# Third-Party Risk Management – Proposed Rulemaking

AUGUST 2021


**AUTHORS:**

**Joe Sergienko**
Managing Director
jsergienko@thinkbrg.com
617.925.4091

**Michael Canale**
Managing Director
michael.canale@thinkbrg.com
646.809.8082

**Saule Kassengaliyeva**
Managing Consultant
skassengaliyeva@thinkbrg.com
202.480.2743

**Lindsay Furr**
Senior Managing Consultant
lfurr@thinkbrg.com
646.876.4659


INTELLIGENCE THAT WORKS

BRG


*In July, the Federal Reserve Board, Federal Deposit Insurance Corporation, and Office of the Comptroller of the Currency (OCC) (collectively, "the agencies") published "Proposed Interagency Guidance on Third-Party Relationships: Risk Management"[1] (herein referred to as the "Proposed Guidance").*

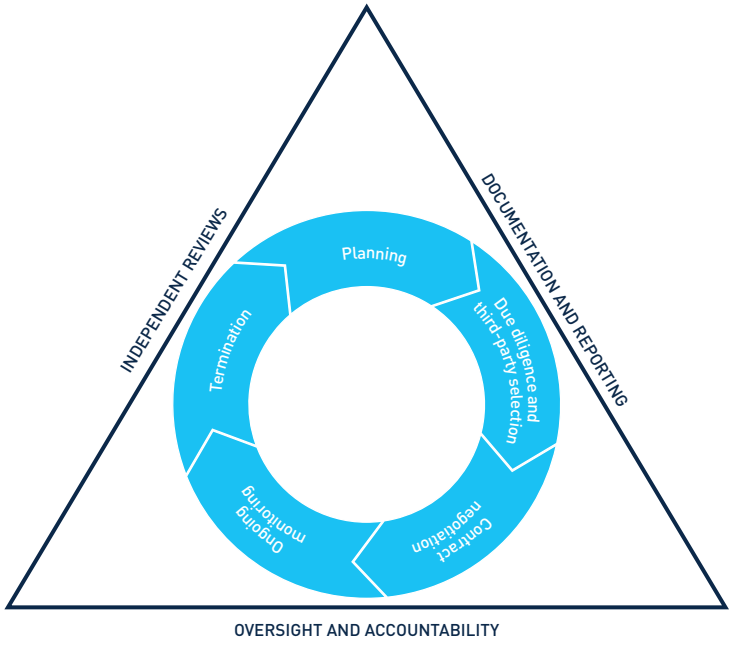
The Proposed Guidance emphasizes the importance of managing risks associated with third-party relationships, including an increased focus on relationships with fintechs and other technology providers. The comment period for this proposed rule is sixty days from the distribution date. While the Proposed Guidance likely will change based on comments received, it provides important insight into current supervisory thinking and what the agencies are looking for at banking institutions, particularly those with significant third-party relationships.

The agencies note that each has issued previous third-party risk management guidance and aims to promote consistency with the Proposed Guidance by leveraging the OCC's Third-Party Risk Management Guidance from 2013. The Proposed Guidance recognizes the differences in nature, level of risk, and complexity of the banking organization and the third-party relationships.

The Proposed Guidance emphasizes that the use of third parties does not diminish a banking organization's responsibility to perform activities in a safe and sound manner and in compliance with applicable laws and regulations. This underscores the need for an organization to understand its relationship with a third party, including what services the third party is performing for the organization or its customers and how these are performed. The banking organization also should understand the third party's risk and compliance framework to ensure the organization is comfortable with the third party's control environment and that it is in compliance with the applicable laws and regulations.

1 Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, and Office of the Comptroller of the Currency, "Agencies request comment on proposed risk management guidance for third-party relationships," press release (July 13, 2021), available at: https://www.federalreserve.gov/newsevents/pressreleases/bcreg20210713a.htm

The agencies provide a framework through which a banking organization can manage its third-party relationship and, therefore, the associated risk.




SOURCE: Board, FDIC, and OCC

The Proposed Guidance breaks down and provides expectations for the lifecycle elements as banking organizations are considering/managing the use of third-party relationships.

1. **Planning:** Consider the service offering provided by the third party, and conduct a risk assessment of the third party and the service offering. Depending on the risk level for the organization, additional reviews or escalations may be needed.
2. **Due Diligence and Third-Party Selection:** Consider the operating environment, the risks associated with the third party, the control environment, and whether the control environment mitigates the risks. In addition, understand and determine whether residual risk is appropriate given the relationship and the banking organization's risk appetite.

## *Items That Are Typically Considered*

- Strategies and goals
- Legal and regulatory compliance
- Financial condition
- Business experience
- Fee structure and incentives
- Qualifications and backgrounds of company principals
- Risk management
- Information security
- Management of information systems
- Operational resilience
- Incident reporting and management programs
- Physical security
- Human resource management
- Reliance on subcontractors
- Insurance coverage
- Conflicting contractual arrangements with other parties

3. **Contract Negotiations:** Consider the contract provisions the banking organization needs to protect itself, its customers, and other stakeholders. Organizations will need to consider what information is required by regulators to meet reporting requirements.
4. **Oversight and Accountability:** Since the board of directors ultimately is responsible for overseeing the banking organization's risk management processes, consider how management and the board will review the activity of the third party, including what reporting is needed and on what periodicity and what type of independent reviews will be conducted.

### *Items to Consider in Contracts*

- Nature and scope of arrangement
- Performance measures/service-level agreements or benchmarks
- Responsibilities for providing, receiving, and retaining information
- The right to audit and require remediation
- Responsibility for compliance with applicable laws and regulations
- Cost and compensation
- Ownership and license
- Confidentiality and integrity
- Operational resilience and business continuity
- Indemnification
- Insurance
- Dispute resolution
- Limits on liability
- Default and termination
- Customer complaints
- Subcontracting
- Foreign-based third parties
- Regulatory supervision

5. **Ongoing Monitoring:** Consider how the banking organization will review the performance of the third party: what key performance indicators (KPIs), reports, and information will the third party will provide? What type of periodic assessments (i.e., on-sites, scorecarding) or independent reviews will be completed? What day-to-day level of interaction is necessary for the relationship to be successful? Consider also that the relationship may change over time; therefore, a review of the appropriateness of the KPIs will be necessary.
6. **Termination:** Consider the logistics for terminating a third-party relationship and if alternatives are needed; how the banking organization's intellectual property and data will be secured/transferred; and the potential impact to customers, employees, and other stakeholders.

While much of this is not new, particularly to OCC-regulated institutions, the Proposed Guidance stresses banking organizations' ability to apply strong third-party risk management programs to more recent and future third-party relationships, such as fintechs. Many fintechs are relatively new and may not fit into the traditional box for some criteria, such as length of operation. The Proposed Guidance is clear that a banking organization may do business with entities that are still building controls or do not have the longevity of some other third parties, as long as the organization considers the risk, accepts the risk, implements appropriate controls, and monitors the risk on an ongoing basis.

Key considerations for third-party oversight of technology based vendors include:

1. Evaluate operational and compliance maturity. The vendor, depending on its lifecycle stage, may be operationally mature but lack the appropriate compliance management systems and controls.
2. Understand who is developing the technology, where data is being stored, and the risks associated with different models (e.g., is development performed in house or outsourced, are the resources onshore or offshore).
3. Pay particular attention to the legal, regulatory, and functional risks relating to cybersecurity. Evaluate system design, testing procedures, and written policies and procedures to deal with security breaches, notifications of breaches, and carrying the appropriate levels of insurance. (Note that if your data is being hosted, data breach insurance should be considered.)
4. Consider data privacy and the measures necessary based on where the banking organization and vendor collect and process data.
5. Review the Consumer Financial Protection Bureau's complaints database to see if the vendor has issues. Even if the company is below $10 billion in assets, the bureau has previously exercised its enforcement authority on fintechs using the Consumer Financial Protection Act's unfair and deceptive practices provisions. If a complaint is customer facing, obtain and review complaints data from your customers.
6. Define service level agreements (SLAs) in the contract and consider adding penalties for nonperformance, as well as incentives for exceeding expectations. Provide appropriate time for vendors to cure failures, and include the right to reevaluate SLAs thresholds on a periodic or annual basis.

In our experience, third parties are often willing to work with banking organizations on their needs and address concerns when the organizations outline the requirements and try to limit the surprises. For example, if a third party is offering a service that will likely need to be audited, providing for that requirement in the contract is critical.

These requirements may seem daunting, but if banking organizations take a thoughtful approach and depict the processes and services the third party is providing, the organizations will be able to risk-rate and prioritize its efforts. Through the Proposed Guidance, the agencies are seeking to ensure that banking organizations have processes to identify, manage, and monitor the risks associated with third parties, including those newer relationships with fintechs, including an understanding that these relationships change on an ongoing basis and should be reassessed regularly

## HOW BRG CAN HELP

- Review third-party risk management programs
- Conduct gap assessments to regulatory guidance
- Conduct third-party risk assessments
- Create ongoing monitoring programs
- Draft third-party risk management programs


## About BRG

Berkeley Research Group, LLC (BRG) is a global consulting firm that helps leading organizations advance in three key areas: disputes and investigations, corporate finance, and performance improvement and advisory. Headquartered in California with offices around the world, we are an integrated group of experts, industry leaders, academics, data scientists, and professionals working beyond borders and disciplines. We harness our collective expertise to deliver the inspired insights and practical strategies our clients need to stay ahead of what's next. Visit thinkbrg.com for more information.

**THINKBRG.COM**