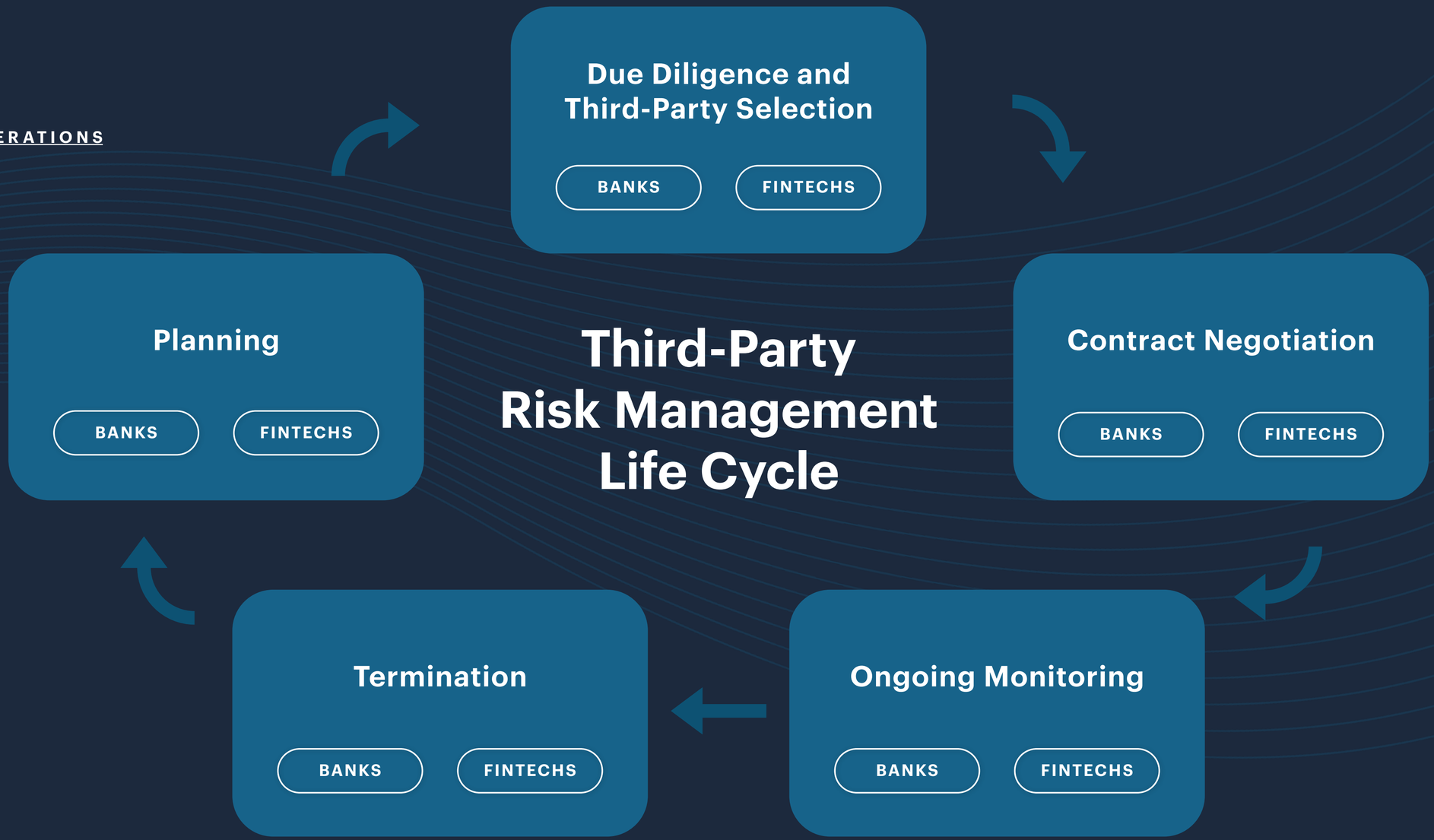
Federal Banking Agencies Final Third Party Risk Management Guidance: **A Tactical Resource for Banking Organizations and Fintechs Across the Risk Management Life Cycle**

## Table of Contents






DWT.COM | SRARISK.COM

SRA WATCHTOWER

Davis Wright Tremaine LLP

# Guidance Topic: Overview

BACK TO START

## Key Points

Definitions:

"Business Arrangement"

"Third-Party Relationship"

"Critical Activities"

## Considerations for Banking Organizations

**Business arrangements/third-party relationships** are interpreted broadly. Relationships can exist despite a lack of contract and can include outsourced services, referral arrangements, merchant payment processing services, services provided by affiliates and subsidiaries, and joint ventures

- Ensure your banking institution has a current list of all business arrangements/third-party relationships
- Periodically conduct risk assessments for each third-party relationship to determine whether risks have changed over time and whether risk management practices need to be updated accordingly

**Critical activities** include those activities that could (i) cause a banking organization to face significant risk if the third party fails to meet expectations; (ii) have significant customer impacts; or (iii) have a significant impact on a banking organization's financial condition or operations

- Be transparent with your third-party relationship partners; relationships supporting critical activities will receive more comprehensive and rigorous oversight

## Considerations for Fintechs or Service Providers

Fintechs are included in the list of third-party relationships, regardless of whether that relationship is governed by contract.

- Assume your relationship with each bank partner is covered by the Guidance
- Ensure your company maintains a current list of all business arrangements opposite your bank partners

Know whether your third-party relationship supports a bank partner's critical activities by directly asking your bank partner(s). If your view differs from your bank partner's, be prepared to explain it, but understand characterization is ultimately up to your bank partner(s)

- If you disagree with your bank partner's determination, consider partnering with a different bank that may be better suited to treat its activities as non-critical based on its risk profile

# Guidance Topic: Risk Management

BACK TO START

## Key Points

Principles-based guidance is designed to provide a flexible, risk-based approach that can be adjusted to the unique circumstances of each third-party relationship

## Considerations for Banking Organizations

Each banking organization is responsible for analyzing and calibrating the risks associated with each third-party relationship

- Develop or refine a sound methodology for identifying your critical activities and the third-party relationships that support them based on your institution's risk profile

Guidance is neither exhaustive nor mandatory – it is not a compliance checklist

- Before entering into a third-party relationship, understand its strategic purpose, how it aligns with the organization's overall strategic goals, objectives, risk appetite, risk profile, and broader corporate policies
- Leverage Interagency Guidance as a tool for explaining to third parties why certain protections may be necessary – e.g. audit rights

## Considerations for Fintechs or Service Providers

Each partner bank will likely have differing risk management practices based on their individual risk profiles

- Consider building/refining your fintech's risk management practices as a means of calibrating the risks associated with each of your bank partnerships

Fintechs that partner with multiple banks to support the same product or functionality should not expect that each bank will view the fintech's business and the risk profile of the third-party relationship similarly

- Expect your banking partner(s) to rely on all aspects of the Interagency Guidance as a basis for seeking protections during contract negotiations; also understand that the principles-based nature of the guidance means it is intended to be adjusted as needed based on unique circumstances

# Guidance Topic: Relationship Lifecycle

BACK TO START

## Key Points

Provides examples of life cycle risk management considerations at each stage

## Considerations for Banking Organizations

Involve staff with requisite knowledge and skills across your organization through each stage of the relationship life cycle

- Include the right experts across disciplines (e.g., compliance, risk, tech, legal)
- Ensure you have needed external support on issues that cannot be handled by in-house staff

# Guidance Topic: Relationship Lifecycle

BACK TO START

## Key Points

Provides examples of life cycle risk management considerations at each stage

## Considerations for Fintechs or Service Providers

Understand at the outset how your bank partner(s) support(s) fintech relationships across their organization. Consider differences in organizational structure as well as involvement of regulatory and risk experts

- Identify a single point of contact who will manage the relationship either directly with the fintech or through an intermediary

# Guidance Topic: Due Diligence and Third-Party Selection

BACK TO START

## Key Points

Activity must be conducted in a safe and sound manner

Relying solely on experience with or prior knowledge of a third party is not an adequate proxy for performing due diligence

## Considerations for Banking Organizations

Third parties that support critical activities warrant a greater degree of planning and consideration, and may require approval by the board or board committee. Understand the scope of diligence required at the outset. If due diligence is not obtainable from a third party, identify and document any limitations, understand the associated risks, and consider potential risk mitigants

- For community banks/MDFIs: consider using services of industry utilities or consortiums to supplement due diligence, but ensure any collaborative activities among banks comply with antitrust laws

**Review legal and regulatory compliance** considerations, including whether third party has requisite licensing, is subject to sanctions by the Office of Foreign Assets Control, or responsive to regulatory compliance issues; and whether third party has identified and articulated a process to mitigate areas of potential consumer harm

- Assess financial condition through public information to evaluate financial capability to perform
- Evaluate resources/staffing, prior experience, and history of addressing customer complaints or litigation
- Assess qualifications and experience of third party's key personnel, including practice of background checks
- Assess effectiveness of a third party's risk management (policies, processes, internal controls), including an assessment of their governance processes and review of System and Organization (SOC) reports
- Assess the third party's information security program, including through review of its major information security policies and practices against the bank's own standards and the results of recent vulnerability scans, penetration tests or program audits
- Review the partner's business continuity and disaster recovery (BC/DR) program, including its BC/DR policies, on- and offline backup solutions, backup frequency, the results of any BC/DR testing, and dependence on a single vendor for critical operations; among other things, financial regulators have focused on

# Guidance Topic: Due Diligence and Third-Party Selection

BACK TO START

## Key Points

Activity must be conducted in a safe and sound manner

Relying solely on experience with or prior knowledge of a third party is not an adequate proxy for performing due diligence

## Considerations for Fintechs or Service Providers

Understand important threshold questions during the planning stages to gauge the implications of entering into a third-party relationship

- Ask the bank whether it considers the proposed third-party relationship as supporting higher-risk or critical activity. If so, expect a more intensive diligence process

Expect that a bank's diligence process aims to give the bank a comprehensive view of the fintech's business, performance, and operations. Understand that a bank's diligence needs are flexible – to a point. If a fintech prefers not to share certain information requested by a bank in connection with the bank's diligence, be ready to share the reason for that preference and engage with the bank on whether alternate information may meet the bank's needs

**Expect that the bank will require the fintech to engage with service providers** that are relevant to the activities the fintech will perform

- If a bank partnership involves a fintech having custody of the bank's confidential or customer information and the fintech will store that information with a cloud service provider, expect the bank's diligence to involve a fintech's engagement with the cloud service provider on security, systems performance, and compliance, among other risk areas

The results of a bank's diligence of a fintech bear directly on how the bank views the fintech from a risk management perspective. Suboptimal diligence responses may cause a bank to view a fintech partner as higher risk, thereby leading to tougher contract demands and more rigorous monitoring expectations

# Guidance Topic: Contract Negotiation

BACK TO START

## Key Points

Banks may need to modify standard terms in third-party contracts to suit their needs

Periodic review of contracts allow banks to confirm whether existing provisions continue to address relevant risk controls and legal protections

## Considerations for Banking Organizations

Third-party contracts should clearly identify rights and responsibilities of each party, including any dual-hatted employees.

Certain relationships may require defined performance measures to assist the bank in evaluating the performance of a third party.

- Ensure appropriate provisions specifying the third party's retention and provision of information that is needed by the bank to perform its risk monitoring function, and for legal compliance
- Ensure appropriate audit rights are included with respect to the third party (and any relevant subcontractors) consistent with the risk and complexity of the relationship
- Ensure contracts clearly describe all costs and compensation agreements (including consistency with applicable laws and regulations)
- Determine whether it is the bank's or the fintech's responsibility for responding to **customer complaints**; if it's the bank's responsibility, include provisions for the bank to receive prompt notification from the fintech of any third-party complaints
- Ensure fintech notifies the bank of its use or intent to use a subcontractor; consider, among other points, whether the contract should prohibit assignment, transfer, or subcontracting of the third party's obligations to another entity without the bank's consent
- Address each party's ownership of and rights and responsibilities with respect to personal data and other sensitive bank data; this is essential for determining which data privacy laws, each party's obligations under those laws, and how data can be used within and outside the partnership context
- Assess security risks to systems, data and physical locations that will support partnership operations and clearly delineate the parties' responsibilities to address those risks; in many cases, risks will be properly addressed through shared responsibilities by multiple parties

# Guidance Topic: Contract Negotiation

BACK TO START

## Key Points

Banks may need to modify standard terms in third-party contracts to suit their needs

Periodic review of contracts allow banks to confirm whether existing provisions continue to address relevant risk controls and legal protections

## Considerations for Fintechs or Service Providers

If a banking organization considers a fintech's activities to be higher-risk or critical to the bank, expect more rigorous contract demands, e.g.,:

- Plan to negotiate terms governing the banking organization's ability to monitor and audit the fintech's activities and performance, including terms governing the exchange, custody, and security of data; business continuity and disaster recovery; and indemnification and limitations of liability
- Plan on negotiating terms governing the fintech's insurance coverage, which may involve change management mechanics to throttle coverage based on changes to exposure during the term of the relationship
- Plan on negotiating terms governing the fintech's relationships with its service providers

Banks and fintechs may negotiate from the bank's or fintech's form agreement. If it's critical to a fintech to negotiate from its own form, draft the form to cover the applicable substantive risk management areas addressed by the Guidance

Banks are not required under the law or Guidance to de-risk financial exposure under fintech relationships using broad, bank-favorable indemnities or limitations of liability, but doing so is consistent with the risk management principles articulated in the Guidance

As with banks, it is crucial for fintechs and other bank partners to carefully address each party's ownership of and rights and responsibilities with respect to personal and other sensitive data processed as part of the bank partnership. Bank partners may need to segregate data processed as part of the bank partnership from other data they process because of special restrictions that may apply to bank data

It likewise is essential for bank partners to understand their responsibilities for information security under the relationship. Responsibilities may need careful delineation for shared web portals and other systems, as multiple parties may have an effect on the security of such systems. Consider pursuing generally accepted security certifications (e.g., ISO 27000, PCI DSS, and SOC II) to streamline the bank's assessment of your security practices

To the extent the bank will be processing personal or other sensitive data belonging to a partner, the partner should assess the bank's information security program, leveraging third-party audit standards and assessment programs where applicable

# Guidance Topic: Ongoing Monitoring

BACK TO START

## Key Points

Enables a bank to:

confirm the quality and sustainability of a third party's controls and ability to meet contractual obligations; escalate significant issues; and respond to such issues when identified

## Considerations for Banking Organizations

**Ongoing monitoring of third-party bank partners has been noted several times by regulatory staff as an area most worthy of bank industry attention**

Banks can accomplish effective ongoing monitoring in various ways, consistent with the nature of the third-party relationship. Typical monitoring activities include review of the third party's effectiveness of controls, periodic visits and meetings, and regular testing of controls (where appropriate)

- For community banks/MDFIs: as noted above, consider using services of industry utilities or consortiums to supplement due diligence, but ensure any collaborative activities among banks comply with antitrust laws

# Guidance Topic: Ongoing Monitoring

BACK TO START

## Key Points

Enables a bank to:

confirm the quality and sustainability of a third party's controls and ability to meet contractual obligations; escalate significant issues; and respond to such issues when identified

## Considerations for Fintechs or Service Providers

Monitoring may be periodic or continuous. It may rely on varied tactics, including any combination of direct systems access (giving banking organizations direct, ongoing visibility into the fintech product or service that's supported through a bank partnership), periodic reporting (daily, weekly, monthly, etc.), informal visits, function-specific testing, formal audits

Real-time access to information is a powerful risk mitigant that may reduce the need for other periodic monitoring functions like reporting, testing, and audits. Where real-time access isn't available, expect that banks will need to use other monitoring tactics to compensate

# Guidance Topic: Termination

BACK TO START

## Key Points

Termination should be efficient

## Considerations for Banking Organizations

When structuring rights and effects of termination, key considerations should include costs to terminate; managing data retention and destruction; unwinding technology integrations; and disposition of jointly developed intellectual property

Where appropriate, termination terms should also consider transition of services to successor third parties and how that transition would be completed

- Terms governing transition of services from one third party to another are most appropriate where the third party's services support a bank-branded, bank-managed product and the third-party transition will ultimately have little or no effect on customer experience
- Terms governing transition of services from one third party to another are more challenging (and potentially less appropriate) where the third-party's services support a third-party-branded or third-party-managed product and the third-party transition would have a material effect on customer experience or present risk of customer confusion

# Guidance Topic: Termination

BACK TO START

## Key Points

Termination should be efficient

## Considerations for Fintechs or Service Providers

Banking organizations will expect termination rights that provide the bank with quick, low-friction exit ramps in certain high-risk circumstances, particularly with respect to a fintech's compliance failures and formal directions from regulators

Banking organizations may be averse to transition terms that require them to invest resources in and negotiate with other banks, but may be willing to engage such terms when the effect of a transition to a successor bank is in the mutual best interests of the banking organization and end customers

- Expect that banking organizations will need quick-turn termination rights tied to the order or direction of a regulator, but also expect openness to reasonable guardrails
- Have a view on how the fintech's business would transition its relationship with one bank to another, and build in terms to facilitate that transition. Transition terms don't need to contemplate every transition scenario; transition terms need only lay the groundwork for negotiating transition specifics under the otherwise stressful circumstances of a wind down

# Guidance Topic: Governance

BACK TO START

## Key Points

Highlights establishment of clear roles, responsibilities, and segregation of duties pertaining to the activity

## Considerations for Banking Organizations

Governance structures vary across banking organizations, with some preferring to centralize oversight within the department or team engaging the third-party bank partner, and others assigning responsibility to compliance, information security, procurement, or risk management functions. Regardless of format, the bank's governance structure should facilitate the board's management of third-party relationships broadly, with management collecting and reviewing documentation, arranging for independent review of third-party business functions, and reporting the results of these activities to the board periodically

- Conduct a risk assessment for each third-party relationship to determine whether the relationship is aligned with the bank's overall risk tolerance
- Ensure the bank's third-party risk management is integrated with overall risk processes
- Ensure the bank has sufficient access, audit, and escalation rights necessary to monitor the relationship and mitigate risks
- In addition to creating and maintaining an inventory of all third-party partnerships, document all due diligence and ongoing monitoring efforts, including risk identification and remediation plans
- Develop a framework for reporting material components of the third-party relationship program to the board

## Considerations for Fintechs or Service Providers

Fintechs should recognize that banks have significant oversight and reporting responsibilities, and that they may receive direction passed down from a bank's board or other management teams that are not directly involved with the day-to-day management of the partnership

- Expect that banks will insist on comprehensive access, audit, and escalation rights in order to meet the risk management objectives of federal regulators
- Document internal and external risk and compliance management protocols and collaborate with banks to ensure the relationship remains within the bank's risk tolerance. In addition to creating a formidable and effective bank partnership, these efforts will also help reduce and manage regulatory scrutiny of your practices

# Guidance Topic: Supervisory Reviews

BACK TO START

## Key Points

Evaluate risks and the effectiveness of risk management to determine whether activities are conducted in a safe and sound manner and in compliance with applicable laws and regulations

Scope depends on the degree of risk and the complexity associated with the banking organization's activities and third-party relationships

## Considerations for Banking Organizations

Expect that federal banking agencies will exercise their supervisory authority in connection with third-party bank partnerships. The scope and complexity of the review will depend on the risk and complexity of the partnership and any associated products or services

- Collaborate with third-party partners to prepare for supervisory reviews, which will often require educating regulators about the workings of the products and services offered in connection with each partnership, as well as any risks and rewards to markets and consumers
- When designing documentation and reporting frameworks, consider regulatory agencies and intended audience and ensure each deliverable effectively addresses a component of the interagency third-party risk management objectives
- Familiarize the board with the applicable rating system and how supervisory findings impact the bank's risk profile
- Keep third-party partners informed of supervisory reviews and findings, and ensure they are prepared to cooperate to resolve findings as needed

## Considerations for Fintechs or Service Providers

Federal banking agencies may use their supervisory authority to examine fintechs directly. In addition to cooperating with any indirect examination via bank supervision, fintechs should ensure that they have effective risk and compliance management controls and demonstrate how they facilitate each bank partners' oversight and reporting obligations

- Banks will pass supervisory findings and recommendations on to the fintech and assess whether the recommended changes should also apply to uninvolved bank partnerships
- Ensure effective tracking of adjustments and root cause analysis for all material changes to demonstrate to regulators that the fintech's compliance and risk management systems are responsive to risks identified by both banks and regulators

## DWT Contacts

BACK TO START

**Alexandra Steinberg Barrage**
PARTNER

Washington, D.C.
202.973.4208
abarrage@dwt.com

**Michael Borgia**
PARTNER

Washington, D.C.
202.973.4282
michaelborgia@dwt.com

**Ryan Richardson**
PARTNER

New York
212.603.6417
ryanrichardson@dwt.com

**Aisha Smith**
COUNSEL

Washington, D.C.
202.973.4285
aishasmith@dwt.com

## SRA Contacts

BACK TO START

**Michael Glotz, MBA, CRP**
CEO and Co-Founder
mglotz@srarisk.com

**Edward Vincent, CFA**
President, SRA SaaS Business
evincent@srarisk.com

**Niki White, CPA**
Chief Customer Officer
nwhite@srarisk.com

**Mike Jones**
Chief Compliance Officer
mjones@srarisk.com

Davis Wright Tremaine LLP

SRA WATCHTOWER

srarisk.com/watchtower/fintech-risk-management

**DWT.COM | SRARISK.COM**