TEVORA™

Interagency Guidance: A Thorough Guide for Effectively Managing Third-Party Risk in the Financial Sector

Initially proposed in 2021, the Federal Deposit Insurance Corporation (FDIC), the Federal Reserve Board (FRB), and the Office of the Comptroller of the Currency (OCC) (collectively referred to as the 'Agencies') proposed guidance to support a risk-based approach for how banking organizations should conduct business with third parties.

Since then, the guidance has undergone several rounds of careful revisions and has been finalized as of June 6, 2023.

Who does this guidance apply to?

This guidance is directed to **all banking organizations supervised by the Agencies** and replaces all previously issued guidance. The guidance takes a purposefully expansive approach, including all third parties with a business arrangement with a banking organization, whether by contract or otherwise. It requires banking organizations to implement a comprehensive third-party risk management (TPRM) framework that accounts for the entire lifecycle of its third parties, including suppliers, vendors, partners, holding companies, and associated financial technology (fintech) entities.

If you have questions or would like to connect with our team of security professionals, call at (833) 292-1609 or email us sales@tevora.com.

Securing Critical Infrastructure

The **financial sector** is one of the most strictly regulated industries, with numerous disparate frameworks imposed upon its organizations to protect highly sensitive information used in transactions and maintain the economic stability of the nations these organizations support.

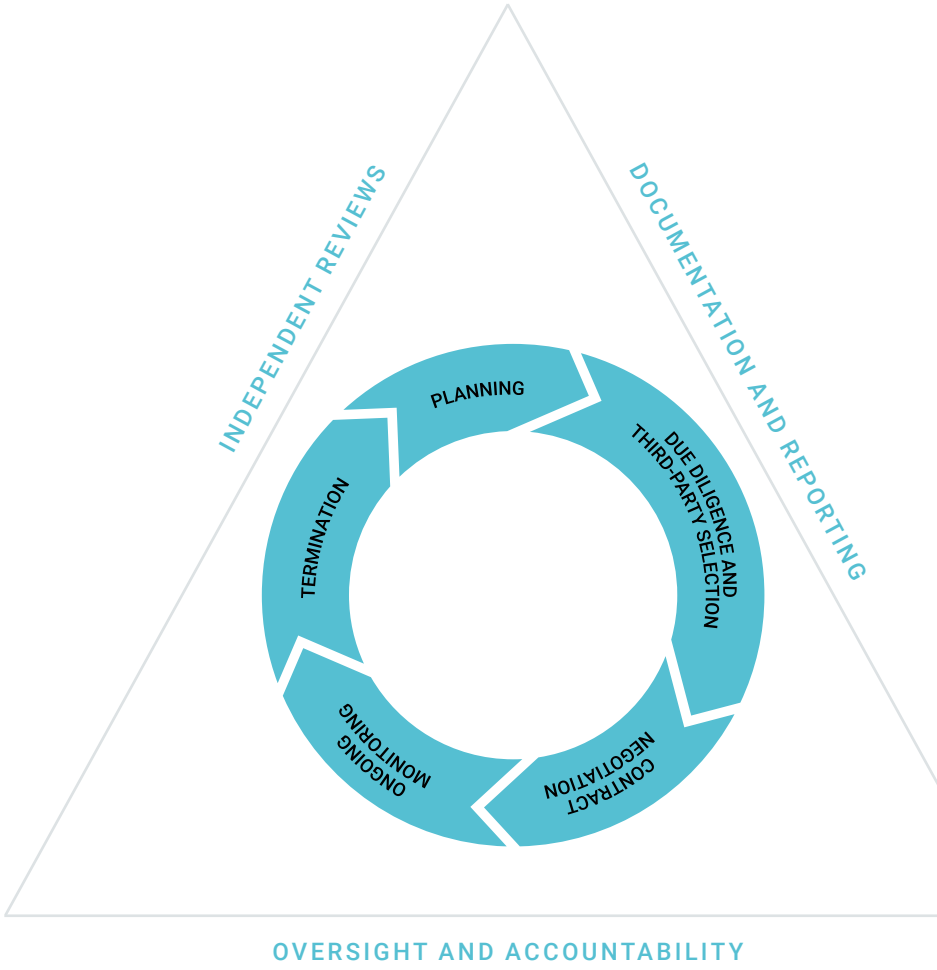
With 94.6% of data breaches being financially motivated[1], it is no surprise that these threat actors would directly target the source of financial information. Thankfully due in no small part to the litany of regulatory requirements, robust security controls are commonplace in large banking organizations to mitigate the most of would-be ransomware attacks. However, the complex network of partners and third parties interconnecting between financial service enterprisesdoes not boast this same level of maturity.

Rather than targeting the banking organizations directly, crafty threat actors exploit these less secure third parties to impact business operations or gain access to larger enterprises' infrastructure. The prevalence of this attack methodology has increased significantly across all industries, with the financial sector being the second most breached industry by its third parties[2]. When the threat landscape comprises threat actors with nation-state resources and the total weight of multiple economies relies on these banking organizations to remain resilient, nothing can be left to chance. **This interagency guidance provides an excellent foundation for mitigating third-party weaknesses and preventing widespread damage.**

If you have questions or would like to connect with our team of security professionals, call at (833) 292-1609 or email us sales@tevora.com.

Navigating the Interagency Guidance

The finalized interagency guidance promotes standardization of how banking organizations should approach the various types of third-party relationships involved when conducting business and how to manage risk through each stage of the lifecycle: Planning, Due Diligence and Third-Party Selection, Contraction Negotiation, Ongoing Monitoring, and Termination:



If you have questions or would like to connect with our team of security professionals, call at (833) 292-1609 or email us sales@tevora.com.

Planning

To manage a system as complex as third-party networks, enterprises must establish a standardizing framework to create consistency. This means identifying the criteria by which third parties should be evaluated to determine risk and then creating supporting workflows. Depending on each organization's resources, this criterion can vary but should align with the business strategy and mission. **Examples of some requirements:**

COST Both direct and indirect costs are associated with the third-party relationship.
Direct: contractual agreements, ongoing maintenance costs, software purchase
Indirect: staff adjustments, process creations, training requirements

CUSTOMER IMPACT How could this third-party relationship potentially impact customers' information?

SYSTEM ACCESS Potential increase in attack surface by providing system access as part of the engagement.

PHYSICAL ACCESS Potential physical security implications associated with third-party relationships.

CONTINGENCY PLANS Is a single point of failure created within the banking organization's business operations or supply chain, and is the business sufficiently prepared to handle such an incident from occurring?

REGULATORY COMPLIANCE Will engagement with a particular third party result in noncompliance with regulatory requirements that may result in fines or loss of business?

By formally and thoroughly evaluating the potential risk of engaging with a third party, banking organizations will be much more capable of maintaining a resilient supply chain and protecting business interests.

Due Diligence and Third-Party Selection

Once the potential risk involved with a third-party relationship is understood, the banking organization must conduct a sufficient investigation to determine if the risks can be effectively managed and controlled. Although many organizations may opt to send an extensive, standardized questionnaire to cover all risk domains, this typically results in excessive delays and poor response quality as questionnaire fatigue sets in. Organizations should tailor due diligence processes based on the initial criteria gained during the Planning phase to foster a more synergistic relationship with third parties.

The Agencies purposefully built-in flexibility for this stage to allow banking organizations to perform due diligence commensurate with current capabilities and resource constraints. A Third-Party Risk Management (TPRM) program must work with multiple internal departments to operate effectively, and this guidance supports that notion.

For third parties that are involved in highly critical activities, a tailored questionnaire along with third-party monitoring intelligence, validation of third-party certifications or attestations, assessment of current financial standing, and a review of information security policies could be sufficient while for a third party with minimal exposure to critical activities may only need to provide a subset of due diligence evidence to be properly vetted.

Below is a list of potential factors banking organizations should consider when conducting due diligence:

STRATEGIES AND GOALS How the third party's strategy may affect the banking organization.

LEGAL AND REGULATORY COMPLIANCE Review to ensure the third party can uphold the requirements imposed on the banking organization.

FINANCIAL CONDITION Evaluate if the third party has the financial capacity and stability to perform or support the proposed activity.

BUSINESS EXPERIENCE Evaluate the depth of resources and history providing a product or service to ensure the product or service in scope is accurately represented.

QUALIFICATIONS AND BACKGROUND OF KEY PERSONNEL Determine if the third party upholds the banking organizations background checks and suitability requirements.

RISK MANAGEMENT Evaluation of the third party's risk management processes relevant to its size, regulatory requirements, and the product or service it supports.

INFORMATION SECURITY Understand potential security implications associated with the confidentiality, integrity, and availability of the banking organization's systems and data.

MANAGEMENT OF INFORMATION SYSTEMS Identify service-level expectations and interoperability issues, especially when technology is a significant component of the third-party relationship.

OPERATIONAL RESILIENCE Determine if the third party can effectively operate or recover from disruptions or incidents.

INCIDENT REPORTING AND MANAGEMENT PROCESSES Review the third party's ability to manage incidents to ensure they meet contractual requirements.

PHYSICAL SECURITY Evaluate if sufficient physical and environmental controls are in place to secure both staff and systems involved in the relationship.

SUBCONTRACTORS Evaluate the volume and types of subcontractors the third party relies on to provide a product or service.

INSURANCE COVERAGE Consider if existing insurance coverage helps mitigate potential losses the third party poses.

CONTRACTUAL AGREEMENTS Evaluate a third party's commitments to other parties and if this may introduce negative implications to the banking organization.

Contract Negotiation

Contracts should facilitate effective risk management and oversight that specify the expectations and obligations of the banking organization and the third party. As with the previous stages, this should be tailored to the complexity of the third-party relationship. This does not mean that standard contracts cannot be employed but rather that these standard contracts should include provisions that support the risk domains relevant to the relationship.

Under challenging negotiations, banking organizations must understand the resulting risk of omitting specific contractual requirements. Efforts should prioritize contractual requirements and determine what can be omitted as acceptable risks and non-negotiable to ensure the banking organization can take a proactive approach. This will allow the organization to conduct negotiation activities more efficiently without introducing unacceptable risks.

If feasible, banking organizations should also implement a periodic review of contractual agreements to determine if renegotiation is necessary.

Factors to consider in initial negotiation and renegotiation include:

NATURE AND SCOPE OF ARRANGEMENT Explicitly describing and stating the rights and responsibilities of each party, including rights to termination and renegotiation.

PERFORMANCE MEASURES OR BENCHMARKS Well-defined metrics are crucial for assessing the performance of third parties, such as Service Level Agreements (SLAs) or other performance monitoring methods. These metrics serve to penalize inadequate performance and reward exceptional achievements.

INFORMATION RESPONSIBILITIES Obligations imposed on third parties for retention and provision of information to allow the banking organization to monitor risk and performance.

RIGHT TO AUDIT Clause to facilitate the banking organization's ability to monitor remediation activities.

COMPLIANCE RESPONSIBILITIES Requirements for third parties to uphold the applicable laws and regulations relevant to the relationship with the banking organization.

COSTS AND COMPENSATION Explicit descriptions of billing and payment arrangements, including additional fees.

OWNERSHIP AND LICENSE Provision to describe the extent to which the banking organization's information, technology, intellectual property, or copyright may be used by the third party.

CONFIDENTIALITY AND INTEGRITY Requirements prohibiting the disclosure of sensitive information except as necessary to complete contractual obligations.

OPERATIONAL RESILIENCE AND BUSINESS CONTINUITY Addressing the specific controls that must be maintained by the third party to support the product or service being provided.

INDEMNIFICATION AND LIMITS ON LIABILITY Provisions to reduce the banking organization's liability for claims arising from a third party's misconduct.

INSURANCE Specifying the types and amounts appropriate to the product or service.

DISPUTE RESOLUTION Establishing a defined process to resolve problems between both organizations expeditiously.

CUSTOMER COMPLAINTS When customer interaction is a critical component of the third-party relationship, specifications should be made to determine responsibility when handling customer inquiries or issues.

SUBCONTRACTING Notification requirements for when a subcontractor may be used and for what intent.

DEFAULT AND TERMINATION Stipulating what constitutes a default, identifying remedies, allowing opportunities to cure defaults, and establishing the circumstances for termination.

REGULATORY SUPERVISION Defining when a third party is subject to regulatory examination and what may be in scope for validating compliance.

Ongoing Monitoring

No matter how effective due diligence efforts may be, a point-in-time assessment cannot be relied upon to represent a third party's adherence to contractual obligations or ability to defend against a constantly evolving threat landscape. Like previous stages, ongoing monitoring of third parties can be tailored according to the risk the relationship presents– whether the residual risk after contract negotiations, the inherent risk based on the initial criteria, or a combination of the two.

As for how the banking organization implements the different forms of ongoing monitoring, the typical activities include:

REVIEW SECURITY REPORTS Review third-party reports that relate to security control effectiveness or overall performance.

PERIODIC MEETINGS To facilitate an ongoing partnership and discuss relevant operational or performance issues.

THIRD-PARTY CONTROL TESTING Whether conducted by the banking organization or an authorized third-party assessor, direct assessment or testing of controls to identify risk.

MONITORING TOOLS Employ monitoring technologies to continuously monitor a third party's external infrastructure and online presence to detect security control deteriorations, significant impacts to financial standing, active threat campaigns, or other signals that would warrant action.

Termination

Whether an expiration or breach of contract, the banking organization must maintain an effective process for discontinuing involvement with a third party. This involves establishing procedures for transitioning to alternative third parties, evaluating termination costs,managing risks associated with data retention and destruction, access revocation, and how the termination may impact customers the third party interacted with on behalf of the banking organization.

If you have questions or would like to connect with our team of security professionals, call at (833) 292-1609 or email us sales@tevora.com.

Maturing TPRM through governance

Although the Agencies' guidance provides a sturdy foundation comprised of TPRM best practices, the program as a whole must be governed and managed appropriately to realize its benefits. Without buy-in from the organization as a whole, without strong collaboration amongst related business units (Enterprise Risk, Security, Legal, Procurement, Human Resources), and periodic reviews of the program's effectiveness, third-party risks will prove laborious and cumbersome to both the banking organization as well as all engaged third parties. Due to this, the guidance emphasizes the importance of governance. It assigns ultimate responsibility to the board of directors that TPRM processes are evaluated, reviewed, and matured throughout the organization's lifetime.

These reviews should validate that third-party relationships align with the overall business strategy and risk appetite. A third-party inventory must be maintained to support such a review. All due diligence activities associated with each third party should have a documented audit trail to serve as evidence. Formal policies and procedures must be adopted and reviewed regularly to validate that the program complies with relevant laws and regulations-response activities associated with third-party breaches must be documented and examined to identify potential process improvements.

If a banking organization cannot immediately support this program level or does not have the requisite personnel, experienced third parties can assume responsibility for the entire TPRM program, aside from the ultimate approval of third parties or smaller segments as necessary. Additionally, as internal auditors may be unable to allocate the time required to assess and review the TPRM program thoroughly, independent third parties can conduct these assessments and provide valuable benchmarks to peers, process recommendations, and attestations the board of directors may use to validate resource spend.

Realizing ROI from TPRM

As with most security investments, it is sometimes difficult to portray success factors to business leadership when success means a lack of news. To validate the expenditure and highlight the value of a program's efforts, here are **two key considerations** to emphasize:

Long-Term Cost Reduction

Third-party breaches invariably incur financial losses from fines, penalties, or restoration activities during operational downtime. According to research by IBM and the Ponemon Institute, nearly one-fifth of breaches were caused by supply chain compromise in 2022. These compromises tended to be more expensive and resulted in a longer lifecycle3. With banking organizations classified as critical infrastructure, which statistically incurs highercosts when breaches occur, and the financial sector already amassing the second-highest average costs per data breach at $5.97 million, avoidance of even a single third-party breach would more than cover the investments made into a robust TPRM program.

Foster Investor Confidence

Maintaining and inspiring customer trust is critical for many organizations, but this is especially true financially. Customers trust their livelihood to these types of organizations, which makes them incredibly discerning clientele whose business may be easily lost if trust is degraded due to a financial institution's name being associated with with a third-party breach – this is especially true for publicly traded companies whose stock prices can be significantly impacted by this loss of trust.By both mitigating potential damages from occurring and partnering with engaged third parties to improve their security posture, a mature TPRM program promotes a positive reputation in the marketplace where peers may wane.

If you have questions or would like to connect with our team of security professionals, call at (833) 292-1609 or email us sales@tevora.com.

HOW **TEVORA** CAN HELP

Although we primarily focused on banking organizations operating out of the United States in the post, our third-party risk team has helped client organizations across the globe and among many highly regulated industries. Whether you need assistance in these highly-regulated sectors or your organization wants to structure its approach after these best practices, **our team is ready and eager to assist!** We match you with third-party risk experts specializing in your industry so they can best assist with tailoring a TPRM program to meet your regulatory requirements and long-term strategic goals.

If you have questions or would like to connect with our team of security professionals, call us at (833) 292-1609 or email us sales@tevora.com.

REFERENCES

1. 2022 Data Breach Investigations Report
2. Third-Party Breach Report by Black Kite
3. IBM Cost of Data Breach Report

TEVORA™

Tevora is a specialized management consultancy focused on cyber security, risk, and compliance services. Our combination of collaborative strategic planning and skillful execution make us a trusted partner to some of the most famous brands in the world.

Go forward. **We've got your back.**

Tevora | **833.292.1609** **sales@tevora.com** | **tevora.com**