Davis Polk

Bank risk management of third-party relationships – Final interagency guidance

June 12, 2023

Table of contents

Background and highlights

01

Background

On June 6, 2023, the Federal Reserve, FDIC and OCC (the Agencies) released final Interagency Guidance on banking organizations' management of risks associated with third-party relationships.

- This joint guidance replaces the Agencies' existing, separate third-party risk management guidance.
- The Interagency Guidance responds to the continued and growing prevalence of relationships between banking organizations and third parties, including both traditional service providers and fintechs.

The Interagency Guidance is largely consistent with the proposal released on July 13, 2021 (the Proposed Guidance). Like the Proposed Guidance, it is based on the OCC's existing guidance and broadly consistent with each of the Agencies' existing guidance it replaces.

- Like the Agencies' existing guidance, the Interagency Guidance:
  - Emphasizes that **a banking organization is ultimately responsible** for conducting its activities—including activities conducted through a third party—in a safe and sound manner.
  - Provides that a banking organization should adopt risk management practices that are **commensurate with the risk posed by its third-party relationships**.

Changes from Proposed Guidance

Key changes from the Proposed Guidance include:

- Explicitly referencing as in scope **partnerships with new or novel structures and features**, which would include those in which fintechs interact directly with customers.
- The Interagency Guidance also adds a reference to maintaining a **complete inventory of all third-party relationships**, noting that the inventory and periodic risk assessments for each third-party relationship are supportive of a banking organization's sound risk management over time.
- Stating that **each Agency will tailor the scope of its supervisory review** of a banking organization to the degree of risk and the complexity associated with the banking organization's activities and third-party relationships. The Interagency Guidance adds that examiners will consider that "not all third-party risk relationships present the same risks, and that banking organizations accordingly tailor their practices to the risks presented."
- Unlike the Proposed Guidance, the final Interagency Guidance **does not specifically exclude customer relationships** from the definition of "business arrangement." In the preamble, the Agencies state the change is intended to reduce ambiguity because some business relationships may incorporate elements or features of a customer relationship.
  - In a related statement, FDIC Director Jonathan McKernan argued the change itself creates ambiguity as to whether the Interagency Guidance "applies to arrangements involving depositors, borrowers, or other customers of traditional banking services."
  - The FDIC's Financial Institution Letter accompanying the Interagency Guidance clarifies that: "Relationships that are only between banks and their direct customers of traditional bank products and services (such as deposit accounts or retail or commercial loans) would not be addressed in a third-party risk management framework . . . ."

Changes from Proposed Guidance

Further key changes from the Proposed Guidance include:

- Revising the **definition of "critical activities,"** including by eliminating from the definition the proposed concepts of "significant bank functions" and activities "requir[ing] significant investment in resources to implement the third-party relationship and manage the risk."
- Placing greater emphasis on the nature of the considerations listed in the Interagency Guidance as **merely illustrative examples, not requirements**, and noting that they may not apply to every banking organization or to each third-party relationship.
- Incorporation of concepts from several of the OCC's 2020 FAQs on Third-Party Relationships within the text of the Interagency Guidance. For example, the Interagency Guidance:
  - acknowledges that a bank may have **limited negotiating power in contract negotiation**, consistent with OCC FAQ 5;
  - emphasizes the importance of a banking organization having a "**sound methodology to designate which activities and third-party relationships** receive more comprehensive oversight," similar to OCC FAQ 8; and
  - clarifies expectations for banking organizations' risk management of a third party's reliance on **subcontractors**, in line with OCC FAQ 11.
- Adding an explicit statement that as guidance, the Interagency Guidance **does not have the force and effect of law** and does not impose new requirements on banking organizations.
  - Nevertheless, the Interagency Guidance will inform how the Agencies will engage in supervision of banking organizations' third-party risk management programs.
- Clarifying the **responsibilities of a board of directors** of a banking organization, including providing oversight for third-party risk management and holding management accountable, providing clear guidance regarding acceptable risk appetite, approving appropriate policies and ensuring that appropriate procedures and practices have been established.
- Clarifying that the term **"foreign-based third party"** refers to a third party whose servicing operations are located in a foreign country and subject to the law and jurisdiction of that country, not U.S.-based subsidiaries of foreign firms.

Broad, principles- and risk-based approach

The Interagency Guidance applies to *all* third-party relationships—i.e., "any business arrangement between a banking organization and another entity, by contract or otherwise."

- Such relationships "may exist despite a lack of a contract or remuneration" and can include "outsourced services, use of independent consultants, referral arrangements, merchant payment processing services, services provided by affiliates and subsidiaries, and joint ventures."

The Interagency Guidance provides a principles- and risk-based framework that can be used by a banking organization to develop its third-party risk management practices.

- The Interagency Guidance emphasizes that a banking organization is responsible for conducting its activities—including through a third party—in a safe and sound manner. Effective risk management practices underpin a safe and sound operation.
- The Agencies underscore that 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.
- In response to public feedback on the prescriptiveness of the Proposed Guidance, the Agencies reiterated that the Interagency Guidance is principles-based, noting that the examples provided in the Interagency Guidance are "not intended to be interpreted as exhaustive or to be used as a checklist."

Implications for banks and fintechs

02

Implications for banks

- Together with recent actions taken by the OCC and FDIC against banking organizations related to fintech partnerships and Acting Comptroller Hsu's frequent remarks highlighting risks associated with such partnerships and Banking-as-a-Service (BaaS) models, the Interagency Guidance underscores the Agencies' increased focus on third-party risk management in general and fintech partnerships in particular. It also underscores the vulnerabilities the Agencies see in the risk management of these relationships.

- We do not, however, expect banking organizations with mature compliance and third-party risk management processes and policies will need to make significant changes to their third-party risk management frameworks to meet the expectations outlined in the Interagency Guidance, given that it is broadly consistent with the Agencies' previous guidance.

- Banking organizations may still want to compare these frameworks to the Interagency Guidance to identify any potential gaps. Where gaps are identified banking organizations may consider updates to their policies and procedures, as well as whether reviews of existing third-party relationships are warranted.

- State banks may have to make more updates to their third-party risk management frameworks given that the Interagency Guidance is based on the OCC's previous guidance, which was more prescriptive and detailed than that of the Federal Reserve and FDIC.

Implications for banks

- Because examination staff often focus on documentation of risk-management activities, banking organizations may want to consider whether enhancements to documentation related to third-party risk management would be helpful to formalize or evidence existing processes or procedures. In particular, banking organizations should consider implementing or enhancing an existing inventory of all third-party relationships.

- Banking organizations may also want to review their policies and procedures to assess whether they appropriately reflect a risk-based approach to third-party risk management. We expect that most banking organizations already take such an approach, even if not formally documented. In particular, banking organizations may want to update or implement a process for identifying "critical activities" as defined in the Interagency Guidance.

- Given that the preamble to the Interagency Guidance confirms that the intended scope of relationships covered is broad, banking organizations may want to review the scope of their existing third-party risk management framework and consider whether any changes are warranted (e.g., the Federal Reserve's previous guidance was limited to outsourcing relationships with service providers).

Implications for fintech partnerships

- Although the Interagency Guidance applies directly only to banking organizations, **fintechs that partner or want to partner with banking organizations will need to be aware** of the framework it creates.
  - For example, fintechs should expect their banking organization counterparties to point to the Interagency Guidance as the basis for due diligence requests, contract negotiation positions and the need for ongoing monitoring procedures.
  - Fintechs may see increased focus on third-party risk management from state banks in particular, as the Interagency Guidance is more prescriptive and detailed than the previous guidance applicable to state banks.
  - The scope of relationships covered by the Interagency Guidance is broader than that of existing Federal Reserve guidance, which is limited to outsourcing relationships with service providers and would not necessarily apply to, for example, partnership arrangements with fintechs. Some state member banks may begin applying third-party risk management processes to fintech partnerships where they did not do so previously.

Implications for fintech partnerships

- The Agencies **declined to provide guidance on specific third-party relationships—such as data aggregators and other fintechs—within the Interagency Guidance**, instead providing guidance applicable to all third-party relationships.
  - In the preamble to the Interagency Guidance, however, the Agencies noted that some relationships between banking organizations and fintechs involve "new or novel structures and arrangements" that "may introduce new or increase existing risks to a banking organization," including through interactions directly between the fintech and the bank's customers.
  - Such relationships may be subject to heightened scrutiny by banking organizations due to the risk-based approach reflected in the Interagency Guidance.
- It remains to be seen whether the Agencies' increased focus on third-party relationships will result in an increased number of examinations of service providers under the Bank Service Company Act.
  - The Bank Service Company Act authorizes the Agencies to regulate and examine the performance of services authorized under the Act provided to banking organizations by third-party service providers.

Implications for fintechs and community banks

- The Agencies underscore that the framework **provides flexibility to banking organizations** in their approach to assessing the risk posed by a third-party relationship and the Interagency Guidance **provides illustrative examples** to help banking organizations.
- In the preamble to the Interagency Guidance, the Agencies state they "plan to develop additional resources to assist smaller, non-complex community banking organizations in managing relevant third-party risks."
- Nonetheless, the complexity and cost of the onboarding process for both smaller banks and fintechs alike may hinder bank-fintech partnerships.
  - Federal Reserve Governor Michelle W. Bowman did not support the Interagency Guidance, citing in her statement concerns that the Agencies have not yet developed "clear, usable, and more appropriately tailored expectations for small banks when considering third-party risk management" like those accompanying the Federal Reserve's past third-party risk management guidance.
  - In remarks shortly before the release, FDIC Vice Chairman Travis Hill described his support for a proposed public/private standards-setting organization that "would enable banks to on-board fintechs and technologies that had received a 'seal of approval,' reducing the need for each bank to conduct costly, time-consuming due diligence of its own."

Implications for BSA/AML compliance for fintechs and banks

- Bank-fintech partnerships pose many challenges both for banking organizations and their fintech partners, especially with respect to BSA/AML compliance.
  - This is particularly true for BaaS models, where the fintech's customers are able to access bank products and services but the banking organization has no customer-facing role and is dependent on its fintech partner to apply customer identification and due diligence procedures, monitor transactions and identify suspicious activity, among other things.
- As demonstrated by recent enforcement actions, a banking organization risks enforcement action if a fintech third party does not have a compliance program commensurate with the BSA/AML risks posed by the customer.
  - Banking organizations can manage these risks through application of the principles set forth in the Interagency Guidance, such as conducting due diligence, including contractual provisions that clearly address allocation of responsibilities and having adequate oversight.
  - However, ensuring that a third party has an adequate compliance program can be difficult operationally where there are misalignments in regulatory requirements, compliance culture or resources.

Overview of the Interagency Guidance

03

Organization of the Interagency Guidance

The Interagency Guidance is organized in **four parts**:

- **Risk Management**
- **Third-Party Relationship Life Cycle**
  - Planning
  - Due Diligence and Third-Party Selection
  - Contract Negotiation
  - Ongoing Monitoring
  - Termination
- **Governance**
  - Oversight and Accountability
  - Independent Reviews
  - Documentation and Reporting
- **Supervisory Reviews of Third-Party Relationships**

Risk management

According to the Interagency Guidance, banking organizations should analyze the risks associated with each third-party relationship, applying "more comprehensive and rigorous oversight and management of third-party relationships that support higher-risk activities, including **critical activities**."

- Critical activities are identified by each banking organization, and include 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 the banking organization's financial condition or operations**.

- The Interagency Guidance describes as key elements of risk management:
  - Maintaining a **complete inventory** of third-party relationships and periodically conducting **risk assessments** for each third-party relationship; and
  - Applying a **sound methodology** to designate which activities or relationships require more comprehensive oversight.

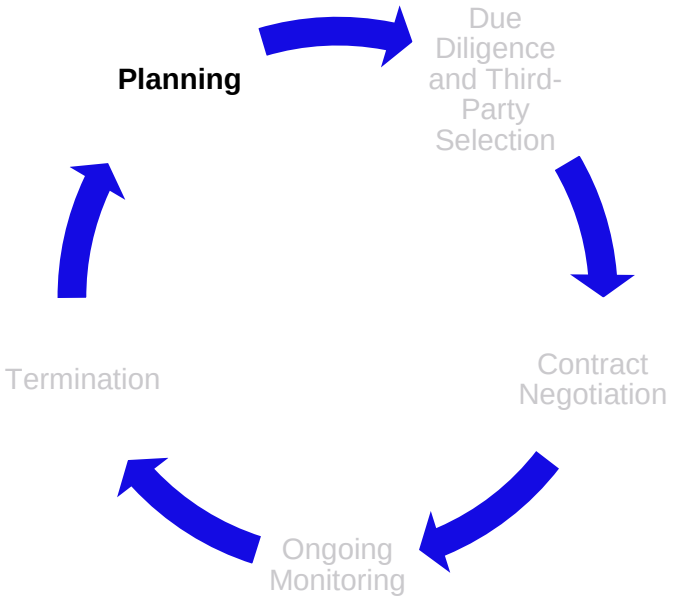
Third-party relationship life cycle – Overview

Effective third-party risk management generally follows a five-stage continuous life cycle, according to the Interagency Guidance.

- The Interagency Guidance provides a non-exhaustive set of examples of considerations that a banking organization typically may consider at each stage of this life cycle.
- The Agencies emphasize that the relevance of any particular example depends upon the facts and circumstances of the banking organization.
- No matter the stage of the life cycle, the Agencies stress the importance of involving staff with the requisite knowledge and skills.

The governance overlay across the life cycle involves independent reviews, documentation and reporting, and oversight and accountability.

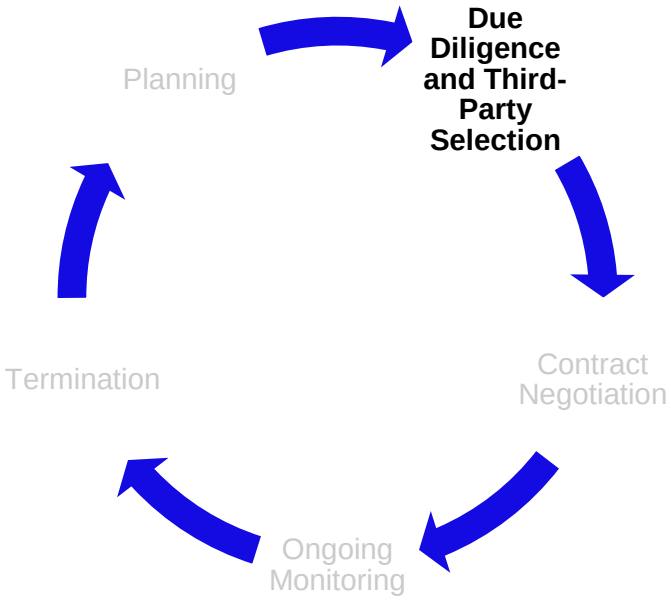
Planning stage



At the planning stage, a banking organization evaluates risks before entering into a third-party relationship. 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:

- The strategic purpose of the arrangement
- The benefits and risks of the relationship and how to manage them
- The nature of the business arrangement
- The estimated costs of the relationship
- How the relationship will affect the banking organization's employees
- The impact on customers
- Information security implications
- Physical security implications
- How the banking organization will select, assess and oversee the third party
- The banking organization's ability to provide adequate oversight and management
- Contingency plans if the relationship needs to be terminated

Due diligence and third-party selection stage

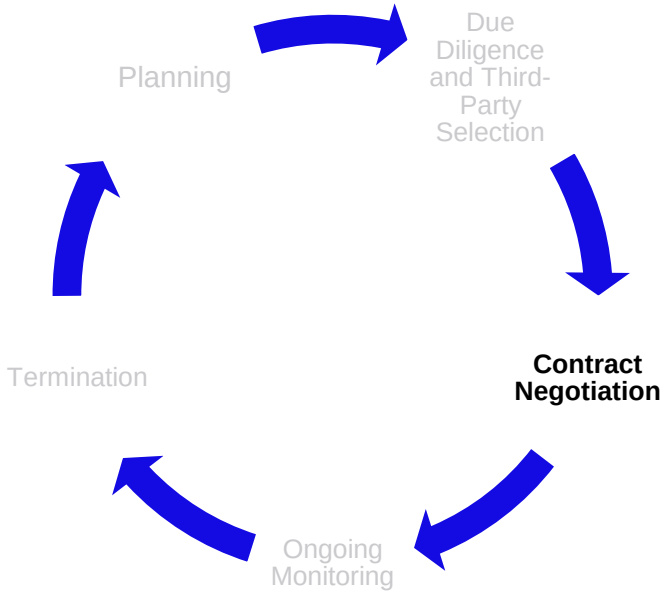


The Agencies note in the preamble that collaboration with other banking organizations and engaging with third parties that specialize in conducting due diligence could be beneficial and reduce burdens, and made clarifying revisions in that regard. A banking organization must nonetheless evaluate the conclusions from those collaborative efforts based on its own circumstances.

The Agencies emphasize the importance of due diligence before entering into a relationship with each third party, at a level commensurate with the level of risk and complexity of the relationship. Typically, a banking organization reviews factors including a third party's:

- Business strategy and goals
- Ownership structure and legal and regulatory compliance capabilities
- Financial condition (including review of audited financial statements and other filings)
- Depth of resources and prior business experience
- Qualifications and experience of key personnel
- Overall risk management effectiveness
- Information security program
- Management of information systems
- Operational resilience in the event of disruptions or incidents
- Incident reporting and management processes
- Physical security measures
- Reliance on subcontractors
- Scope of insurance coverage
- Contractual arrangements with other parties

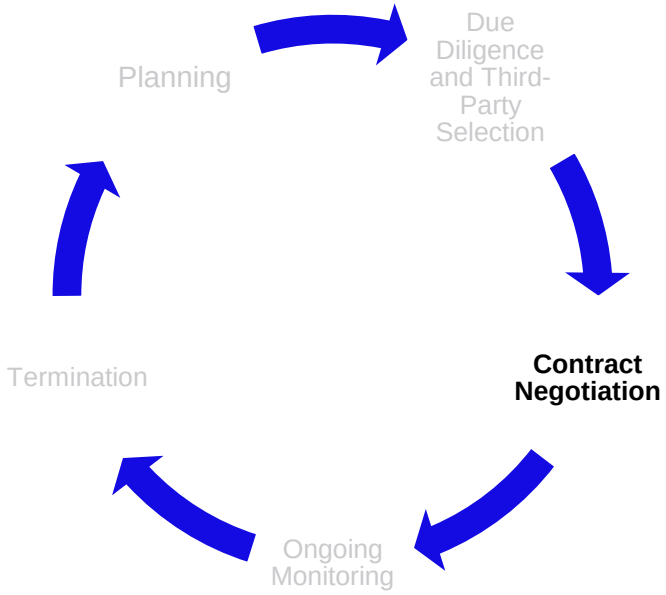
Contract negotiation stage



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:

- Whether a written contract is needed
- The establishment of clear rights and responsibilities of each party
- Clearly defined performance measures to evaluate the third party
- Responsibilities for providing, receiving and retaining information
- The banking organization's right to audit and require remediation of identified issues
- Responsibility for compliance with applicable laws and regulations
- Clear descriptions of all cost and compensation arrangements
- Ownership and licensing rights to the bank's property
- Confidentiality and integrity of information
- Operational resilience and business continuity
- Indemnification provisions and limits on liability
- Insurance requirements for the third party
- Methods of dispute resolution
- Procedures for handling customer complaints
- The permissibility of subcontracting
- Choice-of-law and jurisdictional provisions in the case of a foreign-based third party
- Default and termination procedures
- Stipulating that the third party's performance of activities is subject to regulatory examination and oversight

Contract negotiation stage

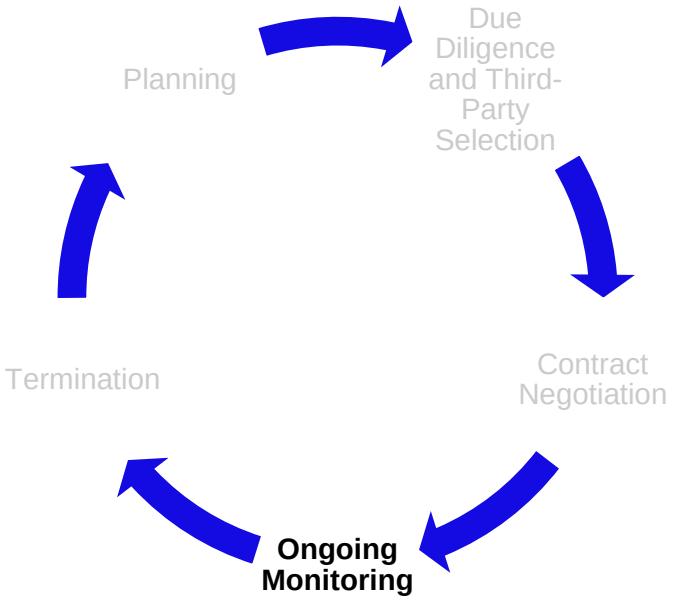


In response to feedback on the Proposed Guidance, the Interagency Guidance acknowledges the possibility of a banking organization having limited negotiating power.

- According to the Interagency Guidance, in such difficult contract negotiations, it is important for the banking organization to understand any resulting limitations and consequent risks, for example by 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.
- The Interagency Guidance notes that in certain circumstances, banking organizations may gain an advantage by negotiating contracts as a group with other organizations.

A banking organization's board of directors should be aware of and, as appropriate, may approve or delegate approval of contracts involving higher risk activities.

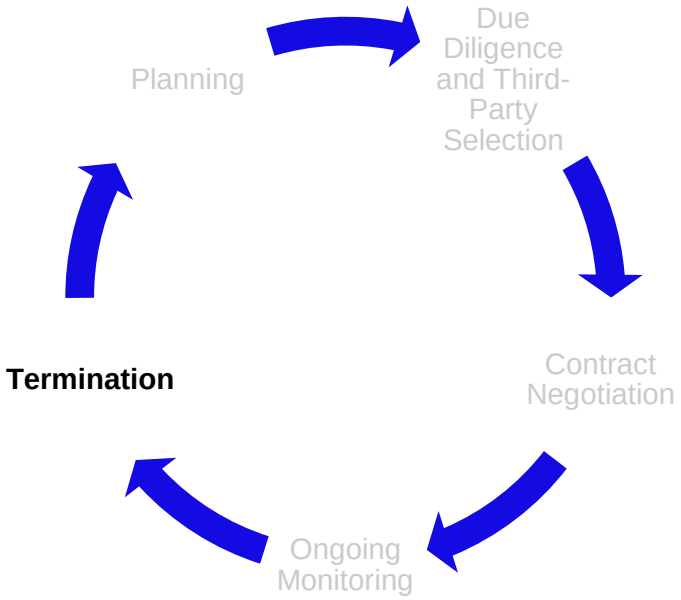
Ongoing monitoring



The Interagency Guidance describes ongoing monitoring throughout the duration of the relationship as integral to effective risk management. Depending on the risk and complexity of the relationship, a banking organization typically considers the following factors, among others:

- The overall effectiveness of the relationship
- Changes to the third party's business strategy
- Changes to the third party's financial condition
- Changes to the third party's insurance coverage
- Relevant audits, testing results and similar reports
- The third party's ongoing compliance with laws and regulations
- Changes in key personnel
- Reliance on and exposure to subcontractors
- Training provided to banking organization and third-party employees
- The third party's response to changing threats and vulnerabilities
- The third party's ability to maintain the confidentiality, availability and integrity of the banking organization's systems and information
- The third party's response to incidents and business continuity and resumption plans
- External factors and conditions that could affect performance, finances or operations
- The volume and nature of customer inquiries and complaints, and the adequacy of the response

Termination



The Interagency Guidance notes that where a banking organization terminates a third-party relationship, management should do so in an efficient manner and consider how to transition services by bringing them in-house, contracting with another third party or discontinuing the activity.

Depending on the risk and complexity of the relationship, banking organizations typically consider the following factors to facilitate termination:

- Options for an effective transition of services
- Relevant capabilities and resources and the timeframe for transition
- Associated costs and fees
- Risks associated with data retention and destruction
- Handling of joint intellectual property
- Managing the risks to the banking organization and its customers if the termination happens as a result of the third party's inability to meet expectations

Governance

Oversight and accountability | Independent reviews | Documentation and reporting

The Interagency Guidance does not describe how a banking organization should structure its third-party risk management governance process. Rather, it describes three categories of practices typically considered through all five stages of the life cycle.

Oversight and accountability: The banking organization's board of directors bears ultimate responsibility for oversight of third-party risk management and for holding management accountable. The board should provide clear guidance on acceptable risk appetite for the banking organization, approve appropriate policies and ensure that policies and procedures are established. Management, in turn, is primarily responsible for developing and implementing the requisite policies, procedures and practices. The Interagency Guidance provides several factors typically considered by a board and activities typically performed by management when carrying out their responsibilities.

Independent reviews: The Interagency Guidance emphasizes the importance of conducting periodic independent reviews to assess the adequacy of risk management processes, and provides several factors considered in such reviews. The Interagency Guidance expands upon the Proposed Guidance by making explicit that, in addition to reviewing the third party's alignment with the banking organization's business strategy, independent reviews should also assess the adequacy of the design and operation of the banking organization's own processes and controls.

Documentation and reporting: A banking organization should properly document and report on its third-party risk management processes and specific relationships throughout the life cycle. Documentation will vary among banking organizations based on the risk and complexity of their third-party relationships, but may include several items listed in the Interagency Guidance, including an inventory of all third-party relationships.

Supervisory reviews of third-party relationships – Banking organizations

Each Agency will review its supervised banking organizations' risk management of third-party relationships as part of the standard supervisory process. 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.

Examiners will typically conduct the following activities as part of their review:

- Assess the ability of the banking organization's management to oversee the third-party relationships
- Assess the impact of third-party relationships on a banking organization's risk profile and performance
- Perform transactional testing or review the results of testing
- Highlight and discuss any material risks and deficiencies in the risk-management process
- Review the banking organization's plans for remediation of any deficiencies, particularly involving critical activities
- Consider supervisory findings when assigning the components of ratings systems

Supervisory reviews of third-party relationships – Third-party service providers

The Interagency Guidance clarifies that, when circumstances warrant, an Agency may use its legal authority (e.g., under the Bank Service Company Act) to examine "functions or operations that a third party performs on a banking organization's behalf."

- Those 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, if needed, against the third parties in connection with their findings.

Davis Polk contacts

Contacts	Phone	Email
Dana Seesel Bayersdorfer	+1 212 450 3423	dana.bayersdorfer@davispolk.com
Luigi L. De Ghenghi	+1 212 450 4296	luigi.deghenghi@davispolk.com
Ledina Gocaj	+1 202 962 7054	ledina.gocaj@davispolk.com
Eric McLaughlin	+1 212 450 4897	eric.mclaughlin@davispolk.com
Daniel E. Newman	+1 212 450 4992	daniel.newman@davispolk.com
David L. Portilla	+1 212 450 3116	david.portilla@davispolk.com
Byron B. Rooney	+1 212 450 4658	byron.rooney@davispolk.com
Gabriel D. Rosenberg	+1 212 450 4537	gabriel.rosenberg@davispolk.com
Daniel P. Stipano	+1 202 962 7012	dan.stipano@davispolk.com
Margaret E. Tahyar	+1 212 450 4379	margaret.tahyar@davispolk.com