Approved by Board Compliance Committee August 10, 2023
Approved by the Board of Directors August 15, 2023

First Bank Vendor Management Policy

Policy and Program Management

The Board of Directors and management recognize the need to establish and implement policies and procedures with respect to the appropriate oversight of third-party entities who provide various support and/or product services for First Bank. For purposes of this policy, a third-party relationship is a broadly defined term to include any entity that has entered into a business arrangement with First Bank by contract or otherwise.

The third-party relationship may be positioned directly or indirectly between First Bank and its customers or otherwise have unfettered access to First Bank customers. Consequently, the quality of that third party's performance is critical to First Bank's long-term success.

Mission

The purpose of the vendor management program is to assist the Board of Directors and Management. The use of third parties can assist First Bank in attaining strategic objectives by increasing revenues or reducing costs. The use of a third party also commonly serves as a vehicle for First Bank to access greater expertise or efficiency for a particular activity. The decision about whether to use a third party is considered by the Board of Directors or management by taking into account the circumstances unique to the potential relationship. The use of third parties in no way diminishes the responsibility of the Board of Directors and management to ensure that the third-party activity is conducted in a safe and sound manner and in compliance with applicable laws, regulations, and internal policies.

The time and resources devoted to managing third party relationships is based on the risk the relationship presents to First Bank.

Authority & Responsibility

The Board of Directors and management are ultimately responsible for identifying, controlling and properly overseeing outsourced relationships to mitigate risk against First Bank. The Compliance Officer is responsible for maintaining the program, assisting with new vendor contracts, ensuring that annual vendor reviews are conducted, and that risk ratings are kept up to date as part of the review process. The Board of Directors and management have developed and implemented this policy to consistently govern the outsourcing process for the entire organization. This policy addresses outsourced relationships from an end-to-end perspective including:

1. Establishing servicing requirements and strategies

2. Selecting a provider by conducting due diligence activities

3. Negotiating the contract to provide First Bank with the ability to control and monitor third party activities (e.g., growth restrictions, underwriting guidelines, external audits, etc.) and costs.

4. Monitoring, changing, and discontinuing the outsourced relationship if it does not meet high quality standards or uphold contractual terms.

5. Conducting annual reviews of high risk or critical third-party's audit results, financials and vendor provided documentation.
6. Reporting any exceptions to the Board of Directors to ensure exceptions are immediately addressed to evaluate the risk to First Bank.

Board of Directors

Appropriate reporting through Board committees or the entire Board of Directors shall address risk management considerations and the overall operation of vendor management activities.

Authority

This policy is a general statement of First Bank's objectives, direction and expectations regarding the oversight of third-party vendors providing support for First Bank's products, services and other such activities. As such, it is the authority, basis and platform for the development, communication, implementation, interpretation and enforcement of appropriate and applicable operating standards.

Enforcement

No part of this policy or its supporting operating procedures should be interpreted as contravening or superseding any other legal and regulatory requirements placed upon First Bank. Protective measures should not impede other legally mandated processes such as records retention or subpoenas. Any conflicts should be submitted immediately to management for further evaluation and/or subsequent submission to First Bank's legal counsel.

Exceptions

Requests for exceptions to this policy must be very specific and may only be granted on specific items, rather than to entire sections. First Bank personnel with exceptions are to communicate their requests to management who may need to seek Board of Director approval prior to approving or granting the exception.

Planning/Risk Management

It is the policy of First Bank to appropriately assess, measure, monitor, and control the risks associated with the use of third-party relationships in any capacity. While engaging another entity may assist the Board of Directors and management in achieving strategic goals, First Bank realizes that such an arrangement reduces management's direct control. Therefore, the use of a third party increases the need for oversight of the process by First Bank from start to finish by utilizing the following main elements of an effective third-party risk management process:

1. Risk assessment,
2. Due diligence in selecting a third party,
3. Contract structuring,
4. Legal review,
5. Ongoing oversight, and
6. Vendor Termination

While these elements apply to any third-party activity, the precise use of this process is dependent upon the nature of the third-party relationship, the scope and magnitude of the activity, and the risks identified. These guidelines are not intended to result in an expansion or a decrease in the use of third parties by First Bank, but to provide a framework for assessing, measuring, monitoring, and controlling risks associated with third parties throughout the relationship life cycle.

First Bank's comprehensive risk management process, which includes management of all third-party relationships and all third-party relationships attained through acquisition, enables First Bank to ensure that capital is sufficient to support First Bank's underlying risk exposures and that the third party is operating in a manner consistent with federal and state laws, rules, and regulations, including those intended to protect consumers.

In certain instances, a third-party relationship may be classified by First Bank as "high risk" if the:

1. Relationship has a material or critical effect on First Bank revenues or expenses;
2. Third party performs critical functions;
3. Third party stores, accesses, transmits or performs transactions regarding confidential customer/member or employee information; or
4. Third party poses risks that could significantly affect earnings or capital

Third party relationships that fall into the high risk or critical category require the highest level of due diligence, legal review and ongoing oversight.

Program Management utilizing Vendor Management Software

First Bank Board of Directors and management recognize the resource intensive nature of vendor management, especially as it relates to managing the risks involved with outsourced service providers. Considering this, management chose to partner with a software vendor that provides First Bank with critical vendor management support including:

1. Centralization of all vendor information
2. Vendor and service risk assessment
3. Vendor and associated service performance monitoring
4. Vendor relationship portals for easier vendor management
5. Automation of due diligence and request for proposal (RFP) process
6. Incident reporting and management
7. Centralized contracts and document storage
8. Third party vendor due diligence services and ongoing monitoring support

The software assists First Bank with documenting the significance of the vendor relationship by allowing relationship managers the ability to assess the risk of the products and/or services provided in order to derive one of these three vendor relationship types:

1. Critical – extreme liabilities result if the information is compromised, could cause major financial loss, result in legal action against the institution, or severely damage the institution's reputation. Appropriate vendor oversight is required and due diligence must be conducted annually.

2. Material – serious liabilities result if the information is compromised, could cause moderate financial loss, legal action against the institution would be likely, or damage to the institution's reputation

would be moderate. Appropriate vendor oversight is necessary and due diligence will be conducted every two years.

3. Minor – Liabilities could possibly result if the information is compromised, would likely cause only minor financial loss, litigation unlikely or damage to the institution's reputation would be minimal. Due diligence should be conducted on an as needed basis.

Overall Vendor Risk Rating

It is the policy of First Bank to review service provider relationships on an ongoing basis, with the frequency and level of detail determined according to the risk categories mentioned above. The overall risk rating is determined by the relationship manager's initial due diligence and the results of the completed vendor software risk rating review. This process takes into consideration the relationship significance, due diligence collected, recent performance assessments and any incidents reported. Overall vendor risk ratings include:

High
The risk associated with the vendor/service relationship could be significant, either due to the service or the vendor providing the service.

Medium
There is measurable risk associated with the vendor/service relationship, either due to nature of the service or the vendor providing the service.

Low
There is little risk associated with the vendor/service relationship. Impact is minimal and could be considered a cost of doing business. Additional controls could further reduce the impact and might be considered as part of an optimization process. Appropriate vendor oversight is minimal.

Product and Service Risk Categories

First Bank realizes that there are numerous risks that may arise from the use of a third party that can contribute to operational and transaction risks in each process involved in the delivery of First Bank's products or services.

Not all of the following risks will be applicable to the products or services provided to First Bank. However, complex or significant arrangements may have definable risks in most areas. It is the responsibility of the Board of Directors and management to understand the nature of these risks in the context of First Bank's current or planned use of its third party's products and services.

Compliance Risk

Compliance Risk is the current and prospective risk to earnings or capital arising from violations of, or non-conformance with laws, rules, regulations, prescribed practices, internal policies and procedures, or ethical standards. Compliance Risk also arises in situations where the laws or rules governing certain financial institution products or activities of the financial institution's customers may be ambiguous or untested. This risk exposes the financial institution to fines, civil money penalties, payment of damages, and the voiding of contracts. Compliance Risk can lead to diminished reputation, reduced franchise value, limited business opportunities, reduced expansion potential, and an inability to enforce contracts.

Credit Risk

Credit Risk is the current and prospective risk to earnings or capital arising from an obligator's failure to meet the terms of any contract with the financial institution or otherwise to perform as agreed. Credit Risk is found in all activities in which success depends on counterparty, issuer or borrower performance. It arises any time financial institution funds are extended, committed, invested or otherwise exposed through actual or implied contractual agreements, whether reflected on or off the balance sheet.

Interest Rate Risk

Interest Rate Risk is the current and prospective risk to earnings or capital arising from movements in interest rates. Interest Rate Risk arises from differences between the timing of rate changes and the timing of cash flows (repricing risk), from changing rate relationships among different yield curves affecting financial institution activities (basis risk), from changing rate relationships across the spectrum of maturities (yield curve risk), and from interest related options embedded in financial institution products (options risk).

Liquidity Risk

Liquidity Risk is the current and prospective risk to earnings or capital arising from a financial institution's inability to meet its obligations when they come due without incurring unacceptable losses. Liquidity Risk includes the inability to manage unplanned decreases or changes in funding sources. Liquidity Risk also arises from the failure to recognize or address changes in market conditions that affect the ability to liquidate assets quickly with minimal loss in value.

Reputation Risk

Reputation Risk is the current and prospective impact on earnings and capital arising from negative public opinion. This affects the institution's ability to establish new relationships or services or continue servicing existing relationships. This risk may expose the financial institution to litigation, financial loss, or a decline in its customer base. Reputation Risk exposure is present throughout the organization and includes the responsibility to exercise an abundance of caution in dealing with its customers and the community.

Strategic Risk

Strategic Risk is the current and prospective impact on earnings or capital arising from adverse business decisions, improper implementation of business decisions, or lack of responsiveness to industry changes. This risk is a function of the compatibility of an organization's strategic goals, the business strategies developed to achieve those goals, the resources deployed against these goals and the quality of implementation. The resources needed to carry out business strategies are both tangible and intangible. They include communication channels, operating systems, delivery networks, and managerial capacities and capabilities. The organization's internal characteristics must be evaluated against the impact of economic, technological, competitive, regulatory, and other environmental changes.

Transaction Risk

Transaction Risk is the current and prospective risk to earnings and capital arising from fraud, error, and the inability to deliver products or services, maintain a competitive position, and manage information. Transaction Risk is inherent in efforts to gain strategic advantage, and in the failure to keep pace with changes in the financial services marketplace. Transaction Risk is evident in each product and service offered. Transaction Risk encompasses product development and delivery, transaction processing, systems development, computing systems, complexity of products and services and the internal control environment.

Service Provider Due Diligence

General

The Board of Directors and Management recognize the need to incorporate a complete and extensive due diligence process before a contract is awarded and as a condition of continuing support for any of First Bank's significant vendors (i.e., subcontractors, support vendors, and other parties). Ultimately, the depth of due diligence will vary depending on the scope and importance of the outsourced services in addition to the risk to First Bank from these services.

Due Diligence Standards

It is the responsibility of the Board of Directors or management to select a qualified entity to implement the activity or program following an assessment of risks and a decision to proceed with a plan to establish a third-party relationship in response to a request for proposal (RFP) or contract. The due diligence process provides First Bank with the information needed to address qualitative and quantitative aspects of potential third parties to determine if a relationship would help achieve First Bank 's strategic and financial goals and mitigate identified risks. Not only is due diligence to be performed prior to selecting a third party, but it is also to be performed periodically during the course of the relationship, particularly when considering the renewal of a contract.

The scope and depth of due diligence is directly related to the importance and magnitude of First Bank's relationship with the third party. For example, large scale, highly visible programs or programs dealing with sensitive data integral to First Bank 's success warrant an in-depth due diligence of the potential third party, while the due diligence process for isolated low risk third party activities would be much less comprehensive.

Entities with whom we do business must adhere to the following principles, which are addressed in our vendor questionnaire:

- We explicitly prohibit human trafficking and the use of involuntary labor within our supply base including forced, bonded, or indentured labor, involuntary or exploitative prison labor, and other forms of modern slavery. Vendors must pay their employees and contractors appropriate wages.
- Vendors must not employ child labor.
- First Bank recognizes its responsibility to protect human rights. Examples of such rights are articulated in internationally recognized standards, including the United Nations Guiding Principles on Business and Human Rights (UNGPs), the Universal Declaration of Human Rights, and the International Labor Organization (ILO) Core Conventions.
- Vendors are required to comply with all applicable laws regarding discrimination in hiring and employment practices. Vendors are expected to maintain a workplace free of discrimination, harassment, victimization, intolerance of any other form of inappropriate behavior or abuse on any grounds, including but not limited to age, disability, ethnic or social origin, gender, gender identity, nationality, race, sexual orientation, marital status, parental status, pregnancy, political convictions, religious beliefs, union affiliation, or

veteran status. Vendors are expected to maintain an environment free of harassment, violence, and abuse (physical or verbal) at all times.

- Vendors must provide a safe and healthy working environment that minimizes health and safety risks and supports accident prevention and ensures the health and safety of all personnel and all others affected by their activities. Vendor's workers must be provided with ready access to clean toilet facilities and potable water. Vendors must ensure that workers do not work excessive hours which jeopardizes their health and safety.
- Vendors and their subcontractors are expected to engage and provide opportunities for a workforce that is inclusive of diverse groups. Vendors are expected to take proactive steps to include the hiring of historically underrepresented groups, such examples are of workers who self-identify as minorities, ethnically diverse, women, LGBTQ+, Veteran, or a person with a disability.
- Vendors should identify and manage risks and opportunities related to climate change. Where appropriate to the size and nature of their operations, vendors should address the environmental impacts from its operations including raw material usage, greenhouse gas emissions, water, waste, air quality and biodiversity. Any waste, and in particular hazardous waste, must be managed in a responsible manner.

Comprehensive due diligence involves a review of all available information about a potential third party, focusing on the entity's financial condition, its specific relevant experience, its knowledge of applicable laws and regulations, its social and environmental practices, its reputation, and the scope and effectiveness of its operations and controls. The evaluation of a third party may include the following items:

- Audited financial statements, annual reports, SEC filings and other available financial indicators.
- Inspecting as far back in the supply chain as needed to obtain assurances that the entire supply chain is free from unethical social and environmental conditions and to ensure that component and material substitutions are aligned with agreed-upon materials. This is on a global scale.
- Significance of the proposed contract on the third party's financial condition.
- Experience and ability in implementing and monitoring the proposed activity.
- Business reputation, including existence and corporate history.
- Qualifications, backgrounds, and reputations of company principals, including criminal background checks when appropriate.
- Strategies and goals, including service philosophies, quality initiatives, efficiency improvements, and employment policies.
- Legal and regulatory compliance, including the existence of any significant complaints or litigation, or regulatory actions against the company.
- Ability to perform the proposed functions using current systems or the need to make additional investment.
- Reliance on and success in dealing with the use of other third parties or subcontractors by the third party.
- Scope of internal controls, systems and data security, privacy protections, and audit coverage.

- Business resumption strategy and contingency plans.
- Knowledge of relevant consumer protection and civil rights laws and regulations.
- Adequacy of management information systems.
- Insurance coverage.
- Other companies using similar services from the provider that may be contacted for reference.
- Service delivery capability, status, and effectiveness.
- Technology and systems architecture.

The depth and formality of the due diligence performed by Management may vary according to the risk of the outsourced relationship, First Bank's familiarity with the prospective service providers, and the stage of the provider selection process.

Contracts

Each purchase or service order is based upon an individual situation, and the selection of an appropriate vendor is to be selected on the basis of quality, service and price in addition to the due diligence directives of this policy. Price should not be the driving force in this decision-making process. Some degree of loyalty to a vendor may generate a more immediate response when a need of First Bank becomes a priority.

Contract Considerations
It is the responsibility of the Board of Directors and Management to ensure that the specific expectations and obligations of both First Bank and the third party are outlined in a written contract prior to entering into the arrangement after selecting a third party. The Board of Directors will be informed by Management prior to entering into any critical or material third party arrangements. Appropriate legal counsel is also to review significant contracts prior to finalization.

It is the responsibility of Management to ensure that a critical or material risk contract, at a minimum:

1. Portrays an accurate description of the outsourcing relationship.

2. Is clearly written and contains sufficient detail to comprehensively define the rights and responsibilities of each party.

3. Is reviewed by First Bank counsel, when appropriate.

The following is a list of key contract elements that every vendor owner should consider including in new agreements during the contract negotiation process or existing agreements during the contract renewal review process. The inclusion of various elements listed will depend on the type of service provided and risk rating of the vendor.

1. Nature and Scope of Arrangement
2. Performance Measures or Benchmarks
3. Responsibilities for Providing, Receiving, and Retaining Information
4. The Right of the Company to Audit and Require Remediation
5. Responsibility to Comply with Applicable Laws and Regulation
6. Cost and Compensation
7. Ownership and License
8. Confidentiality and Integrity
9. Business Resumption and Contingency Plans

10. Indemnification
11. Insurance
12. Dispute Resolution
13. Limits on Liability
14. Default and Termination
15. Customer Complaints
16. Subcontracting
17. Foreign-Based Third Parties
18. Legal Review
19. Regulatory Supervision
20. Cybersecurity

Ongoing Monitoring

It is the policy of First Bank to maintain adequate oversight of third-party activities and adequate quality control over those products and services provided through third party arrangements in order to minimize exposure to potential significant financial loss, reputation damage and supervisory action. For vendors that interact with customers directly, it's a policy of the Bank to monitor consumer complaints concerning products or services provided through the vendors. Because the regulators regard the actions of the vendors as those of the Bank, and as the monitoring of consumer complaints can reveal trends or causes indicating a violation of UDAAP requirements, we include ongoing monitoring of consumer complaints as part of its vendor management program. At a minimum, such monitoring should address the following:

a. Specific requirements for monitoring (i.e., reports and frequency)
b. Identification of products or services in complaints
c. Timing (i.e., when the complaint is received and resolved)

First Bank's oversight program generally includes monitoring of the third party's quality of service, risk management practices, financial condition, and applicable controls and reports. First Bank utilizes vendor management software and professional services to manage the ongoing monitoring process of each vendor and third-party service provider.

Results of oversight activities for material third party arrangements are periodically reported to the Board of Directors. Identified weaknesses are documented and promptly addressed.

Proper documentation facilitates the monitoring and management of the risks associated with third party relationships. Therefore, it is the policy of First Bank to maintain documents and records on all aspects of the third-party relationship, including valid contracts, business plans, risk analysis, due diligence, dispute resolution and oversight activities (including reports to the Board of Directors and management). This critical documentation and reporting functionality is housed and maintained in the software.

Vendor Termination

Any vendor not in compliance with First Bank's Vendor Management Program will be required to make the necessary enhancements to correct noted deficiencies and assure compliance within an acceptable timeframe. Any weakness that a vendor is unwilling or unable to correct to the Bank's satisfaction will be addressed with the Compliance Officer. Management will determine whether the weakness presents an unacceptable risk to the institution and forward any findings to the Board of Directors for final approval.

In instances when a solution that controls/mitigates the weaknesses found cannot be reached, alternative vendors will be sought.