augment or alter bank staffing, processes, and technology?
- Do the expected benefits of the relationship exceed the potential costs and risks?
- How will the bank integrate third-party technology with the bank's existing systems and infrastructure? What changes would need to be made to the bank's technology to ensure compatibility, and what would be the associated risks and costs? Does staff have the requisite skills to manage risks associated with integrating the third party's technology into the bank's environment (if not, how will the bank integrate the technology)?
- What physical and/or system access would the third party have to bank facilities, systems, and records, and what record-keeping processes would the bank require the third party to implement?
- What interaction will the third party have with customers, and how would customer complaints be handled?
- What are the information security implications, and how will the third party access, process, and protect customers' information?
- Has the bank considered how to exit the activity or transition the activity to an alternative third party or in-house?

Potential Sources of Information

- The bank's strategic plan to assess the proposed activity's alignment with the bank's risk appetite, policies, and business objectives.
- The bank's budget or cost-benefit analysis to assess the financial considerations of the relationship.
- The bank's human resources staff to assess whether management and staff have the expertise and capacity to manage the relationship.
- The bank's internal policies, processes, and controls to assess the impact to the bank of entering into and managing the proposed relationship.
- The bank's inventory of existing third-party relationships to assess whether an existing relationship could support the new activity.
- The bank's technology infrastructure and staff to assess how readily it could integrate with a third party to support the new activity.
- The perspectives of the bank's subject matter experts, including those in information technology, legal, and compliance risk.
- Board policies, including risk limits, to assess alignment with the proposed third-party relationship.

Example: Planning

A community bank experiences financial losses due to a recent surge in fraudulent transactions. The bank's management identifies the root cause and decides to introduce additional internal controls and training to mitigate future losses. Management contemplates two alternatives for carrying out new preventative measures.

The first approach is to allocate internal resources to develop and implement new internal controls and training across the bank. The second approach is to outsource to a third party, which will develop new fraud controls and applicable employee training.

When evaluating the in-house option, the bank's management

- assesses its existing in-house expertise and capabilities, including the ability to ensure that new fraud controls would comply with applicable laws and regulations;
- evaluates whether dedicating internal resources to this project will strain the bank's business-as-usual operations; and
- assesses the timeline for completing the project internally and whether it aligns with the urgency to strengthen the bank's defenses against fraud incidents.

When evaluating whether to outsource this project, the bank's management

- considers data security risk in light of the fact that the third party would have access to confidential bank and customer information during the project;
- considers the potential compliance risk exposure from a third party, such as the risk that new internal controls would not ensure compliance with applicable laws and regulations;
- assesses the financial feasibility of the outsourcing option by comparing estimated direct and indirect costs with the bank's budget;
- determines minimum requirements for the service level agreement, which will establish clear performance standards for the third party, supported by a resolution mechanism; and
- evaluates whether the bank has appropriate policies and internal controls as well as sufficient resources, to adequately monitor the third party's performance.

The examples are provided for illustrative purposes, are not comprehensive, and will not be applicable to all situations.

Due Diligence and Third-Party Selection

Due diligence is the process by which a community bank assesses, before entering into a third-party relationship, a particular third party's ability to perform the activity as expected, adhere to the community bank's policies, comply with all applicable laws and regulations, and conduct the activity in a safe and sound manner. Effective due diligence assists with the selection of capable and reliable third parties to perform activities for, through, or on behalf of the community bank. If the bank cannot obtain desired due diligence information from the third party, the bank may consider alternative information, controls, or monitoring.

TPRM Guidance

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.

Potential Considerations

- Has the third party demonstrated financial and operational capability to meet its obligations to the bank? If no, what alternative information is available?
- What resources and expertise are available at the third party to support the activity?
- What third-party policies, processes, and internal controls support performance of the service in alignment with the bank's expectations and standards?
- Has the third party demonstrated an ability to comply with applicable laws and regulations, including anti-money laundering and countering the financing of terrorism (AML/CFT) as well as fair lending and consumer protection laws and regulations (as applicable)?
- Is the third party's information security program consistent with the bank's program and expectations related to protecting the confidentiality, integrity, and availability of information?
- Does the third party demonstrate the ability to effectively operate through and recover from both internal and external operational incidents or disruptions?
- How has the third party performed in the past during periods of economic or financial stress?
- Does the third party rely on subcontractors, and could that reliance pose additional or heightened risk to the bank?

Potential Considerations*—continued*

- Does the third party use technologies that could introduce additional risk?
- Does the third party have a robust consumer complaint program? Does it have a history of prompt and satisfactory resolution of consumer complaints?
- Is the third party involved in ongoing litigation or other public matters of concern?
- Can the third party demonstrate that it has successfully provided the prospective services for other banks or similar clients?

Potential Sources of Information

- The third party's audited financial statements and other financial information to assess the third party's financial condition.
- The third party's licenses and any other legal authority necessary to perform the activity.
- The third party's relevant policies and procedures, including those related to AML/CFT, to assess the effectiveness of its risk-management practices, control environment, and alignment with the bank's expectations and standards and with applicable legal requirements.
- Independent reviews of the effectiveness of those policies and procedures, including AML/CFT.
- The third party's strategic plan or other disclosures to assess whether the business strategy and its agreements with other entities pose new or increased risks.
- The third party's staffing levels and qualifications to assess whether the third party's resources can fulfill its obligations to the bank, including those of principals and other key personnel related to the activity.
- The third party's training program to assess if its employees understand their duties and responsibilities, are knowledgeable about applicable laws and regulations, and have requisite certifications and licenses.
- The volume and nature of consumer complaints against the third party.
- The Office of Foreign Assets Control Specially Designated Nationals and Blocked Persons list ("SDN List") and all other sanctions lists to ensure the third party and its employees, contractors, or grantees are not sanctioned by the U.S. government.
- System and Organization Controls (SOC) reports, independent assessments, and industry certifications to assess the third party's operational risk management and internal controls.
- Audit reports to assess the third party's risk management and internal controls.
- References and feedback from peer institutions or clients that are currently using the third party's service.
- The third party's current insurance coverage to determine if sufficient for the activity.

***Potential Sources of Information**—continued*

- Disclosures and information in the media or in any of the third party's publications, including its website, to assess potential risks to the bank.
- Internet searches of the third party's company name to determine whether it has been partnered with institutions subject to consent orders related to third-party transactions or conducts business with companies that misrepresent deposit insurance coverage.

Example: Due Diligence

A community bank is exploring enhancements to its information security program with respect to its user access practices. The bank's board and management explore strengthening its user access practices by implementing multi-factor authentication for user access to the bank's network by contracting for an authentication service offered by its core service provider. Although the bank has an established relationship with its core service provider, the new service is outside the scope of the current contracted services. Bank management requests that the core service provider submit a proposal, including scope and pricing, for the new service.

The bank completes a third-party risk assessment and identifies potential risk issues, including, but not limited to, risk associated with the service provider's technical expertise and training, robustness of controls, and system connectivity. The results of this risk assessment help guide the bank's due diligence. As part of its due diligence process, the bank evaluates a range of information regarding the financial, compliance, and operational aspects of the prospective expanded relationship.

The bank's management takes the following measures to conduct due diligence and evaluate the core service provider's capabilities, expertise, and resources related to the new service:

- Reviews the core service provider proposal to understand the financial cost, time, and resources required for implementation of the authentication service. This review leverages bank staff's existing knowledge and experience with the core service provider's technologies and services;
- Reviews the core service provider's staffing levels and qualifications to evaluate whether the core service provider has sufficient skill and technical expertise to implement the new service;
- Reviews the core service provider's proposed contract to evaluate key terms, costs, timeline, and other service terms;
- Evaluates the core service provider's proposed implementation plan to assess its impact on bank operations, including any proposed downtime, and its ability to adhere to the expected timeline; and
- Compares the core service provider's proposal with the bank's existing policies for security. Specifically, the bank reviews the core service provider's security policies regarding customers' data and authentication of users and devices.

The examples are provided for illustrative purposes, are not comprehensive, and will not be applicable to all situations.

Contract Negotiation

Before entering a contractual relationship with a third party, a community bank typically considers contract provisions that meet its business objectives, regulatory obligations, and risk-management policies and procedures. The community bank typically negotiates contract provisions that facilitate effective risk management and oversight, including terms that specify the expectations and obligations of both the community bank and the third party. When a community bank has limited negotiating power, it is important for bank management to understand any resulting limitations and consequent risks. Possible actions that bank management might take in such circumstances include determining whether the contract can still meet the community bank's needs, whether the contract would result in increased risk to the community bank, and whether residual risks are acceptable.

TPRM Guidance

…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… 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.

Potential Considerations

- To what extent does the contract specify the parties' responsibilities and cover all aspects of the relationship (including costs, reimbursements, and other liabilities)?
- What provisions does the bank need to include regarding termination events (for example, default or force majeure), continuity planning, and associated costs and fees?
- What are the governance and escalation protocols regarding the third party's performance and security measures or benchmarks?
- To what extent does the contract enable the bank to obtain timely information it needs to perform adequate ongoing monitoring, demonstrate compliance with applicable laws and regulations, and respond to regulatory requests? For example, will the bank have access to application and loan data, account opening and customer information, audit reports, suspicious activity monitoring information, and reports to identify safety and soundness and consumer compliance issues?
- What arrangements will be negotiated for sharing and using information, technology, and intellectual property?

Potential Considerations*—continued*

- Does the contract specify limitations on the third party's use and retention of data (including customer data) related to the activity, including its disclosure, storage, delivery to the bank, and destruction?
- Does the contract appropriately address the bank's right to access its data at the third party and the process by which the bank will access its records and data (including customer data)?
- When and how will the third party notify the bank of a disruption, including degradation or interruptions in delivery, and how will the third party assist the bank with continuation of the activity?
- When and how will the third party notify the bank of strategic changes, such as mergers and acquisitions and leadership changes?
- What continuity plans, processes, and controls will the third party maintain to ensure contract adherence, including recovery time and recovery point objectives?
- For higher-risk activities, including critical activities, what are likely scenarios for breach of contract, and has the bank considered the potential exposure and cost?

Potential Sources of Information

- The bank's risk assessment and due diligence findings to determine the provisions to include in the contract.
- The third party's proposed service level agreements to set applicable performance and security metrics.
- Assessments from business units regarding their business needs and customer service objectives to determine performance and security measures to include in the contract.
- Contract provisions outlining the bank's access to the third party's audit, testing, and self-assessment reports for ongoing monitoring.
- Legal, compliance, and other stakeholders' perspectives to advise bank management on the contract provisions to appropriately protect the bank's interests.

Example: Contract Negotiation

A community bank seeks to upgrade its computing capabilities to meet competitive challenges and customer demands. The bank's management identifies several benefits in outsourcing its computing for higher-risk activities, including critical activities, and determines that contracting with a service provider is the appropriate option for its business needs.

When reviewing the contract with the bank's subject matter experts and its legal counsel, the bank's management identifies that the provider's contract contains standard provisions related to audit rights and determines them to be inadequate for ongoing monitoring. The bank's board and management want the contractual right to review the service provider's reports of its business continuity and disaster recovery tests performed on a monthly basis or to periodically conduct on-site visits for certain audit purposes. As a result, bank management finds that the standard contractual provisions would present challenges to the bank in complying with its regulatory requirements, business objectives, and risk-management needs.

To address these challenges with the service provider, the bank's management

- requests that the service provider modify the contract terms to require providing monthly test reports to the bank and to allow the bank to conduct visits (either virtual or on site);
- considers if these modifications would make the contract satisfactory for the bank's regulatory requirements, business objectives, and risk-management needs; and
- conducts additional research on alternative providers to determine if they will include contract terms that support the bank's regulatory requirements, business objectives, and risk-management needs.

The examples are provided for illustrative purposes, are not comprehensive, and will not be applicable to all situations.

Ongoing Monitoring

A community bank's ongoing monitoring of the third party's performance enables bank management to determine if the third party is performing as required for the duration of the contract. The bank may also use information from ongoing monitoring to adapt and refine its risk-management practices.

TPRM Guidance

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… 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.

Potential Considerations

- Is the third party performing its obligations under the contract?
- Has the third party's financial condition changed, including declining revenues or increasing debt obligations?
- Has the third party complied with applicable laws, regulations, and service level agreements?
- Do audit and test results indicate the third party is managing risks and meeting contractual obligations and regulatory requirements effectively?
- Is the third party demonstrating an ability to maintain its systems within the bank's availability requirements (e.g., latency, bandwidth, and uptime)?
- Is the third party demonstrating reliability throughout its relationship with the bank?
- How do the third party's business continuity and disaster recovery plans and practices demonstrate its capability to respond and recover from service disruptions?
- Has the third party maintained the confidentiality, availability, and integrity of customer data (where applicable) and the bank's systems, information, and data?
- Do reports from the third party align with the bank's internal reports and observations?
- Has the third party's performance changed due to mergers, acquisitions, or divestitures?
- Has the bank's reliance on the third party to conduct bank activities changed over the life of the relationship?

Potential Considerations*—continued*

- For third parties that interact with customers or access customer data, has the third party responded appropriately to the bank's requests for its records and information?
- Have there been changes in the third party's strategy, corporate culture, leadership, or risk exposure? If so, what is the impact on the relationship with the bank?

Potential Sources of Information

- Service level agreements and standards to assess the third party's performance and to confirm that existing provisions continue to address risks and the bank's expectations.
- Audited and other financial reports to confirm the third party's financial condition remains sound and in compliance with contractual requirements.
- Audits and reports to confirm the third party's compliance with all applicable laws and regulations.
- Internal reports to review changes in the bank's risk assessment and supporting risk-management processes.
- The bank and third party's contingency testing results to evaluate the ability to respond to and recover from service disruptions or degradations.
- Review and testing of control effectiveness to assess whether the third party's control environment remains sound, including SOC reports and self-assessments to industry standards.
- Information security testing results to assess the third party's ability to maintain the confidentiality, availability, and integrity of customer data (where applicable) and the bank's systems, information, and data.
- Customer complaints to assess the volume and subject matter of complaints and the timeliness and appropriateness of the third party's response to them.
- Communication with the third party to assess changes in key processes.
- The third party's staffing and succession plans and organizational charts to assess changes in the third party's key personnel involved in the activity and to determine whether key personnel have assumed responsibilities that may detract from their ability to perform under the third party's agreement with the bank (e.g., affiliation with other entities).
- Training materials provided to the third party and bank staff for continued education.
- Public filings, news articles, social media, and customer feedback about experiences with the third party.

Example: Ongoing Monitoring

A community bank offers banking products and services through a relationship with a nonbank third party. In this arrangement, customers interact directly with the third party to access products and services, such as opening and accessing deposit accounts, conducting transactions, viewing account details, and receiving customer support.

The bank conducted a risk assessment during the planning stage and identified multiple risks associated with this arrangement. Consistent with the bank's risk-management practices, bank management conducts ongoing monitoring of third parties to ensure that the third party continues to manage the risks and abide by contractual terms.

For illustrative purposes, this example **only** focuses on the bank's ongoing monitoring activities related to a limited set of AML/CFT as well as compliance and consumer protection considerations:[1]

- The third-party relationship may expose the bank to increased risk of noncompliance with applicable AML/CFT requirements in the areas of Customer Identification Program (CIP), Customer Due Diligence (CDD), and suspicious activity monitoring if the third party fails to meet its contractual or other obligations.
- The third-party relationship may expose the bank to increased risks of noncompliance with consumer protection laws and regulations that may arise from the third party's disclosure of personal customer information, misrepresentations, or misleading statements to customers about products or services, or failure to comply with applicable dispute-resolution requirements.

Before entering the arrangement, the third party undertook several remedial actions related to AML/CFT and consumer protection compliance controls to help mitigate risks identified in the bank's risk assessment. These actions included strengthening controls at the third party related to CIP and CDD requirements, suspicious activity monitoring, providing required consumer disclosures, monitoring of customer support interactions, and the handling of customer disputes.

The bank's ongoing monitoring covers the full range of risks associated with the arrangement. In particular, to manage the identified risks noted above, bank management

- maintains regular communications regarding the third party's risk-management practices, such as those related to AML/CFT and consumer protection;
- provides feedback on any changes to the third-party's risk-management practices that may impact the bank's compliance with applicable laws and regulations;
- obtains and reviews copies of the third party's internal and external audit reports (independent testing), compliance reviews, and other testing of internal controls. This testing may include sampling the third party's files related to CIP information collected at account opening, documentation related to ongoing CDD, and ongoing suspicious activity monitoring conducted on behalf of the bank. This information may include transaction reviews, escalations of potentially suspicious activity, and other documentation related to compliance functions fulfilled by the third party;

---

[1] This example does not identify all potential third-party risks posed by this relationship. Further, the actions noted are not all-inclusive of ongoing monitoring actions that may be appropriate to manage identified AML/CFT and consumer protection risks.

Example: Ongoing Monitoring—*continued*

- confirms access to customer, transaction, and monitoring information consistent with the contractual arrangement;
- monitors the third party's impact on customers, including access to or use of consumer information, the third party's interaction with customers, handling of customer complaints and inquiries, and communications with customers to ensure accurate representation of the bank's products and services; and
- maintains an effective compliance management system (i.e., board and management oversight, policies and procedures, training, monitoring, audit, and consumer complaint resolution process) that addresses this and other third-party relationships, including compliance with applicable consumer protection laws and regulations.

The examples are provided for illustrative purposes, are not comprehensive, and will not be applicable to all situations.

Termination

A community bank may choose to end its relationship with a third party for a variety of reasons. A bank typically considers the impact of a potential termination during the planning stage of the life cycle. This consideration may help to mitigate costs and disruptions caused by termination, particularly for higher-risk activities, including critical activities.

TPRM Guidance

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.

Potential Considerations

- How will the termination affect the bank's operations and its compliance with applicable laws and regulations? Will any higher-risk activities, including critical activities, be affected?
- What are the financial implications of terminating the relationship?
- What alternative third parties are available to which the bank can transition, or can the bank perform the activity in-house?
- How ready are bank staff, systems, and control environments to move the outsourced activity in-house, if needed?
- How will the bank and the third party handle intellectual property?
- What access to bank systems or information has the third party been granted? How and when will this access be removed?
- If the third party has access to bank or customer data, when and how will the bank confirm that the data has been returned or destroyed?
- Will the bank have access to data to meet its AML/CFT requirements and other recordkeeping obligations?
- How will the bank manage risks associated with the termination or migration, including the impact on customers?
- What additional controls and processes will the bank put in place during the transition?

Potential Sources of Information

- The bank's contract with the third party, to verify how parties may exit the relationship and the conditions under which fees or penalties will be imposed for early termination.
- The bank's budget to assess the impact of costs and fees associated with termination.
- Any outlines of steps or resources that the bank had previously developed to support its exit from the activity or to transition the activity to an alternative third party or in-house.
- Inventory of the bank or customers' data at the third party to support risk management associated with data retention and destruction, information system connections and access control, or other control concerns.
- Assessments of the bank's systems, processes, and human resources to determine whether the bank has the capability, resources, and time to transition the activity to another third party or bring the activity in-house with limited disruption to the bank's operations.
- The bank's third-party inventory to assess existing relationships with other third parties to transition the activity to them, if appropriate.
- The bank's considerations for transitioning customer accounts with limited disruption to customers and the bank's operations.

Example: Termination

A community bank's contract requires that the third party receive approval before it uses a foreign-based subcontractor to perform its obligations to the bank. As part of its ongoing monitoring of the third-party relationship, the bank's management discovers that the third party has relied on a foreign-based subcontractor for a higher-risk activity without informing the bank. The contract states that the bank can terminate the relationship if the third party breaches a requirement in the contract.

Management considers terminating the relationship, as the third party has defaulted on its contract with the bank by not obtaining approval for engaging the foreign-based subcontractor. To facilitate the decision for termination, management reassesses the relationship through the following practices:

- Review of contract terms to confirm the bank's rights and options for termination, including notification and timelines. Management also consults with its legal counsel to determine whether early termination fees, penalties, or other restrictions may apply;
- Consultation with the bank's operations and compliance teams to determine the potential impact, costs, and risks related to termination;
- Assessment of potential operational, compliance, and financial risks to transition to a new service provider;
- Assessment of potential customer impacts arising from termination and transition to a new service provider and considers steps to mitigate them;
- Evaluating whether the bank's risk-management practices are adequate and capable of managing the risks anticipated from the termination of the contract and potential transition of the activity to a new service provider; and
- Reporting to the board of directors on the potential risks of the termination. The report can include management's recommendations on legal, operational, and compliance risks arising from termination and transition, including risk and cost mitigation.

The examples are provided for illustrative purposes, are not comprehensive, and will not be applicable to all situations.

Governance

Community banks typically consider the following governance practices throughout the third-party relationship life cycle: oversight and accountability, independent reviews, and documentation and reporting.

TPRM Guidance: Oversight and Accountability

A banking organization's board of directors has ultimate responsibility for providing oversight for third-party risk management and holding management accountable… 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.

TPRM Guidance: Independent Review

It is important for a banking organization to conduct periodic independent reviews to assess the adequacy of its third-party risk management processes… 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.

TPRM Guidance: Documentation and Reporting

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.

Potential Considerations

- How do the bank's policies and procedures promote effective third-party risk-management governance?
- How do documentation and reporting enable the bank's board of directors to consistently oversee third-party risk management?
- How does the bank's board of directors hold management accountable for third-party risk management?
- Do the bank's governance structure and internal control environment effectively promote compliance with bank policies and procedures and applicable laws and regulations?
- Has the bank accurately assessed the resources required (including level and expertise of staffing) to manage third-party risks?
- Does the bank effectively document and maintain a current inventory of all third-party relationships that clearly identifies those relationships associated with higher-risk activities, including critical activities?

Potential Considerations*—continued*

- Has the bank effectively evaluated the accuracy and timeliness of risk and performance reporting?
- Has the bank effectively conducted periodic independent reviews of the bank's third-party risk management?
- When and how does the bank's management inform its board of directors about third-party risks?

Potential Sources of Information

- The bank's strategic plan to verify that the bank's third-party risk-management practices are aligned with its strategic objectives.
- Applicable policies and procedures to assess whether they address risks posed by third-party relationships.
- The bank's contingency testing plans to understand how the bank maintains operations during disruptions.
- Audit reports to assess the bank's risk management and pertinent internal controls.
- The bank management's periodic reporting to the board of directors on third parties that support higher-risk activities, including critical activities.
- Documentation of the bank's actions to remedy material third-party issues, including performance deterioration.
- Other internal reports regarding the bank's third-party relationships.

Appendix

Government Resources for Community Banking Organizations' Third-Party Risk Management

These resources are not all inclusive, and other sources of information may be available, particularly on specific topics.

- Interagency Guidance on Third-Party Relationships: Risk Management, 88 Fed. Reg. 37,920 (June 6, 2023), https://www.federalregister.gov/documents/2023/06/09/2023-12340/interagency-guidance-on-third-party-relationships-risk-management.

- SR 21-15/CA 21-11, FIL 59-2021, and OCC Bulletin 2021-40: "Guide for Community Banking Organizations Conducting Due Diligence on Financial Technology Companies," https://www.federalreserve.gov/supervisionreg/srletters/sr2115.htm, https://www.fdic.gov/sites/default/files/2024-03/pr21075a.pdf, https://www.occ.gov/news-issuances/news-releases/2021/nr-ia-2021-85a.pdf.

- Federal Register (86 Fed. Reg. 66,424), SR 22-4/CA 22-3, FDIC: FIL-12-2022, and OCC Bulletin 2022-8: "Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers," https://www.federalregister.gov/documents/2021/11/23/2021-25510/computer-security-incident-notification-requirements-for-banking-organizations-and-their-bank.

- "Protecting Against Cyber Threats to Managed Service Providers and their Customers," Cybersecurity & Infrastructure Security Agency (CISA), Alert (AA22-131A), last modified May 11, 2022, https://www.cisa.gov/news-events/alerts/2022/05/11/protecting-against-cyber-threats-managed-service-providers-and-their.

- CISA, *Securing Small and Medium-Sized Business (SMB) Supply Chains: A Resource Handbook to Reduce Information and Communication Technology Risks* (Arlington: CISA, January 2023), https://www.cisa.gov/resources-tools/resources/securing-smb-supply-chains-resource-handbook.

- CISA Alert, "NCSC-UK Releases Guidance on Using MSP for Administering Cloud Services," last modified January 11, 2023, https://www.cisa.gov/news-events/alerts/2023/01/11/ncsc-uk-releases-guidance-using-msp-administering-cloud-services.

- Federal Financial Institutions Examination Council (FFIEC), "Joint Statement: Security in a Cloud Computing Environment," news release, April 30, 2020, https://www.ffiec.gov/press/pr043020.htm.
- FFIEC, *Bank Secrecy Act/Anti-Money Laundering Examination Manual* (Arlington: FFIEC, February 2015), https://bsaaml.ffiec.gov/manual.
- FFIEC, *Cybersecurity Assessment Tool* (Arlington: FFIEC, May 2017), https://www.ffiec.gov/pdf/cybersecurity/ffiec_cat_may_2017.pdf.
- FFIEC, *Cybersecurity Resource Guide for Financial Institutions* (Arlington: FFIEC, September 2022), https://www.ffiec.gov/press/pdf/FFIECCybersecurityResourceGuide2022ApprovedRev.pdf.
- FFIEC, *Authentication and Access to Financial Institutions Services and Systems* (Arlington: FFIEC, August 2021), https://www.ffiec.gov/guidance/Authentication-and-Access-to-Financial-Institution-Services-and-Systems.pdf.
- Financial Crimes Enforcement Network, "Interagency Statement on Sharing Bank Secrecy Act Resources," news release, October 3, 2018, https://www.fincen.gov/news/news-releases/interagency-statement-sharing-bank-secrecy-act-resources.
- National Institute of Standards and Technology (NIST), "NIST Cybersecurity Framework," https://www.nist.gov/cyberframework.
- National Security Agency – Cybersecurity Information, *Mitigating Cloud Vulnerabilities* (Washington: NSA, January 2020), https://media.defense.gov/2020/Jan/22/2002237484/-1/-1/0/CSI-MITIGATING-CLOUD-VULNERABILITIES_20200121.PDF.