THOMPSON HINE

Privacy & Cybersecurity Update

May 2024

Banking Regulators Publish Third-Party Risk Management Guide

On May 3, the Federal Deposit Insurance Corporation, Federal Reserve System Board of Governors and Office of the Comptroller of the Currency published "Third-Party Risk Management: A Guide for Community Banks" ("2024 Guide") as a resource to help community banks develop and implement third-party risk management programs, policies, and practices. Although the 2024 Guide is intended for community banks, all organizations that rely on third-party service providers, especially for technology-related services (e.g., cloud storage, online platforms, data retention), will find it useful.

Background

The banking regulators understand that there is significant risk when third parties collect and retain customer data on behalf of a financial institution, and some of the most significant data breaches in recent years have targeted information technology (IT) service providers, who often furnish IT services to hundreds, if not thousands of companies. The banking regulators have indicated that "engaging a third party does not diminish or remove a bank's responsibility to operate in a safe and sound manner and to comply with applicable legal and regulatory requirements, including consumer protection laws and regulations, just as if the bank were to perform the service or activity itself."

In June 2023, the banking regulators published "Interagency Guidance on Third-Party Relationships: Risk Management" ("Interagency Guidance"), which set forth principles to support a risk-based approach to third-party risk management that banking organizations should consider when developing and implementing risk management practices for all stages in the life cycle of third-party relationships. The 2024 Guide is intended to assist community banks when developing and implementing their third party risk-management practices and is *not* a substitute for, nor does it replace, the Interagency Guidance.

The 2024 Guide: Key Principles

According to the 2024 Guide, not all business relationships require the same level of oversight, and organizations should apply more rigorous risk-management practices for service providers that support higher-risk activities. In determining whether an activity is higher-risk, a bank should assess various factors, such as if the third party has access to sensitive data (including customer data), processes financial transactions, or provides essential IT or other business services. Further, it should "adjust and update [its] third-party risk-management practices commensurate with [its] size, complexity, and risk profile by periodically analyzing the risks associated with each third-party relationship."

The 2024 Guide describes key principles within each of the five stages of risk management: planning, due diligence and third-party selection, contract negotiation, ongoing monitoring, and termination.

Planning

According to the 2024 Guide, "careful planning enables a community bank to consider potential risks in the proposed third-party relationship" and "risk assessments are an important component of managing third-party relationships and help a bank evaluate the extent of risk-management

resources and practices for effective oversight of the proposed third-party relationship throughout the subsequent stages of the third-party relationship life cycle." Key issues to consider in the planning stage include identifying:

- The activities the service provider will perform and how responsibilities will be allocated between all the applicable parties
- Any legal and compliance obligations
- The benefits, risks, and costs of using a service provider
- Whether retention of service provider aligns with the organization's strategy
- The internal controls needed to manage and mitigate the potential risks
- How will the services be integrated into existing IT infrastructure and information security practices
- Whether the services can be transitioned to another third party or in-house
- Whether existing service providers can furnish new or expanded services

The 2024 Guide reinforces the Interagency Guidance, noting that "[a]s part of sound risk management, effective planning allows a banking organization to evaluate and consider how to manage risks before entering into a third-party relationship."

Due Diligence and Third-Party Selection

Due diligence is the process for assessing a third party's ability to perform its services in accordance with its contractual expectations, applicable law and regulations, and internal policies and procedures. According to the 2024 Guide, "[e]ffective due diligence assists with the selection of capable and reliable third parties to perform activities for, through, or on behalf of the community bank" and "[i]f the bank cannot obtain desired due diligence information from the third party, the bank may consider alternative information, controls, or monitoring." Key issues to consider in this phase include:

- Whether the third party has appropriate financial and operational capabilities, including its resources and expertise
- If the third party demonstrates an ability to comply with applicable laws and regulations and corporate policies and procedures, especially with respect to information security
- How the third party has performed in the past during periods of economic or financial stress
- Whether the third party uses subcontractors, and if so, how it oversees them
- If the third party is involved in ongoing litigation or other public matters of concern

The 2024 Guide identifies several sources that can provide information on a third party's capabilities and risk profile, such as its financial statements, business licenses, internal policies and procedures, independent audit results, staffing level, volume and nature of consumer complaints against it, sanctions list reports, current insurance coverage, press releases, references and feedback from peer institutions or clients, disclosures and information in the media or in any of its publications, and internet searches to determine whether the service provider has been partnered with institutions subject to certain consent orders and litigation.

Contract Negotiation

Before entering a formal business relationship with a third party, an organization needs to ensure that its contract provisions satisfy its business objectives, regulatory obligations, and risk-management policies and procedures. The 2024 Guide provides that when an organization "has limited negotiating power," it is important for it "to understand any resulting limitations and consequent risks" and "[p]ossible actions [it] might take in such circumstances include determining whether the contract can still meet the community bank's needs, whether the contract would result in increased risk to the community bank, and whether residual risks are acceptable." Key issues to consider include:

- To what extent does the contract specify the parties' responsibilities and cover all aspects of the relationship (e.g., costs, reimbursements, and other liabilities)
- How termination events are addressed (e.g., default, force majeure, continuity planning)
- The governance and escalation protocols regarding the third party's performance and security measures or benchmarks

- Whether the contract addresses oversight and performance monitoring
- The arrangements for sharing and using IT and intellectual property
- Whether the contract specifies limitations on the third party's use and retention of data (including customer data)
- How the third party will notify the organization of a disruption, including degradation or interruptions in delivery, and how the third party will assist the organization with continuation of the activity
- If the third party is required to disclose strategic changes, such as mergers and acquisitions and leadership changes

Importantly, the 2024 Guide notes that an organization's risk assessment and due diligence findings must be used to determine the provisions to include in the contract, and the third party's proposed service level agreements should be included in contracts to "set applicable performance and security metrics."

Ongoing Monitoring

According to the 2024 Guide, an organization's "ongoing monitoring" of the third party's contract performance enables it to determine if the third party is performing as required for the duration of the contract and to adapt and refine its risk-management practices. Key issues to consider in this phase include:

- Whether the third party is performing its obligations under the contract, and if it is a reliable partner
- If, during the term of the contract, the third party's financial condition changed, including declining revenues or increasing debt obligations
- If the third party complied with applicable laws, regulations, and service level agreements
- Whether audit and test results indicate the third party is managing risks and meeting contractual obligations and regulatory requirements effectively
- If the third party has demonstrated an ability to maintain its systems within the organization's availability requirements (e.g., latency, bandwidth, and uptime)
- Whether the third party has been subject to a security incident
- If the third party's performance has changed due to its corporate restructuring

The 2024 Guide emphasizes the following point set forth in the Interagency Guidance: "Ongoing monitoring enables [an organization] to (i) confirm the quality and sustainability of a third party's controls and ability to meet contractual obligations; (ii) escalate significant issues or concerns [such as data breaches]; and (iii) respond to such significant issues or concerns" in a timely manner.

Termination

There are a variety of reasons an organization may choose to end its relationship with a third party. It should consider the impact of a potential termination during the planning stage of the life cycle, which may assist in mitigating costs and disruptions caused by termination, particularly for higher-risk activities. Accordingly, organizations should consider:

- How the termination will affect the organization's operations, especially with respect to critical activities, and its compliance with applicable laws and regulations
- The financial implications of terminating the relationship
- If there are alternative third parties or in-house resources and how quickly a transition could happen
- How the parties will handle intellectual property, confidential information, IT access, and recordkeeping obligations after termination

An organization's contract with the third party should assess how parties may exit the relationship and the conditions under which fees or penalties will be imposed for early termination.

Conclusion

A third-party risk management framework is an essential part of any organization's operations. Given the recent trend in cybersecurity attacks against third-party service providers, this type of framework is especially important for organizations to comply with their legal and regulatory obligations.

FOR MORE INFORMATION

For more information, please contact:

Steven G. Stransky
216.566.5646
202.263.4126
Steve.Stransky@ThompsonHine.com
Certified Information Privacy Professional/Government (CIPP/G)
Certified Information Privacy Professional/United States (CIPP/US)

Thomas F. Zych
216.566.5605
Tom.Zych@ThompsonHine.com

Marla M. Izbicky
312.998.4253
Marla.Izbicky@ThompsonHine.com
Certified Information Privacy Professional/United States (CIPP/US)

Thora Knight
212.908.3971
Thora.Knight@ThompsonHine.com

Jennifer N. Elleman
937.443.6927
Jennifer.Elleman@ThompsonHine.com

Julie D. Honor
312.998.4246
Julie.Honor@ThompsonHine.com