Third-Party Risk Management (TPRM)

Why is third-party risk management important?

Financial institutions do not operate in a vacuum. Institutions rely on service providers and other third-party vendors to help with everything from the most mundane administrative tasks to the most mission-critical activities. And it's this reliance that makes managing these relationships so critically important. Furthermore, as third-party artificial intelligence (AI) solutions continue to emerge and find their way into financial institutions, the need for diligent vendor risk management practices will only continue to increase. A sound **third-party risk management (TPRM) program** that actively addresses all stages of the third-party relationship life cycle is the foundation for identifying, managing, and mitigating these existing and emerging risks.

Interagency Guidance on Third-Party Relationships: Risk Management

In June 2023, the federal banking agencies released *Interagency Guidance on Third-Party Relationships: Risk Management*, which "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 also provides some foundational considerations for third-party relationship management, including the following:

- **Sound third-party risk management takes into account the level of risk, complexity, and the size of the banking organization and the nature of the third-party relationship.**
- **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.**
- **Sound risk management includes an analysis of risk with each relationship and tailored risk management practices commensurate with the banking organization's size, complexity, and risk profile and with the nature of the third-party relationship.**[1]

While the aforementioned regulatory guidance applies to banking institutions, the principles outlined here are **equally important for nonbank financial institutions** as well – particularly in view of service provider oversight requirements contained in the Federal Trade Commission's Safeguards Rule.

Third-party risk management governance

Management of third-party relationships can be complex, depending on the volume, complexity, and risk associated with the institution's portfolio of relationships. **Oversight and accountability for the TPRM process ultimately lies with the institution's board of directors**, which provides "clear guidance regarding acceptable risk appetite, approves appropriate polices, and ensures that appropriate procedures and practices have been established." Similarly, 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." The interagency guidance notes that, "It is important for a banking organization to conduct **periodic independent reviews to assess the adequacy of its third-party risk management processes**." Finally,

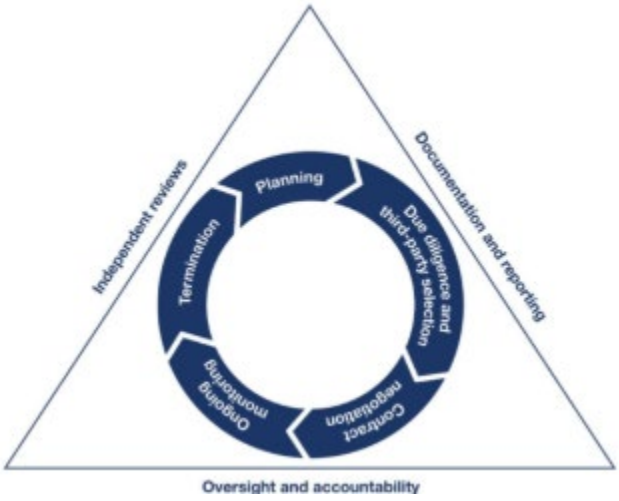
[1] Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, and Office of the Comptroller of the Currency. Interagency Guidance on Third-Party Relationships: Risk Management. June 2023.

thorough documentation and reporting of third-party risk management processes is also important to "assist those within or outside of the banking organization who conduct control activities."[2]

The third-party risk management life cycle

Generally, third-party relationships follow a logical life cycle:

- Planning
- Due diligence and third-party selection
- Contract negotiation
- Ongoing monitoring
- Termination[3]



Graphic Source: Board, FDIC, and OCC

Planning

At its core, the **planning stage** "allows a banking organization to evaluate and consider how to manage risks before entering into a third-party relationship." Considerations in the planning stage include:

- Evaluation of the strategic purpose of the relationship and its alignment with, among other things, the institution's overall goals, risk appetite, and corporate policies
- Benefits and risks of the relationship
- Nature of the relationship (activity volume, technology needed, etc.)
- Relationship costs
- Impact on employees
- Potential physical and information security implications
- How the institution will select, assess, and oversee the third party
- Ability to provide adequate oversight
- Contingency plans for exiting the relationship[4]

[2] Ibid.
[3] Ibid.
[4] Ibid.

Due diligence and third-party selection

Pre-selection due diligence allows the institution to "determine if a relationship would help achieve a banking organization's strategic and financial goals", and "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. 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." Due diligence considerations for prospective relationships include:

- Strategies and goals of the third party
- Legal and regulatory compliance
- Financial condition
- Business experience
- Qualifications and background of key personnel
- Risk management effectiveness
- Information security implications
- Business processes and management information systems
- Operational resilience
- Incident reporting and management processes
- Physical security
- Reliance on subcontractors
- Insurance coverage
- Contractual arrangements with other parties[5]

Contract negotiation

Once the institution performs its initial due diligence and chooses to enter into a relationship with a third party, the institution (in conjunction with legal counsel, if warranted) will determine whether the relationship warrants a formal contract and, if so, **negotiates contract terms** that "will facilitate effective risk management and oversight and that specify the expectations and obligations" of both parties. Considerations for negotiating an appropriate contract include:

- Nature and scope of the arrangement
- Well-defined performance measures or benchmarks
- Responsibilities for providing, receiving, and retaining information
- Right to audit and require remediation
- Responsibility for compliance with applicable laws and regulations
- Costs and compensation
- Ownership and license
- Confidentiality and integrity
- Operational resilience and business continuity
- Indemnification and limits on liability
- Insurance
- Dispute resolution and customer complaints

[5] Ibid.

- Use of subcontractors
- Provisions for foreign-based third parties (where applicable)
- Default and termination terms
- Considerations for regulatory supervision[6]

Ongoing monitoring

A critical step in the TPRM life cycle model is the **ongoing monitoring of third-party relationships**. Once the institution has entered into the relationship, ongoing monitoring of the relationship "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." This monitoring, as with other aspects of the TPRM life cycle, should be "commensurate with the level of risk and the 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." Considerations for the ongoing monitoring of relationships include:

- Effectiveness of the relationship
- Changes to the third party's business strategies and agreements with other entities
- Changes in financial condition
- Changes to or lapses in insurance coverage
- Audits, testing results, and other reports
- Ongoing compliance with laws and regulations
- Changes in key personnel
- Reliance on subcontractors
- Training; responses to new threats, vulnerabilities, and incidents
- Ability to maintain confidentiality, integrity, and availability of systems and data
- Business resiliency capabilities
- External factors that might impact the third party
- Volume and nature of complaints against the third party.[7]

Termination

There are instances where an institution may elect to **sever a relationship** with a third party. This might be due to a breach of contract, a failure of the third party to comply with laws or regulation, or simply because the institution wants to move in a different direction. However, simply severing a relationship with a third party isn't always easy. Depending on the nature and complexity of the relationship, there are a number of factors to consider, including:

- Options to facilitate the transition of services
- Capabilities, resources, and timeframes for transitioning
- Costs and fees associated with the termination

[6] Ibid.
[7] Ibid.

- Management of risks associated with data retention and destruction, access control, and connections with systems
- Joint intellectual property issues
- Management of risks to the institution and its customers if termination occurs due to the third party's inability to meet institutional expectations.[8]

Third-party risk management and emerging technologies

The continued emergence of AI and other technologies has provided institutions with a glimpse into new efficiencies, cost savings, and even improvements to the customer experience. However, as with the integration of any technology into the institution's environment, appropriate product and vendor due diligence is necessary to ensure that the technology **meets the institution's strategic and operational needs** and **does not introduce unacceptable risks to the institution**. In the early stages of the new technology life cycle, new products- as well as their vendors- may be numerous but may also lack the maturity and experience associated with long-standing technologies and providers. For these reasons, the utilization of strong third-party risk management practices is essential to ensure that new relationships with emerging technology providers and their products are beneficial, well-understood, and secure for the organization and its customers.

[8] Ibid.

Third-Party Risk Management (TPRM)
Questions Board Members Should Ask

Below are some questions to ask management to ensure that the institution's third-party risk management program addresses all stages of the third-party relationship life cycle for its vendors and service providers.

1. ***Does the institution's TPRM program and policy address the planning stage of the TPRM life cycle?***

   WHY THIS IS IMPORTANT: At its core, the ***planning stage*** *of the TPRM life cycle "allows a banking organization to evaluate and consider how to manage risks before entering into a third-party relationship." Considerations in the planning stage include, among other things, whether the proposed relationship strategically aligns with the institution's goals, risk appetite, and policies; benefits and risks of the relationship; the nature of the relationship; costs and potential impact to employees; and the ability to provide adequate oversight of the relationship.*[1]

2. ***Does the TPRM program and policy address due diligence and selection requirements for prospective third-party relationships?***

   WHY THIS IS IMPORTANT: ***Pre-selection due diligence*** *allows the institution to "determine if a relationship would help achieve a banking organization's strategic and financial goals", and "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. 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." Important due diligence considerations include, among other things, the financial condition and business experience of the vendor or service provider, information security implications, vendor resilience, and reliance on subcontractors.*[2]

3. ***Does the TPRM program and policy address the negotiation of contracts?***

   WHY THIS IS IMPORTANT: Once the institution performs its initial due diligence and chooses to enter into a relationship with a third party, the institution (in conjunction with legal counsel, if warranted) will determine whether the relationship warrants a formal contract and, if so, ***negotiates contract terms*** *that "will facilitate effective risk management and oversight and that specify the expectations and obligations" of both parties. Typical considerations for negotiation include the nature and scope of the agreement; well-defined performance measures or benchmarks; responsibilities for providing, receiving, and retaining information; costs and compensation; data confidentiality and integrity; use of subcontractors; dispute resolution; and default and termination terms.*[3]

---

[1] Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, and Office of the Comptroller of the Currency. Interagency Guidance on Third-Party Relationships: Risk Management. June 2023.
[2] Ibid.
[3] Ibid.

4. ***Does the TPRM program and policy address the ongoing monitoring of third-party relationships?***

   WHY THIS IS IMPORTANT: ***Ongoing monitoring*** *of the relationship "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." This monitoring, as with other aspects of the TPRM life cycle, should be commensurate with the level of risk and the complexity of the relationship and the activity performed by the third party.

   Further, "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." Considerations for the ongoing monitoring of relationships include, among other things, an evaluation of the effectiveness of the relationship; changes in financial condition; ongoing compliance with laws and regulations; changes in key personnel; reliance on subcontractors; and the ability to maintain the confidentiality, integrity, and availability of systems and data.[4]

5. ***Does the TPRM program and policy address the termination of third-party relationships?***

   WHY THIS IS IMPORTANT: There are instances where an institution, for a variety of reasons, may elect to ***terminate a relationship*** *with a third party. Simply severing a relationship with a third party isn't always easy. Depending on the nature and complexity of the relationship, there are a number of factors to consider including, but not limited to, options to facilitate the transition of services; capabilities, resources, and timeframes for transitioning; costs and fees associated with the termination of services; management of risks associated with data retention, access control and system connections; and impacts to the institution and its customers if termination occurs due to the third party's inability to meet institutional expectations.*[5]

[4] Ibid.
[5] Ibid.