NAME

Vendor Management Policy

Approved by Board of Directors – Date

**Introduction**

The Board of Directors and Management of <NAME> recognize the Bank acquires services from various third-party service providers/vendors. The service providers include hardware/software vendors, outside consultants, data processing service providers and vendors who provide customer information and transaction processing support services as well as support to Bank equipment and facilities. Acquiring such services involves risks similar to the risks encountered when these functions are performed internally by Bank personnel. Included are such risks as: threats to the availability of systems used to support customer transaction processing, threats to the security of bank customers’ personal information and threats to our ongoing effort to maintain compliance with all banking regulations.

Under third-party contract arrangements, risk management measures commonly taken by the Bank generally fall under the control of the vendor. However, the Bank is ultimately responsible for managing these risks just as if the services were performed internally. The Bank could be exposed to financial loss, reputational damage and other adverse consequences, either from actions taken by a Bank vendor, or as a result of the vendor’s failure to adequately manage these risks. Consequently, it is incumbent upon the Bank to: (1) manage and oversee the vendors’ performance and ability to fulfill their contractual obligations and (2) prepare formal assessments of the risks associated with placing reliance on a vendor to fulfill critical services, such as data processing or customer service support functions.

# Purpose

<NAME> relies on third party vendors to provide a variety of products and services, including hardware/ software, data processing, transaction processing, marketing, technology and telecommunication, as well as outside support consultants. A list of vendors classified as critical is included as Appendix A of this policy statement.

The Board of Directors and Management of the Bank must ensure that: (1) The risks associated with the use of vendors for the Bank’s critical operations are fully understood, and (2) A process is established to monitor each vendor’s risk management controls, financial condition, and contractual performance.

**Responsibilities**

The Bank’s Risk Manager is responsible for the Bank’s vendor management program, which includes:

* Updating the Vendor Management Policy as needed
* Obtaining policy approval annually from the Board of Directors
* Overseeing the critical vendor monitoring process
* Keeping the Board of Directors abreast of changes regarding the Bank’s critical vendors
* Reporting the results of the critical vendor risk assessments annually to the Board of Directors

The Division Manager who has the primary responsibility for the service or product provided by a third-party service provider/vendor is responsible for managing that vendor relationship. Their responsibility includes:

* Reviewing the criticality of the services and products provided to the Bank by third-parties
* Identifying the Bank’s critical vendors
* Evaluating the risks and exposures associated with the critical vendor relationship
* Completing an annual Critical Vendor Risk Assessment, with the assistance of appropriate staff

## New Vendors and Contractual Relationships

## The appropriate Division Manager who is the Bank’s primary point of contact for a critical vendor is responsible to ensure the vendor contract has been reviewed (by the bank’s legal counsel when appropriate), and that it includes, as required, appropriate non-disclosure agreements and statements of responsibility for the maintenance of the security, accuracy and integrity of customers’ non-public, personal financial information.

In addition to ensuring the vendor contract is in compliance with the Bank’s requirements, the applicable Division Manager will be responsible to assess the criticality of the services the vendor will provide, giving consideration to the following factors:

1. The scope of customer service responsibilities being entrusted to the vendor and the potential impact on the image of the Bank.
2. Potential impact on earnings (i.e., potential for “real” dollar losses which might be incurred).
3. Bank’s ability to control and monitor the vendor’s compliance with regulatory requirements.
4. Potential impact on the ability to deliver minimum acceptable levels of service if the vendor fails or the level of performance declines.
5. Sensitivity to the scope and nature of sensitive customer information maintained by the vendor or accessible by the vendor.

**The following definitions are used to classify the relative importance of vendors:**

**Critical** – Services provided by the vendor are considered “critical” to the Bank’s operations if the services are required in order for the Bank to (1) operate at adequate capacity, or (2) deliver minimally acceptable levels of customer service. Also, there is no immediate replacement or back-up for such services, and contingency plans are required to ensure continuity of the Bank’s operations.

The use of outside vendors to perform *critical* services exposes the Bank to significant levels of strategic, operational or reputation risk. Additionally, the vendor’s business may be subject to high levels of credit or other financial risk (i.e., they may be highly leveraged, or dependent on a small market segment, etc.). The collection and remittance of payments by a vendor on behalf of the Bank could expose the Bank to operational, interest rate, market or liquidity risk. In some cases a vendor may have access to, or be in possession of, confidential customer data. Significant “hard” dollar losses (e.g., unbudgeted, extraordinary, or out-of-pocket cash expenditures for additional assistance, legal costs, etc.) and soft dollar losses (e.g., damage to the Bank’s reputation, disruption to service, or staff time/overtime) could be incurred because of the vendor’s failure to adequately manage risks.

**Important** – Services provided by the vendor are considered to be “important” to the Bank’s operations if, in the event of a failure by the vendor, the Bank would still be able to (1) operate at a minimum acceptable level of service or (2) have readily available an acceptable alternative means to process transactions or provide management information and service, such that minimal costs or losses are incurred.

The use of outside vendors to perform *important* services may expose the Bank to moderate levels of strategic, operational, or reputation risk, but the Bank has some degree of control or influence over these risks, or has systems in place to monitor such risks on an ongoing basis. Also, there are available replacements, including other vendors, or alternatives for such services, to ensure the continuity of the Bank’s operations. The vendor’s business may be subject to moderate levels of credit risk or other financial risk. The important vendor does not collect and remit payments on behalf of the Bank, or does so only on a limited basis, exposing the Bank to minimal operational, interest rate, and market or liquidity risk. Similarly, the vendor may have access to or possession of only limited confidential customer data. Acceptable minimal hard/soft dollar losses could be incurred from the vendor’s failure to adequately manage risk.

**Incidental** – Services provided by the vendor are considered “incidental” to the Bank’s operations when the Bank would have readily available (1) an acceptable alternative vendor, or (2) an adequate, alternative means to process transactions or provide management information and service; or would be able to (1) operate at acceptable levels of service with little or no risk of financial loss, or (2) deliver minimally acceptable levels of customer service.

The use of vendors to perform incidental services exposes the Bank to minimal levels of strategic, operational or reputation risk, or the Bank has significant control or influence over these risks, or has comprehensive systems in place to monitor such risks on an ongoing basis. Also, there are immediately available replacement vendors, or back-up alternatives for such services that ensure the continuity of the Bank’s operations. The vendor’s business is subject to minimal levels of credit risk or other financial risk. The vendor does not collect and remit payments on behalf of the Bank, exposing the Bank to little or no operational, interest-rate, market or liquidity risk. The vendor does not have access to or possession of confidential customer data, or only incidentally, as part of completing one-by-one transactions. Little or no hard dollar losses and minimal, acceptable soft dollar losses would be incurred from the vendor’s failure to adequately manage risk.

**Critical Service Vendor Assessment**

Before entering into a contract with a vendor for a critica**l** service, the key risks and the options for controlling the key risks will be assessed. It is the responsibility of the business unit Division Manager, serving as the primary point of contact with the vendor, to perform and document the steps taken to complete the vendor risk assessment.

Factors to consider when completing the risk assessment include: (1) the criticality of the function to the Bank, (2) the nature of servicing activities to be performed by the vendor (including handling funds or implementing credit decisions), (3) the availability of alternative vendors for the particular function, (4) insurance coverage available for particular risks, and (5) the cost and time required to switch vendors should problems arise. The assessment will ensure that the Bank understands the roles, responsibilities, and contractual obligations of all parties.

The following criteria will be included in the vendor assessment process:

1. **Selection of Vendor** – Management will determine the process for selecting new or replacement vendors based on the criticality of the product or service being sought. When deemed necessary, a formal request for proposal process will be used. Management will select which vendors will be invited to participate in the vendor selection process based on the requirements established for the product or service, the availability of established vendors within the bank’s market area, and the vendor’s experience and reputation. Management will also decide, based on the information available, how many vendors will be sent a request for proposal. The criteria used to evaluate the proposals will be based on a variety of qualitative considerations, based on the most important requirements of the prospective relationship.

The Bank will perform appropriate due diligence in addition to the risk assessment to satisfy itself regarding the vendor’s proven operational competence and financial stability, through reference checks and a review of the most recent financial statements.

1. **Contracts -** The written contract between the Bank and the vendor should clearly specify all relevant terms, conditions, responsibilities and liabilities of both parties. These would normally include terms such as:

* + Statements supporting the business reason for requiring access to non-public, personal financial information related to the Bank’s customers.
  + Agreements not to disclose non-public, personal financial information of Bank customers, either in possession of the vendor or accessible to them, and statements of vendor responsibility and liability in the event such sensitive customer information is in fact disclosed to an unauthorized party.
  + Required service levels, performance standards, and penalties.
  + Internal controls, insurance, disaster recovery capabilities, and other risk management measures maintained by the vendor.

* + Data and system ownership and access.
  + Liability for delayed or erroneous transactions and other potential risks.
  + Provision to provide Bank access to internal or external audits or other reviews of the vendor’s operational and financial condition.
  + Compliance with applicable regulatory requirements.
  + Provisions for handling disputes, contract changes, and contract termination.

Vendors with access to non-public sensitive customer information for covered accounts must have policies and procedures in place to detect, prevent and mitigate Identity Theft, as required to comply with the FACT Act. Specifically, this involves recognizing any “red flag” indicators that may arise or become apparent during the course of the vendor performing contracted processing services and operational support duties on behalf of the Bank.

The terms and conditions of each critical vendor contract will be reviewed by the Bank’s legal counsel if/when deemed advisable 1) to ensure the terms and conditions are appropriate for the type of service(s) being provided, and 2) to ensure the level of risk involved is acceptable to the Bank.

1. **Policies, Procedures, and Controls** – The vendor should implement internal operational control procedures, data security measures and contingency planning capabilities which are comparable to those the Bank would utilize if the activity or service was performed internally. Appropriate controls are required whenever a vendor processes transactions and handles customer funds on behalf of the Bank.
2. **Ongoing Monitoring** – The Bank will review the operational performance of critical vendors on an ongoing basis to ensure the vendor is meeting the service level commitments of the contract. Division Managers will be primarily responsible for completing this evaluation at least annually.
3. **Information Access** – The Bank will ensure that it has complete and immediate access to current data and appropriate back-up information for critical operations maintained or processed by an outside vendor.

6. **Audit Consideration** – The Bank’s auditors will review the oversight of critical vendors by Bank management and others, including regulators. Audits of critical vendors should be conducted according to

a scope and frequency appropriate for the particular function. For third-party data processing services, the Bank will obtain copies of the audit report(s) describing the service organizations internal controls and management’s response. Audit reports of critical vendors will be available to the Audit Committee of the Board of Directors. Audit results and management responses will be available to examiners at their request. The Bank’s auditors will also audit compliance with vendor service level commitments and agreements.

7 **Contingency Plans** – The Bank will ensure that appropriate business resumption plans have been prepared by the vendor. Where appropriate, the Bank’s contingency plans will also include provision for continuance of processing activities (either in-house or with another provider) if the vendor is no longer able to provide the contracted services or the arrangement is otherwise unexpectedly disrupted.

**Ongoing Vendor Risk Evaluations**

Annually, each Division Manager will evaluate the risks and exposures associated with the critical vendor relationships they manage. The evaluation process will include the following for each vendor relationship managed:

1. An update of the key information regarding the vendor.
2. A review of the nature and purpose of the vendor relationship.
3. A review of the service level performance being provided by the vendor.
4. A review of the vendor’s report(s) on operational controls and testing (if available), and a written response to the User Control Considerations contained in the report(s).
5. A review of the credit analysis of the vendor’s financial statements, completed by a Bank Credit Analyst.

1. An assessment of the relative level of strategic, credit, operational, compliance and legal reputation risk associated with the vendor relationship.

A risk assessment will be prepared for each critical vendor utilizing the Vendor Risk Assessment form attached as Appendix B of this policy. The Division Manager who acts as the Bank’s primary point of contact with the vendor will be primarily responsible for completing the risk assessment, with the assistance of other appropriate departmental staff.

The Risk Manager will review the risk assessments and associated documentation, and prepare a summary report of the Bank’s critical vendor risk assessments to be presented to the Board of Directors for review.

<NAME>  **Bank**

**Vendor Management Policy**

**Appendix A – Critical Vendor List**

**Critical Vendor Services Provided**

**Information deleted because policy is being shared.**

**Vendor Management Policy - Appendix B - Vendor Risk Assessment**

A risk assessment is completed for all new vendors, and updated annually for existing vendors, who maintain or will maintain a contractual relationship with the Bank to provide critical services. The objectives of the annual assessment are to identify the risks present in the relationship between the vendor and the bank, and to document the measures taken to monitor the vendor’s level of service performance and financial stability.

**VENDOR CONTACT INFORMATION**

Company Name: Contact Name:

Address: Telephone:

E-mail:

**BANK MANAGER RESPONSIBLE FOR THE VENDOR RELATIONSHIP**

Name: Position:

Assessment Prepared By: Date:

**CHECK ALL OF THE FOLLOWING THAT APPLY TO THIS VENDOR’S RISK ASSESSMENT:**

\_\_\_\_\_ **NEW VENDOR REVIEW**

If yes, list other vendors considered \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_ **EXISTING VENDOR REVIEW**

If yes, how long has the bank conducted business with this vendor? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_ Vendor is an affiliate of the bank

Describe the affiliation \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Vendor’s Operational Controls\***

**\_\_\_\_\_** AuditReports describing the Vendor’s operational controls and testing were obtained and analyzed.

Which reports were provided: \_\_\_\_ SSAE18 \_\_\_\_ SOC 1 \_\_\_\_ SOC 2 \_\_\_\_ Other

If *Other* was checked, please explain: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_ The User Control Considerations listed in the vendor’s description of controls have been addressed and a written response to each consideration has been included as part of this risk assessment.

**Vendor’s Financial Information\***

\_\_\_\_\_ Audited financial statements were obtained and reviewed.

\_\_\_\_\_ Other financial information was obtained and reviewed (audited financial statements were not available).

Type of information (ex. credit report, quarterly reports) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_ An evaluation of the vendor’s financial condition, completed by a bank’s credit analyst, is attached.

**\*All risk assessment documentation obtained, reviewed, or produced, will be reviewed by the bank’s Risk Manager and retained by vendor in the bank’s vendor management files.**

**RISK ASSESSMENT CONSIDERATIONS**

Complete the vendor risk assessment providing the information requested in each category. Consider (1) any potential risk issues, (2) the degree of exposure to loss, (3) the methods used to measure/monitor risks (i.e., the primary systems, reports, committees, etc.), and (4) the frequency of risk measuring/monitoring.

**DESCRIPTION OF VENDOR RELATIONSHIP**

**1. BRIEFLY DESCRIBE THIS VENDOR:** (Include the type of business, products/services offered, relative size and geographic market, length of time in business…)

**2. LIST OR EXPLAIN THE PRODUCTS/SERVICES THIS VENDOR PROVIDES TO <NAME>:**

**3. NOTE THE KEY ELEMENTS OF THE CONTRACT BETWEEN THE BANK AND THIS VENDOR:**

* Date of Contract \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* Contract Term \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* Contract Expiration Date \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* Auto-Renewal Terms \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* Non-Renewal Notification (# Days) \_\_\_\_\_\_\_\_\_\_\_\_
* Is Notification of Vendor Breach Required \_\_\_\_\_\_\_
* Signed Confidentiality Agreement \_\_\_\_\_\_\_\_\_\_\_\_\_
* Is an Electronic Copy of the Current Contract Available for the Vendor’s File \_\_\_\_\_\_\_\_\_\_

Note any service level commitments incorporated into the contract, along with the method used to measure/monitor the service performance level \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**4. HOW CRITICAL IS THIS VENDOR TO THE BANK’S BUSINESS OPERATIONS:** (Access to sensitive information; transaction processing; technology interface; customer contact**…**)

**5. HOW STRONG IS THIS VENDOR:** (Financial position; technical advancements; reliance on subcontractors; ability to meet growth; strength of internal controls, policies and procedures; background checks and compliance training for employees**……**)

**6. HOW RELIABLE IS THIS VENDOR:** (Business continuity plan; communication/responses; connectivity…)

**DETERMINING THE LEVEL OF RISK**

The charts and definitions below should be used to assess the level of risk, or the Bank’s risk exposure, in each of the major risk categories listed on the following page. A particular risk level is determined after considering both the severity of the impact, and the likelihood of the event occurring. Using the descriptions in the charts below, determine the *Severity* (Chart II) and *Likelihood* (Chart III) for the risk category being rated. Then use Chart I to determine the level of risk.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CHART I - RISK LEVEL ASSESSMENT** | | | | | | |
| **Likelihood**  **Of**  **Occurrence** | **Impact Severity** | | | | | |
| Insignificant | Minor | Significant | Damaging | Serious | Critical |
| Negligible | Low | Low | Low | Low | Low | Low |
| Very Low | Low | Low | Low | Low | Moderate | Moderate |
| Low | | Low | Low | Moderate | Moderate | High | High |
| Medium | Low | Low | Moderate | High | High | High |
| High | Low | Moderate | High | High | High | High |
| Very High | Low | Moderate | High | High | High | High |
| Extreme | Low | Moderate | High | High | High | High |

|  |  |
| --- | --- |
| **CHART II - IMPACT SEVERITY LEVELS** | |
| **Severity** | **Description** |
| Insignificant | Almost no effect if the threat is realized and the vulnerability is exploited. |
| Minor | Only a minor effect is realized, and minimal effort will be required to restore operations. |
| Significant | Some negligible yet tangible harm is realized, which will require some expenditure of resources to restore operations. |
| Damaging | Damage to the reputation of the Bank, and/or notable loss of confidence by bank stakeholders, which will require the expenditure of significant resources to repair. |
| Serious | Considerable business disruption and/or loss of customer/business partner confidence.  May result in the compromise of services, or a large amount of customer/bank information. |
| Critical | Extended outage or permanent closure, requiring operations to resume in a hot site environment. May result in complete compromise of services or confidential information. |

|  |  |
| --- | --- |
| **CHART III - LIKELIHOOD OF OCCURRENCE** | |
| **Likelihood** | **Description** |
| Negligible | Unlikely to occur |
| Very Low | Likely to occur two/three times every five years |
| Low | Likely to occur once every year or less |
| Medium | Likely to occur once every six months or less |
| High | Likely to occur once a month |
| Very High | Likely to occur multiple times a month |
| Extreme | Likely to occur multiple times a day |

|  |  |  |
| --- | --- | --- |
| **CATEGORIES OF RISK** | **RISK LEVEL**  **Low - Moderate - High - NA**  (New and Existing Vendors) | **DIRECTION OF RISK**  **Decreasing - Stable - Increasing**  (Existing Vendors Only) |
| **CREDIT RISK –** Arises when the vendor fails to meet its obligations according to agreed-upon terms. |  |  |
| **MARKET RISK –** Arises when an adverse change occurs in market rates or the vendor’s price, which impacts the services provided. |  |  |
| **LIQUIDITY RISK –** Arises when the vendor’s ability to provide services impacts the bank’s ability to meet financial obligations. |  |  |
| **STRATEGIC RISK -** Arises when the bank’s decision to utilize this vendor, product or service, turns out to be improper or inappropriate, due to an inadequate risk assessment, insufficient knowledge of the product or business, or inconsistency with the bank’s goals or expected return on investment. |  |  |
| **OPERATIONAL RISK –** Arises when the vendor is unable to deliver its product or provide its services, due to inadequate or failed processes, people or systems. |  |  |
| **COMPLIANCE RISK -** Arises when the vendor’s operations violate regulations, laws, standards, or the bank’s prescribed policies and procedures. |  |  |
| **REPUTATION RISK -** Arises when the vendor’s service, products, or information breach elicits negative publicity, public scrutiny, or a negative perception of the bank, which could lead to costly litigation, or the loss of customers or revenue. |  |  |

**VENDOR RISK MANAGEMENT NARRATIVE**

Describe in narrative form the reasoning behind the risk ratings above. In particular, explained risks that are considered “Moderate” or “High”. If the bank’s exposure to risk within any of the categories is “Increasing” document the reason, and indicate whether the increased risk is expected to be temporary or continuing. Include information about past occurrences which led you to characterize the “likelihood of occurrence”. Explain the “impact severity” as it specifically relates to <NAME>.

|  |  |
| --- | --- |
| **CREDIT RISK** |  |
| **MARKET RISK** |  |
| **LIQUIDITY RISK** |  |
| **STRATEGIC RISK** |  |
| **OPERATIONAL RISK** |  |
| **COMPLIANCE RISK** |  |
| **REPUTATION RISK** |  |

**COMMENTS:**

SI 3/2019