BANK OF AMERICA

Third Party Assessment Activities Guide

October 2023

Introduction

The Bank of America Enterprise Third Party Policy and Third Party Program Standard establishes requirements for third party risk management, including outsourcing activities. Bank of America manages third party relationships across the globe in accordance with all applicable U.S. and international laws, rules, and regulations. Third Party Program controls allow for the oversight of third parties' activities including, but not limited to, the oversight of data sharing, information security, offshoring activity and outsourcing. The controls set out to establish management over the following risk types: compliance, reputational, operational, and strategic.

The purpose of the Third Party Assessment Activities Guide (TPAAG) is to inform third parties of the potential risk management controls that may apply once on-boarded or during due diligence as a Bank of America third party. Bank of America requests third parties to, when able, use the English language when submitting policies, procedures, and any type of evidence to satisfy the activities listed in this document through a secure application or method as defined by Bank of America.

While this document addresses most of Bank of America's risk management deliverables, please keep in mind that those requirements may vary for particular third parties and is not comprehensive of all controls required such as those set forth in our Service Provider Security Requirements Document for example. Furthermore, the assessment activities in this document may change in the future and should not substitute requirements set forth in the contract.

Third Party Assessment Activities

Third parties are assessed when entering into a written agreement with Bank of America for the first time, as well as on an ongoing, pre-determined cadence during the lifecycle of the relationship. Communication of activities between third parties and Bank of America are conducted through a secure application or method as defined by Bank of America. Third Party Assessment team (TPA), an independent team of assessors, will be communicating and working with each third party to determine which requirements are in scope for each third party and request the appropriate documentation/evidence.

In addition to the Third Party Assessment team (TPA) Bank of America has an ongoing initiative, with the company - "Know Your 3rd Party" or also known as KY3P (KY3P is Legacy TruSight Solutions, now part of S&P Global). KY3P is an assessment provider for the financial services industry. Once an assessment is completed at KY3P, it can be purchased by Bank of America and other institutions in place of each individual institution's assessments. If a KY3P product is purchased for a third party assessment, TPA will adjust the questions and/or documentation request accordingly. KY3P products do not replace TPA assessments fully but will be leveraged to complete as many relevant requirements as possible.

Bank of America Third Party Management has two phases for third parties:

1. Sourcing Phase – where Due Diligence activities and requirements will be performed prior to contract signing. Many of the requirements are based on the products and services a third party provides and risk factors. Several of the requirements in the Source phase are similar to those in the third party Manage phase.
2. Manage Phase - when a third party has been onboarded as a Managed third party. This is the phase where the relationship will be managed in its E2E lifecycle and assigned an Enterprise Vendor Manager (EVM). A set of requirements will be applicable, also determined by the products and services provided, and multiple risk factors.

Sourcing requirements

Standard diligence – Pre Contract Signing

a. Bank of America performs standard diligence on all prospective third parties.

b. This diligence may include, but is not limited to, a review of business experience, human resources and ethics and internal controls that are specific to the product and/or service the third party provides.

Requirement Focused Diligence – Pre Contract Signing

a. Bank of America performs requirement focused diligence on all net new third parties.

b. This diligence includes all managed vendor requirements and other pre contract only requirements, such as: flood insurance requirements, financial crimes compliance, customer facing requirements that are specific to services being offered to Bank of America.

c. Many third parties, net or new or expanding their services, require an information security as a requirement.

All precontract assessments are reviewed and remediation of findings is attempted. This is suggested to have the most effective relationship with Bank of America Third Party Assessment Teams (TPA and GIS).

Most common requirements

The following assessment activities are the most frequently required and are specific to the service or product detailed in the agreement.

Anti-bribery and anti-corruption

a. Third parties that interact with government employees while providing services to Bank of America present higher risk for bribery and corruption.

b. Third parties should escalate any requests for cash payment, installation payments, and other acts that may be considered as bribery or corruption red flags to their Bank of America vendor manager.

Financial crimes compliance – suspicious activity (also known as Anti-Money Laundering)

a. Significant criminal or regulatory action and severe reputational damage can occur when financial institutions fail to comply with these laws, rules and regulations surrounding financial crimes.

b. Third parties performing services such as account opening, account servicing, customer on-boarding, or customer servicing, on behalf of Bank of America, or any of its Affiliates, will therefore be required to maintain policies and procedures that include the following attributes:

- Understanding the nature and purpose of customer relationships for the purpose of developing a customer risk profile
- Ongoing monitoring to identify, track and report suspicious activity and transactions
- On a risk basis, maintaining and updating customer information including information regarding the beneficial owner(s) of legal entity customers
- Maintaining internal and external reporting requirements
- Adhering to Anti-Money Laundering document retention requirements

Background checks

a. Third parties are required, to the extent permitted by local laws, rules, or regulations, to conduct background checks and other inquiries on their employees and ensure that their subcontractors conduct similar checks.

b. Third party employees must undergo a comprehensive background screening process prior to being assigned to any Bank of America work (for example, access to Bank of America systems, facilities, accessing any bank data, or customer-facing activities).

c. Third parties are prohibited from assigning work on the Bank of America account to those employees, subcontractors and representatives who have not successfully completed background checks.

d. If a third party or its subcontractor's employee had a break in continuous service of longer than ninety (90) consecutive days (not including leave of absence), the third party or subcontractor shall perform a new background check.

e. Third parties must maintain a background check policy, procedure or standard that requires the performance of background checks on all employees and subcontractors. Third parties must also provide redacted copies of performed background checks as requested by Bank of America.

f. These policies, procedures or standards should be in line with the local laws, rules, and regulations where the third party's employees are located and include the following attributes:

- Validation of citizenship and/or certification to work in the country in which services are performed

- Search of the employee's government identification number to verify accuracy of the individual's identity – Including alias and former names
- Comprehensive criminal background check (inclusive of alias and former names) with a look-back period of 10 years, unless local laws, rules or regulations mandate a lesser period or scope. This includes but not limited to all local, regional, and national criminal court records (misdemeanor and felony or equivalent level offenses) in each location of the employees current and previous home addresses.
- Employment eligibility of criminal background check adjudication criteria
- Samples for Bank of America to review of redacted background check documentation of third party employees

g. Dependent upon the products or service provided by the third party, additional verifications such as education check, credit check, or fingerprint check may be requested by Bank of America.

Privacy Program

a. Third parties must comply with privacy requirements in how it collects, stores, processes, handles, or transfers the personal data or personally identifiable information of the bank's clients' data subjects (employees/consumers/clients) in accordance with all global, country, state, city, or provincial laws/regulations.

b. Third parties should have adequate controls in place to prevent, monitor and report privacy events (information security breach or incident) involving unauthorized or inappropriate access, use or disclosure of personal information that is collected, processed, or maintained by Bank of America or by a third party on behalf of Bank of America.

c. In addition, the third party's documentation should ensure compliance with privacy laws and regulatory requirements related to maintaining security, confidentiality, processing integrity, disposal, and protection of personal data. A copy of the documentation for those controls may be requested by Bank of America which should include the following attributes:

- Requirements for data/privacy events and/or issue management
- Requirements for notifying your clients when impacted (Bank of America)
- If publicly facing, provide your privacy notice or privacy policy at all points where personal data or personally identifiable information is collected, transmitted, processed, handled, accessed, or stored (for Bank of America)
- If your company changes a bank client's data, provide a description of the process for completion of those requests (fulfilling data subject rights)

ePrivacy

a. Applicable to third parties that host websites and utilizes cookies and other similar tracking technology should obtain affirmative consent to store non-essential cookies or

provide a notification for use of essential cookies on devices that originate outside the U.S.

b. Documentation of this control would include specifying the type of cookies being tracked and the screen shot of affirmative consent to store non-essential cookies, or notification for the use of essential cookies on devices that originate outside the U.S.

Fraud

a. Third parties should have policies and procedures in place to prevent, monitor and report fraudulent and suspicious activities, including your subcontractors. Fraud is an intentional act which includes misrepresentation or omission of material fact designed to deceive for improper gain or other benefit regardless of whether financial loss occurs.

b. An act of fraud occurs when any individual or group of individuals or entity intentionally deprives or attempts to deprive another of assets, financial instruments, property, or a legal right. Fraud may include "internal fraud" by current or former employees or vendors, "first party external fraud" by external actors against Bank of America, and "third party external fraud" against bank customers or clients.

c. Applicable to third parties that handle, process, store any bank data, access to bank systems, process transactions, or interact with customers. A copy of those policies and procedures may be requested by Bank of America which should address the following attributes:

- A list of fraud risks that apply to the product(s) and/or service(s) provided to or performed for Bank of America
- Prevention and detection of fraudulent and suspicious activities
- Immediate reporting, escalation, and tracking of fraud events and suspicious activities
- Remediation and resolution plans for fraud events and suspicious activities
- Procedures to notify impacted third parties, including Bank of America

Supplier diversity

a. Bank of America is committed to ensuring inclusion of diverse-owned companies in our supply chain based on our longstanding dedication to support and improve the communities where we work and live. This includes contracting and subcontracting with certified diverse-owned companies.

b. Third parties are expected to maintain policies, procedures, and programs to ensure inclusion of diverse-owned companies in their supply chain. Third parties may be expected to report dollars spent with certified diverse-owned businesses in their supply chains, both directly and indirectly, that support the Bank of America account to evidence this inclusion.

Environmental and social risk

a. Bank of America is focused on Responsible Growth and ensuring third party alignment with our environmental and social values. We are dedicated to doing business with third parties that respect ethics, human rights, diversity and inclusion and the environment. We set expectations of our third parties through our Supplier Code of Conduct, which we expect all third parties to adhere to while conducting business with or on behalf of Bank of America.

b. Third parties are expected to self-monitor their compliance with this code and inform the bank in a timely manner of any non-conformance. Third parties may be asked to provide written information on their environmental and social policies, risk management procedures, targets, and impacts.

If third party utilizes subcontractors, the following will be applicable:

Subcontractor risk management and roster collection

a. Third parties should have a process to complete risk-based oversight of subcontractors, including processes for due diligence, risk identification and risk management.

b. A subcontractor is defined a party to whom the third party has delegated and/or subcontracted any portion of its contractual obligations to Bank of America.

c. Subcontractors include any entity performing obligations or providing any products or services related to external hosting, retention or destruction of Bank of America data or having access to Bank of America's premises or systems. Third parties should have a process to complete risk assessments of existing subcontractors and conduct due diligence of potential subcontractors that is commensurate with the risk of the relationship.

d. The third party's process should include the identification of applicable risks to the service being provided by the subcontractor. The documentation should include the following attributes:

- Detailed inventory or roster of subcontractors they use
- Background check policy that also covers subcontractors, as well as employees
- Procedure for conducting due diligence that is commensurate with the risk of the subcontractor
- Risk assessment process (criticality or tiered classification) that identifies risks
- Identification and escalation process to track issues, including remediation (such as risk committee, defined escalation triggers)
- Performance monitoring (such as Service Level Agreements (SLAs), scorecards, metrics, reporting)

e. When dictated by the contract, third parties are required to receive written bank approval prior to changing or engaging in new subcontractor relationships.

If third party presents incremental inherent risk, the following items may be required

Independent deliverables may be applicable to select third parties

The Third Party Assessment team may also collect information from select third parties. Deliverables are not included in Third Party Assessments and will be due upon their unique cadence requirement as applicable to certain contractual, operational, and strategic risks. The following Third Party's reports are from approved, independent auditors of the third party:

a. SSAE18/SOC I -applicable to third parties that impact bank financials

b. SOC II type I or II – applicable to third parties that are registered on the Card Networks, or hosting certain applications

c. PCI Attestation of Compliance (AOC) – applicable to third parties registered on the Card Networks, and those who collect, process, store active credit and debit card data