Introduction

The Bank of America Enterprise Third Party Policy and Vendor Management 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.

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 “SPSRD” Service Provider Security Requirements Document. 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. The following assessment activities are the most frequently required and are specific to the service or product detailed in the agreement.

**Most common requirements:**

1. **Standard Diligence**
   Bank of America performs standard diligence on all prospective third parties. 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.

2. **Anti-Bribery and Anti-Corruption**
   Third parties that interact with government employees in the course of providing services to Bank of America present higher risk for bribery and corruption. 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.

3. **Financial Crimes Compliance**
   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.

   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:
   
   a) Understanding the nature and purpose of customer relationships for the purpose of developing a customer risk profile
   b) Ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information including information regarding the beneficial owner(s) of legal entity customers

4. **Background Checks**
   Third Parties are required, to the extent permitted by law, to conduct background checks and other investigations ensure that subcontractors conduct similar background checks. They should also have a policies and procedures detailing the background check process for employees and subcontractors, a copy of which may be requested by Bank
These policies and procedures should be in line with the local laws, rules and regulations where the third party’s employees are located and include the following attributes:

a) Validation of citizenship and/or certification to work in the country in which services are performed
b) Search of the employee’s government identification number to verify accuracy of the individual’s identity
c) Comprehensive criminal background check with a look-back period of 10 years (as legally permissible in each country)
d) Employment eligibility or criminal background check adjudication criteria
e) Samples of redacted background check documentation of third party employees

5. Privacy Events
Third parties should have adequate controls in place to prevent, monitor and report privacy events (i.e. 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. A copy of the documentation for those controls may be requested by Bank of America which should address the following attributes:

a) Incidents that would be classified as a privacy event/information security breach
b) Prevention and detection of privacy events/information security breaches
c) Immediate reporting, escalation and tracking of privacy events/information security breaches
d) Remediation/resolution plans
e) Notification to impacted third parties, including Bank of America

6. Fraud
Third parties should have policies and procedures in place to prevent, monitor and report fraudulent and suspicious activities. Fraud is an intentional act which includes misrepresentation or omission of material fact for improper gain or other benefit regardless of whether financial loss occurs. 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 against Bank of America may include “internal fraud” of third party employees, “first party external fraud” of external actors and third party external fraud of subcontractors.

A copy of those policies and procedures may be requested by Bank of America which should address the following attributes:
a) A list of fraud risks that apply to the product(s) and/or service(s) provided to or performed for Bank of America
b) Prevention and detection of fraudulent and suspicious activities
c) Immediate reporting, escalation, and tracking of fraud events and suspicious activities
d) Remediation and resolution plans for fraud events and suspicious activities
e) Procedures to notify impacted third parties, including Bank of America

7. Supplier Diversity
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. 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 supporting the Bank of America account to evidence this inclusion.

8. Environment, Social and Governance (ESG)
Bank of America is focused on responsible growth and environmental, social and governance (ESG) leadership. We are dedicated to doing business with third parties that respect ethics, human rights, diversity and inclusion and the environment. Our ESG expectations are conveyed to third parties through our Vendor Code of Conduct. Third parties must conform to this code and self-monitor their efforts to ensure compliance while conducting business with or on behalf of Bank of America and inform the bank in a timely manner of any non-conformance. Third parties may be asked to provide written information on their environmental, social and governance (ESG) policies, procedures and impacts.

9. Compliance Training
Third parties should provide an overview and/or examples of their process for ensuring employees are assigned and complete all required, applicable training courses via a relevant learning method. Third Parties shall comply and shall require Representatives and Subcontractors to comply with all Company requirements for training of personnel performing Services and shall provide certification of completion of such training to Bank of America when requested.

If Third Party engages a Sub-Contractor:
10. **Subcontractor Risk Management and Roster Collection**

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. 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:

a) Inventory or roster of subcontractors they use
b) Procedure for conducting due diligence that is commensurate with the risk of the subcontractor
c) Risk assessment process (quantifiable risk score, tiered classification) that identifies risks
d) Identification and escalation process (i.e. risk committee, defined escalation triggers)
e) Performance monitoring (i.e. scorecards, metrics, reporting)

When dictated by the contract, Third Parties are required to receive bank approval prior to changing or engaging in new subcontractor relationships.

If the Third Party is providing services that are customer facing, they may be requested to comply and provide evidence for the following:

11. **Customer Complaints**

Third Parties should have procedures, processes, and controls to ensure customer complaints are captured, addressed, reviewed, and reported in an accurate and timely manner, consistent with regulatory and Bank of America defined requirements.

12. **Call Listening for Unfair, Deceptive, Abusive Acts or Practices (UDAAP) Risk**

Third Parties should maintain call listening programs that are established and include review for compliance to UDAAP requirements. This includes calls conducted near the end of associated incentive periods (month-end or other high-risk times) when applicable.

13. **Call Recording & Retention**

Third Parties should have a process in place to record and retain customer calls in accordance records retention requirements, including Bank of America standards and international or federal and state laws.

14. **Compensation and Incentive Plans**
Compensation plans should reasonably ensure they do not incent prohibited acts or practices such as UDAAP risks. Third parties should provide reporting that allows Bank of America to review and validate components of the compensation plan have been executed as defined and agreed to.

Based on the products and/or services provided, additional items may be validated to ensure adherence to Bank of America policies:

15. Privacy: Autodialer; Call Monitoring and Recording; Telemarketing; Email Marketing; Capture of Privacy Choices

16. Bankruptcy

17. ADA Compliance – Web Content Accessibility Guideline (WCAG)

18. Deceased Customers/Clients

19. Fair Credit Reporting Act (FCRA)

20. Flood Insurance Compliance

21. Non English Language

22. Notary and Signer Policy & Requirements Validation

23. Payment Card Industry (PCI) certification

24. Postal Compliance

25. Servicemember Civil Relief Act (SCRA)

26. UDAAP Regulatory Change Review

27. Unclaimed Property and Escheatment (UPE)