KPMG

Regulatory Alert

Regulatory Insights for Financial Services

June 2023

Third-Party Risk Management: Final Interagency Guidance

KPMG Regulatory Insight:

- *Replaces each agency's prior guidance on third-party risk management; third-party "business arrangements" are defined to capture the full range of third-party relationships.*
- *Principles-based, allowing for a risk-based approach that can be adjusted to the unique circumstances of each third party; places the most comprehensive considerations on "higher-risk" activities, including "critical activities"; examples provided are illustrative and non-exhaustive.*
- *Expect continued supervisory intensity, particularly to large organizations, "new or novel structures and features" such as fintech 'partnerships', and services for "critical activities".*
- *Reiterates the importance of sound risk management regardless of bank size and varying with the degree of risk and complexity of each third-party relationship; not expressly "tailoring", but with acknowledgement of potential use of industry utilities, consortiums, and/or third-party certifications.*
- *TPRM expectations throughout life cycle (planning, due diligence and selection, contract negotiation, ongoing monitoring, and termination).*

The FRB, FDIC, and OCC (collectively, Agencies) jointly issued final third party risk management guidance. The guidance replaces each agency's prior guidance on the topic and is applicable to all of their supervised banking organizations.

Third-Party Relationships

Banking organizations' use of third parties to perform "business arrangements", as defined, does not diminish their responsibility to operate in a safe and sound manner and in compliance with applicable laws and regulations; the term is intended to capture the "full range of third-party relationships that may pose a risk to banking organizations". The guidance states that it is the responsibility of each banking organization to analyze the risks associated with each third-party relationship and to calibrate its risk management processes accordingly.

The Agencies final TPRM guidance is organized into four sections: 1) risk management, 2) third-party relationship life cycle, 3) governance, and 4) supervisory reviews.

Risk Management. As part of sound TPRM, banking organizations would:

- Analyze the risks associated with each third-party relationship and tailor risk management practices, commensurate with the banking organization's size, complexity, and risk profile and with the nature of the individual third-party relationship.
- Maintain "complete" inventories of third-party relationships and periodically conduct risk assessments for each third-party relationship to support changes in

risk determinations over time and to update risk management practices accordingly.

— Engage in "more comprehensive and rigorous oversight and management" of third-party relationships that support "higher-risk" activities, including "critical activities". "Critical activities" include those that could:

- Cause the banking organization to face significant risk if the third party fails to meet expectations.
- Have significant customer impacts.
- Have a significant impact on the banking organization's financial condition or operations.

Third-Party Relationship Life Cycle. Effective TPRM follows the Life cycle of third-party relationships and requires the involvement of staff with requisite knowledge and skills at each stage of risk management as well as "experts" across disciplines (e.g., compliance, risk, technology, legal). The TPRM Life cycle incudes:

Life Cycle	Actions	Factors may consider:
Planning	— Evaluate and consider risk management before entering into third-party relationships; certain third parties, including those that support "higher-risk" or "critical activities", may warrant a greater degree of planning and consideration, such as board approval.	— The strategic business purpose for the arrangement; the associated benefits, risks, and costs; potential information security and physical security implications; and contingency planning.
Due Diligence and Selection	— Evaluate whether they can appropriately identify, monitor, and control risks associated with a particular third-party relationship. The scope and degree of due diligence should be commensurate with the level of risk and complexity of the third-party relationship. — Any limitations on due diligence efforts should be documented and alternatives considered to mitigate related risks. (Note: Banking organizations may use external parties, such as consultants or consortiums, to supplement the information gathering.)	— The third party's: business strategies and goals; ownership structure; financial condition; staffing resources and experience with the relevant activity; governance and risk management; information security management; and reliance on subcontractors. ***Note:*** The regulators state that where there are collaborative efforts to reduce the burden of due diligence, they do not abrogate the responsibility of the banking organization to manage third party relationships in a safe and sound manner. Further, where there are challenges collecting information from third parties, the guidance provides that banking organizations should consider taking steps to mitigate risks or determine is the residual risk is acceptable. With regard to subcontractors, the guidance clarifies that the focus should be on the banking organizations approach to evaluating its third party's own processes for overseeing subcontractors and managing risk.

Contract Negotiation	— Tailor the level of detail and comprehensiveness of contract provisions based on the risk and complexity posed by a particular relationship. — Conduct periodic reviews of executed contracts to address pertinent risk controls and legal protections.	— The nature and scope of the business arrangement (rights and responsibilities of each party); performance measures and benchmarks; obligations related to data (e.g., access, retention); right to audit; operational resilience and business continuity; and default and termination.
Ongoing Monitoring	— Confirm the quality and sustainability of a third-party's controls, escalate significant issues or concerns, and respond to them when identified. — Conduct on a periodic or more continuous basis, where more comprehensive or frequent monitoring is appropriate for third-party relationships that support "higher risk" activities, including "critical activities".	— Overall effectiveness of the relationship; changes in financial condition; relevant audit or testing results; compliance; changes in key personnel; changing laws or regulations; and customer complaints and remediation.
Termination	— Assess and execute termination of a third-party relationship.	— Potential alternate third parties; transition timeframes; data-related risks such as access, retention, and destruction; joint intellectual property; and potential impacts to customers.

Governance. Regardless of how banking organizations structure their TPRM and governance processes (e.g., dispersed across business lines or centralized under compliance, information security, procurement, or risk management functions), the following governance practices should be considered through the TPRM Life cycle, commensurate with risk and complexity.

See table on the following page.

Governance	Actions	Factors may consider:
Oversight and Accountability	**Management:** — Integrating TPRM with overall risk management processes. — Directing planning, due diligence, and ongoing monitoring activities. — Reporting periodically to the board or designated committee on TPRM activities. — Providing that third-party contracts are appropriately reviewed, approved, and executed. — Establishing appropriate organizational structures and staffing, including level and expertise, to support TPRM processes. — Implementing and maintaining an appropriate system of internal controls to management risks associated with third-party relationships. — Assessing whether the banking organization's compliance management system is appropriate to the nature, size, complexity, and scope of its third-party relationships. — Determining whether the banking organization has appropriate access to data and information from its third parties. — Escalating significant issues to the board and monitoring any resulting remediation, including actions taken by the third-party. — Terminating business arrangements with third parties when they do not meet expectations or no longer align with strategic goals, objectives, or risk appetite.	**Board:** — Third-party relationship management and consistency with strategic goals, risk appetite, and compliance with applicable laws and regulations. — Appropriate periodic reporting on third-party relationships. — Whether management has taken appropriate actions to remedy significant deterioration in performance or address changing risks or material issues identified. ***Note***: The guidance seeks to avoid the appearance of a prescriptive approach to the board's role in the risk management life cycle while emphasizing their ultimate oversight responsibility.
Independent Reviews	— Periodically conducted to assess the adequacy of TPRM processes.	— Alignments with the banking organization's business strategy and internal policies; identification, measurement, monitoring, and control of third party-related risks; engagement of TPRM staff over the life cycle; and conflicts of interest.
Documentation and Reporting	— Processes that support effective documentation and internal reporting.	— A current inventory of third-party relationships identifying those with "higher risk" activities; reports spanning the TPRM life cycle (planning/risk assessments, due diligence reports; executed contracts, performance reports from ongoing monitoring, customer complaints and remediation, service disruptions/security breaches); board reports; independent reviews.

Supervisory Reviews. The scope of supervisory reviews will depend on the degree of risk and the complexity associated with the bank's activities and third-party relationships and will be part of standard supervisory processes.

For more information, please contact Amy Matsuo or Todd Semanco, Greg Matthews.

Contact the author:

Amy Matsuo
Principal and National Leader
Regulatory Insights
amatsuo@kpmg.com

kpmg.com/socialmedia