National Bankers Association

Fintech Playbook:

Information Technology Third Party Evaluation Checklist

October 2023

Minority Depository Institutions (MDIs) are entering a new and dynamic period following historic investments from the public and private sector, including the U.S. Department of the Treasury's Emergency Capital Investment Program, as well as deposit growth from 2020-2022. Given this growth and changing banking landscape, many MDIs have expressed an increased interest in utilizing innovative technologies for a variety of objectives. MDIs have reported that sustainably onboarding and managing new technology partners for areas such as payments, lending, and account opening is a top priority, but many have noted concerns with their capacity to successfully conduct diligence on new technologies and manage new relationships.

The document provided is intended to be used to aid in identifying and tracking key priorities and information MDIs may wish to consider when performing due diligence on prospective relationships with technology companies. The checklist also includes a non-exhaustive list of potentially applicable regulatory publications, such as the interagency guide on "Conducting Due Diligence on Financial Technology Companies: A Guide for Community Banks."

Use of this checklist is voluntary and may not anticipate all types of third-party relationships and risks. It is meant to serve as a checklist to evaluate your bank, your bank's readiness as it relates to items such as your information technology environment, potential regulatory impact, or your strategic plan. The checklist is broken down into five sections that may help you to plan, prepare, execute, and assess the third-party relationship. Below are terms and definitions to assist in the use of this checklist.

Definitions

Owner: The owner is the person assigned to that question/task. They are responsible for collecting the information and completing the question/task.

Status: The status outlines where the question/task is currently at. Typical statuses noted may be: Not Started, Started, Partially Complete, Complete, Not Applicable.

Sections

Internal Assessment: This section is the process of assessing your banking environment. It is a chance to understand your use case, ensure you have internal support and resources available, and identify the impact to your bank.

Bank Profile: This section contains questions about your bank. This may help you when talking to third parties about who you are, your customer base, and the size of your bank.

Due Diligence with Third Party: This section is your opportunity to interview your third party. The questions help you with identifying any potential red flags and alignment to your risk appetite, your readiness, the third party's ability to support you, and potential items that may cause delays to the deployment schedule.

Third Party Management: This section is used as a checklist of items to obtain from the third party, if applicable. These items can be used to determine the maturity of a third party and their readiness to support you and comply with applicable laws and regulations. Once obtained, these items should be used to perform your third-party due diligence.

Next Steps: This section provides you with a list of potential items for follow up. Depending on the third-party relationship and type of implementation, some of these items may not be applicable. You can work with your third party to determine how you will proceed through this list of items. Depending on their maturity and experience, they may have a similar checklist to provide to you as part of their project plan.

MDI Innovation Partnership
Technical Assistance Subgroup

Information Technology Third Party Evaluation Checklist

Using the Strength, Weakness, Opportunity, and Threat (SWOT) analysis framework, the below checklist identifies key activities that should be performed when preparing a formal business plan. This checklist may serve as a supplement to a bank's existing due diligence processes in order to determine the bank's readiness to partner with a third party.

Internal Assessment

Define the issue or task to develop or solve Owner _____ Status _____

Define goal or intended results (What's your why?) Owner _____ Status _____

Assess customer impact Owner _____ Status _____

Regulatory impact Owner _____ Status _____

Is there budget availability? Owner _____ Status _____

Is board approval(s) required? Owner _____ Status _____

Decide on whether you have the resources to address the issue or task internally, or do you need to buy or partner with a tech company Owner _____ Status _____

Decision tree (Build or partner?) Owner _____ Status _____

Bank alignment (executive sponsor or project lead) Owner _____ Status _____

Core alignment with strategic plan and goals Owner _____ Status _____

Existing process analysis (internal and external IT systems, client process and reporting, management, and regulatory reporting) Owner _____ Status _____

For each new product or relationship, identify and report on impacts to reputation, strategic, operational, compliance, credit, interest rate, and liquidity risks (perform risk assessment) Owner _____ Status _____

Bank Profile

Description of your bank (profile yourself: community bank, commercial bank, target customer base, etc.) Owner _____ Status _____

Bank asset size Owner _____ Status _____

Number of employees Owner _____ Status _____

Number of customers Owner _____ Status _____

Does the bank have a chief technology officer (or equivalent)? Owner _____ Status _____

Due Diligence With Third Party

Execute mutual NDA Owner _____ Status _____

Describe the integration process for your product Owner _____ Status _____

Do you have an integration checklist that includes the technical detail required for integration into our network? Owner _____ Status _____

What transport protocols are being used with your product? (sftp/MQ/JMS/HTTPS, etc.) Owner _____ Status _____

Do you use any datacenters outside the continental U.S. in support of this solution? Owner _____ Status _____

Do you use offshore development and/or foreign owned as part of your solution? Owner _____ Status _____

Is this a cloud solution and/or does this require resources to be deployed internally? Owner _____ Status _____

What are your security requirements, and how are they monitored and managed (passwords, usernames, SSL certificates, single sign-on, multi-factor authentication, etc.)? Owner _____ Status _____

Does the solution have any custom requirements such as sub domain records or modifications to the customer website? Owner _____ Status _____

Are public IPs required? Owner _____ Status _____

Does the solution require trusted tunnels and firewall/IDS IPS configuration changes or entries? Owner _____ Status _____

Do you support IP whitelisting? Owner _____ Status _____

How is retention of data and data at rest managed? Owner _____ Status _____

What training resources do you make available and is there an active online user community? Owner _____ Status _____

Are there any significant quantifiable limitations to be aware of in terms of supported user counts, data records, storage or bandwidth usage? Please discuss Internet bandwidth requirements. Owner _____ Status _____

What changes do we need if we double our expected usage of the solution? Owner _____ Status _____

What are the OS and database requirements we need to meet to efficiently run the program? Owner _____ Status _____

What authentication, encryption, audit trails, and protection methods are in place for data loss or theft, changes, or entries? Owner _____ Status _____

Are there any prerequisites that include additional software or hardware within the customer environment or resources required for manual processes (report uploads, FileZilla, timelines for uploads, etc.)? Owner _____ Status _____

Will this be considered a new product or service to the bank (regulatory implications)? Owner _____ Status _____

Does the third party currently have in place any agreement, arrangement, or other program with a sponsor bank to originate loans, deposits, investment advisory accounts, or any other bank products or services? Owner _____ Status _____

What is the cost model (enterprise licensing, per user, or per transaction)? Are there tiers? Owner _____ Status _____

Do you integrate with my core? How does connection and integration with my core work? Are there additional costs to integrate? Do I need to open a project with my core provider? Is the integration real time and two way or one time and batch? Owner _____ Status _____

Due Diligence With Third Party

Is this solution customer facing? If so, does it work with my online banking provider? Please provide a reference. Owner _____ Status _____

Are there additional costs to integrate? Do I need to open a project with my online banking provider? Owner _____ Status _____

Does the third party OFAC screen employees? Owner _____ Status _____

Compliance with regulatory, state and federal requirements (GLBA, privacy, BSA, etc.) Owner _____ Status _____

Third Party Management

SOC Reports (SSAE 16/SSAE 18), audit documents, or any other type of security documents available) (SOC 1, SOC 2, SOC 3, and/or SOC for Cybersecurity) Owner _____ Status _____

Has the third party had any data breaches in the last 12 months? Owner _____ Status _____

Standardized Information Gathering (SIG) Questionnaire (if available) for all systems and locations Owner _____ Status _____

Consensus Assessments Initiative Questionnaire (CAIQ) (Only applies to a cloud provider to ascertain their compliance to the Cloud Controls Matrix) Owner _____ Status _____

DR/BCP testing results (probably only available if they provide data center solutions to customers), test frequency, bank participation options, backup schedules Owner _____ Status _____

Certificate of Insurance Owner _____ Status _____

Certificate of Good Standing Owner _____ Status _____

Copy of active contract / agreement Owner _____ Status _____

3 years annual reports Owner _____ Status _____

Any other documents they have that may be valuable pertaining to internal controls, policies, procedures, etc. Owner _____ Status _____

List of references Owner _____ Status _____

Has the third party ever (a) been investigated by a federal or state government agency regarding its failure to obtain a required license or (b) received a written letter or oral communication from a federal or state government agency regarding the applicability of a license requirement? Owner _____ Status _____

Does the third party hold any licenses from a foreign government agency? Owner _____ Status _____

Does the third party provide services to companies that are in any way involved in the cannabis industry? Owner _____ Status _____

Has the third party ever been subject to a formal or informal enforcement action relating to its data privacy or cybersecurity practices? Owner _____ Status _____

Does the third party comply with the PCI-DSS requirements? Owner _____ Status _____

Incident response plan, reporting procedures and responsibilities for bank and third party. Owner _____ Status _____

Deconversion fees, responsibility, timing Owner _____ Status _____

Identify what constitutes default, cure, remedies and termination in contract Owner _____ Status _____

Project management resources Owner _____ Status _____

Internal/external Owner _____ Status _____

Third party provided Owner _____ Status _____

Training assessment Owner _____ Status _____

Employee communication and training Owner _____ Status _____

Next Steps

Customer communication and training (if needed) Owner _____ Status _____

Beta testing Owner _____ Status _____

Review and analysis of beta testing Owner _____ Status _____

Decision tree (Do we test with a larger sample or move forward with the implementation?) Owner _____ Status _____

Lessons learned Owner _____ Status _____

Implementation and Assessment Owner _____ Status _____

Project team (Bank and third party) Owner _____ Status _____

Next Steps

Timeline and Periodic integration assessment Owner _____ Status _____

Solution Assessment Owner _____ Status _____

Did the solution meet the objective (i.e. improved customer service or expand a product offering; enhance the customer experience; etc.) Owner _____ Status _____

Periodic review and reporting of the solution Owner _____ Status _____

Lessons learned Owner _____ Status _____

Regulatory Publications

Interagency Publications

- "Interagency Guidance on Third-Party Relationships: Risk Management"
- "Conducting Due Diligence on Financial Technology Companies a Guide for Community Banks"
- "Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers: Final Rule"

FFIEC Publications

- IT Examination Handbook
- "Authentication and Access to Financial Institution Services and Systems"
- "Cybersecurity Resource Guide for Financial Institutions"
- Cybersecurity Assessment Tool
- "Joint Statement on Cyber Insurance and Its Potential Role in Risk Management Programs"
- "Joint Statement on Office of Foreign Assets Control Cyber-Related Sanctions Program Risk Management"
- "Joint Statement on Security in a Cloud Computing Environment"

OCC Publications

- OCC Bulletin 2023-22, "Cybersecurity: Cybersecurity Supervision Work Program"
- OCC Bulletin 2022-8, "OCC Points of Contact for Banks' Computer-Security Incident Notifications"
- OCC Bulletin 2017-43, "New, Modified, or Expanded Bank Products and Services: Risk Management Principles"