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.