RADIANT CREDIT UNION

Policy No: 511.01
Date: March 22, 2022
Replaces: March 24, 2021
Effective: March 22, 2022

POLICY

SUBJECT: Vendor Management

Reference: NCUA Letter to Credit Union Number 01-CU-20, Due Diligence Over Third Party Service Providers
NCUA Letter to Credit Union Number 00-CU-11, Risk Management of Outsourced Technology Services, Appendix
Supervisory Letter Number 07-01-Evaluating Third Party Relationships
Policy Number 1007.01, Concentration Risk (Section V. Vendor Oversight)

I. OVERVIEW

A. Radiant Credit Union (Credit Union) receives contracted services from third party suppliers. Senior management and the Board of Directors (Board) recognize that vendor relationships present potential risks that must be properly managed on an ongoing basis. It is the Credit Union's policy to effectively assess measure, monitor and control the risks associated with vendor relationships. The Credit Union has established and will maintain adequate procedures for managing its third-party relationships throughout the life cycle of that relationship through pre-defined selection requirements, informed risk assessment, due-diligence review, contract analysis, and ongoing management oversight and monitoring.

B. The purpose of this Vendor Management Policy (Policy) is to provide guidance for the appropriate risk management of vendor relationships and to tailor vendor monitoring based upon initial and ongoing risk assessments of those relationships. This policy addresses the vendor management process and the risks associated with those vendor relationships from an end-to-end perspective, including establishing servicing requirements and strategies, selecting a provider, negotiating the contract, and monitoring, changing, and/or discontinuing the outsourced relationship.

C. Management and the Board maintain ultimate responsibility for managing activities conducted by vendors and for identifying and controlling the risks arising from such relationships. The use of third-party service providers in no way diminishes the responsibility of management and the Board to ensure that the third-party activity is conducted in a safe manner and in compliance with applicable laws, regulations, and internal policies, including, but not limited to, The Gramm-Leach-Bliley Act (GLBA).

II. VENDOR RISK ASSESSMENT PROCESS

A. An effective vendor management process is one that establishes Management and Board awareness of the risks associated with outsourcing agreements; ensures effective risk management practices; ensures that an outsourcing arrangement is prudent from a strategic risk perspective; and is consistent with the business objectives of the Credit Union.

B. The Credit Union analyzes the benefits, costs, legal aspects, and potential risks associated with outsourcing certain services and functions to determine the inherent risk of working with the third party. A risk analysis is performed before outsourcing significant services, to include those services that directly interact with Credit Union members.

C. The Credit Union will research and/or interview several prospective organizations to determine which is best qualified to meet the Credit Union's needs. If the relationship will require a significant investment of resources and capital, the Credit Union will consider hiring a consultant or industry expert to assist in its evaluation, upon approval of the President/CEO. It is also important to understand how the third party has performed in other relationships.

D. The Credit Union assigns criticality levels to vendors based upon the risk the relationship presents to the Credit Union. A vendor inherent risk may be defined and differentiated by cost/fees; scope and complexity of services; access to or custody of sensitive member information; availability of alternative vendors; and other factors, which may require significant efforts to mitigate risk.

E. The third-party risk assessment may include the use of internal auditors, compliance officers, technology officers, and legal counsel. A senior manager may be assigned responsibility for management and/or oversight of certain Tier 1 relationships. If this occurs, the management official will have the requisite knowledge and skills to manage all aspects of the relationship.

F. The Credit Union has defined its inherent risk tiers for third-party vendor relationships as described below. Vendors in a higher inherent risk tier require a higher level of initial review and ongoing monitoring and will be managed accordingly. The risk areas to be reviewed are Strategic Risk, Reputation Risk, Operational Risk, Transaction Risk, Credit Risk, Compliance Risk, and Other Risk. The Credit Union will then conduct an appropriate residual risk analysis based on the vendors' identified inherent risk

III. ROLES AND RESPONSIBILITIES

A. The responsibility for properly overseeing outsourced relationships lies with the *Credit Union's Board of Directors and senior management*. The Board and Management may delegate responsibility to various staff members to ensure compliance with this policy. The Vendor Management Specialist ensures that the criticality of each vendor relationship is defined; appropriate due diligence is obtained based upon that defined criticality; contracts between the Credit Union and vendors are appropriately reviewed; risks associated with the use of each

third-party provider is assessed and monitored; and records associated with each vendor relationship are maintained. The VP of Compliance and Risk Management reviews and updates the Policy annually.

B. The VP of Compliance and Risk Management is responsible for presenting the Policy annually to the Board for their review and approval, and for ensuring that an annual status report on the performance of critical vendors is presented to the Board for their review. Management will review the Credit Union's ability to provide adequate oversight and management of its vendor relationships on an ongoing basis and will perform a formal evaluation of the effectiveness of the Vendor Management Policy annually.

C. It is the primary responsibility of the relationship manager acquiring the services of a third-party vendor to evaluate the related risk; however, management maintains responsibility to ensure the evaluation has been completed.

D. The Board is responsible for annual review and approval of the Policy, and for review and response to other reports related to risk oversight and management of third-party vendor relationships.

IV. VENDOR INHERENT RISK LEVEL ASSIGNMENTS

A. Before entering into a contract with a vendor, the Credit Union will assess the associated services and products provided to assign the appropriate vendor inherent risk level, or tier, based on the services the vendor provides to the Credit Union.

The following definitions are utilized to assess and assign the criticality level of vendors:

- **TIER 1** ***(Critical/Significant)*****:** These vendors provide services considered critical to the Credit Union's daily operations. The vendors may be involved with the frequent transmission and storage of the non-public personal information of Credit Union's members, may pose significant earning, capital, or reputation risks to the Credit Union, and/or significant disruption in services could result from the vendor's failure to adequately provide services and manage risks. Examples include core or item processing, lending, credit card transactions/processing, etc.

- **TIER 2** ***(GLBA)*****:** These vendors have access to the non-public personal information of the Credit Union's members; however, the data is stored on Credit Union's servers, provided in a limited capacity, and/or encrypted if stored with the vendor. The vendor's activities may affect Credit Union's revenues, expenses, or operations; however, the services can be replaced by another vendor without significant disruption to the Credit Union's members. These vendors expose the Credit Union to higher levels of risk due to their access to non-public personal information and the Credit Union will regularly verify

the vendor's ability to mitigate those risks. Examples include check printing, payment processing, credit bureaus, etc.

- **TIER 3** ***(Infrastructure)*****:** These vendors supply a service that the Credit Union relies on for business activities and represent a single point of failure. These vendors may be considered more important from a business continuity perspective; however, they do not store or access any non-public personal information. The Credit Union will regularly verify all risks associated with these vendors have been mitigated with appropriate controls. Examples include utilities, communication, firewall, etc.

- **TIER 4** ***(Indirect Lending)*****:** Auto dealers with whom the Credit Union has an indirect lending relationship. These vendors may receive non-public information from the member, but not directly from the Credit Union. These vendors may expose the moderate to high risk. The Credit Union has some degree of control over the risk.

- **TIER 5** ***(Financial Institutions)*****:** Credit Unions and banks with whom the Credit Union has a third-party relationship. These vendors are regulated under FRB Regulation F. These vendors are closely regulated by their regulator, mitigating most of the risks associated with doing business with these vendors, although moderate levels of risk remain. These vendors may have periodic or incidental access, or be involved with the storage of encrypted personal, non-public information of Credit Union members.

- **TIER 6 (*Professional*):** Vendors that provide professional services licensed by the state or federal government. These vendors are governed by strict privacy and other legal regulations. These vendors may have incidental or low frequency access to member information during the delivery of professional services. These vendors provide services that may expose the Credit Union to moderate levels of risks, and may include law firms, certified accounting firms, and professional auditors.

- **TIER 7 (*Government*):** Vendors that are government agencies and provide particularized services to the financial institution. Services provided are highly regulated. The Credit Union understands the risks involved in working with a government institution and monitors the vendor for any material changes that might affect the Credit Union. Examples include county clerks, federal regulators, etc.

- **TIER 8** ***(Moderate)*****:** These vendors perform a useful function that may be heavily relied on by the Credit Union, however the vendor could be replaced without significant disruption to the Credit Union's operations and/or without the Credit Union's members feeling the effects of the replacement. These vendors expose the Credit Union to moderate levels of risk; however, the Credit Union can often mitigate these risks through its control or influence over how the services are provided. If these vendors are exposed to non-public personal information, their access is highly limited and controlled. This may also include vendors that must come in or on the Credit Union's premises. Examples include software vendors, landscapers, rate analysis, etc.

- **TIER 9** ***(Low/Immaterial)*****:** All other vendor relationships not included in the above Tier assignments. These vendors meet the legal definition of a vendor, however there is no risk associated with the services provided. The loss of these vendors would not cause a disruption in services and they could be replaced very easily. These vendors have no

real or potential access to non-public personal information. Examples include memberships, subscriptions, consumables, etc.

V. VENDOR RISK CATEGORIES

A. There are numerous risks that may arise from the Credit Union's use of vendors. Some of the risks are associated with the underlying activity itself and would still exist if the Credit Union conducted the activity internally. Other risks arise from, or are heightened by, the involvement of a vendor. The time and resources devoted to managing outsourcing relationships are based on the risk the relationship presents to the institution.

B. The risk categories assessed for each vendor are determined by the vendor's defined inherent risk tier, as designated in the applicable sections below. Not all the following risks are applicable to every vendor relationship. The risk levels that are assessed are defined per the criticality level assigned for the vendor. All of the below risks are assessed for Tier I (Critical) vendors.

1. *Strategic Risk*

Strategic risk is the risk to earnings or capital arising from adverse business decisions or improper implementation of those decisions. Credit Unions are individually exposed to strategic risk if utilizing third parties to conduct Credit Union functions, offer products and services that are not compatible with the Credit Union's strategic goals or that do not provide an adequate return on investment. Strategic risk may exist if appropriate initial and ongoing risk assessments of third-party relationships are not performed or the appropriate risk management infrastructure to oversee the vendor's activities are not in place. Strategic risk also arises if management does not possess adequate expertise and experience to properly oversee the activities of the third party. The Board and management should fully understand the risks associated with the use of third- party relationships.

2. *Reputation Risk*

Reputation risk is the risk to earnings or capital arising from negative public opinion as a result of actions involving or against the vendor. Third party relationships that do not meet the expectations of the Credit Union's members expose the Credit Union to reputation risk. Poor service, disruption of service, inappropriate sales recommendations, and violations of consumer law can result in litigation, loss of business to the Credit Union, or both. This risk may arise when the third party interacts directly with Credit Union members (in joint marketing arrangements or from call centers, for example), such arrangements pose reputation risk if the interaction is not consistent with the Credit Union's policies and standards. Publicity about adverse events surrounding third parties may increase the Credit Union's reputation risk. Credit Unions utilizing third party relationships to offer new products or services or expand existing ones should closely monitor the quality and appropriateness of the provider's products and services to ensure ongoing member satisfaction.

3. *Operational Risk*

Operational risk is the risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events. Third party relationships often integrate the internal processes of other organizations with the Credit Union's processes and can increase the overall operational complexity.

4. *Transaction Risk*

Transaction risk is the risk to earnings or capital arising from problems with service or product delivery. Transaction risk is evident in each product or service offered by the third party. Transaction risk can increase when the products, services, delivery channels, and processes that are designed or offered by a third party do not fit with the Credit Union's systems, member demands, or strategic objectives. A third party's inability to deliver products and services, whether arising from fraud, error, inadequate capacity, or technology failure, exposes the Credit Union to transaction risk. Lack of effective business resumption and contingency planning for such situations may increase the Credit Union's transaction risk.

5. *Credit Risk*

Credit risk is the risk to earnings or capital arising from an obligor's failure to meet the terms of any contract with the Credit Union or otherwise to perform as agreed. Credit risk may arise under many third- party scenarios. Third parties that market or originate certain types of loans subject the Credit Union to increased credit risk if Credit Union management does not exercise effective due diligence over, and monitoring of, the third party. Third party arrangements can have substantial effects on the quality of receivables and other credit performance indicators when the third party conducts account management, member service, or collection activities. Improper oversight of third parties that solicit and refer members (e.g., brokers, dealers, merchant processing ISOs, and credit card marketers), conduct underwriting analysis (credit card processing and loan processing arrangements), or set up product programs (overdraft protection, payday lending, and title lending) can also result in substantial credit risk. The credit risk for some of these third- party programs may be shifted back to the Credit Union if the third party does not fulfill its responsibilities or have the financial capacity to fulfill its

obligations. In those situations, it will be important for Credit Union management to assess the financial strength of the third party at the outset of the relationship and periodically thereafter. If issues are identified in the review, then Credit Union management should have a contingency plan in the event the third party is unable to perform.

6. *Compliance Risk*

Compliance risk is the risk to earnings or capital arising from violations of laws, rules, or regulations, or from nonconformance with internal policies and procedures or ethical standards. This risk exists when products, services, or systems associated with the third-party relationship are not properly reviewed for compliance, or when the third party's operations are not consistent with law, ethical standards, or the Credit Union's policies and procedures. The potential for serious or frequent violations or noncompliance exists when a Credit Union's oversight program does not include appropriate audit and control features, particularly when the third party is implementing new activities or expanding existing ones. Compliance risk increases when privacy of consumer and member records is not adequately protected, when conflicts of interest between a Credit Union and affiliated third parties are not appropriately managed, and when a Credit Union or its service providers have not implemented an appropriate information security program. Credit Unions should involve their compliance management function in the due diligence and monitoring process when third party products or services present significant risk to regulatory compliance.

7. *Other Risk Considerations*

Depending on the circumstances, third party relationships may also subject a Credit Union to liquidity, interest rate, price, foreign currency translation risk. In addition, a Credit Union may be exposed to country risk when dealing with a foreign-based service provider. Country risk is the risk that economic, social, and political conditions and events in a foreign country will adversely affect the Credit Union's financial interests.

Cybersecurity risks should be considered and assessed for all third-party relationships with access to confidential Credit Union or member data. Cybersecurity risks will receive increased scrutiny and monitoring if Cloud Services are utilized by a third-party vendor during the delivery of services. Cloud computing offers advantages such as lowered costs and increased performance, however, if not properly managed, it may expose the Credit Union and/or its members to online threats in the form of data loss/compromise and unauthorized access to corporate networks.

Increased scrutiny and oversight will be implemented for any third-party relationships that perform significant aspects of lending processes.

VI. CLASSIFYING CLOUD VENDORS AND DUE DILIGENCE WITH CLOUD VENDORS

Cloud vendors are vendors that provide services that can only be accessed through the internet. These vendors will be considered cloud-based vendors. Additional considerations should be utilized in classifying cloud vendors. The first step is to determine whether the vendor will have access to GLBA non-public personal information (NPPI) through the cloud service. If the answer is yes, the vendor will be either a Tier 1 (Critical) or Tier 2 (GLBA).

VII. CONTRACTS

Prior to entering into a contract with a new vendor, the Credit Union will ensure that expectations and obligations are properly outlined in a written agreement that has been reviewed by appropriate management personnel and ensure that contracts are also reviewed by the Credit Union's legal counsel, VP of Risk Compliance and Risk and appropriate subject matter experts, when applicable, prior to execution. The Credit Union shall consider the following when negotiating contracts:

a. General:

i. Ensure the rights and responsibilities of both parties to the contract are clearly described.

ii. Ensure appropriate performance standards and service level agreements (SLAs) are in place, if applicable, and review penalty provisions.

iii. Ensure fees and other charges are clearly disclosed (review price increase provisions).

iv. Ensure that the contract includes a requirement that the minimum required insurance coverage is maintained by the vendor, if applicable, and that the vendor provides evidence of coverage.

v. Review indemnification provisions of the Credit Union and the Vendor. Consider clauses that indemnify the Credit Union from the Vendor's failure to perform and obtain any necessary intellectual property licenses. Carefully assess clauses that require the Credit Union to hold the Vendor harmless.

vi. Review limitation of liability provisions to determine whether the proposed limit is acceptable. Consider whether the contract would subject the Credit Union to undue risk of litigation and whether the contract should establish a dispute resolution process.

vii. Review each party's right to modify, re-negotiate, and/or change the contract.

viii. Review the Vendor's representations and warranties and ensure that the contract includes a representation that the Vendor is, and will remain, in compliance with all laws and regulatory requirements applicable to the services provided.

ix. The President/CEO, COO, CTO, SVPs, and VP of Compliance and Risk Management are the only individuals authorized to

execute a contract on behalf of the Credit Union.

x. The President/CEO, Chief Operations Officer, and members of the management team are the only authorized individuals that may execute a Non-Disclosure Agreement (NDA) also known as a Confidentiality Agreement on behalf of the Credit Union.

b. Term and Termination:

i. Ensure that the term, including the commencement date of the term and the expiration of the term is clearly defined.

ii. Review right to terminate without cause, right to terminate for cause, and costs for early termination. Contracts should define events that constitute contractual default (e.g., inability to meet SLAs, business continuity plan (BCP) provisions, recovery point objectives and/or recovery time objectives) and provide a list of acceptable remedies and opportunities for curing a default.

iii. Ensure that the contract permits the Credit Union to terminate the relationship without prohibitive expense and that termination and notification provisions allow for the orderly conversion to another third party, if applicable.

c. Confidentiality and Security:

i. Ensure appropriate confidentiality and security provisions are included to protect the Credit Union's data and member information, including a requirement to address security issues associated with the Vendor's services and notify the Credit Union of security breaches and any other breaches of the Vendor's confidentiality obligations and information security procedures.

ii. Ensure data ownership and handling expectations (availability, transport methods, backup requirements, etc.) during the relationship and following termination are clearly defined, including the timely return or destruction of the Credit Union's data and other resources.

iii. If Cloud Services are utilized for the storage or transmission of member non-public, personal information, that should be disclosed to the Credit Union.

d. Business Resiliency and Audits

i. Ensure that the contract provides for continuation of operations in the event of business interruption and includes specific time frames for resumption and recovery that meet the Credit Union's requirements. The contract should include provisions addressing incident management, BCP testing frequency, availability of test results and the Credit Union's ability to jointly practice business resumption and disaster recovery plans and participate in the Vendor's BCP testing on a periodic basis, if applicable.

ii. Ensure that the contract includes a requirement for the Vendor to permit annual

independent audits, regulatory examinations, and provide all requested compliance reports and information at the Credit Union's request and at no cost, including the Vendor's response to relevant regulations, supervisory guidance, or other notices published by federal and/or state Credit Union agencies and available audit reports addressing the Vendor's resiliency capabilities and interdependencies (e.g., subcontractors), BCP testing, and remediation efforts.

e. Assignment and Subcontractors:

i. Review assignment provisions and ensure the Vendor cannot assign the contract to a third party without the Credit Union's prior written consent.

ii. Ensure that the Vendor is required to obtain approval of subcontractors used by the Vendor to provide key services and to obtain the Credit Union's prior approval of any changes to these subcontractors. If applicable, ensure that the contract also addresses the Credit Union's right to audit subcontractors and BCP requirements for subcontractors.

iii. Ensure that the contract prohibits the Vendor from using foreign-based subcontractors without the Credit Union's consent.

iv. Ensure that contracts with foreign-based vendors or vendors that back up and/or store data offshore clearly address the need for data security and confidentiality and require the Vendor to adhere to U.S. regulatory standards.

f. Performance and Consumer Complaints:

i. All vendor contracts shall specify whether the Credit Union or the third-party vendor has the duty to respond to any complaints received by the vendor from the Credit Union's members. If the vendor is responsible for such responses, a copy of any complaint and the response should be forwarded to the Credit Union. The contract should also provide for periodic summary reports detailing the status and resolution of complaints.

ii. Ensure the vendor has a process in place to track member satisfaction, performance metrics, and reporting.

g. Regulation and Compliance:

i. Ensure the contract addresses compliance with the specific laws, regulations, guidance, and self-regulatory standards applicable to the activities involved, including provisions that outline compliance with certain provisions of the GLBA, BSA/AML, OFAC, Fair Lending, and other consumer protection laws and regulations.

ii. Ensure the contract requires the vendor to maintain policies and procedures which address the Credit Union's right to conduct periodic reviews to verify the

vendor's compliance with the Credit Union's policies and expectations.

iii. Ensure the contract states the Credit Union has the right to monitor the third-party's compliance with applicable laws, regulations, and policies on an ongoing basis and requires remediation if issues arise.

h. Document Destruction*:*

i. Ensure the vendor is required to destroy, or otherwise delete, any confidential data belonging to the Credit Union and/or its member's information or documentation as soon as practical once the contract between the Credit Union and vendor has terminated.

ii. Require proof from the vendor that the information or documentation has been destroyed or deleted, including the method and date.

i. Report Frequency and Type*:*

i. Ensure the vendor provides performance reports, control audits, financial statements, and security and business resumption testing reports as needed, including the guidelines and fees for obtaining such reports.

VIII. DUE DILIGENCE IN SELECTING A THIRD PARTY

A. In addition to reviewing the contract, appropriate due diligence documentation should also be gathered and reviewed when selecting third-party vendors. . The documentation for each vendor will be gathered and systematically reviewed based on the inherent risk assigned to the vendor as determined by the relationship manager. The senior management team will ensure that the contract between the vendor and Credit Union has been appropriately reviewed and that all relevant documents are gathered and reviewed prior to establishing a new vendor relationship.

B. For **new** vendors that are Tier 1 (Critical) and Tier 2 (GLBA), the Credit Union will perform the following initial due diligence procedures:

1. Business Model Review: Before entering into a third-party relationship, the Credit Union will investigate and understand the third party's business model – the conceptual architecture or business logic employed to provide services to its clients. Management will understand and be able to explain the third party's role in the proposed arrangement and any processes for which the third party is responsible

2. Cost/Benefit Analysis: Ensure that the services meet the Credit Union's business strategy, risk tolerance, and values. Perform a cost vs. benefit analysis and determine the impact or risk to the Credit Union (e.g., technology, space, staffing, communication, etc.).

3. Reputation: Evaluate the vendor's experience providing services and assess its reputation. Contact other financial institutions for references and conduct reference checks with external organizations such as the Better Business Bureau, Federal Trade Commission, and/or other applicable industry associations. Review member complaints and the resolution of the complaints. Review the vendor's website and marketing materials and determine how the vendor plans to use the Credit Union's name and reputation in marketing efforts.

4. Financial Review: Obtain and review financial statements and inquire in reference checks about the financial stresses that may have been detected.

5. Insurance Coverage Review: Review the vendor's insurance coverage, including fidelity bond, errors and omission coverage, property and casualty coverage, fraud, cyber, etc.

6. Operational Review: Review the vendor's most recent SSAE 16 report and/or other third- party evaluations to determine the effectiveness of the vendor's internal controls. Verification of appropriate staffing with required experience to withstand key personnel departures.

7. Business Resumption & Contingency Plan: Review business continuity/disaster recovery plan, cyber resiliency, incident management procedures and disaster recovery test results.

8. Privacy Issues: Evaluate the controls in place to protect member data. Determine if the vendor will be sharing it with any other parties and how/where, the data will be transmitted and stored. Evaluate the vendor's compliance with privacy regulations and confirm the vendor has appropriate security measures to safeguard non-public personal information of members.

9. Legal Review: Ensure that legal counsel reviews the contract for Tier 1. Ensure that legal counsel or audit services reviews the contract for Tier 2.

10. Onsite Visit: If Necessary, the credit union will conduct an onsite visit of the vendor.

C. For **new** vendors that are Tier 3 (Infrastructure), the Credit Union will perform the following initial due diligence procedures:

1. Cost/Benefit Analysis: Ensure the services meet the Credit Union's business strategy, risk tolerance, and values. Perform a cost-benefit analysis to determine the impact or risk to the Credit Union and whether the benefit of outsourcing the service to the vendor is worth those risks.

2. Company Information: Examine the qualifications, backgrounds, and reputations of company principals, including criminal background checks where appropriate. Evaluate prior relationships between the Credit Union and vendor, if applicable.

3. Reputation: Evaluate the vendor's experience providing services and assess its reputation. Contact other financial institutions for references and conduct reference checks with external organizations such as the Better Business Bureau, Federal Trade Commission, and/or other applicable industry associations. Review complaints and complaint resolutions. Review the vendor's website and marketing materials to determine how the vendor plans to use the Credit Union's name and reputation in marketing efforts.

4. Financial Review: Obtain and review financial statements or other relevant information and inquire during reference checks about the financial stresses that may have been detected. Determine the significance of the proposed contract on the vendor's financial condition.

5. Insurance Coverage Review: Review the vendor's insurance coverage, including fidelity bond, errors, and omission overage, property and casualty coverage, fraud, etc.

6. Business Resumption & Contingency Plan: Review business continuity/disaster recovery plan, cyber resiliency, incident management procedures, and disaster recovery test results,

7. Legal Review: Ensure the Credit Union's Management and/or legal counsel reviews the contract.

D. For **new** vendors that are Tier 4 (indirect lending), the Credit Union will perform the following initial due diligence procedures:

1. Reputation: Evaluate the vendor's experience providing services and conduct reference checks with other Credit Unions and external organizations, such as the Better Business Bureau.

E. For **new** vendors that are Tier 5 (Financial Institutions), the Credit Union will perform the following initial due diligence procedures:

1. Business Resumption & Contingency Plan: Review business continuity/disaster recovery plan, cyber resiliency, incident management procedures and disaster recovery test results.

2. Privacy Issues: Evaluate the controls in place to protect member data. Determine if the vendor will be sharing it with any other parties and how/where, the data will be transmitted and stored. Evaluate the vendor's compliance with privacy regulations and

confirm the vendor has appropriate security measures to safeguard non-public personal information of members.

F. For **new** vendors that are Tier 6 (Professional), the Credit Union will perform the following initial due diligence procedures:

1. Reputation: Evaluate the vendor's experience providing services and confirm vendor's licensure and authority to perform professional services in the appropriate jurisdictions. Conduct reference checks with applicable external organizations such as the Better Business Bureau, state bar associations, public company accounting oversight board, etc.

2. Financial Review: Obtain and review financial statements, if available.

3. Insurance Coverage Review: Review the vendor's insurance coverage.

4. Contract Review: Ensure that appropriate management personnel, VP of Compliance and Risk Management and, if applicable, legal counsel, reviews the contract.

G. For **new** vendors that are Tier 7 (Government), the Credit Union will document the risks involved in working with the vendor and ensure that appropriate management personnel review the contract, if applicable.

H. For **new** vendors that are Tier 8 (Moderate), the Credit Union will perform the following initial due diligence procedures:

1. Reputation: Evaluate the vendor's experience providing services and assess its reputation. Contact other financial institutions for references and conduct reference checks with external organizations such as the Better Business Bureau, and/or other applicable industry associations.

2. Financial Review: Obtain and review financial statements, if available and appropriate.

3. Insurance Coverage Review: Review the vendor's insurance coverage including property and casualty coverage, where applicable.

4. Contract Review: Ensure that appropriate management personnel, audit services and, if applicable, legal counsel, reviews the contract.

I. For **new** vendors that are Tier 9 (Low/Immaterial), the Credit Union will review the vendor's insurance coverage and ensure that appropriate management personnel and the VP of Compliance and Risk Management reviews the contract, if applicable.

VIII. RISK ASSESSMENT REVIEWS

A. The relationship manager ensures that vendor due diligence documentation is updated annually and is responsible for conducting a systematic residual risk assessment on an ongoing basis based on the vendor's assigned risk tier. The Vendor Management Specialist is responsible for ensuring that all Credit Union vendors are assessed annually, or per the time-period required by the assigned risk tier.

- **TIER 1** ***(Critical/Significant)*****:** The Credit Union will review the following on an annual basis: A review of the contractual terms of the agreement. If contract is up for renewal, then ensure VP of Compliance and Risk reviews before renewal occurs.
  a. Financial Review
  b. Reputation Review
  c. Operational Effectiveness of Internal Controls as documented through a third- party audit (SOC) report, and the Credit Union's response to any User Control Considerations that are included with the audit
  d. Business Continuity, Disaster Recovery, and associated testing results
  e. Incident Management and Response Plans
  f. Information Security, Privacy, and Cyber Security Plans
  g. Evidence of Insurance Coverage
  h. Compliance with privacy and other applicable regulatory requirements.
  i. Documentation of actions or incidents involving the vendor that could adversely impact the Credit Union, its members, or the vendor's continued ability to meet service level expectations. (Monitoring Reports)
  j. Onsite visit, if necessary.
  k. Other information deemed appropriate based on the services provided by the vendor and the associated level of risk.
- **TIER 2** ***(GLBA)*****:** The following documentation is utilized for Tier 2 vendor reviews on an annual basis:
  a. A review of the contractual terms of the agreement. If contract is up for renewal, then ensure VP of Compliance and Risk reviews before renewal occurs.
  b. Financial Analysis
  c. Operational Effectiveness of Internal Controls as documented through a third-party audit (SSAE/SOC) report, and the Credit Union's response to any User Entity Control Considerations that are included with the audit
  d. Business Continuity, Disaster Recovery, and associated testing results
  e. Evidence of Insurance Coverage
  f. Documentation of actions or incidents involving the vendor that could adversely impact the Credit Union, its members, or the vendor's continued ability to meet service level expectations. (Monitoring Reports)
  g. Other information deemed appropriate based on the services provided by the vendor.
- **TIER 3** ***(Infrastructure)*****:** The following documentation is utilized for Tier 3 vendor reviews every two years:
  a. A review of the contractual terms of the agreement. If contract is up for renewal, then ensure VP of Compliance and Risk Management reviews before renewal occurs.
  b. Financial Review
  c. Business Continuity, Disaster Recovery, and associated testing results.
  d. Evidence of Insurance Coverage

e. Documentation of actions or incidents involving the vendor that could adversely impact the Credit Union, its members, or the vendor's continued ability to meet service level expectations. (Monitoring Reports)
f. Other information deemed appropriate based on the services provided by the vendor.

- **TIER 4** ***(Indirect Lending)*****:** The following documentation is utilized for Indirect Lending vendor reviews on an annual basis:
  a. A review of the contractual terms of the agreement
  b. Documentation of actions or incidents involving the vendor that could adversely impact the Credit Union, its members, or the vendor's continued ability to meet service level expectations. (Monitoring Reports)
  c. Other information deemed appropriate based on the services provided by the vendor.
- **TIER 5** ***(Financial Institutions)*****:** These vendors are subject to oversight under FRB Regulation F and are closely regulated by their regulator.
- **TIER 6 (Professional):** The Credit Union will review the following every two years:
  a. Review the terms of the Contract
  b. Evidence of Insurance Coverage (on an annual basis),if available
  c. Evidence of applicable professional licensure, where appropriate
  d. Other information deemed appropriate based on the services provided by the vendor
- **Tier 7 (Government):** The Credit Union will document any risks or issues associated with its relationship with the vendor, as applicable.
- **TIER 8** ***(Low)*****:** The following documentation is utilized for Tier 8 vendor reviews:
  a. Evidence of Insurance Coverage (On an annual basis)
  b. Other information deemed appropriate based on the services provided by the vendor.
- **TIER 9** ***(Immaterial)*****:** No action is required regarding Tier 9 vendors.

B. The Credit Union utilizes Ncontracts® to store and track vendor due diligence documentation, to document ongoing monitoring, and for documenting the annual risk assessment process. In doing so, Credit Union personnel create a standardized composite risk assessment for each vendor.

IX. ASSESSMENT RESULTS AND TERMINATION

A. The Credit Union will ensure the Board receives a report of its vendor management program annually, or on request, and will update the Board periodically of any significant changes to a vendor's residual risk or any performance issues impacting the Credit Union's strategic objectives. The report will also make the Board aware of vendors that should be monitored more closely, possibly replaced, or for which additional measures must be taken to mitigate the identified risk, including renegotiation of contracts prior to renewal if applicable.

B. The Credit Union's applicable personnel are responsible for ensuring appropriate actions are taken to address significant deterioration in vendor performance and for ensuring appropriate response to material issues identified through ongoing monitoring. The Credit Union may

terminate third-party relationships for various reasons, including expiration or satisfaction of the contract, a desire to seek an alternate vendor that better aligns with the Credit Union's strategic goals, objectives, and risk appetite, a desire to bring the activity in-house, discontinuation of the activity, or breach of contract.

C. The Board is responsible for ensuring appropriate actions are taken to address significant deterioration in vendor performance and for ensuring appropriate response to material issues identified through ongoing monitoring. The Credit Union's applicable personnel will work with Management as needed to ensure vendor relationships terminate efficiently, whether the activities are transitioned to another vendor, brought in-house, or discontinued. In the event of contract default or termination, the Credit Union should have a contingency plan that addresses transitioning or discontinuing the activity when the contract expires.

X. REVIEWS

The Credit Union's Management will ensure that periodic independent reviews are conducted on the Vendor Management process, particularly when the Credit Union involves vendors in critical activities. The Credit Union's internal auditor or an independent third party may perform the reviews and Management will ensure the results are reported to the Board.

Approved at the March 22, 2022, meeting by the Board of Directors of Radiant Credit Union.

_____
Secretary

_____
Date