Third-Party Vendor
MANAGEMENT GUIDE

By the CUNA Due Diligence Task Force



CUNA
Credit Union
National Association

CUNA DUE DILIGENCE TASK FORCE

Third-Party Vendor Management Guide

Version: 1.14
Last Updated: December 5, 2008

CUNA Due Diligence Task Force:

Henry Wirz (Chairman)	SAFE CU (California)
Bill Raker (Vice Chairman)	U.S. Federal Credit Union (Minnesota)
Mary Ann Clancy	Massachusetts Credit Union League, New Hampshire Credit Union League, & Credit Union Association of Rhode Island
Tom Dare	CUNA Mutual Group (Wisconsin)
Tom Davis	NACUSO (California)
Charles Emmer	ENT Federal Credit Union (Colorado)
Sylvia Fath	California-Nevada Credit Union League
Dave Fearing	Ohio Credit Union League
Tom Gaines	Tennessee Credit Union League
Joseph Ghammashi	Corporate One FCU (Ohio)
Debie Keesee	Spokane Media FCU (Washington)
RoxAnne Kruger	Washington Credit Union League
Erin Mendez	Orange County Teachers FCU (California)
Dave Osborn	Anheuser-Busch Employees CU (Missouri)
Earle Pierce	Community First CU (Florida)
Lisa Pleasure	Community America CU (Kansas)
John Sackett	Royal CU (Wisconsin)
Christina Vaughan	Municipal Employees CU (Maryland)
Kari Wilfong	CO-OP Financial Services (California)

CUNA Staff:

Michael Edwards; Linda Lilledahl; Marcia Barron; Julie Esser, Nichole Seabron

Table of Contents

Executive Summary

CUNA Chairman Tom Dorety formed the CUNA Due Diligence Task Force in order to respond to concerns from credit unions and regulators over how to best meet credit unions' due diligence responsibilities involving third-party vendors without unnecessary duplication of effort. To fulfill this purpose, the Task Force has developed this *Third-Party Vendor Management Guide*. The purpose of this Guide is to provide credit union managers with a comprehensive review of regulatory guidance and best practices, including procedures for reviewing, selecting, and administering the relationships.

While there are due diligence procedures that credit union management should use with respect to all third-party relationships—ones that the National Credit Union Administration (NCUA), state regulators, and/or individual examiners may insist upon in all cases—what practices your credit union should follow generally depends upon the facts underlying each individual third-party vendor relationship and the risks and benefits that the relationship brings to your credit union. Some third-party vendor relationships are more critical to your credit union's operations than others. The more critical the relationship is to your credit union, the greater your risk assessment and planning, due diligence, and relationship monitoring and control responsibilities become.

The NCUA has identified three areas essential to quality third-party vendor management. They are: (1) Risk Assessment and Planning; (2) Due Diligence (including Contracts); and (3) Risk Measurement, Monitoring, and Control. Due to the importance of Contracts, this Guide has dedicated a separate section addressing this topic rather than including it in the overall Due Diligence area.

I. Risk Assessment and Planning

Risk assessment and planning ensures that the business service or product identified complements the credit union's overall mission and goals. It also gathers enough information to ensure that the business service or product is best provided by a third-party vendor instead of by the credit union itself.

Section I of this Guide provides credit unions with specific advice on how to conduct risk assessment and planning with respect to: (A) the adoption of third-party vendor management policies (with specific examples and alternatives provided for possible adoption by individual credit unions); (B) board of directors' vendor management responsibilities; (C) senior management's vendor management responsibilities; (D) what actions the credit union should take during its initial vendor management risk assessment and planning phase; (F) strategic planning in detail; (G) vendor management vis-à-vis CUSOs, Corporate CUs, and other credit union-affiliated organizations; (H) indirect lending relationships; and (I) sections of the NCUA AIRES questionnaire related to risk assessment and planning.

II. Due Diligence

Third-party vendor due diligence is a process used to make an informed business decision concerning the selection of the appropriate vendor. Due diligence is the gathering and analysis of detailed information about possible vendors. As with all

business decisions, there are some risks that cannot be eliminated but can be managed. The purpose of due diligence is to help choose the best third-party vendor relationship given the risks and abilities or services available, and then to negotiate, contract, implement, and monitor to mitigate any residual risks.

Section II of this Guide provides detailed advice and examples of how to conduct credit union due diligence with respect to: (A) the basics of credit union due diligence; (B) requests for information (RFI) and requests for proposals (RFP) that are addressed to potential third-party vendors; (C) how to evaluate information received from third-party vendors; (D) potential due diligence "red flags;" and (E) sections of the NCUA AIRES questionnaire related to due diligence

III. Contracts

This Guide has a separate section devoted to contracts because of the importance of contracts to credit unions' third-party vendor relationships. Contracts govern most aspects of credit unions' relationships with third-party vendors and therefore present myriad due diligence and other third-party vendor management issues.

Section III of this Guide addresses: (A) the credit union's review of existing contracts; (B) how to draft a contract with a third-party vendor; (C) what terms should be included in the contract and what those terms mean; and (D) sections of the NCUA AIRES questionnaire related to contracts.

IV. Risk Measurement, Monitoring, and Control

Risk measurement, monitoring, and control are necessary because due diligence is not a process that starts and ends at the time you have chosen your third-party provider. The relationship must be actively managed throughout the life of a credit union's relationship with a vendor to be successful. This requires continuing communication, monitoring, and control of the product or service provided and measuring the success of the relationship.

Section IV of this Guide addresses: (A) third-party vendor risk-management, monitoring, and control in general; (B) risk-management considerations that are especially relevant to vendor relationships involving) indirect lending; and (C) sections of the NCUA AIRES questionnaire related to third-party vendor risk-management, monitoring, and control.

Preface

This Guide is designed as a resource to provide information to assist you in identifying, establishing, and monitoring third-party vendor relationships that will be beneficial to your credit union and its members. The information contained in this Guide is based on the CUNA Due Diligence Task Force's review of regulatory guidance issued by NCUA, state and other federal depository institution regulators, as well as due diligence procedures now in use by CUNA Strategic Services and credit unions nationwide.

As you use this Guide, keep in mind that the degree of strategic planning, due diligence, and monitoring required for a given third-party vendor relationship is fact specific. This Guide is not intended to be list of mandatory procedures to be applied to every third-party vendor relationship regardless of whether doing so would be informative, relevant, or cost-effective with respect to protecting the interests of your credit union and its members.

The more critical and more risky the relationship is to the credit union, the greater the credit union's risk assessment and planning, due diligence, and relationship monitoring and control responsibilities become. Conversely, a credit union's responsibilities are less demanding when a third-party vendor relationship is less critical and less risky to the credit union.

Use the definitions of "**Critical Third-Party Vendor Relationships**" and "**Degrees of Criticality**" contained in the "**Key Concepts**" section immediately following this Preface as a means to determine the degree of risk assessment and planning, due diligence, and relationship monitoring and control appropriate for a given third-party vendor relationship. Based on this factual analysis, determine which practices and procedures recommended by this Guide should be applied to protect the credit union's interests vis-à-vis this specific relationship. Rarely, if ever, will the facts of a given third-party vendor relationship require you to use all or nearly all of the practices and procedures included in this Guide.

Trade associations and other credit union related organizations often have relationships with "preferred" or "endorsed" vendors. Due diligence by the trade associations or other credit union-related organizations on a third-party vendor does not relieve the credit union from responsibility for independent due diligence and decision making concerning those third-party vendors.

Some sections of this Guide contain redundant information (in the sense that the same or similar principles may be included in more than one section). The editors of this Guide have, in some sections, provided redundant information in order to reduce the chances that credit unions will accidentally overlook important regulatory guidance.

Key Concepts and Definitions

Key Concepts

1) Critical Third-Party Vendor Relationships: Certain third-party vendor relationships are considered "critical" to the continued operation of the credit union and therefore—depending upon the specific facts underlying the relationship and the risks involved, see **Degrees of Criticality**, below—require moderate to substantial risk assessment and planning, due diligence, and monitoring and control by the credit union. A credit union should give consideration to the following factors in performing its evaluation of the criticality of the relationship:[1]

- Whether the relationship involves implementing new credit union activities;
- Whether the relationship has a material effect on the credit union's revenues or expenses;
- Whether the third-party vendor poses risks to or could have a material effect upon the credit union's reputation;
- Whether the third party performs significant operational functions***;***
- Whether the third-party vendor stores, accesses, transmits, or performs transactions on sensitive member information;
- Whether the third-party vendor markets credit union products or services to members;
- Whether the third-party vendor provides a product or performs a service involving outsourced or indirect lending;
- Whether the third-party vendor provides a product or performs a service involving debit or credit card processing;
- Whether the third-party vendor poses risks that could significantly affect members' shares or loan balances;
- Whether the third-party vendor poses risks that could significantly affect the credit unions' earnings or capital; or
- Whether the third-party vendor relationship is otherwise "material" to the credit union's operations.

It is important to note that any one factor that is applicable to a third-party vendor relationship may not, in isolation, be determinative that the third-party vendor relationship is "critical" to the credit union.

The credit union should evaluate, in the aggregate, on a case-by-case basis, all factors deemed to be applicable to appropriately make an assessment as to whether the relationship is "critical," including the **Degrees of Criticality**, below, and the cost of the

[1] *See* NCUA, "Evaluating Third Party Relationships," Supervisory Letter No. 07-01, at 3-4 (2007) (enclosed with Letter to Credit Unions 07-CU-13); *see also* FDIC, "Guidance for Managing Third Party Risk," FIL-44-2008, at 2-4 (2008).

contract. Each relationship that is determined to be "critical" is deemed to be a Critical Third-Party Vendor Relationship.

For many credit unions, Critical Third-Party Vendor Relationships will be the exception—rather than the rule—but these institutions' "critical" relationships will nonetheless require a robust and thorough planning, due diligence, and relationship management process.

2) Degrees of Criticality: With third-party vendors, the degree of planning, due diligence, and monitoring required depends upon the degree of risk that the third-party vendor poses to the credit union.

The higher the risk to the credit union, the more likely it is that the third-party vendor relationship is "critical" and will require a thorough strategic planning, due diligence, and monitoring process. Renewing a longstanding third-party vendor relationship, however, typically requires less analysis than a new third-party vendor relationship.[2]

In the context of e-commerce strategic planning, due diligence, and risk management, NCUA has provided, as an example, three degrees of risk/criticality that should be applicable to many other types of third-party vendor relationships:

> "**Criticality of Data & Systems**
>
> Performing an effective risk assessment requires a comprehensive understanding of the value (e.g., degree of sensitivity or criticality) of the systems and information being assessed. This value can be expressed in many different ways; one possible example follows:
>
> · **High** – Extreme liabilities result if the information is compromised (e.g., damaged, destroyed, made public); could cause major financial loss; result in legal action against the credit union; or severely damage the credit union's reputation.
>
> · **Moderate** - Serious liabilities result if the information is compromised; could cause moderate financial loss; legal action against the credit union would be likely; or damage to the credit union's reputation would be moderate.
>
> · **Low** - Liabilities could possibly result if the information is compromised; would likely cause only minor financial loss; litigation unlikely; or damage to the credit union's reputation would be minimal."[3]

3) Non-Critical Third-Party Vendor Relationships: Third-party vendor relationships that do not rise to the level of being "critical"—after consideration of the factors noted above under both **Critical Third-Party Vendor Relationships** and **Degrees of Criticality**—are "non-critical" to the continued operation of the credit union and therefore generally require a lesser degree of risk assessment and planning, due diligence, and monitoring and control by the credit union than would a critical vendor.

---

[2] *See* NCUA, "Evaluating Third Party Relationships," Supervisory Letter No. 07-01, at 2 (2007) ("Less complex risk profiles and third party arrangements typically require less analysis and documentation. Further, where credit unions have a longstanding and tested history of participating in a given third party relationship, less analysis is required to renew the relationship.").

[3] NCUA, "e-Commerce Guide for Credit Unions," NCUA Publication No. 8072, at 9 (2002) (enclosed with Letter to Credit Unions No. 02-CU-17).

Each relationship deemed "non-critical" is also deemed to be a Non-Critical Third-Party Vendor Relationship.

For many credit unions, the majority of third-party vendor relationships will fall into the "non-critical" category. Be prepared to explain to your examiner why you believe that a given third-party vendor relationship is a Non-Critical Third-Party Vendor Relationship, citing factors such as the nature of the activity and the perceived degree of risk involved. For example, if you believe that a particular relationship is a Non-Critical Third-Party Relationship because it is low risk, be prepared to present a fact-based argument supporting this conclusion. Ideally, you should document such conclusions and supporting facts in writing at the time you decide how to categorize the vendor.[4]

NCUA Letter to Credit Unions 01-CU-20 ("Due Diligence Over Third Party Service Providers")[5] outlines "minimum procedures that a credit union should follow" with respect to third-party vendor relationships. Letter to Credit Unions 01-CU-20 is likely a good source to consult with respect to your credit union's minimum responsibilities vis-à-vis Non-Critical Third-Party Vendor Relationships, to the extent that the requirements contained therein are rationally applicable to a given relationship. For example, review of an office supply products vendor's financial statements or insurance coverage would generally not be necessary; further, the necessary "controls" for such a relationship would generally consist of: (1) making sure that the credit union receives the office supplies contracted for in a timely manner; and (2) ensuring that the credit union is not over-billed. A copy of this letter is attached in Appendix B to this Guide.

Definitions

CUSO: A Credit Union Service Organization (CUSO) is a limited partnership, corporation, or limited liability company that credit unions have invested in and/or lent to, and which operates primarily to serve the needs of credit unions and/or credit union members.[6]

Due Diligence: "Due diligence is the systematic, on-going process of analyzing and evaluating new strategies, programs, or operations to prepare for and mitigate unnecessary risks."[7] Also: "A prospective buyer's or broker's investigation and analysis of a target company, a piece of property, or a newly issued security."[8]

[4] *See* NCUA, "Evaluating Third Party Relationships," Supervisory Letter No. 07-01, at 4 (2007) (enclosed with Letter to Credit Unions No. 07-CU-13) ("Risk assessments for less complex third party arrangements may be part of a broader risk management program or documented in board minutes.").
[5] NCUA, "Due Diligence Over Third Party Service Providers," Letter to Credit Unions No. 01-CU-20, at *2 (2001), *available at* http://www.ncua.gov/letters/2001/01-CU-20.pdf (last visited Oct. 17, 2008).
[6] For the regulations applicable to CUSOs that federal credit unions have invested in and/or lent to, see 12 C.F.R. part 712. CUSOs that state-chartered credit unions have invested in and/or lent to are governed by applicable state law.
[7] NCUA, "Evaluating Third Party Relationships," Supervisory Letter No. 07-01, at 2 n.1 (2007).
[8] *Black's Law Dictionary* 468 (7th ed. 1999).

Existing Relationships: With regard to due diligence required by NCUA, "where credit unions have a longstanding and tested history of participating in a third-party relationship, less analysis is required to renew the relationship."[9]

Material: "Material" is a term of art in both law and accounting. Its definitions include:

> **Material (General Definition):** "Of such a nature that knowledge of the item would affect a person's decision-making process; critical; essential."[10]
>
> **Material (Accounting Definition):** "The omission or misstatement of an item in a financial report is material if, in the light of surrounding circumstances, the magnitude of the item is such that it is probable that the judgment of a reasonable person relying upon the report would have been changed or influenced by the inclusion or correction of the item."[11]

Payment Card Industry (PCI) Compliant: The PCI Security Standards Council has developed a set of comprehensive requirements for enhancing payment account data security called PCI Data Security Standards (PCI DSS), which the payment card brands (e.g., Visa, MasterCard, etc.) require compliance by parties using their cards to comply with.[12] Entities that process credit or debit card information, including merchants and third-party providers that store, process or transmit credit card/debit card data who pass a PCI DSS audit will have a Certificate of Compliance and are considered Payment Card Industry (PCI) Compliant.

Request for Information (RFI) or Request for Proposal (RFP): The credit union's request, made in writing, to the prospective third-party during due diligence of the vendor management process asking for specific information about the third-party and its business activities.

SAS70 or Statement of Auditing Standards No. 70: Under some circumstances, third-party vendors will initiate a SAS 70 examination to ensure the integrity of controls at the third-party vendor service provider (known as a service organization). A SAS 70 report is performed following standards established by the American Institute of CPAs, specifically *Statement on Auditing Standards Number 70, Service Organizations, As Amended*. There are two types of SAS 70 examinations: (1) A Type 1 report which is a report on the controls placed in operation and is as of a point in time, such as of June 30, 2008; and (2) the Type 2 report which is a report on controls placed in operation and tests of the operating effectiveness of those controls. A Type 2 report generally covers a period of time such as six months to a year. Type 1 reports are considered less

---

[9] NCUA, "Evaluating Third Party Relationships," Supervisory Letter No. 07-01, at 2 (2007).
[10] *Black's Law Dictionary* 991 (7th ed. 1999).
[11] American Institute of Certified Public Accountants, AU § 312, at ¶ 4; Financial Accounting Standards Board, *Statement of Financial Accounting Concepts No.2* ¶ 132 (FASB 2008) (1980), *available at* http://www.fasb.org/pdf/aop_CON2.pdf; *see also id.* at ¶¶ 123-132.
[12] *See* PCI Security Standards Council, "FAQ: What are the Deadlines for Complying with PCI DSS," *available at* https://www.pcisecuritystandards.org/index.shtml (follow link to "FAQ" and choose "What are the Deadlines for Complying with PCI DCC?") (last visited Sep. 3, 2008); PCI Security Standards Council, "About the PCI Data Security Standard (PCI DSS)," https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml (last visited Sep. 3, 2008).

effective because they do not provide assurance that the controls at the service organization are operating effectively. As such, a Type 2 is generally considered more effective. SAS 70 examinations are especially important if the third-party has access to sensitive member information; however, NCUA does not require companies to have completed a SAS 70 examination.[13]

Third-Party: All entities that the credit union has or is considering entering into a business relationship with, including other credit unions, corporate credit unions, CUSOs, and entities that are not part of the credit union system.

[13] *See* NCUA, "Evaluating Third Party Relationships," Supervisory Letter No. 07-01, at 3-4 (2007) ("If available, officials may use copies of SAS 70 (type II) reports prepared by an independent auditor, audit results, or regulatory reports to evaluate the adequacy of the proposed vendor's internal controls. If these items are not available, credit unions should consider whether to require an independent review of the proposed vendor's internal controls.").

FOUR STAGES OF EFFECTIVE THIRD-PARTY VENDOR RELATIONSHIP MANAGEMENT

I. Risk Assessment and Strategic Planning
II. Due Diligence
III. Contracts
IV. Risk Measurement, Monitoring and Control

Following is a detailed outline of considerations and procedures for third-party vendor relationship management. The applicability of what follows depends on the facts and circumstances specific to each third-party vendor relationship.

All steps taken by a credit union in its third-party vendor management process should be documented and appropriately approved in writing to ensure the procedures are followed and to memorialize how decisions were made and justified.

I. RISK ASSESSMENT & PLANNING

A. Vendor Management Policies

Each credit union should have in place a third-party vendor relationship management policy which includes determination of need for assistance from third-party vendors and procedures for reviewing, analyzing, selecting and administering those relationships.[14] The credit union's policies should outline credit union staff responsibilities and authorities for third-party vendor relationships and program oversight.[15] The policies should distinguish that which is required for "critical" relationships versus "non-critical" relationships.[16]

The credit union's management should make the decision regarding whether or not to use a third-party vendor.[17] This analysis should be consistent with the credit union's strategic plan and business model, with its tolerance for and ability to assess and manage risk, and should take into account the circumstances unique to the potential third-party vendor relationship.[18]

Part of the credit union's policy should stipulate which employee(s) are authorized to sign contracts (e.g., a specific officer or officers for contracts above a certain dollar amount and/or requiring two levels of management review unless the credit union is a small credit union). It is important that the credit union's employees follow this policy because the credit union may be bound to any

[14] *See* NCUA, "Evaluating Third Party Relationships," Supervisory Letter No. 07-01, at 3-4 (2007) (enclosed with Letter to Credit Unions No. 07-CU-13); NCUA, "Due Diligence Over Third Party Service Providers," Letter to Credit Unions No. 01-CU-20 (2001).
[15] *See* NCUA, "Evaluating Third Party Relationships," Supervisory Letter No. 07-01, at 3-4 (2007) (enclosed with Letter to Credit Unions No. 07-CU-13); NCUA, "Due Diligence Over Third Party Service Providers," Letter to Credit Unions No. 01-CU-20, at *2-*3 (2001).
[16] *See* NCUA, "Evaluating Third Party Relationships," Supervisory Letter No. 07-01, at 3-4 (2007) (enclosed with Letter to Credit Unions No. 07-CU-13).
[17] *See id.* at 2-3.
[18] *See id.* at 2-4.

contract signed by an employee who "apparently" (from the viewpoint of the third-party vendor) had authority to sign the contract, even if the employee did not in fact have such authority.

B. Responsibilities of the Board of Directors

The credit union's board of directors has a fiduciary duty to operate the credit union in the best interests of the members and of the credit union as an institution, and also to operate the credit union in a reasonably prudent manner when making decisions.[19] As part of this fiduciary duty, the board is responsible to ensure that the credit union has a legally sound third-party vendor management policy in place and that it is followed by credit union management and is safe and effective. The process, its application, and effectiveness should be reviewed at least annually by the board.[20] In a 2002 issuance, NCUA described the third-party risk management, monitoring, and control responsibilities of the board of directors as:

> "**The use of third parties does not diminish 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.** Thus, an effective due diligence process and on-going director oversight process are critical to the effective management of third-party vendor relationships. Specifically, the credit union should have a process in place to:
>
> - assess how outsourcing arrangements will support the credit union's objectives and strategic plans;
> - understand the risks associated with outsourcing arrangements . . . ;
> - ensure appropriate contractual provisions are in place to facilitate effective oversight; and
> - implement an oversight program to monitor each service provider's controls, conditions and performance."[21]

---

[19] *Id.* at 2-3; NCUA, "Due Diligence Over Third Party Service Providers," Letter to Credit Unions No. 01-CU-20, at *1 (2001); *see, e.g.*, *Gully v. NCUA*, 341 F.3d 155, 165 (2d Cir. 2003) (applying New York state fiduciary duty law to a federal credit union officer); *In re Gully*, NCUA, Final Decision & Order, Docket No. 00-0701-I, at n.1 (2002) ("Fiduciary duty is defined as a 'duty to act in the best interest of the institution, its shareholders and its depositors.'"), *available at* http://www.ncua.gov/administrative_orders/Admin/2000/00-0701-I.htm; Conversion of Insured Credit Unions to Mutual Savings Banks, 71 Fed. Reg. 77,150, at 77,154-57 (Dec. 22, 2006) (to be codified at 12 C.F.R. pt. 708a); *see also* Mergers, Conversion From Credit Union Charter, and Account Insurance Termination, 73 Fed. Reg. 5,461, at 5,463-64 (advance notice proposed Jan. 30, 2008) (to be codified at 12 C.F.R. pts. 708a, 708b).

[20] The editors of the Guide believe that at least annual review of this policy is generally consistent with the "on-going" director oversight process recommended by NCUA, see for example NCUA's Supervisory Letter No. 07-01 at pages 8 to 9, as well as generally consistent with the obligations of the directors of FDIC-insured depository institutions. *See* FDIC, "Guidance for Managing Third-Party Risk," FIL-44-2008, at 9 (2008) ("The board should initially approve, oversee, and review at least annually significant third-party arrangements, and review these arrangements and written agreements whenever there is a material change to the program.").

[21] NCUA, "e-Commerce Guide for Credit Unions," NCUA Publication No. 8072, at 20 (2002) (enclosed with Letter to Credit Unions No. 02-CU-17).

If the board has approved prudent, safe and sound vendor management policies and processes consistent with NCUA policy, the members of the board *may* be protected from legal liability by the "Business Judgment Rule."[22] Note that some courts have declined to apply the protection of the Business Judgment Rule to directors of depository institutions, especially in trying economic times such as the savings and loan crisis.[23]

Even if a court declines to apply the protections of the Business Judgment Rule, however, a director would likely be protected from legal liability so long as he or she exercised reasonable prudence—i.e. acted in accordance with his or her fiduciary duty—when making decisions as a member of the board.

Reviewing the credit union's policies on third-party vendor management at least annually and making inquiries to management regarding specific situations or policies of concern is evidence of reasonably prudent board actions. The more that the board can document reasoned, informed, and prudent decision-making, the less likely it is that the board's members would breach their fiduciary duty.

C. Senior Management's Oversight Responsibilities

The credit union's officers have the same fiduciary duty as directors, as discussed above, to make reasonably prudent management decisions and operate the credit union in the best interests of the members and the credit union as an institution.[24] Senior management has a more direct role in third-party vendor management than the board of directors, however, and should keep the board informed about material third-party vendor-related concerns. In addition:[25]

1. Senior Management should initially approve, oversee, and review at least annually critical third-party vendor arrangements, and document these arrangements and written agreements whenever there is a material change to the program.
2. Management should periodically review the third-party vendor's operations in order to verify that they are consistent with the terms of the existing written agreement and that risks are being controlled.
3. The institution's compliance management system should ensure continuing compliance with applicable federal and state laws, rules, and regulations, as well as internal policies and procedures.

---

[22] *See generally* Committee on Corporate Laws, ABA Section of Business Law, *Corporate Director's Guidebook Fifth Edition*, 62 Bus. Law. 1479 (2007) ("The business judgment rule presumes that in making a business decision, disinterested directors acted on an informed basis, in good faith, and in the honest belief that the action taken was in the best interests of the corporation.").

[23] *See* John Canfield, *The Evolution of a More Stringent Business Judgment Rule in Banking -- The Minimalization of Director Deference*, 6 U.C. Davis Bus. L.J. 153 (2006); Patricia A. McCoy, *The Notional Business Judgment Rule in Banking*, 44 Cath. U. L. Rev. 1031 (1995).

[24] See sources cited in note 18, above.

[25] *See* NCUA, "Evaluating Third Party Relationships," Supervisory Letter No. 07-01 (2007); *see also* FDIC, "Guidance for Managing Third-Party Risk," FIL-44-2008, at 9-10 (2008).

4. Management should allocate sufficient qualified staff to monitor critical third-party vendor relationships and provide the necessary oversight.

5. The extent of oversight of a particular third-party vendor relationship will depend upon the criticality, potential risks and the scope and magnitude of the arrangement.

6. An oversight program will generally include monitoring of the third-party vendor's quality of service, risk management practices, financial condition, and applicable controls and reports.

7. Results of oversight activities for material third-party vendor arrangements should be periodically reported to the financial institution's board of directors or designated committee. Identified weaknesses should be documented and promptly addressed.

8. Credit unions should maintain documents and records on all aspects of the third-party vendor relationship, including valid contracts, business plans, risk analyses, due diligence, and oversight activities (including reports to the board or delegated committees). You should make sure all information collected is dated. Also, retain documents regarding any dispute resolution.

D. Suggested Actions During Initial Risk Assessment/Planning Stage

Once you have determined that a business objective requires assistance from third-party vendors, you will perform due diligence as deemed necessary and appropriate in the circumstances. Use your common sense and ask yourself several questions, always keeping in mind your credit union's risk tolerance, as well as its ability to manage the risk, and the significance of the third-party vendor's service or product to the credit union:

- How does the business service or product fit into the credit union's strategic plans?
- Have you considered all alternatives, including using internal sources, collaboration with other credit unions, available credit union service organizations (CUSOs), and several other third-party vendors?
- Will this third-party vendor enable the credit union to be more efficient and effective? What could possibly go wrong in a worst case scenario? What would be the impact to the credit union in a worst case scenario?
- How much do I really know about this third-party, its business, and its reputation in the business community? From what sources did you learn or become aware of what you know about the third-party?
- What additional information about this third-party and its business would my regulator and/or its examiners think that I should have known or asked for, especially if my credit union later experiences financial problems that can, in part, be tied to the relationship with this vendor? Would my regulator and/or its examiners think that this relationship is a good idea? Why or why not?

- Has this third-party had service or financial problems in the past, either in our relationship or in its relationships with other institutions? What was the nature of those problems and how were they resolved?
- How could problems with this relationship negatively impact service to our members or negatively impact the financial performance and reputation of the credit union?
- If this vendor were to disrupt or poorly perform its service or product delivery, what is the maximum potential loss exposure to the credit union?
- If this vendor does not perform according to our expectations, or goes out of business, or otherwise cannot provide the service, what is our backup plan or exit strategy?
- Does this vendor carry sufficient insurance (e.g., professional liability insurance)?

Finally, ask yourself:

- Considering all of the benefits and risks and my knowledge (or lack thereof) about the third-party and its business, would a prudent credit union manager decide to enter into or continue this relationship?

E. Strategic Planning in Detail

1. **Strategic Goals:** The first step is to ensure that the proposed third-party vendor relationship is consistent with the credit union's strategic goals, objectives, and overall business needs.

    a. Management should be able to thoroughly understand what using the third-party vendor will do for the credit union and also why it would be (or not be) in the best interest of the credit union to use the third-party vendor's service. Consider risks and benefits of outsourcing these services versus performing them in-house.

    b. Determine long and short term goals to be achieved by this relationship. The goals should be measurable and achievable, and also be monitored by management.

2. **Significance/Criticality of the Third-Party Vendor:** The second step is to determine whether or not the proposed third-party vendor relationship is a "critical third-party vendor relationship." See **Definitions and Key Concepts**, above, for specific criteria.

    a. If the relationship is a "critical" one, a substantial risk-analysis, planning, due diligence, and monitoring process is in order. The degree of thoroughness required for this process depends upon the specific facts and risks underlying the relationship, and

the level of criticality the third-party vendor has to the credit union's operations.[26]

b. If the third-party vendor relationship is "non- critical" (e.g. the credit union's landscaper and similar third-party vendors that generally do not pose a material threat to the credit union), you should employ the relevant procedures contained in this Guide to the extent that doing so is economically rational (considering factors such as the dollar amount of the contract, estimated risk of a loss to the credit union, etc., versus the expense of the review in employee-hours and other costs).

3. **Analyze Costs, Benefits, and Risks:** The third step is to analyze the costs, potential benefits, potential risks, and legal/compliance issues (such as: "Are we legally authorized to engage in this activity?" or "Can we be sued?") relevant to the proposed relationship.

The thoroughness of this analysis is dependent upon the criticality of the relationship as well as the potential costs and potential risks associated with the activity.[27] The greater the criticality and cost and/or risk, the more thorough and detailed the analysis should be. It may also be appropriate to do a more thorough and detailed cost-benefit and/or risk-reward analysis if the product or service is a new activity or product for the credit union.

If the proposed relationship will be a Non-Critical Third-Party Vendor Relationship a formal cost-benefit or risk-reward analysis is generally unnecessary. Do, however, consider the potential costs, benefits, risks, alternatives, etc., of the proposed relationship by doing an informal cost-benefit or risk analysis.[28]

a. **Risk-Reward Analysis:** If appropriate, do a formal risk-reward analysis and/or cost-benefit analysis, and memorialize the analysis or analyses in writing. Items of consideration would be:[29]

1) Such analyses should outline the range of expected and possible financial outcomes, depending on the circumstances.

---

[26] *See* NCUA, "Evaluating Third Party Relationships," Supervisory Letter No. 07-01, at 2-4, 8-9 (2007) (enclosed with Letter to Credit Unions 07-CU-13); NCUA, "e-Commerce Guide for Credit Unions," NCUA Publication No. 8072, at 9 (2002) (enclosed with Letter to Credit Unions No. 02-CU-17).

[27] See sources cited in note 25, above.

[28] *Cf.* NCUA, "Evaluating Third Party Relationships," Supervisory Letter No. 07-01, at 3-4 (2007) (enclosed with Letter to Credit Unions 07-CU-13) ("Risk assessments for less complex third party relationships may be part of a broader risk management program or documented in board minutes.").

[29] *See id.* at 2-3; NCUA, "Due Diligence Over Third Party Service Providers," Letter to Credit Unions No. 01-CU-20, at *2 (2001) ("The credit union should project its expected revenue, expenses, and net income on its investment, and recognize how each of these factors may change under different economic conditions.").

2) It may be appropriate to include a worst case scenario.

3) It may be appropriate to consider other options, such as performing the activity or product offering in another manner, including the use of other third-party vendors or performing the function in-house.

4) Certain aspects of the risk assessment phase may include the use of internal auditors, compliance officers, technology officers, and legal counsel.

5) Project expected returns based on expected revenues, direct costs, and indirect costs (e.g., when dealing with a potential outsourced lending relationship, consider the potential effect of borrower prepayments and third-party vendor fees, as well as the expected loan yields).

6) Evaluate financial projections in the context of the credit union's overall strategic plans and asset-liability framework. Examiners will generally evaluate such projections based upon a "reasonableness" standard, considering the following factors:[30]

   - Historical performance;
   - Underlying assumptions;
   - Stated business plan objectives; and
   - Complexity of the credit union's risk profile.

4. Legal/Compliance Issues: The proposed activity should be reviewed for legal and compliance purposes by an attorney with experience in depository institution regulatory matters (i.e. likely not your collections attorney unless he or she also has experience with credit union regulation) and/or an experienced compliance officer.[31]

"In addition to a legal review of contracts and written agreements relevant to a prospective third party arrangement, it may be prudent for credit unions to obtain a legal opinion about any services provided by the third party under the arrangement. For example, if a third party is engaged to perform loan collections for the credit union, a legal review of their collection methods may be prudent to ensure debt collection and reporting practices comply with applicable state and federal laws."[32]

---

[30] NCUA, "Evaluating Third Party Relationships," Supervisory Letter No. 07-01, at 4 (Oct. 2007) (enclosed with Letter to Credit Unions 07-CU-13).

[31] *See id.* at 6-7; NCUA, "e-Commerce Guide for Credit Unions," NCUA Publication No. 8072, at 9 (2002) (enclosed with Letter to Credit Unions No. 02-CU-17) ("A process should be in place to ensure that the credit union is aware of, and has addressed all relevant legal and compliance issues . . . . Therefore, it is prudent to involve legal counsel in the review . . . . If legal counsel historically utilized by the credit union is unfamiliar [with issues related to the business activity at hand], they may be able to refer the credit union to counsel with such expertise.").

[32] NCUA, "Evaluating Third Party Relationships," Supervisory Letter 07-01, at 7 (2007) (enclosed with Letter to Credit Unions No. 07-CU-13).

5. **Parameters/Scope of the Relationship:** Credit unions should clearly define the nature and scope of their needs and responsibilities of the parties.[33]

   a. Who is responsible for what; where do the credit union's responsibilities end and the third-party vendor's begin? The contract with the third-party vendor should outline credit union staff responsibilities and authorities for third-party vendor processes and program oversight. With outsourcing, the contract should specifically identify the frequency, content, and format of the service or product to be provided.

   b. Ensure that both the credit union and the third-party vendor have expectations that do not materially differ. Credit Union expectations should be spelled out in the form of service level agreements in both the RFP (request for proposal) and the eventual vendor contract.

   c. It is important to consider establishing limitations to control the pace of third-party vendor program growth in order for your credit union to develop expertise with the program (e.g., credit unions using a third-party vendor lending program should initially limit the number of loans granted so that any problems can be identified in a timely manner before your are in possession of a large number of problem loans).

   d. "Generally, contracts establish requirements for periodic audits or access to third party records."[34]

   e. If applicable, the contract should expressly address ownership of the resulting "know-how" from the relationship as well as all other forms of resulting intellectual property.

   f. The credit union should take into account all aspects of the long-term potential of the third-party vendor relationship, as well as the managerial expertise and other associated costs that would result from the decision to use a third-party vendor, and not be unduly influenced by short-term cost savings.

   g. How will the results of the business service or programs provided through the third-party vendor be monitored for success against expectations and for compliance with the contract agreement?

6. **Staff Expertise:** Management should ensure that the responsible credit union personnel have the knowledge and skill to adequately analyze and oversee the potential relationship.[35]

---

[33] *Id.* at 6-7.
[34] *Id.* at 6.
[35] *See*, *e.g.*, NCUA, "e-Commerce Guide for Credit Unions," NCUA Publication No. 8072, at 1, 5-7, 20-22 (2002) (enclosed with Letter to Credit Unions No. 02-CU-17).

a. Generally, this means that the employee in question—or in limited situations a consultant, an employee of another credit union, or a disinterested CUSO[36]—has or could run such a product program themselves (e.g. an individual analyzing a member business lending program should have at least two years experience with such loan products[37]).

b. If the credit union does not have an employee with the requisite expertise, it should consider not engaging in the proposed relationship unless it hires an employee with such expertise. In most cases, hiring a temporary consultant alone would not be sufficient.[38]

c. For critical third-party relationships, it may be appropriate for the credit union to consider appointing a senior manager to be responsible for the relationship between the credit union and the third-party vendor, including due diligence, implementation, ongoing oversight, and periodic reporting to the CEO. This management official should have the requisite knowledge and skills to critically review all aspects of the relationship.[39]

7. Insurance: Determine whether the third-party vendor relationship will create additional potential liabilities for the credit union and determine whether additional insurance coverage would be prudent, if so, make sure you require the third-party vendor to maintain insurance coverage as a contractual matter.

a. Is the credit union's insurance coverage sufficient?

b. Is the third-party vendor's insurance coverage sufficient?

1) When determining whether or not the third-party vendor carries sufficient insurance coverage, do not forget that numerous other parties would likely be making claims for compensation from the third-party vendor at the same time that your credit union would make its claim.

---

[36] *See* 12 C.F.R. § 723.5 (2008) (outlining NCUA Member Business Lending program regulatory requirements); NCUA, Risk Alert No. 05-RISK-01, at 5-6 (2005) ("[S]ound business practice requires you to . . . consult with, or retain on staff, an independent expert in subprime automobile financing to calculate . . . your credit union's anticipated subprime auto loan yield . . . and conduct sensitivity analyses . . . .").

[37] *See* 12 C.F.R. § 723.5 (2008); NCUA, "Evaluating Third Party Relationships," Supervisory Letter No. 07-01, at 8 (2007) ("Credit unions engaging in third party relationships must have an infrastructure (i.e. staffing, equipment, technology, etc.) sufficient to monitor the performance of third party arrangements.").

[38] *See id. But see* 12 C.F.R. § 723.5 (2008) (providing for the use of independent contractors and other third-party assistance with respect to using "the services of an individual" with the requisite expertise to understand a Member Business Lending program); NCUA, Risk Alert No. 05-RISK-01, at 5-6 (2005) (requiring credit unions engaging in indirect subprime auto lending to hire an independent expert in that activity as either a consultant or as an employee).

[39] *See, e.g.*, NCUA, "Evaluating Third Party Relationships," Supervisory Letter 07-01, at 5, 8 (2007) (enclosed with Letter to Credit Unions No. 07-CU-13); FDIC, "Guidance for Managing Third Party Risk," FIL-44-2008, at 5 (2008).

2) If the third-party vendor has a key employee or employees who are material to its operations (i.e. the third-party vendor might go out of business if he/she/they die), it may be appropriate to determine whether or not the third-party vendor carries “key man” life insurance in an amount sufficient to protect the credit union’s interests.

3) Does the third-party vendor carry Professional Liability Insurance (if applicable)?

4) The credit union may determine the sufficiency of the third-party vendor’s insurance coverage by requesting copies of the policy documents both initially and on an annual basis.

8. Controls and Reporting: Identify necessary controls and reporting processes.

a. Agreed upon controls and reporting requirements should be explicitly included in the terms of the credit union’s contract with the third-party vendor.

b. Set up action plans, controls and measures to achieve the goals of the relationship and plan on-going analysis and appropriate reporting to monitor consistency with strategic plans and relationship goals.

c. There should be sufficient reports for the credit union to be able to measure the risks of the third-party vendor relationship, as well as the third-party vendor’s performance in terms of profitability, benefits to the credit union, and delivery of products or services.

d. The contract should include provisions requiring the third-party vendor to report any material changes in the company or its financial condition as soon as the company is aware of any changes. You may also consider requiring advance notice of changes in management, pricing, marketing strategies, or other activities important to the credit union’s monitoring of the third-party vendor and its activities.

e. The third-party vendor should be required to inform the credit union if any legal action is taken or threatened against it or any of its employees.

9. Potential Impact on Membership: Consider how this arrangement will positively or negatively impact your members; how will you gauge this impact; and how will you manage member expectations?

10. **Exit Strategy/Contingency Plans:** The credit union should always have an exit strategy.

    a. Make sure that the credit union has a reasonable way out of the relationship if plans change or if the product or service does not expectations.

    b. If you enter into the relationship, the contract should include the ability to terminate the relationship if the third-party vendor fails to meet its obligations (breaches or defaults on the contract terms) or if changes in the company or its activities may cause additional risk to the credit union or its members.

    c. Determine what alternatives (either internally at your credit union or with other third party vendors) are available to provide the services or products if the credit union needs to stop doing business with the third-party vendor.

    d. If there are no reasonable alternatives it may be appropriate to question whether you need or want to enter into the relationship and, if you do, what will you do if the service or product is not longer available.

F. Potential Risks to Consider

The nature of the relationship will determine which of the following risks will be present. The more complex and integral the relationship is to the credit union's operations, the more likely that most—if not all—of the following risks will be present:[40]

1. **Strategic Risk:** Risk arising from making the wrong business decision, including failing to make business decisions that are consistent with the credit union's strategic plan.

2. **Reputation Risk:** Risk arising from negative member and public opinion of the credit union, either as the result of poor service or as the result of bad publicity in the media.

3. **Operational Risk:** Risk of loss stemming from; inadequate or failed internal controls, credit union employees, information or other systems, or from external events.

4. **Transaction Risk:** Risk arising from problems with delivery of products or services (especially important in core processing, card processing, wire transfer, and indirect lending relationships).

5. **Credit Risk:** Risk that the third-party (or any other creditor-party necessary to the third-party relationship, such as your insurance company's reinsurer) is financially unable to meet the terms of its

[40] *See* NCUA, "Evaluating Third Party Relationships," Supervisory Letter 07-01, at 2-4 (2007) (enclosed with Letter to Credit Unions No. 07-CU-13); *see also* FDIC, "Guidance for Managing Third-Party Risk," FIL-44-2008, at 2-4 (2008).

contract with the credit union or is otherwise financially unable to perform its duties.

6. **Compliance Risk:** Risk arising from violations of statutes or regulations, or from noncompliance with the credit union's policies, procedures, or business standards.

7. **Interest Rate Risk:** Risk arising from changes in interest rates, especially short-term versus long-term interest rates (e.g., an inverted yield curve).

8. **Liquidity Risk:** Risk arising from holding non-liquid assets when the credit union experiences cash flow difficulties.

9. **Other Risks:** Such as price risk, foreign currency exchange risks, political instability abroad, etc.

G. Credit Union Relationships with CUSOs, Corporate CUs, and Other Credit Union Organizations

Credit unions should keep in mind that CUSOs, corporate credit unions, and other credit union organizations are not exempt from NCUA third-party vendor management requirements simply because these organizations have close ties to the credit union movement. Keep in mind, however, that if you have a pre-existing relationship with one of these entities, significantly less review is generally required to renew the relationship than would be needed to commence a new relationship.[41]

H. Indirect Lending Relationships

Indirect lending relationships, such as loans made through correspondents and brokers, are an area of critical concern for NCUA and other regulators.[42] The NCUA principles articulated below with respect to mortgage and subprime auto lending are generally applicable to most credit union indirect lending relationships.

Keep in mind that:

> "Both brokers and correspondents are compensated based upon mortgage origination volume and, accordingly, have an incentive to produce and close as many loans as possible. Therefore, credit unions should perform comprehensive due diligence on third-party originators prior to entering into a relationship. In addition, once a relationship is established, the credit union should have adequate audit procedures and controls to verify that fees paid to third parties

[41] NCUA, "Evaluating Third Party Relationships," Supervisory Letter 07-01, at 2 (2007) (enclosed with Letter to Credit Unions No. 07-CU-13) ("Further, where credit unions have a longstanding and tested history of participating in a given third party relationship, less analysis is required to renew the relationship.").

[42] *See, e.g.*, NCUA, "Third-Party Relationships: Mortgage Brokers and Correspondents," Letter to Credit Unions No. 08-CU-19 (2008); NCUA, "Specialized Lending Activities—Third-Party Subprime Indirect Lending and Participations," Risk Alert No. 05-RISK-01 (2005); NCUA, "Specialized Lending Activities," Letter to Credit Unions No. 04-CU-13, at 2-3 (2004).

are legitimate, that mortgage applications are complete and do not contain fraud, and that referral or unearned income or fees are legal and not contrary to RESPA prohibitions."[43]

In addition to the issues listed below, all indirect lending relationships pose the risk that funds collected by the third-party vendor on behalf of the credit union are not segregated in an escrow or trust account. Such practices may lead to commingling of funds and a loss of funds for the credit union.

1. Mortgage Lending Using Correspondents or Brokers

In a 2008, NCUA issued Letter to Credit Unions number 08-CU-19 outlining guidance on credit union relationships with third-party mortgage brokers and correspondents.[44] The principles expressed in this guidance are likely applicable to other types of indirect lending relationships.

This NCUA Letter to Credit Unions number 08-CU-19 states in part:

"Contract Issues and Legal Review

- Is the credit union adequately protected and are there adequate default, termination, and escape clauses?
- Are there agreements that the broker or originator will comply with all applicable laws, including safety and soundness regulatory standards applicable to credit unions?
- Does the agreement stipulate that best efforts will be made by originators to ensure loans offered to borrowers are consistent with their needs, objectives, and financial situation?
- Credit unions should reserve the right to not purchase, or to put back to the broker or originator, any loans failing to comply with these standards.

Additionally, in performing due diligence in the use of mortgage brokers and correspondents, credit unions should also be aware of the following potential issues:

- The broker or correspondent may be operating in their own best interests and not necessarily putting the interests of the credit union or the member first;
- Fees and yield spread premiums paid to the third parties may be excessive, and the existence of prepayment penalties may not be clear to the borrower at the time they obtained the loan, or may serve as a deterrent to refinancing

[43] NCUA, "Third-Party Relationships: Mortgage Brokers and Correspondents," Letter to Credit Unions No. 08-CU-19, at 1-2 (2008).
[44] *See id.*

early in the lending relationship should financial difficulties with the member occur;[45]

- Loan fees, terms, and practices that are abusive or considered "predatory"[46] could lead to critical legal, reputation, and other risks to the credit union;
- Obtaining or retaining loans with repayment based on a member's stated income (i.e., unverified income) are high risk loans, especially when the amount of income stated does not pass the reasonableness test;
- Control over the appraisal process can be compromised if the credit union is not obtaining the appraisals directly or is not closely monitoring the quality of completed appraisals;
- The broker or correspondent could structure the transactions to limit their liability. They may have no continuing liability after the credit union finalizes the loan or loan purchase;
- The broker or correspondent may not have the financial capability to continue operations over the long-term or the ability to support any claims that may arise;
- Closed loan documents may not be reflective of written or verbal agreements;
- Product volume may develop at a level in excess of what the third-party and/or the credit union can safely manage; and
- Funding commitments may have to be honored despite developing concerns with the third-party vendor relationship or the loan program in general.

This is not an exhaustive list of considerations, but represents some of the key issues management needs to be mindful of before entering into a mortgage broker or correspondent relationship, and ongoing throughout the relationship."[47]

2. Indirect Auto Lending

Indirect auto lending is another area of NCUA concern. In 2005, NCUA issued Risk Alert No. 05-RISK-01[48] on the subject of indirect, subprime auto lending. A federal bankruptcy court found that this "Risk Alert had the practical effect of prohibiting Credit

[45] "Note that federal credit unions may neither grant loans with prepayment penalties nor enforce such penalties if they exist in promissory notes that the federal credit union acquires or participates in. *See* 12 U.S.C. § 1757(5)(A)(viii); 12 C.F.R. § 701.21(c)(6). Whether or not state-chartered credit unions may originate such loans or enforce such penalties depends upon state law."

[46] "*See* NCUA, Letter to Credit Unions No. 07-CU-09 (2007); OCC, Advisory Letter No. AL-2003-3 (2003)."

[47] NCUA, "Third-Party Relationships: Mortgage Brokers and Correspondents," Letter to Credit Unions No. 08-CU-19, at 3-4 (2008).

[48] NCUA, "Specialized Lending Activities — Third-Party Subprime Indirect Lending and Participations," Risk Alert No. 05-RISK-01 (2008).

Unions from continuing to purchase newly originated sub-prime automobile loans underwritten and serviced by Centrix,"[49] which was, at that time, an indirect, subprime auto lender doing business with some credit unions.

Notable guidance in 05-RISK-01 on indirect lending activities includes:

- "You should analyze the vendor's program to ensure you understand how the loan application, underwriting, servicing, and collections processes work. You should also monitor the program on an ongoing basis to ensure the vendor is executing the program as described."[50]
- "Adoption of any third-party's subprime underwriting criteria without careful and comprehensive evaluation is unsafe and unsound. For federal credit unions, this is a violation of the board's responsibility under §113 of the Federal Credit Union Act (Act) to establish lending policies and internal controls. For all federally-insured credit unions, this is an unsafe and unsound practice subject to possible NCUA action under §206 of the Act."[51]
- "With any static loan pool data, it is critical to verify the source of the cash flows. If the vendor provides the report, sound business practice requires an independent auditor to verify the reporting process, including verifying the source of the cash flows. If you prepare the report, sound business practice requires you to verify the source of the cash flows independently of the vendor, including affirmative confirmation of a sample of borrowers' payments and payoffs and insurance payouts."[52]
- "In addition to projecting expected rates of return based on static pool data, sound business practice requires you perform a sensitivity analysis to calculate the impact on the expected rates of return by varying your assumptions . . . If the expected performance based on static pool data is critically different than the expected performance based on published industry statistics, you should ask the vendor to explain why. If the vendor claims that the vendor's underwriting process or servicing is somehow better than industry standards, you should ask the vendor to provide details and proof of this claim. You should consider such claims very carefully."[53]

---

[49] *In re Centrix Financial LLC*, First Amended Disclosure Statement for Liquidating Chapter 11 Plan Proposed by Debtors and Creditors' Committee, Case No. 06-16403 (Bankr. D. Colo. 2008), at *4, *available at* http://www.kccllc.net/centrixfinancial (last visited August 27, 2008).
[50] NCUA, "Specialized Lending Activities — Third-Party Subprime Indirect Lending and Participations," Risk Alert No. 05-RISK-01, at 3 (2008).
[51] *Id.* at 4.
[52] *Id.* at 4-5.
[53] *Id.* at 5.

- "To carry out your responsibilities, sound business practice requires you to:
    - Perform a due diligence review of the vendor's policies, procedures, and practices, ensuring consistency with your policies and risk appetite; and
    - Consult with, or retain on staff, an independent expert in subprime automobile financing to:
        - Calculate on a periodic basis your credit union's anticipated subprime auto loan yield using assumptions based on the audited or verified static pool data, and
        - Conduct sensitivity analyses of changes to expected return from varying assumptions based on industry statistics.

You may conduct alternative due diligence in lieu of (a) and (b) if the alternative satisfies the concerns expressed in this section. Analysis based solely on marketing claims or unaudited performance data is not, however, acceptable alternative due diligence."[54]

It should also be noted that Centrix's contracts with credit unions did not give the credit unions the right to collect on Centrix-issued loans in the event that Centrix became bankrupt. The lack of a contractual right to collect such payments was a significant problem for Centrix-exposed credit unions after Centrix declared bankruptcy.

[54] *Id.* at 5-6.

I. NCUA's Questionnaire Related to Risk Assessment and Planning

The following questions are taken directly from the NCUA ARIES Questionnaire and should be answered as part of your third-party vendor relationship analysis during the Risk Assessment and Planning stage.

Background

4. Does the third-party relationship(s) complement the credit union's overall mission and philosophy?

Planning/Risk Assessment

1. *Does the credit union's planning and risk assessment address the following areas, which it should, based on the type and critical nature of the relationship(s):*
    - *(a) Risk areas which could be affected by the third-party arrangement (credit, interest rate, liquidity, transaction, compliance, strategic, and reputation;*
    - *(b) Expectations of third-party relationship;*
    - *(c) Staff expertise;*
    - *(d) Criticality of the activity to be outsourced;*
    - *(e) Cost/Benefit analysis;*
    - *(f) Impact on membership; and*
    - *(g) Exit strategy.*

2. *Has the credit union evaluated the costs of monitoring and providing support to the third-party program (i.e., staffing, capital expenditures, communications, and technological investment)?*

3. *Does the credit union's strategic business plan include measurable and achievable goals and clearly defined levels of authority and responsibility related to the third-party arrangement?*

4. *Has the credit union performed and documented a cost-benefit financial analysis to determine they are receiving sufficient reward for the risk associated with the proposed relationship (The financial projections should address a range of expected and possible financial outcomes)?*

5. *Do the financial projections align with the credit union's overall strategic plan and ALM framework?*

II. DUE DILIGENCE

A. Due Diligence Basics

Comprehensive due diligence involves gathering and reviewing all available information about a potential third-party vendor, focusing on the entity's:

1. Corporate ownership structure and background,
2. Financial history and current condition,
3. Business model and practices,
4. Scope and effectiveness of its operations and controls, including:
   a. "Security and data handling practices;
   b. Business continuity planning;
   c. Operations controls relevant to the third-party vendor's work;
   d. Hiring/screening practices;"[55]
5. Reputation & relevant experience,
6. All other available and material information.

B. Request for Information (RFI) or Request for Proposal (RFP)

1. Involve all appropriate stakeholders at the credit union to help prepare the "Request for Information" to be submitted to third parties.
2. Define and communicate the credit union's requirements for the third-party vendor relationship within the written Request for Information. In general, an RFI or RFP should be specific to the credit union, its particular situation, and the third-party vendor; generic or "boilerplate" documents should be avoided.
3. Identify/evaluate potential third-party vendor candidates.
4. Investigate business reputation using sources such as the these examples:[56]
   - Better Business Bureau
   - Federal Trade Commission
   - State agencies (e.g., departments of state, departments of corporations, state consumer protection agencies, state attorneys general, etc.)
   - Credit reporting agencies (Equifax, Experian, TransUnion).
   - NASDAQ or NYSE

[55] BITS, "Key Considerations for Managing Subcontractors, at 11 (2008).
[56] *See, e.g.*, NCUA, "Third-Party Relationships: Mortgage Brokers and Correspondents," Letter to Credit Unions No. 08-CU-19, at 2 (2008); NCUA, "Evaluating Third-Party Relationships," Supervisory Letter No. 07-01, at 4-5 (2007) (enclosed with Letter to Credit Unions No. 07-CU-13).

- Current and former clients.
- Dun & Bradstreet, Acxiom, infoGROUP, etc.
- Moody's, Standard & Poor's, Fitch, A.M. Best, Morningstar, etc.
- others

C. Evaluating the Third-Party Vendor Responses

As with the credit union's risk/benefit analysis of the proposed relationship, the scope and depth of due diligence is directly related to the criticality of the institution's relationship with the third-party vendor. Information that you want to verify and consider includes:

1. Corporate structure & background[57]
    a. Any lawsuits or legal proceedings involving the third-party/vendor.
    b. Length of time the third-party vendor has been in business; how long it has been offering the business service or program that you are considering.
    c. Whether the third-party is a privately-held or public company.
    d. Under some circumstances, it may be appropriate to scrutinize the reputations of the third-party vendor's principal executives. This is especially true if the company is a start-up or has recently undergone a transition in management.
    e. The third-party vendor's strategies and goals, including service philosophies, quality initiatives, efficiency improvements, and employment policies.
    f. The adequacy of third-party vendor's insurance coverage.
2. Business model[58]
    a. The longevity and adaptability of the third-party vendor's business model and how it fits with the credit union's vision.
    b. That the third-party vendor has obtained proper licenses/certifications and that they remain current during length of agreement.
    c. The third-party vendor's ability to perform the proposed functions using current systems or the need to make additional investment.
    d. Use of other parties or subcontractors by the third-party.
    e. The third-party vendor's knowledge of relevant consumer protection and civil rights laws and regulations.

[57] *See* NCUA, "Evaluating Third Party Relationships," Supervisory Letter 07-01, at 4-5 (2007) (enclosed with Letter to Credit Unions No. 07-CU-13).
[58] *See id.* at 5.

3. Financial condition

a. Review the third-party's financial statements, annual reports, SEC filings, Call Reports, and any other available financial indicators. Consider other sources of information, such as the Better Business Bureau, Federal Trade Commission, Dun & Bradstreet, Moody's, etc.[59]

1) Financial statements should be in accordance with Generally Accepted Accounting Principles (GAAP)[60] or, in some cases, International Financial Reporting Standards (IFRS).

2) Closely scrutinize pro forma metrics (i.e. non-GAAP, non-IFRS metrics); these can often be misleading.

3) It may be appropriate to insist upon audited financial statements depending upon the third-party vendor's criticality to the credit union and the risks involved.[61] "A credit union's audit scope should provide for independent reviews of third party arrangements and associated activities."[62] Keep in mind, however, that some privately held companies may refuse to disclose such information.

4) The footnotes to the financial statements often provide information that is critical to the relationship. These should be reviewed for "off balance sheet items" such as contingent liabilities, pending litigation and other items relative to the financial stability of the company.

5) "Credit unions should consider that third party relationships might create accounting complexities. Credit unions must have adequate accounting infrastructures to appropriately track, identify, and classify transactions in accordance with Generally Accepted Accounting Principles (GAAP). Credit unions often develop third party arrangements to outsource new products or functions, and may not have experience in accounting for the particulars of those new products or functions. Conversely, although credit unions may be familiar with the accounting rules for a given function, the nature of a third party arrangement may change the required accounting procedures."[63]

6) "In some instances, a certified public accountant's guidance may be necessary to ensure proper accounting treatment."[64]

---

[59] *See id.* at 6.
[60] *See id.* at 7 ("Credit unions must have adequate accounting infrastructures to appropriately track, identify, and classify transactions in accordance with Generally Accepted Accounting Principles (GAAP).").
[61] *Id.* at 6.
[62] *Id.* at 7-8.
[63] *Id.* at 7.
[64] *Id.*

7) Remember that the statement of cash flows is generally derived from the income statement. Therefore errors or misstatements in the income statement will also exist in the statement of cash flows unless the third-party vendor derives the statement of cash flows independently from the income statement (which rarely happens).

8) Take into account the significance of the proposed contract on the third-party vendor's financial condition and on the credit union's financials.

9) It is a red flag if the third-party vendor refuses to disclose its financial statements.

- Many of the worst stories involving credit union third-party vendor relationships begin: "Well, we asked them for their financial statements but they said that those were private and that they did not give them to anyone."
- Keep in mind, however, that many third-party vendors will "push back" with respect to requests for disclosure of financials because they will not want to reveal their business model, profit margins, etc. In this instance, settling for, e.g., an abbreviated version of the business model may be sufficient. A non-disclosure agreement may be another way to assuage a third-party vendor's concerns.
- Depending upon the circumstances, it may not be appropriate to do business with a third-party vendor for a potentially "critical" relationship if the third-party vendor will not disclose its financial statements.

b. Understand the third-party vendor's sources of income and expenditures.[65]

c. Keep in mind that some business models may be well suited for periods of economic expansions, but untenable during a recession.[66]

d. Cash Flows in the Proposed Relationships[67]

1) "Perhaps one of the most important considerations, when analyzing a potential third-party relationship, is the

[65] *See id.* at 6.
[66] *See id.* at 5.
[67] *See* NCUA, "Evaluating Third Party Relationships," Supervisory Letter 07-01, at 6 (2007) (enclosed with Letter to Credit Unions No. 07-CU-13); *see also* NCUA, "Third-Party Relationships: Mortgage Brokers and Correspondents," Letter to Credit Unions No. 08-CU-19 (2008); NCUA, "Specialized Lending Activities—Third-Party Subprime Indirect Lending and Participations," Risk Alert No. 05-RISK-01, at 4-5 (2005).

determination of how cash flows move between all parties in a proposed third-party arrangement."[68]

2) "Credit unions should be able to explain to examiners how cash flows (both incoming and outgoing) move between the member, third-party, and credit unions," as well as "be able to independently verify the source of these cash flows and match them to related individual accounts."[69]

3) Analyze how money flows between the parties (e.g., from members to the third party to the credit union):[70]

   - If the money will be held by the vendor (even for less than a day), escrow accounts or similar arrangements are advisable. The lack of an escrow or similar arrangement may result in a loss to the credit union in the event that the third-party vendor declares bankruptcy.
   - Depending upon the circumstances: It may be appropriate to insist on clearing funds received by the third-party to the credit union on a daily basis, if not more frequently.
   - A well-known third-party practice is delaying clearing funds—such as on members' loan payments made to a third-party loan servicer—so that the third-party can earn interest on those funds during the clearing process. Sometimes the third-party will do this even if doing so is in violation of the contract.[71]
   - Sometimes delays of more than a day on money transfers are unavoidable, but this is generally not the case.
   - Also consider potential opportunities for fraud.

4. Operational effectiveness

   a. If available, review SAS No. 70 audit reports.[72] See appendix on SAS No. 70 Audits prepared by the accounting firm BDO Seidman for further detail, including the differences between SAS No. 70 "Type I" reports and "Type II" reports. It is important to remember that a SAS 70 is an audit tool, not a regulatory or legal designation.

---

[68] NCUA, "Evaluating Third Party Relationships," Supervisory Letter 07-01, at 6 (2007) (enclosed with Letter to Credit Unions No. 07-CU-13).
[69] *Id.* at 6.
[70] *See, e.g.*, *id.* at 6 ("Perhaps one of the most important considerations, when analyzing a potential third party relationship, is the determination of how cash flows move between all parties in a proposed third party arrangement.").
[71] *Cf.* NCUA, "Specialized Lending Activities — Third-Party Subprime Indirect Lending and Participations," Risk Alert No. 05-RISK-01, at 4-5 (2008).
[72] *See* NCUA, "Evaluating Third Party Relationships," Supervisory Letter 07-01, at 6 (2007) (enclosed with Letter to Credit Unions No. 07-CU-13).

b. If SAS No. 70 reports are not available, it may be prudent under some circumstances to require another form of review of the third-party vendor's internal controls,[73] such as an "Agreed Upon Procedures" engagement or another form of audit.

c. Consider the third-party vendor's scope of internal controls, systems and data security, privacy protections, and audit coverage.

d. Consider the third-party vendor's business resumption strategy and contingency plans.

e. Consider the third-party vendor's adequacy of management information systems.

5. Reputation & relevant experience[74]

a. Gather insight into third-party vendor's performance with past clients.

1) Contact credit unions, trade associations, and other institutions which have previously done business with the executives when they were at other companies.

2) Verify third-party vendor's expertise/qualifications.

3) Consider the vendor's experience and ability in implementing and monitoring the proposed activity.

4) Under some circumstances, it may be appropriate to seek out institutions which have done business with the third-party vendor other than those which the third-party vendor offers as references. It is unlikely that a third-party vendor will offer references which have had negative experiences with the third-party vendor.

5) "A well-respected third party may have little or no experience implementing and supporting a new service offering. In these cases, the qualifications, competence, and training of key individuals within the third party's organization become even more important to verify. While it would be tempting to rely solely upon the vendor's reputation alone, a more prudent practice would be to verify the expertise the vendor has obtained to provide this new service."[75]

b. Gather insight into the third-party vendor's industry reputation from credit unions, trade associations, and other institutions that have previously done business with the third-party vendor (and possibly also with institutions that previously did business with

[73] *See id.*
[74] *See id.* at 4-5.
[75] *Id.* at 4.

the third-party vendor's principle executives when they were with other businesses, see below).[76]

c. Consider conducting background checks on the executives and on the company, such as records from civil lawsuits, prohibition orders (e.g., those issued NCUA, FTC, FDIC, state regulatory agencies, etc.), criminal records, news article searches, etc.[77]

D. Potential Red Flags

A red flag is anything that you believe to be a warning sign. Red flags can come in many forms, from intentional deceit to lack of knowledge. A red flag does not mean that you do not deal with the vendor. They simply mean that you need to investigate further to insure that you have a good comfort level with the vendor. The following are examples of red flags that you may experience during due diligence.[78]

1. "Falling for the Great Sales Pitch"

Vendors should never be selected because you like the salesperson. Of course you like the salesperson. They are paid to get you to like them and to like what they tell you about the product or service. It is a red flag whenever you hear, "we like this salesperson better."

2. "Ahead of your time"

The most advanced product or service may not be the ideal for your credit union members. Many products and services work best after some experience—such as if they have bugs that must be corrected—and just because it sounds great to you does not always indicate interest on the part of your members. The "latest and the greatest" should raise a red flag for you.

[76] *See* NCUA, "Third-Party Relationships: Mortgage Brokers and Correspondents," Letter to Credit Unions No. 08-CU-19, at 2 (2008); NCUA, "Evaluating Third-Party Relationships," Supervisory Letter No. 07-01, at 4-5 (2007).
[77] *See* NCUA, "Third-Party Relationships: Mortgage Brokers and Correspondents," Letter to Credit Unions No. 08-CU-19, at 2 (2008); NCUA, "Evaluating Third-Party Relationships," Supervisory Letter No. 07-01, at 4-5 (2007).
[78] Marcia Barron, CUNA, *The Volunteers' Role in Vendor Due Diligence* (2008).

3. “Going to make or save tons of money”

It is a red flag whenever unreasonable financial expectations are the primary consideration for a deal. All deals should be based on reasonable financial expectations.

4. “Doing business with relatives or friends”

It is a red flag whenever you hear something like “this is my brother or my best friend or the sister of a board member.” These “golf course” relationships should never be made based solely on the fact that you know the person with whom you are dealing.

5. “People helping people”

Remember that credit unions are the folks subscribing to this philosophy. Your vendors may not support this. Do not fall into the trap of thinking that they always have your best interest at heart.

6. “Unanswered questions”

Do not give the vendor the benefit of the doubt for failing to answer your RFP questions. Often they intentionally do not answer because the answer would put their company in an unfavorable light. Remember that no questions should ever be off limits when you are forming a business relationship.

7. “Failure to benefit both parties”

If the agreement is very one sided, it is a red flag. Neither side should agree to a contract that does not have sufficient benefit for all parties. This does not mean that the benefits need to be equal. The party not receiving sufficient benefit will quickly become dissatisfied with the deal.

8. “ALPHA – BETA”

Be very skeptical of any vendor who wants you to be the first to use their product or service especially if the product or service is critical to your operations. In cases where you can not find a fully tested product or service, be sure to add additional protective language to your contract to allow you to terminate if the product or service is not meeting your defined expectations.

9. “THEY are taking care of it”

It is always a red flag when you ask questions and you are told that someone else is taking care of it. This is sometimes used when no one is taking care of it. Ask to see what is being done.

10. “Too good to be true”

Any deal that is unbelievably good is probably just that and should raise a red flag.

11. “Does the business model make sense?”

If the proposed transaction does not “make sense” to you—especially with respect to how it would be more profitable than the credit union performing

the service itself—that is another red flag. For example, if the credit union knows that loans it makes to borrowers with certain FICO scores are not profitable, how could such loans be profitable if made by an indirect lender? Even if those loans were "insured," how could an insurance company make money off of insuring an unprofitable product? While the third-party vendor may have plausible answers—for example, the third-party vendor may have special expertise in a given business activity—the credit union should insist that the third-party vendor provide information that addresses such concerns to the credit union's satisfaction.

12. Other Red Flags

This list is not intended to be all inclusive. It should give you some ideas about what a warning sign or red flag might be. Remember to trust your instincts or feelings. If it does not seem right, for whatever reason, keep looking until you have enough information to be comfortable with your decision.

E. NCUA's Questionnaire Related to Due Diligence

The following questions are taken directly from the NCUA ARIES Questionnaire and should be answered as part of your third-party vendor relationship analysis during the Due Diligence stage.

Background

3. *Did the credit union consider more than one third-party before entering into a relationship?*
5. *Has the credit union completed an appropriate risk assessment to determine the exposure related to each third-party relationship?*

Due Diligence - Background Check

1. *Did the credit union consider the third-party's experience providing the proposed service or program?*
2. *Did the credit union request referrals from the prospective third-party clients to determine their satisfaction and experience with the proposed arrangement?*
3. *Did the credit union review and consider any lawsuits and/or legal proceedings involving the third-party or its principals?*
4. *Did the credit union ensure the third-party or their agents have any required licenses or certifications and that they remain current for the duration of the arrangement?*
5. *Did the credit union consider other sources of information such as the Better Business Bureau, Federal Trade Commission, credit reporting agencies, state consumer affairs offices, or state attorney general offices?*

Due Diligence - Business Model

1. *Does the credit union understand the third-party's business model?*
2. *Does the credit union understand the vendor's sources of income and expense and have they considered any conflicts of interest that may exist between the third-party and the credit union?*

Due Diligence - Cash Flows

1. *Is the credit union tracking and identifying the cash flows of the third-party accurately?*

Due Diligence - Financial and Operation Control Review

1. *Does the credit union's analysis of the financial statements of the third-party and its closely related affiliates provide reasonable assurance that the third-party has the ability to fulfill the contractual commitments proposed?*
2. *Did the credit union use other available sources in evaluating the overall financial health of the prospective or existing third-party (i.e., Nationally Recognized Statistical Rating Organizations, SAS 70 (Type II) reports, etc.)?*

Due Diligence – Accounting Considerations

1. *Does the credit union have an adequate accounting infrastructure to appropriately track, identify, and classify transactions for the vendor relationship under consideration in accordance with Generally Accepted Accounting Principles (GAAP)?*

III. CONTRACTS

The credit union should have a written contract with every third-party vendor. All agreed upon aspects of the credit union's relationship with the third-party vendor—both material and non-material—should be memorialized in the contract.[79]

A. Existing Contract Review.

1. Collect and verify that contracts exist for all existing third-party vendor relationships.
2. Review for accuracy of current relationship terms, signatures, etc. and update as appropriate with legally binding amendments or restatements.
3. Make sure all original contracts are maintained in a safe centralized document storage system for easy reference.
4. Enter into existing contract control system – or create a system – for tracking terms, termination procedures, etc.

B. How to draft a contract with a third-party

1. As with the credit union's risk-benefit analysis of the proposed relationship, whether legal review of contract by legal counsel is required depends on the criticality of the institution's relationship with the third-party vendor. The more critical and/or complex a contract, the more necessary review by legal counsel becomes. Appropriate legal counsel should be involved in negotiating, drafting and/or reviewing critical and/or complex contracts prior to finalization.[80] This review can be performed by your in-house counsel if you have one.[81]

2. Contracts written by third parties are typically very biased in favor of the third-party and against you. Have your lawyer review the proposed contract and suggest changes for you to negotiate. Whatever your lawyer charges to review contracts will be much less than the legal bills your credit union will have if something goes wrong with the third-party vendor relationship and litigation ensues, or if you are required to pay damages under the terms of the contract.

---

[79] *See, e.g.*, NCUA, "Evaluating Third Party Relationships," Supervisory Letter 07-01, at 6-7 (2007) (enclosed with Letter to Credit Unions No. 07-CU-13).

[80] *See id.*; NCUA, "e-Commerce Guide for Credit Unions," NCUA Publication No. 8072, at 21 (2002) (enclosed with Letter to Credit Unions No. 02-CU-17) ("Appropriate legal counsel should review contracts prior to execution."); NCUA, "Due Diligence Over Third Party Service Providers," Letter to Credit Unions No. 01-CU-20, at *2 (2001) ("The credit union's attorneys should review all contracts to ensure that the officials clearly understand the rights and responsibilities of each party. For example, the review should indicate which party bears the costs of collateral disposition, and whether or not there are recourse arrangements . . . . Further a credit union should understand what actions it may take if the contract is breached or services are not performed as expected.").

[81] *See* NCUA, OGC Letter No. 08-0417, from Robert M. Fenner, General Counsel, NCUA, to Faith Anderson, Vice President & General Counsel, American Airlines FCU (Apr. 18, 2008).

3. If the lawyer writes you a letter commenting on potential problems with the contract, try to negotiate to get the suggested changes even if it might jeopardize the transaction;[82] contractual review by an attorney is not simply so that you can check a box on a form. In general, your supervisory authority will criticize a contract if your attorney did not approve of it. Further, do not send your attorney's letters to the third-party vendor asking for a response; this will do little good (they usually claim that the attorney's concerns are unfounded even when they are legitimate) and sending your attorney's communications to a third-party will impair your legal rights.

4. **Negotiate, Negotiate, Negotiate:**[83] Everything is negotiable for a credit union. If the third-party vendor will not negotiate over a material contract provision that you want changed, it may be appropriate to walk away from the negotiations and find a third-party vendor who will meet your terms to provide the product or service to the credit union. Keep in mind that some third-party vendors think that credit unions "have never met a contract that they did not like."

5. **Put it in Writing:** Most courts are reluctant to enforce oral agreements that are not written into the contract and, in many cases, will disregard oral agreements or conditions when a written contract exists. If the issue is important enough for you to discuss it with the service provider, add it to the contract as a written addendum.

6. Many contracts, especially IT contracts, do not actually specify what the credit union is getting. If that is the case you will not likely get what you anticipate getting and your legal rights will be limited or nonexistent. A brochure or vague platitudes (e.g., "cutting edge solutions") are not sufficient. With respect to IT contracts, it is usually a good idea to speak with the third-party vendor's IT professionals about what exactly the product does because the salesperson either may not really know or may intentionally misrepresent the product in order to earn his or her commission.

---

[82] *See, e.g.*, NCUA, "Due Diligence Over Third Party Service Providers," Letter to Credit Unions No. 01-CU-20, at *2 (2001) ("The credit union should exercise its right to modify contracts to make them fair and equitable.").

[83] *See* NCUA, "Evaluating Third Party Relationships," Supervisory Letter 07-01, at 6-7 (2007) (enclosed with Letter to Credit Unions No. 07-CU-13); NCUA, "Due Diligence of Third Party Service Providers," Letter to Credit Unions No. 01-CU-20, at *2 (2001) ("The credit union should exercise its right to modify contracts to make them fair and equitable.").

7. **Letters of Intent:** Letters of intent are usually binding contracts, they are just called by another name. Treat all letters of intent like you treat contracts; do not agree to one unless you would agree to a full-dress contract.

8. **Addendums:** If the third-party vendor refuses to negotiate changes to the contract itself, add an addendum to the contract instead. Addendums are generally just as good as altering the contract itself. Do not be afraid to add an addendum that is longer than the contract itself.

9. **Terms and Conditions In Another Source:** Some third-party vendors present contracts that have terms and conditions that are not incorporated into the contract itself but are instead in another source, such as on the third-party vendor's website (in which case the vendor can change these terms and conditions whenever it wants without informing the credit union). This is not sufficient; all terms and conditions should be in either the contract itself or in an addendum to the contract. If the vendor will not agree to put the terms and conditions in the contract, print out the terms and conditions from the web or other source and add them to the contract as an addendum.

10. Any material or critical contract with a third-party vendor should prohibit assignment, transfer or subcontracting by the third-party of its obligations to another entity, unless and until the credit union determines that such assignment, transfer, or subcontract would be consistent with the due diligence standards for selection of third party vendors and approves the assignment or transfer in writing.

11. Consider and address any potential conflicts of interest that may exist between the credit union and the third-party vendor.

12. The credit union should take into consideration whether or not the third-party vendor relationship will impact the credit union's accounting standards. Will the nature of the relationship change the required accounting procedures?

13. In some cases, particularly as it relates to critical third-party vendors, it is advisable to require the third-party vendor to include their responses to the RFI or RFP as an addendum to the contract. This helps ensure the validity, integrity, and relevance of the third-party vendor's responses and representations of their business.

14. If the contract has already been executed and you subsequently need to make changes or additions, make a written addendum or amendment that clearly references the original contract.

15. It is appropriate to insist on plain, easy-to-understand language in the contract. You must be able to understand your contract to determine if it accurately reflects the expectations of all parties. Contrary to popular belief, lawyers and judges often have trouble understanding excessive "legalese" or "boilerplate" contract language. If the contract has confusing, overly-legalistic or boilerplate language in it, it can often take years of litigation just for the judge to decide what the contract really says.

16. Make sure the contract is flexible enough to allow for changes (technology, financial, etc.) that may develop in the future.

17. As noted in the section on **Strategic Planning** above, the credit union should have a policy with respect to which employee(s) are authorized to sign contracts. It is important that the credit union's employees follow this policy because the credit union may be bound to any contract signed by an employee who "apparently" (from the viewpoint of the third-party vendor) had authority to sign the contract, even if the employee did not in fact have such authority.

18. Do not forget that your credit union will likely be bound by a contract even if it is grossly unfair. Buyer beware!

C. What terms should be included in the contract and what do they mean?

The length and detail of a contract depends on the criticality of the relationship and the cost and risk involved. Following is a list of terms and conditions common to most third party vendor relationship contracts.[84] [85]

1. Scope. Describe what the third-party vendor is expected to provide, services offered and authorized activities:

    a. Frequency, format, and specifications of the service or product to be provided.

    b. Other services to be provided by the third-party vendor, such as software support and maintenance, training of employees, and customer service.

[84] This list is, to some degree, redundant with the preceding list. The editors of the Guide have included some of this information more than once in the interest of completeness.

[85] *See* NCUA, "Evaluating Third Party Relationships," Supervisory Letter 07-01, at 5-9 (2007) (enclosed with Letter to Credit Unions No. 07-CU-13); NCUA, "Due Diligence Over Third Party Service Providers," Letter to Credit Unions No. 01-CU-20 (2001). These sources are applicable to most of the statements in this list.

c. Is a marketing plan needed? Determine and include in the contract if, how, when and by whom a marketing plan will be developed.

d. Collection of unpaid participant fees? Consider and specify in the contract whether the credit union will or will not be responsible for any collection activities. (e.g., the credit union may state that it will use reasonable efforts to assist third-party vendor in collection activities.)

e. Conditions for maintenance and access to financial and operating records.

f. Terms relating to any use of credit union premises, equipment, or employees.

2. Responsibilities of all parties (including affiliates and subcontractors):

a. The contract should clearly set forth the rights and responsibilities of each party.

b. Management Coordination & Oversight**:** Credit union management should consider designating a specific officer to coordinate the third-party vendor oversight activities with respect to critical vendor relationships, including involvement of the credit union's compliance audit and information technology staff.[86]

c. Identification of which party will be responsible for delivering any required consumer disclosures to members.

3. Compensation, Fees and Expenses:

a. The contract should outline the fees to be paid by both the third-party vendor and the credit union. This includes any fixed compensation, variable charges, and any fees to be paid for nonrecurring items or special requests.

b. Address the cost and responsibility for purchasing and maintaining any equipment, hardware, software, or other items related to the activity, if applicable.

c. The contract should identify the party responsible for payment of any legal or audit expenses.

d. Compensation payment schedules should be structured to ensure performance and protect the credit union from payment before satisfactory completion. Bonuses or incentives for sales should be subject to quality performance.

[86] See also the discussion regarding establishment of contract signing policies in Section III(A)(17), above, and in the section on **Strategic Planning** (Section I(A)), also above.

4. Term and Termination:

a. Term:

(1) Specify the effective date and the anticipated termination date and how the contract can be renewed or terminated by either party.

(2) Automatic renewals should be avoided if possible. Such renewals are generally not in the credit union's best interest since the credit union may not be cognizant of the renewal date, and therefore may not realize that it has the opportunity to review the relationship until after the contract has automatically renewed.

(3) If a vendor requires a lengthy contractual term, such as three years, it is important that there be a justifiable business reason for this practice (e.g., the relationship would not become profitable for two years given the vendor's initial investment in physical assets specific to this contract). Explanations on the part of the vendor along the lines of "that's how we book revenue" should not be sufficient. A potential red flag is any agreement that carries an initial term of five years or greater.

b. Termination:

(1) The contract should state termination and notification requirements with enough notice—possibly as long as a year prior to the renewal date—to allow the credit union time to make an orderly conversion to another third-party vendor without excessive expense or operational risk.

(2) Termination rights prior to the end of the contract's term may include mutual agreement of the parties, a change in control of the third-party vendor, substantial increases in cost, failures to meet performance standards, breach or default of contract provisions, or insolvency or other items specific to the activity involved. Being able to terminate the contract within a relatively-short period of time, such as 30 days, will generally mitigate the credit union's risk to some degree.

(3) Breach or Default. The contract should specify that non-compliance with the terms and conditions of the contract will constitute default, identify specific remedies, and allow for a reasonable opportunity to cure a default.

c. Effect of Termination:

(1) The contract should address what happens when the agreement terminates (return of the credit union's data, records, and/or other resource, discontinuation of rights to use one another's trademarks, penalties for breach terminations, continued confidentiality, completion of payments due, etc.).

(2) Some contracts contain "liquidated damages" clauses (i.e. set breakup fees) that may require the credit union to pay up to the entire amount remaining on the contract even if the vendor no longer performs the service. Although business realities may require "liquidated damages" in some cases, it is important that these amounts be economically rational and not designed to be punitive. Generally, such clauses should only entitle the third-party vendor to its expected profits (rather than the entire fee that the credit union would have had to pay if the third-party had performed its obligations the contract). Otherwise a breached contract would be more profitable for the third-party vendor than actually performing the contract and incurring expenses.

d. Compliance with Applicable Laws: The contract should contain a requirement that the third-party vendor comply with all applicable laws, regulations, and regulatory guidance.

5. Indemnification of the credit union: Placing indemnification provisions that require a third-party vendor to hold the credit union harmless from liability as a result of negligence by the third-party vendor in the contract are advisable because such provisions may reduce the credit union's potential legal liability.

6. Limited Liability: Third parties may wish to contractually limit the amount of liability that they could incur as a result of the relationship with the credit union. Before agreeing to any limitation on the third-party vendor's liability, the credit union's management should carefully consider whether the proposed damage limitation is reasonable compared to the amount of loss the institution could experience should the third-party vendor fail to adequately perform.

Generally speaking, such limitations on third-party liability may not be in the credit union's best interest.

7. Evidence of current insurance coverage: The third-party vendor should provide reliable evidence of current insurance coverage (such as professional liability insurance) in an amount sufficient to protect the credit union's interests, especially under a set of circumstances where multiple other institutions also make insurance claims at the same time.

8. Subcontracting and Assignment: Permissibility/prohibition of the third-party vendor to subcontract or use another party to meet its obligations with respect to the contract, and notice/approval requirements. The contract should prohibit subcontracting, assignment, assumption, novation, and transfer of the contract and its obligation without approval of the credit union.

9. Relationship of Parties – Independent contractors, partners? This should be fully understood and documented. Partnership can involve shared liabilities. Independent contractor relationships limit responsibility and liability of the parties for one another and their employees.

10. Monitoring: Credit union should include specifics and rights for it to monitor the activities of the third-party vendor:

    a. Authorization for the credit union and the appropriate federal and state regulatory agency to have access to records of the third-party vendor if they are necessary or appropriate to evaluate compliance with laws, rules, and regulations.

    b. Authorization for the credit union to monitor and periodically review the third-party vendor for compliance with its agreement.

    c. Reporting/monitoring requirements should be specific and include the type and frequency of financial and other reports to be received from the third-party vendor.

    d. Reports may include performance reports, audits, financial reports, security compliance and business continuity testing testing reports.

    e. Management should also consider mandating exception-based reports that would serve as notification of any changes or problems that could affect the nature of the relationship or pose a risk to the credit union.

11. Warranties, Service Level Agreements (performance standards and measures):

    a. Performance Standards can be based upon industry standards for certain functions, or the credit union and the vendor can agree upon standards specific to their relationship.

    b. Management should periodically review the performance measures to determine if the objectives of the program are being achieved.

    c. Penalties for lack of performance should be described and a definition of “lack of performance” included.

12. Property Rights and Ownership:

    a. Intellectual Property – protect ownership and rights to name, logo, trademark and copyrighted material of the parties.

    b. Describe and protect ownership and control of any records generated by the third-party vendor.

    c. Use of software if appropriate in the future, including consideration of the need for putting software codes in escrow.

    d. If applicable, the contract should expressly address ownership of the resulting “know-how” from the relationship as well as all other forms of resulting intellectual property.

13. Audit Rights:

    a. Describe the rights and requirements of each party (including responsibility for payments).

    b. Credit unions should make sure that they have the right to audit third party vendors and their subcontractors as needed to monitor performance under the contract and ensure that periodic internal and/or external audits are conducted as appropriate.

    c. Credit unions should ensure that third-party vendor’s internal controls are appropriate and credit union should identify and require specific internal controls if those controls are material to the relationship.

    d. The degree of oversight necessary depends upon the degree of criticality of the relationship to the credit union’s operations.

    e. Consider—based upon the degree of criticality and risks related to the relationship, see **Key Concepts and Definitions**, above—whether to accept internal audits produced by the third-party vendor or to insist on

independent or external audits (such as SAS No. 70 reviews).

f. Audit reports should include a review of the third-party vendor's internal control program as it relates to the product or service. In addition, audit reports should also include reviews of the third-party vendor's security program and business continuity program.

14. Data Security and Member Confidentiality:

a. The contract should require the third-party vendor to report any breaches in the security and confidentiality of information.

b. Except as necessary to perform the functions designated by the contract, the third-party vendor and its agents should be prohibited from using or disclosing financial, personal, and other sensitive information about the credit union and its members.

c. The contract should specify that any nonpublic personal information about the credit union's members must be handled in a manner consistent with the credit union's own privacy policy, and also in accordance with applicable privacy laws and regulations.

d. The contract should allocate liability for data breach costs and data breach-related losses to members to the third-party vendor.

15. Business continuity planning and disaster preparedness:

a. The contract should address the third-party vendor's responsibility for continuation of services in the event of an operational failure.

b. The third-party vendor should maintain disaster recovery and contingency plans with sufficiently detailed operating procedures.

c. If possible, results of testing of the vendor's disaster recovery and contingency plans should be provided to the credit union.

16. Member Complaint and Service Issues:

a. The contract should specify how the parties will respond to any complaints received by the third-party vendor from members of the credit union. The credit union's reputation would generally be best protected if the credit union plays a direct role in dealing with member complaints.

b. If the third-party vendor is responsible for such responses, the contract should also provide for the credit union to receive copies of all complaints and responses as well as

periodic summary reports detailing the status and resolution of complaints.

17. Dispute Resolution: The credit union should consider whether the contract should include a dispute resolution process—such as binding arbitration—for the purpose of resolving problems expeditiously. Continuation of the arrangement between the parties during a dispute should also be addressed. Note that arbitration is a double-edged sword and that reliance upon the U.S. court system is often preferable to arbitration because court decisions can be appealed.

18. Choice of Governing Law and Choice of Venue Clauses:

    a. Depending upon the circumstances, it may be appropriate for the contracts to specify which court (i.e. venue) will hear a dispute and what law will be applied by that court (e.g., based on the contract's "Choice of Law" provision, a Connecticut court could be required to apply Indiana law).

    b. Consider insisting on a venue that is conveniently located for you (such as one located near your credit union's home office) and on local law (which both the judge and your lawyer will be most familiar with, and therefore will be less likely to misinterpret) unless you have a good reason to do otherwise.

D. NCUA's Questionnaire Related to Contracts

The following questions are taken directly from the NCUA ARIES Questionnaire and should be answered as part of your third-party vendor relationship analysis related to Contracts.

Due Diligence – Contract Issues and Legal Review

1. Does the credit union's third-party contract(s) address the following areas:
   (a) Scope of arrangement, services offered, and activities authorized;
   (b) Responsibilities of all parties (including subcontractor oversight);
   (c) Service level agreements addressing performance standards and measures;
   (d) Performance reports and frequency of reporting;
   (e) Penalties for lack of performance;
   (f) Ownership, control, maintenance and access to financial and operating records;
   (g) Ownership of servicing rights;
   (h) Audit rights and requirements (including responsibility for payment);
   (i) Data security and member confidentiality (including testing and audit);
   (j) Business resumption or contingency planning;
   (k) Evidence of current insurance coverage;
   (l) Member complaints and member service;

(m)Compliance with regulatory requirements (i.e., Gramm-Leach-Bliley Act (GLBA), Privacy, BSA, etc.);
(n) Dispute resolutions; and
(o) Default, termination and escape clauses.

b. Did the credit union obtain an independent legal opinion about any services provided by the third-party under the arrangement?

c. Did the credit union ensure the third-party is compliant with state and federal laws and regulations and is contractually bound to comply with applicable laws (i.e., Regulation B, Regulation Z, HMDA, etc.)?

IV. RISK MANAGEMENT, MONITORING AND CONTROL OF THIRD-PARTY VENDOR RELATIONSHIP

Not only should due diligence be performed prior to selecting a third-party vendor, but also periodically during the course of the relationship, particularly when considering a renewal of a relationship contract. Annual review of critical third-party vendor relationships, as well as review when there is a material change in a relationship, are recommended for critical vendors and may be required for some programs, such as member business lending.[87]

Please also consult the responsibilities of the credit union's board of directors and management in the "Key Concepts" section, above.

A. Risk Management, Monitoring and Control Programs:

1. Policies/Procedures
    a. Develop policies/procedures that outline expectations and limitations of third-party vendor relationship (to limit control of program growth).
2. Risk Measurement and Monitoring
    a. Set up a program to measure/monitor risk of third-party vendor relationships and report findings to management.
    b. Measure third-party vendor performance in terms of profitability, benefit and service delivery.
    c. Set up internal controls sufficient to assist in the measurement and monitoring of third-party vendor risk.
    d. Remember, a credit union is always responsible for continued safety and soundness of outsourced functions.
    e. Create an oversight program to monitor each third-party vendor's internal controls, condition, and performance.
    f. Assign responsibility for oversight to personnel with "appropriate expertise" to monitor and manage each third-party vendor relationship.
3. Control Systems and Reporting
    a. Implement ongoing internal controls over third-party vendor relationships to mitigate risks.
    b. Establish internal controls/audit functions sufficient to assure it that the third-party vendor is appropriately safeguarding assets, producing reliable reports and following the terms of the third-party vendor agreement.

[87] *See* NCUA, "Evaluating Third Party Relationships," Supervisory Letter No. 07-01 (2007) (enclosed with Letter to Credit Unions No. 07-CU-13); NCUA, "e-Commerce Guide for Credit Unions," NCUA Publication No. 8072, at 20 (2002) (enclosed with Letter to Credit Unions No. 02-CU-17); *see also* FDIC, "Guidance for Managing Third-Party Risk," FIL-44-2008, at 9-10 (2008).

1) If available, review SAS No. 70 (Type II) audit reports. If SAS No. 70 (Type II) reports are not available, it may be prudent under some circumstances (such as with high-risk relationships, *see* Section I.C, above) to require another form of internal review of the third-party vendor's internal controls. [88]

c. Set aside adequate resources to ensure an effective third-party vendor management program is in place (designated, qualified staff and monetary resources).

d. Implement effective and secure method of communication with third-party vendor.

e. The credit union's performance monitoring should include the following (as they are applicable):

1) Evaluating the overall effectiveness of the third-party vendor relationship, as well as whether it is consistent with the credit union's strategic goals.

2) Review the third-party vendor's license(s) or registration(s) to ensure that the third-party vendor can legally perform its services.

3) Evaluate the third-party vendor's financial condition at least annually.

4) Monitor the adequacy of the third-party vendor's insurance coverage.

5) Determine whether the third-party vendor's financial obligations to others are consistently being met.

6) Review audit reports or other reports of the third-party vendor, and follow up on any needed corrective actions.

7) Review the adequacy and adherence to the third-party vendor's policies relating to internal controls and security issues.

8) Monitor for compliance with applicable laws, rules, and regulations.

9) Review the third-party vendor's business continuity planning and testing.

10) Assess the effect of any changes in key third-party vendor personnel involved in the relationship with the financial institution.

11) Review reports relating to the third-party vendor's performance in the context of contractual requirements and

[88] *See* NCUA, "Evaluating Third Party Relationships," Supervisory Letter No. 07-01, at 6 (2007) (enclosed with Letter to Credit Unions No. 07-CU-13).

performance standards, with appropriate follow-up as needed.

12) Determine the adequacy of any training provided to employees of the financial institution and the third-party vendor.

13) Review customer complaints about the products and services provided by the third-party vendor and the resolution of the complaints.

14) Meet as needed with representatives of the third-party vendor to discuss performance and operational issues.

B. Indirect Lending Risk Management Considerations

NCUA's guidance on mortgage brokers and loan correspondents[89] makes recommendations regarding indirect lending relationship monitoring that are generally applicable to most indirect lending relationships:

"Whenever a credit union outsources a function, it is relinquishing some level of control over that function. To adjust for the lack of direct oversight over outsourced transactions and services, compensating controls need to be implemented over the life of the third-party relationship. When dealing with mortgage brokers and correspondents, compensatory controls need to ensure:

- Adherence to board established lending policies and risk parameters.[90] A sufficient sample of loans, underwritten by a broker or correspondent must be reviewed for compliance with board policies, applicable regulations, and written agreements to ensure that ongoing loan quality is maintained. Additional targeted loan reviews should be performed based on any performance concerns of a third-party such as increasing default rates, foreclosure rates, complaints, and higher than average fees charged to borrowers.
- Loan approval authority, in the use of a mortgage broker, is not delegated to the broker, and that all loan underwriting criteria and subsequent modifications are approved by the credit union.[91]
- Broker and correspondent reports are accurate, timely, and contain sufficient detail to adequately monitor activity.

[89] *See* NCUA, "Third-Party Relationships: Mortgage Brokers and Correspondents," Letter to Credit Unions No. 08-CU-19, at 2 (2008).

[90] "Board policies need to address such issues as: frequent, sequential refinancings with little to no economic benefit to the borrower, negatively amortizing loans, prepayment penalties that are not limited to the early years of the loans, financing points, fees, penalties, and other charges, allowing non-owner occupied property financing, and balloon payments in short-term transactions." *Id.* at 4 n.6.

[91] "Delegation of those authorities to a third-party would be a violation of §113 of the FCU Act for federal credit unions, and an unsafe and unsound practice for all federally-insured credit unions, which could be subject to possible NCUA action under §206 of the FCU Act." *Id.* at 4 n.7.

If ongoing credit or documentation problems are discovered, the credit union should take appropriate action, which could include modification of contract terms or terminating the relationship."[92]

C. NCUA's Questionnaire Related to Risk Management, Monitoring, and Control

The following questions are taken directly from the NCUA ARIES Questionnaire and should be answered as part of your third-party vendor relationship analysis during the Risk Management, Monitoring and Control stage.

Background

1. *Does the credit union maintain a list of the third-party company(ies) or firm(s) which they use for outsourced services?*

2. *Does the credit union maintain a description of the services provided by the third-party company(ies) or firm(s)?*

Risk Measurement, Monitoring and Control

1. *Are reports prepared on a monthly basis adequately reflecting the amount of activity with the third-party and providing sufficient information to properly monitor the activities?*

2. *Are informative summary reports provided to senior management or the board of directors?*

3. *Has the credit union assigned appropriate staff to oversee the third-party relationship to monitor performance and compliance with contracts?*

4. *If the third-party originates member transactions, does the credit union verify the transactions with the member?*

5. *If the third-party services member accounts, does the credit union receive periodic reports of any activity?*
   (a) Are reports received and reviewed timely?
   (b) Do the reports contain sufficient information to determine how the portfolio is performing?
   (c) Do report balances agree with the credit union's records?

6. *Does the credit union control account verifications?*

7. *Does the credit union verify the third-party's reports are accurate?*

[92] NCUA, "Third-Party Relationships: Mortgage Brokers and Correspondents," Letter to Credit Unions No. 08-CU-19, at 4 (2008).

8. *If the third-party services loans, does the credit union verify that member payments are remitted to the credit union in compliance with the contract?*
   (a) Are funds received by the servicer required to be deposited in a trust account on the credit union's behalf or does the servicer use a third-party "retail lockbox"?
   (b) Are reports received showing returned or bounced payments are reversed, the loan re-aged, and any servicing fees reversed?

9. *Does the credit union have the infrastructure (staffing, equipment, technology, etc.) in place to sufficiently monitor the third-party arrangement?*

10. *Has the credit union established appropriate internal controls to ensure internal staff is following policy guidance for third-party relationships?*

11. *Do the credit union's policies appropriately address the third-party relationship?*

12. *Do policies place limits on the activity of the third parties?*

13. *Has the credit union established lists of approved parties?*

Controls Over Member Data

1. *How does the credit union communicate with the third-party?*

2. *Does the communication method ensure member data is protected?*

Appendices

APPENDIX A: Official Sources of Guidance

National Credit Union Administration

NCUA, "Third-Party Relationships: Mortgage Brokers and Correspondents," Letter to Credit Unions No. 08-CU-19 (2008), *available at* http://www.ncua.gov/letters/2008/CU/08-CU-19docx%20(2).pdf

NCUA, "Evaluating Third Party Relationships," Supervisory Letter No. 07-01 (2007) (enclosed with Letter to Credit Unions No. 07-CU-13), *available at* http://www.ncua.gov/letters/2007/CU/07-CU-13.pdf

NCUA, "Specialized Lending Activities - Third-Party Subprime Indirect Lending and Participations," Risk Alert No. 05-RISK-01 (2005), *available at* http://www.ncua.gov/RiskAlert/2005/05-RISK-01.pdf

NCUA, "Specialized Lending Activities," Letter to Credit Unions No. 04-CU-13 (2004, *available at* http://www.ncua.gov/letters/2004/04-CU-13.doc

NCUA, "Weblinking: Identifying Risks & Risk Management Techniques," Letter to Credit Unions No. 03-CU-08 (2003), *available at* http://www.ncua.gov/letters/2003/03-CU-08.doc

NCUA, "e-Commerce Guide for Credit Unions," NCUA Publication No. 8072 (2002) (enclosed with Letter to Credit Unions No. 02-CU-17), *available at*

NCUA, "Account Aggregation Services," Letter to Credit Unions No. 02-CU-08 (2002), *available at* http://www.ncua.gov/letters/2002/02-CU-08.html

NCUA, "Weblinking Relationships," Letter to Federal Credit Unions No. 02-FCU-04 (2002), *available at* http://www.ncua.gov/letters/2002/02-FCU-04.html

NCUA, "Due Diligence Over Third Party Service Providers," Letter to Credit Unions No. 01-CU-20 (2001), *available at* http://www.ncua.gov/letters/2001/01-CU-20.pdf

NCUA, "Risk Management of Outsourced Technology Sources," Letter to Credit Unions No. 00-CU-11(2000), *available at* http://www.ncua.gov/letters/2000/00-CU-11.pdf

NCUA Rules and Regulations, Parts 701 and 741, *available at* http://www.ncua.gov/RegulationsOpinionsLaws/rules_and_regs/rules_and_regs.html

Other Depository Institution Regulators

Federal Deposit Insurance Corporation, "Guidance for Managing Third-Party Risk," FIL-44-2008 (2008), *available at* http://www.fdic.gov/news/news/financial/2008/fil08044a.html

Federal Deposit Insurance Corporation,
“Supervisory Insights: Third Party Arrangements: Elevating Risk Awareness” (2007), *available at* http://www.fdic.gov/

Office of Thrift Supervision, Thrift Bulletin 82 (2003), *available at* http://www.ffiec.gov/ffiecinfobase/resources/outsourcing/ots-tb_82_3rd_party_arrang.pdf

Office of the Comptroller of the Currency, OCC Bulletin 2001-47 (2001), *available at* http://www.ffiec.gov/ffiecinfobase/resources/outsourcing/occbul_2001_47_third_party_relationships.pdf

Office of the Comptroller of the Currency, “Third-Party Risk,” OCC Advisory Letter No. AL-2000-9 (2000), *available at* www.occ.treas.gov/ftp/advisory/2000-9.txt

APPENDIX B: NCUA Supervisory Letter No. 07-01 and NCUA Letter to Credit Unions No. 01-CU-20

SUPERVISORY LETTER

NATIONAL CREDIT UNION ADMINISTRATION
OFFICE OF EXAMINATION AND INSURANCE
1775 DUKE STREET, ALEXANDRIA, VA 22314

DATE: October 2007 **Supervisory Letter No.: 07-01**

TO: All Field Staff

SUBJECT: Evaluating Third Party Relationships

To expand services and product offerings, credit unions increasingly outsource functions and programs through collaboration with third parties. Developing sound third party relationships and alliances can assist credit unions in meeting their strategic objectives. Properly leveraging the skills and experience of qualified third parties may enable credit unions to:

- Provide access to products and services through expanded delivery channels;
- Offer more cost-effective products and services; and
- Manage programs that would not be feasible without external expertise.

In many cases, third party relationships are essential in enabling credit unions to become their members' primary financial institution, While inadequately managed and controlled third party relationships can result in unanticipated costs, legal disputes, and financial loss, NCUA's role as a regulator and insurer is not to stifle the innovative use of third party relationships to meet member needs and strategic objectives. NCUA's goal is to ensure credit unions clearly understand risks they are undertaking and balance and control those risks considering the credit union's safety and members' best interests.

NCUA has previously issued several pieces of relevant guidance on managing third party risk and due diligence in recent years. Additionally, in June of 2006, NCUA amended NCUA Rules and Regulations, Parts 701 and 741, to address *Third Party Servicing of Indirect Vehicle Loans.* This letter sets forth supervisory principles derived and adapted from guidance issued by NCUA and other federal regulatory agencies.[93]

This Supervisory Letter summarizes existing guidance and regulations, and discusses the appropriate evaluation of third party relationships where credit unions outsource key business functions. If you have any questions on this issue, please direct them to your immediate supervisor or regional management.

Sincerely,

David M. Marquis,
Director, Office of Examination and Insurance

[93] Resources consulted on third party relationships are referenced in Appendix B of this Supervisory Letter.

Supervisory Letter

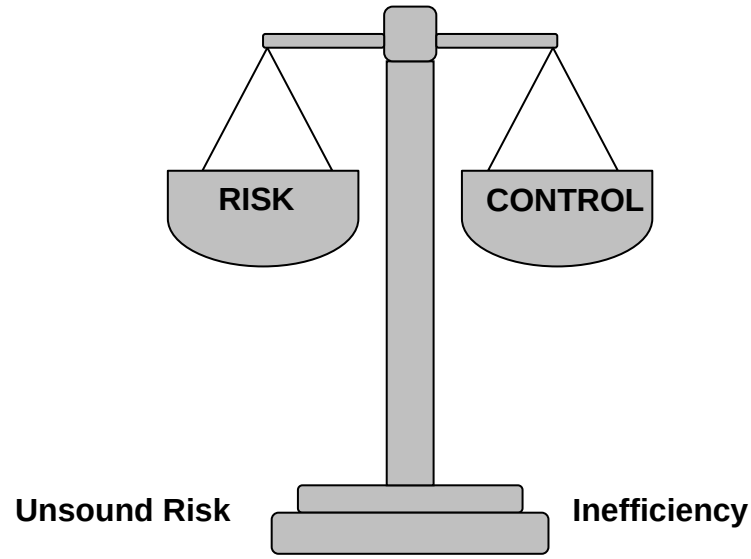
Evaluating Third Party Relationships

Third Party Relationships

In recent years, credit unions have increasingly developed third party relationships to meet strategic objectives and enhance member services. Properly managed and controlled third party relationships provide a wide range of potential benefits to credit unions and their members. Many credit unions have utilized third party arrangements to gain expertise, realize economies of scale, or even reach new members. Leveraging the talents and experience of third parties can assist credit unions in meeting their members' needs while accomplishing their strategic goals. In some cases, third party relationships are critical to the on-going success of a credit union. Credit unions taking the time to properly evaluate and cultivate their participation in third party arrangements can experience a high degree of success.

Collaboration with third parties has become more prevalent in credit unions due to increasing complexity of services and competitive pressures. In some third party arrangements, credit unions surrender direct control over one or more key business functions to a third party in exchange for potential benefits. As credit unions consider the potential benefits of third party arrangements, credit union officials and management (officials) are faced with a balancing act.

Officials must carefully consider the potential risks these relationships may present and how to manage them. As credit unions seek to manage risk, they should carefully consider the correlation between their level of control over business functions and the potential for compounding risks. Credit unions maintaining complete control over all functions may be operationally or financially inefficient. Credit unions outsourcing functions without the appropriate level of due diligence and



oversight may be taking on undue risk. [94] Ultimately, credit unions are responsible for safeguarding member assets and ensuring sound operations irrespective of whether or not a third party is involved.

Outsourcing complete control over one or more business functions to a third party amplifies the risks inherent in those functions. Additionally, credit unions trading direct control over business functions for third party program benefits may expose themselves to a full range of risks including credit, interest rate, liquidity, transaction, compliance, strategic, and reputation risks. Credit unions must complete the due diligence necessary to ensure the risks undertaken in a third party relationship are acceptable in relation to their risk profile and safety and soundness requirements. Less complex risk profiles and third party arrangements typically require less analysis and documentation. Further, where credit unions have a longstanding and tested history of participating in a given third party relationship, less analysis is required to renew the relationship.

Risks may be mitigated, transferred, avoided, or accepted; however, they are rarely eliminated. The risk management process involves identifying and making informed decisions about how to address risk. One of the best ways to employ the risk management process is to start small and gain experience over time. Less complex credit unions unfamiliar with analyzing third party arrangements may utilize this risk management approach by entering third party relationships with small, well-defined goals and expanding their exposure to third party risks as their experience grows.

When evaluating third party arrangements, examiners should ensure credit unions have addressed the following concepts in a manner commensurate with their size, complexity, and risk profile:

- Risk Assessment and Planning;
- Due Diligence; and
- Risk Measurement, Monitoring and Control.

The remainder of this Supervisory Letter outlines considerations for these concepts. The considerations discussed are not an exhaustive list of all possible risk mitigation procedures, but a representation of the considerations necessary when credit unions engage in significant third party relationships. The depth and breadth of due diligence required depends upon a credit union's complexity and risk management process. Smaller or less complex credit unions may develop alternative methods of accomplishing due diligence, while credit unions utilizing a time tested third party relationship may already have addressed these considerations over time.

[94] Due diligence is the systematic, on-going process of analyzing and evaluating new strategies, programs, products, or operations to prepare for and mitigate unnecessary risks.

Risk Assessment and Planning Considerations for Third Party Relationships

Credit union officials are responsible for planning, directing, and controlling the credit union's affairs. Risk assessment and due diligence for third party relationships is an important part of officials' fiduciary responsibilities. Examiners should consider the following elements in evaluating the adequacy of credit unions' risk assessment and due diligence over third party relationships:

Planning and Initial Risk Assessment

Before entering into a third party relationship, officials should determine whether the relationship complements their credit union's overall mission and philosophy. Officials should document how the relationship will relate to their credit union's strategic plan, considering long-term goals, objectives, and resource allocation requirements. Officials should design action plans to achieve short-term and long-term objectives in support of strategic planning for new third party arrangements. All planning should contain measurable, achievable goals and clearly defined levels of authority and responsibility.

Additionally, officials should weigh the risks and benefits of outsourcing business functions with the risks and benefits of maintaining those functions in-house. In order to demonstrate an understanding of a third party relationship's risk, the officials must clearly understand the credit union's strengths and weaknesses in relation to the arrangement under consideration. Credit unions should complete a risk assessment prior to engaging in a third party relationship to assess what internal changes, if any, will be required to safely and soundly participate.

Risk assessments are a dynamic process, rather than a static process, and should be an on-going part of a broader risk management strategy. Credit unions' initial risk assessments for a third party relationship should consider all seven risk areas (Credit, Interest Rate, Liquidity, Transaction, Compliance, Strategic, and Reputation), and more specifically the following:

- **Expectations for Outsourced Functions**- Credit unions should clearly define the nature and scope of their needs. Which needs will the third party meet? Will the third party be responsible for desired results? To what extent?

- **Staff Expertise**- Is credit union staff qualified to manage and monitor the third party relationship? How much reliance on the third party will be necessary?

- **Criticality**- How important is the activity to be outsourced? Is the activity mission critical? What other alternatives exist?

- **Risk-Reward or Cost-Benefit Relationship**- Does the potential benefit of the arrangement outweigh the potential risks or costs? Will this change over time?

- **Insurance-** Will the arrangement create additional liabilities? Is credit union insurance coverage sufficient to cover the potentially increased liabilities? Will the third party carry "key man" insurance or other insurance to protect the credit union?

- **Impact on Membership-** How will officials gauge the positive or negative impacts of the arrangement on credit union members? How will they manage member expectations?

- **Exit Strategy-** Is there a reasonable way out of the relationship if it becomes necessary to change course in the future? Is there another party that can provide any services officials deem critical?

Risk assessments for less complex third party arrangements may be part of a broader risk management program or documented in board minutes.

Financial Projections

In evaluating the cost-benefit or risk-reward of a third party relationship, credit unions should develop financial projections outlining the range of expected and possible financial outcomes. Credit unions should project a return on their investment in the proposed third party arrangement, considering expected revenues, direct costs, and indirect costs. For example, when outsourcing loan functions, credit unions should not only consider the expected loan yield, but also the potential effect of borrower prepayments and third party fees on the overall return.

Officials should evaluate financial projections in the context of their overall strategic plans and asset-liability management framework before making a decision to participate in a third party arrangement. Examiners should evaluate these projections for reasonableness, considering historical performance, underlying assumptions, stated business plan objectives, and the complexity of the credit union's risk profile.

Due Diligence for Third Party Relationships

When considering third party relationships, proper due diligence includes developing a demonstrated understanding of a third party's organization, business model, financial health, and program risks. In order to tailor controls to mitigate risks posed by a third party, credit unions must have an understanding of a prospective third party's responsibilities and all of the processes involved with prospective third party programs. Examiners should consider the adequacy of due diligence in the areas below, given credit unions' risk profiles, internal controls, and overall complexity. Due diligence should be tailored to the complexity of the third party relationship and may consist of reasonable alternative procedures to accomplish acceptable risk mitigation.

Background Check

Credit unions should consider a third party's experience providing the proposed service or program. A well-respected third party may have little or no experience implementing and supporting a new service offering. In these cases, the qualifications, competence, and training of key individuals within the third party's organization become even more important to verify. While it would be tempting to rely solely upon the vendor's reputation alone, a more prudent practice would be to verify the expertise the vendor has obtained to provide this new service.
It is also important for credit unions to understand how a third party has performed in other relationships before entering into a third party arrangement. Credit unions should request referrals from the prospective third party's clients to determine their satisfaction and experience with the proposed arrangement. Credit unions should also review and consider any lawsuits or legal proceedings involving the third party or its principals. Additionally, credit unions should ensure that third parties or their agents have any required licenses or certifications, and that they remain current for the duration of the arrangement. Finally, sources of information such as the Better Business Bureau, Federal Trade Commission, credit reporting agencies, state consumer affairs offices, or state attorney general offices may also offer insight to a third party's business reputation.

Business Model

New business models often emerge due to changes in the regulatory, technological, or economic environment. When evaluating a prospective third party arrangement, credit union officials should consider the longevity and adaptability of third party business models. Some business models may be well suited for economic expansion, but untenable during economic recession. Since new business models are not time tested and have not experienced a complete economic cycle, they may present additional risks to a credit union. Likewise, longstanding business models that cannot easily adapt may not be sustainable in times of rapid technological or regulatory change.

Before entering into a third party arrangement, credit union officials should thoroughly understand the third party's business model. The third party's business model is simply the conceptual architecture or business logic employed to provide services to its clients. If the third party's business and marketing plans are available, officials should review them. Credit union officials should also 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. Examiners should assess credit union officials' understanding and consideration of key third party business models as an integral element of due diligence.

Credit union officials should also understand the third party's sources of income and expense, considering any conflicts of interest that may exist between the third party and the credit union. For example, if a third party's revenue stream is tied to the volume of loan originations rather than loan quality, its financial interest in underwriting as many

loans as possible may conflict with the credit union's interest in originating only quality loans. Credit unions should also identify any vendor related parties (such as subsidiaries, affiliates, or subcontractors) involved with the proposed arrangement and understand the purpose and function of each.[95] Examiners should consider the potential effects of identified conflicts of interest and ensure officials mitigate risks where reasonable.

Cash Flows

Perhaps one of the most important considerations, when analyzing a potential third party relationship, is the determination of how cash flows move between all parties in a proposed third party arrangement. In addition to third party fees, premiums, and claims receipts, many third party arrangements include cash flows between the credit union, the third party, and credit union members. Credit union officials should be able to explain how cash flows (both incoming and outgoing) move between the member, the third party, and credit unions. Credit unions should also be able to independently verify the source of these cash flows and match them to related individual accounts. Examiners should ensure credit unions are tracking and identifying cash flows accurately.

Financial and Operational Control Review

Credit unions should carefully review the financial condition of third parties and their closely related affiliates. The financial statements of a third party and its closely related affiliates should demonstrate an ability to fulfill the contractual commitments proposed. Credit unions should consider the financial statements with regard to outstanding commitments, capital strength, liquidity, and operating results. Additionally, credit unions should consider any potential off-balance sheet liabilities and the feasibility that the third party or its affiliated parties can financially perform on such commitments.

Audited and segmented financial statements or ratings from nationally recognized statistical rating organizations (NRSRO ratings) may be useful in periodically evaluating the overall financial health of a prospective or existing third party.[96] If available, officials may use copies of SAS 70 (Type II) reports prepared by an independent auditor, audit results, or regulatory reports to evaluate the adequacy of the proposed vendor's internal controls. If these items are not available, credit unions should consider whether to require an independent review of the proposed vendor's internal controls. Generally, contracts establish requirements for periodic audits or access to third party records. Examiners should ensure credit unions have adequately reviewed the financial and internal control structure of the prospective third party, considering credit unions' risk profiles and the arrangement's relationship to net worth.

[95] Further due diligence may be required of some of these related parties if they play a critical role in providing the credit union with the proposed service.

[96] Officials should consider the independence of audits or ratings reviewed.

Contract Issues and Legal Review

Contracts outlining third party arrangements are often complex. Credit unions should take measures to ensure careful review and understanding of the contract and legal issues relevant to third party arrangements. It is prudent to seek qualified external legal counsel to review prospective third party arrangements and contracts. Any legal counsel consulted should be independent and have the experience or specialization necessary to review properly the arrangements and contracts.

Typically, at a minimum, third party contracts should address the following:

- Scope of arrangement, services offered, and activities authorized;
- Responsibilities of all parties (including subcontractor oversight);
- Service level agreements addressing performance standards and measures;
- Performance reports and frequency of reporting;
- Penalties for lack of performance;
- Ownership, control, maintenance and access to financial and operating records;
- Ownership of servicing rights;
- Audit rights and requirements (including responsibility for payment);
- Data security and member confidentiality (including testing and audit);
- Business resumption or contingency planning;
- Insurance;
- Member complaints and member service;
- Compliance with regulatory requirements (e.g. GLBA, Privacy, BSA, etc.);
- Dispute resolution; and
- Default, termination, and escape clauses.

Of particular importance, credit unions should exercise their right to negotiate contract terms with third parties for mutually beneficial contracts. For example, some credit unions have entered into third party agreements with significant buyout or termination penalties, believing the penalties or fees were standard or non-negotiable. In many cases, early termination, escape clause, and default terms are negotiable. Credit union officials should ensure that any contract terms agreed to would not adversely affect the credit union's safety and soundness, regardless of contract performance.

In addition to a legal review of contracts and written agreements relevant to a prospective third party arrangement, it may be prudent for credit unions to obtain a legal opinion about any services provided by the third party under the arrangement. For example, if a third party is engaged to perform loan collections for the credit union, a legal review of their collection methods may be prudent to ensure debt collection and reporting practices comply with applicable state and federal laws. Credit unions should ensure compliance with state and federal laws and regulations, and contractually bind the third party to compliance with applicable laws (i.e. Regulation B, Regulation Z, HMDA, etc.). Since credit unions may ultimately be responsible for consumer compliance violations committed by their agents, credit unions should be familiar with

the third party's internal controls for ensuring regulatory compliance and adherence to agreed upon practices.

Accounting Considerations

Credit unions should consider that third party relationships might create accounting complexities. Credit unions must have adequate accounting infrastructures to appropriately track, identify, and classify transactions in accordance with Generally Accepted Accounting Principles (GAAP). Credit unions often develop third party arrangements to outsource new products or functions, and may not have experience in accounting for the particulars of those new products or functions. Conversely, although credit unions may be familiar with the accounting rules for a given function, the nature of a third party arrangement may change the required accounting procedures.

In some instances, a certified public accountant's guidance may be necessary to ensure proper accounting treatment. A credit union's audit scope should provide for independent reviews of third party arrangements and associated activities. Examiners should ensure credit unions have considered the accounting implications of new products or services introduced through third party arrangements.

Risk Measurement, Monitoring and Control of Third Party Relationships

In addition to careful due diligence when entering third party arrangements, credit unions must establish ongoing expectations and limitations, compare program performance to expectations, and ensure all parties to the arrangement are fulfilling their responsibilities. Third party arrangements and risk profiles will vary; thus, credit unions should tailor risk mitigation efforts to the specific nature of considered programs, the materiality of risks identified, and the credit union's overall complexity. Examiners should consider the adequacy of the credit union's policies, risk measurement, and monitoring in light of the same factors.

Policies and Procedures

Credit unions should develop detailed policy guidance sufficient to outline expectations and limit risks originating from third party arrangements. Policies and procedures should outline staff responsibilities and authorities for third party processes and program oversight. Additionally, policy guidance should define the content and frequency of reporting to credit union management and officials. **Credit unions should also establish program limitations to control the pace of program growth and allow time to develop experience with the program.** For example, credit unions participating in third party loan programs should initially limit the volume of loans granted in order to identify any problems with the third party process prior to the volume of loans becoming significant.

Risk Measurement and Monitoring

Credit unions must be able to measure the risks of third party programs, but also the performance of third parties in terms of profitability, benefit, and service delivery. For example, credit unions outsourcing loan servicing functions should be able to identify individual loan characteristics, repayment histories, repayment methods, delinquency status, and any loan file maintenance relative to serviced loans. To the extent that credit unions rely on the third party to provide this type of measurement information, clear controls should be contractually established and subject to periodic independent testing to ensure the accuracy of the information. Examiners should ensure that credit unions are measuring the performance of third party arrangements and periodically verifying the accuracy of any information provided to them by a third party or its affiliate.

Credit unions engaging in third party relationships must have an infrastructure (i.e. staffing, equipment, technology, etc.) sufficient to monitor the performance of third party arrangements. In many cases, credit unions outsource processes or functions due to a lack of internal infrastructure or experience. However, outsourcing processes or functions does not eliminate credit union responsibility for the safety and soundness of those processes and functions. Examiners should ensure officials demonstrate the knowledge, skills, and abilities necessary to monitor and control third party arrangements.

Control Systems and Reporting

After credit unions have conducted internal risk assessments and due diligence over prospective third parties, they must implement on-going controls over third party arrangements to mitigate risks. While control systems need not be elaborate for less complex third party arrangements, credit unions are ultimately responsible for establishing internal controls and audit functions reasonably sufficient to assure them that third parties are appropriately safeguarding member assets, producing reliable reports, and following the terms of the third party arrangement. Additionally, credit unions should tailor internal controls as necessary to ensure staff observes policy guidance for third party relationships. Examiners should ensure credit unions have on-going risk management procedures with regard to any material third party relationship.

Designated credit union staff should be qualified and responsible for continued monitoring and oversight of third party arrangements, exhibiting familiarity with and understanding of the reports available from the third party. Responsible staff should measure the performance of third party programs in relation to credit union policy guidance, contractual commitments, and service levels. Credit unions should implement quality control procedures to review the performance of third parties periodically. Credit union officials should receive periodic reports on the performance of all material third party programs. Examiners should ensure controls are in place, and that management and officials receive periodic reports with information sufficient to assist them in evaluating the performance of the overall arrangement and the adequacy of reserves.

Summary

Third party relationships can be invaluable to credit unions and credit union members. Properly managed third party relationships can allow credit unions to accomplish strategic objectives through increased member service, competitiveness, and economies of scale. However, outsourcing critical business functions increases the risk inherent in those functions. Credit unions are responsible for safeguarding member assets and ensuring sound operations irrespective of whether or not a third party is involved. Smaller or less complex credit unions may have to develop alternative methods of accomplishing due diligence. Examiners should ensure credit unions adequately address risk assessment, planning, due diligence, risk measurement, risk monitoring, and controls when involved in third party relationships.[97]

APPENDIX A

Third Party Relationships- Areas for Consideration

Risk Assessment and Planning

- ✓ **Planning-** Third party arrangements should be synchronized with strategic plans, business plans, and credit unions' philosophies.

- ✓ **Risk Assessment-** Dynamic process should consider the seven areas of risk as well as expectations of the arrangement, staff expertise, criticality of function, cost-benefit, insurance requirements, member impact, and exit strategy.

- ✓ **Financial Projections-** Return on investment should be estimated considering revenue, direct costs, indirect costs, fees, and likely cash flow stream. Return should be considered relative to the credit unions' strategic plans and asset-liability frameworks.

Due Diligence

- ✓ **Background Check-** Credit unions should consider references, prior performance, licensing and certification, and any legal proceedings involving prospective third parties, key individuals of the third party's organization. Credit unions should also consider third party motivations.

- ✓ **Business Model-** Credit unions must understand business logic of the third party arrangement and business model, as well as third party processes and related affiliates.

- ✓ **Cash Flows-** Credit unions must demonstrate an understanding of incoming and outgoing cash flows, and be able to independently verify sources of cash flows in third party programs.

[97] See Appendix A.

- ✓ **Financial and Operation Control Review-** Credit unions must review the overall financial condition of third parties and their closely related affiliates, as well as the state of operational controls in the third party's business model.

- ✓ **Contract Issues and Legal Review-** Credit unions should generally have legal counsel with appropriate expertise and experience review contracts and third party arrangements to ensure equitable contracts and compliance with applicable state and federal laws and regulations.

- ✓ **Accounting Considerations-** Credit unions should be prepared for potential accounting complexity and may need a CPA opinion on accounting for third party relationship activities.

Risk Measurement, Monitoring and Control

- ✓ **Staff Oversight and Quality Control-** Credit unions should have qualified staff designated to oversee and control the quality of the third party relationships.

- ✓ **Policies and Procedures-** Policy guidance must be in place and sufficient to control the risks of the third party relationship. Policy guidance should address responsibilities, oversight, program and portfolio limitations, and content and frequency of reporting.

- ✓ **Monitoring and Reporting-** Adequate infrastructure is required to support monitoring and reporting outlined in policy guidance. Credit unions should be able to measure and verify the performance of third parties and third party programs.

[The editors of this Guide have omitted "Appendix B" to Supervisory Letter 07-01 because the sources of regulatory guidance contained therein are listed in "Appendix A" to this Guide, on pages 56 to 57 above.]

NCUA LETTER TO CREDIT UNIONS

NATIONAL CREDIT UNION ADMINISTRATION
1775 Duke Street, Alexandria, VA

DATE: November 2001 LETTER NO.: 01-CU-20

TO: All Federally Insured Credit Unions

SUBJ: Due Diligence Over Third Party Service Providers

Credit unions are increasingly partnering with outside parties to enhance the services provided to members. This is especially true in the lending arena where third-party relationships are opening the doors to less traditional programs such as leasing, indirect lending, and risk-based lending (also referred to as sub-prime lending). These arrangements can make programs more cost-effective, enable credit unions access to expertise that has not been developed in-house, and promote programs that may not be feasible if entered into independently. However, we are also aware of cases of third-party relationships resulting in financial stresses for credit unions due to unanticipated costs, legal disputes, and asset losses. Generally, these situations occurred because the credit union either failed to exercise proper due diligence before entering into a relationship or failed to set up controls to monitor performance.

Due Diligence Review

Credit union officials are responsible for planning, directing, and controlling the credit union's affairs. To fulfill these duties, the officials should require a due diligence review prior to entering into any arrangement with a third party. The following identifies minimum procedures a credit union should follow; however, this should not be considered an exhaustive list. Many times, information gathered from the review will lead to further inquiries or fact-finding.

Planning. The officials should determine whether the proposed activities are consistent with the credit union's overall business strategy and risk tolerances. These risks include the potential loss of capital invested if the venture fails, the loss of member confidence if the program does not meet their expectations, and the costs associated with attracting and retaining qualified personnel and investing in the required infrastructure (e.g., technology, space, communications). If the officials do not believe the activities would complement their strategic vision for the credit union, the third-party lending relationship should not be pursued.

Background Check. It always is important to understand how the third party has performed in other relationships. Contacting credit unions or other clients of the third-party is essential. Inquire how satisfied these credit unions or third parties are with the

prospective partner, and what pitfalls they may have encountered. Sources such as the Better Business Bureau, and Federal Trade Commission also maintain complaint histories on businesses.

Legal Review. The credit union's attorneys should review all contracts to ensure that the officials clearly understand the rights and responsibilities of each party. For example, the review should indicate which party bears the costs of collateral disposition, and whether or not there are recourse arrangements. The credit union should exercise its right to modify contracts to make them fair and equitable. Further, a credit union should understand what actions it may take if the contract is breached or services are not performed as expected.

Financial Review. Financial statements of the company should be reviewed to determine the strength of the institution. Weakly capitalized companies or those exhibiting weak earnings may not be able to continue as ongoing concerns. This could lead to disruptions in member service, uncollected payments on loans and leases, and potential losses if the third party fails to remit funds due to the credit union. Preferably, a licensed CPA will have audited the financial statements to attest to their accuracy.

Return on Investment. The credit union should project its expected revenue, expenses, and net income on its investment, and recognize how each of these factors may change under different economic conditions. For example, expected losses, collection costs, or the volume of activity would fluctuate depending upon the economy or the members' employment stability. Profit projections generated by the prospective third-party should be scrutinized and the underlying assumptions fully understood by the credit union.

Insurance Requirements. Third party relationships can result in increased liabilities. Therefore they necessitate a thorough review of the credit union's insurance coverage, including the fidelity bond and policies covering such matters as errors and omissions, property and casualty losses, and fraud and dishonesty.

Controls

Once a third-party arrangement is entered into, it is important for a credit union to establish controls to ensure the relationship is meeting its expectations and the third party is meeting its responsibilities. As part of these controls, a credit union should adopt monitoring and reporting practices. Failing to do so constitutes an unsafe and unsound practice.

Policies and Procedures. The credit union should develop detailed policy guidance that sets forth responsibilities, authorities, and reporting requirements. Limits should be established so that the program grows at a controlled pace and reflects the risk tolerance of the officials. For example, a credit union may limit the number of leases initially granted so it can assess performance or identify problems before the leasing volume becomes significant.

Staff Oversight. A credit union staff member should be responsible for monitoring the performance of the program. Actual results should be compared to projections and the third party's performance should be reviewed to determine compliance with expectations and contracts.

Reporting. Reports should be submitted to the credit union's senior officials and the credit union's directors to keep them abreast of significant findings, especially areas of noncompliance. The officials should be informed when targets are met or exceeded, or limits breached. Reports should also consist of appropriate information so that the officials can make informed decisions and take timely corrective action.

Partnering with a third party to expand lending to members can lead to growth, improved profitability, and stronger member relationships. However, the credit union officials are responsible for establishing appropriate due diligence procedures and a system of controls to ensure these goals are met.

Sincerely,

/s/
Dennis Dollar
Chairman

APPENDIX C: Sample Credit Union Third-Party Vendor Management Policies

The sample vendor third-party vendor management policies submitted to the CUNA Due Diligence Task Force by credit unions are available at the following web address:

http://www.cuna.org/initiatives/member/due_diligence_documents.html

Appendix D: BDO Seidman, LLP —SAS 70 Examinations and Reports

Christopher Tower, Assurance Partner, BDO Seidman, LLP
Costa Mesa, Orange County, California
(714) 668-7320

Craig Linnell, IS Assurance Partner, BDO Seidman, LLP
Costa Mesa, Orange County, California
(714) 668-7360

SAS 70 Examinations and Reports

Christopher Tower, Assurance Partner, BDO Seidman, LLP
Costa Mesa, Orange County, California
(714) 668-7320

Craig Linnell, IS Assurance Partner, BDO Seidman, LLP
Costa Mesa, Orange County, California
(714) 668-7360

I. Overview

Many companies, known as *user organizations*, often use outside service providers to provide certain services to them. These outside service providers are known as service organizations and typically provide such services as the processing of transactions, performance of certain tasks or business functions, or providing the software or technology environment to process data and transactions.

Service organizations typically provide the following services to *user organizations*:

- Processing of financial data and transactions including item processing services, loan servicing, indirect lending service providers, etc.;
- Payroll processing services;
- Hardware hosting services;
- Internet service providers (ISPs) and web hosting services;
- Application service providers (ASPs);
- Employee benefit plan services;
- Investment services and processing; and
- Data back up services.

Service organizations will often engage a service auditor to conduct an examination and issue a report on the internal controls over the services provided by the service organization. These reports, known as SAS 70 reports, are issued following guidance established by the American Institute of Certified Public Accountants (AICPA); specifically Statement on Auditing Standards Number 70, *Service Organizations*, As Amended ("SAS 70").

Purpose of SAS 70 Reports
Service auditor reports or SAS 70 reports generally have 2 purposes. The primary purpose is to assist *user auditors* in conducting audits of the financial statements of *user organizations* that use a service organization, where the services provided have some impact on the *user organization's* financial statements.

User auditors are required by the AICPA to obtain a sufficient understanding of the entity it is auditing, its environment, including its internal controls, to assess the risks of material misstatement of the financial statements whether due to error or fraud, and to design the nature, timing, and extent of further audit procedures.

Because many of the functions performed by service organizations affect an entity's financial statements, auditors performing audits of financial statements may need to obtain information about those services, the related service organization's controls, and their affect on an entity's financial statements. Additionally, the controls that affect a *user organization's* financial statements may exist at the user *or* the service organization because when a *user organization* uses a service organization, certain controls at the service organization may be a part of the *user organization's* overall control environment and system for gathering and reporting financial information.

The secondary purpose is to assist *user organizations* in assessing the internal controls over services provided by the service organization. It is an effective tool for assessing whether the service organization is providing its services in a controlled environment. The SAS 70 enables the *user organization* to evaluate and assess the service organization control environment by:

- Understanding the control environment, risk assessment and monitoring activities of service organization management upon which the control activities operate;

- Assess the information systems and related communication methods used by the service organization to provide its services;

- Help the *user organization* identify and understand the specific control activities that a service organization has in place to address specific control objectives; and

- Assess the service organization's compliance with those control activities by evaluating the tests and conclusions reached by the service auditor who conducted tests of those control activities to determine whether the control objectives were achieved.

Additionally, SAS 70 also helps *user organization* management form an opinion of the service organizations:

- Attitude towards internal controls;

- The effectiveness and efficiency of operations; and

- Compliance with applicable laws and regulations, where appropriate.

Types of SAS 70 Reports
There are generally two types of reports that may be issued, either a Type 1 or Type 2 report. A Type 1 report is a report on the controls placed in operation and generally is as of a point in time, such as of June 30, 2008. A Type 2 report is a report on controls placed in operation and tests of operating effectiveness. A Type 2 report generally covers a period of time such as 6 months to a year but can be for a lesser period. The primary difference between the two reports is that a Type 2 report includes tests of the operating effectiveness of the controls whereas a Type 1 report is only a report on the description and design of controls and does not include tests of controls. Type 2 reports provide an opinion as to whether the controls that were tested were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the related control objectives were achieved during the period specified.

A Type 1 report is generally only issued one time when an initial SAS 70 report is performed. The Type 1 report is considered to be less effective to an *auditor* or a *user organization* because it does not provide assurance that the controls are operating effectively.

Both reports generally consist of four sections:

- Section I. The Service Auditor's Opinion

- Section II. Information Provided by the Service Auditor

- Section III. Service Organization's Description of Controls

- Section IV. Other Information Provided by the Service Organization

The Service Auditor's Opinion (Section I) and the Service Organization's Description of Controls (Section III) of the report are the most important components of the report. The Service Auditor's Opinion is important because it provides his or her opinion on the controls and the Service Organization's Description of Controls because it provides a description of the control objectives (the controls that the service organization should strive to achieve), and the controls described by the service organization to achieve those control objectives. In a Type 2 report, this Section also includes (1) a description of the controls tested and related tests performed by the service auditor to determine the operating effectiveness of the controls; (2) the results of the service auditor's tests of controls; and (3) any user control considerations that the *user organizations* should consider.

Section IV of the report often contains a description of the service organization's approach to disaster recovery and business continuity planning. This area is specifically not tested within Section III of the report because AIPCA guidance suggests that business continuity and disaster recovery procedures are plans and not controls and therefore it is not appropriate to include them under Section III of the report. However, this information is relevant to a *user organization* because *user organizations* need to have (1) an understanding of the service organization's plan

for disaster recovery and business continuity planning to help assess whether the service organization can recovery its operations/resume business operations during a disaster or other interruption in services, and (2) to incorporate and coordinate such plans with their own disaster recovery and business continuity plans.

II. Considerations in Requesting and Using A Service Auditor's Report

Criteria for Evaluating the Need for a SAS 70 of a Service Organization

User organizations need to be cognizant that, per AICPA guidance, SAS 70s are not applicable to every service provided by a service organization. It is generally only applicable if the service is part of the *user organization's* information system. By information system, the AICPA implies not only the information technology system but the entire system, both automated and manual, by which the entity's transactions are initiated, authorized, recorded, processed, and reported from their initial occurrence to their inclusion in the financial statements. Per the AICPA, a service organization's services are part of an entity's information system if they affect any of the following:

- The classes of transactions in the entity's operations that are significant to the entity's financial statements;
- The procedures, both automated and manual, by which the entity's transactions are initiated, authorized, recorded, processed, and reported from their occurrence to their inclusion in the financial statements;
- The related accounting records, whether electronic or manual, supporting information, and specific accounts in the financial statements involved in initiating, authorizing, recording, processing and reporting the entity's transactions;
- How the entity's information system captures other events and conditions that are significant to the financial statements; and
- The financial reporting process used to prepare the entity's financial statements, including significant accounting estimates and disclosures.

As such, *user organizations* need to request and receive a SAS 70 report from a third party service organization if that organization performs services that meet any of the above criteria. Additionally, per the AICPA, SAS 70s are often obtained by *user organizations* to meet other needs including regulatory compliance needs, and to assess the effectiveness and efficiency of the service organization's operations and services.

In evaluating the need for a SAS 70 of the service organization, the *user organization* should consider performing the following:

1. Determine whether the service organization performs services that meet any of the above criteria. If they do, then perform an overall risk assessment to determine the impact of the

services on the financial statements of the *user organization*. Some factors to consider when performing this assessment include:

- The nature and materiality of the transactions or accounts affected by the service organization, and

- The degree of interaction between internal control at the *user organization* and the service organization's controls.

2. Determine whether state or federal regulations require a SAS 70 based on the services provided to the *user organization*.

3. Assess whether a SAS 70 report on the effectiveness and efficiency of the service organization's services would be desirable by the *user organization* but also whether such services could be tested to effectively report on their effectiveness and efficiency.

If a service organization provides the following services to your organization, it is generally important that you obtain a SAS 70 of the service organization:

- Outsourcing of data processing services such that all or any part of financial data processing is performed by an outside third party, to include financial data and transactions processing, item processing, loan servicing, indirect lending service providers, etc.;

- Payroll processing services including certain personnel services;

- Hardware hosting services;

- Internet service providers (ISPs) and web hosting services;

- Application service providers (ASPs);

- Employee benefit plan services;

- Investment services and processing;

- Outsourcing of certain IT services such as monitoring and maintenance of computer security and system availability and performance; and

- Data back up services.

When an agreement has been reached to have a SAS 70 examination performed of a service organization, *user organizations* need to be cognizant of several key points:

- Because a service auditor needs to test internal controls during the period in which they operate, there could be a delay in getting the SAS 70 report completed and issued (Generally, service auditors can test the operating effectiveness of controls to a point back in time such as 6 months but when the period extends beyond that it is often difficult to effectively test the controls). As a result, *user organizations* need to factor in an appropriate lead time to have a SAS 70 completed;

- The scope of the SAS 70 including the control objectives and period to be covered by the report should be carefully reviewed and agreed to by the *user organization's* external auditors (user auditors);

- The costs for a SAS 70 examination can vary significantly depending on the scope of the services provided by the service organization, the size of the service organization, the nature of the service organization including its organization and management characteristics, the complexity and diversity of the services provided, applicable legal and regulatory requirements, the period covered by the report, etc.; and

- The costs of the SAS 70 are often passed along to the *user organizations* to which the service organization provides its services.

User organizations need to be aware that not all vendors will be open to having a SAS 70 examination performed. However, most service providers that are well known within the *user organization* community and that meet the criteria identified above will be open to or already have a SAS 70 examination performed of the controls over their services.

If your service organization is not willing to have a SAS 70 examination performed, then certain remedies should be considered:

- Request that the external auditors of the service organization perform certain agreed upon procedures to test the operating effectiveness of selected internal controls at the service organization;

- Ensure that input and controls at your organization over data processed by the service organization are thoroughly tested. These tests will help ensure that data processed by the service operation are operating effectively to help detect material misstatements. These tests should be coordinated with your external auditors; and

- If none of the above is performed, consider terminating your relationship with the vendor.

Type 1 vs. Type 2 Reports

Unless a service auditor is issuing a report on the service organization for the first time, it is almost always essential to obtain a Type 2 report. The scope of a Type 1 report does not include any tests of controls and the service auditor's report does not include an opinion as to whether the controls are operating effectively to achieve the control objectives. After completion of the

risk assessment described above and it is determined that a SAS 70 report is needed, it recommended that the *user organization* request and receive a Type 2 report.

Carefully Review the Opinion (Section I), Period Covered, and Description of Controls (Section III) of the Report

User organizations should carefully review the service auditor's opinion to determine whether the scope of the report is appropriate and whether an unqualified opinion (clean) was issued. The scope of the report should include key control objectives and controls relating to the services provided to the *user organization*. The *user organization* should coordinate its analysis of the appropriateness of the control objectives with their external auditor. The *user organization* should consider using some or all the factors often used by user auditors to evaluate the SAS 70 report, as follows:

- Understand the aspects of the service organization's controls that may affect processing of the *user organization's* transactions;

- Understand the flow of significant transactions through the service organization;

- Determine whether the control objectives are relevant to the *user organization's* financial statement assertions; and

- Determine whether the service organization's controls are suitably designed to prevent or detect processing errors that could result in material misstatements in the *user organization's* financial statements and whether they were in place and operating effectively.

The service auditor opinion will specify the period covered by the report. *The user organization* should review the period covered and determine whether it is adequate for their purposes. Generally, the longer the period covered by the report the more effective the report. It is recommended that the report coincide with the *user organization's* fiscal year and cover a period of 6 months to 1 year. If the SAS 70 report does not coincide with the *user organization's* fiscal year, then the ending period of the report should not be more than 6 months to 1 year older from the period end covered by the report. If the report is older than 6 months to a year, then the *user organization* should discuss with its external auditors whether additional procedures should be performed to the test the effectiveness of controls at the service organization. As discussed below, this could encompass requesting the service auditor to perform certain agreed upon test procedures.

If a qualified opinion was issued, the *user organization* should assess the significance of the control objective(s) not achieved that resulted in the qualification and whether additional control procedures should be performed by the *user organization* on a recurring basis to compensate for the weaknesses identified in the report. In most situations, extensive testing of input and output controls over data processed by the service organization will provide reasonable assurance that the transactions are processed free of material error. However, the effectiveness of this testing can vary depending on the services provided by the service organization and the complexity of

their operations and should be carefully coordinated with the *user organization's* external auditor. The *user organization* should actively monitor the efforts made by the service organization to address and rectify any weaknesses identified in the report, particularly those that resulted in the qualification. The level of monitoring could include such things as periodic calls with appropriate service organization management to monitor progress made to address the weaknesses, or visiting the service organization to discuss action taken to address the weaknesses. Depending on the severity of the weaknesses, the *user organization* should consider requesting the service auditor to perform interim tests of the controls that were implemented to address the control weaknesses.

Each *user organization* should carefully review Section III of the report including the appropriateness of the control objectives, related controls, tests performed by the service auditor and whether any exceptions were identified. While exceptions noted by the service auditor or a qualified report do not automatically mean that the SAS 70 report will not be useful in assessing the risks of material misstatement of a *user organization's* financial statements, the *user organization* should carefully evaluate any exceptions identified in the report. If the *user organization* believes that the report is not sufficient for their purposes, they may want to contact the service organization to request that either (1) the service auditor perform additional agreed upon procedures, or (2) request that the user auditor perform such procedures. Any such requests would need to be agreed to by the service organization and coordinated with the *user organization's* external auditors. Items that could be considered not sufficient for the *user organization's* purposes could include such matters as inappropriate or missing control objectives, insufficient testing of the controls by the service auditor, test exceptions that are consider material or significant weaknesses, etc. Control deficiencies are considered to exist when the design or operation of a control does not allow management or its employees to prevent or detect misstatements on a timely basis.

In addition, the service auditor will often include user control considerations after the tests results in each control objective. The user control considerations are controls that the service auditor's recommends *user organizations* implement in their system of internal control over financial reporting to help strengthen and complement the controls over services provided by the service organization. Each *user organization* should carefully review the user control considerations and ensure they are performing those control procedures within their respective organizations, where appropriate. In evaluating the appropriateness of these user control considerations, the *user organizations* should read the description of controls in the report and determine whether the complementary user controls suggested by the service auditor are relevant to the service provided to the *user organization* (Some service organizations may provide services that are not used by the *user organization* and therefore any related user control consideration would not be considered relevant). Generally, if the combination of the control at the service organization along with the user control at the *user organization* are necessary to prevent or detect a material misstatement in the *user organization's* financial statements, then the user control should be performed.

Carefully Review Other Information (Section IV) of the Report

Each *user organization* should carefully review Section IV of the report to ensure that (1) the service organization's plans for business continuity and disaster recovery are appropriate and (2)

carefully coordinate the *user organization's* disaster recovery/business continuity plans and efforts with those of the service organization, where appropriate. As indicated above, the *user organization* needs to have (1) an understanding of the service organization's plan for disaster recovery and business continuity planning to help assess whether the service organization can recovery its operations/resume business operations during a disaster or other interruption in services, and (2) to incorporate and coordinate such plans with their own disaster recovery and business continuity plans. Because the information provided in Section IV is often described at a high level, the *user organization* should consider having more direct and detailed discussion with the service organization as to the nature and extent of their recovery plans and related plan testing.

III. Vendor Considerations

Each *user organization* should ensure the relationship with the service organization includes a Service Level Agreement (SLA) that considers the following:

- Requirements for the service organization to obtain a Type 2 SAS 70 report on an annual basis with the period of the report to cover at least 6 months;

- Measures for dealing with the service organization's when significant exceptions are identified in the SAS 70 report that result in a qualified opinion by the service auditor;

- Minimum standards for:
  - Specific timelines for completing the processing of data and transactions
  - Errors and exception processing and handling
  - System performance
  - System uptime and availability, where appropriate

- A formal documented disaster recovery/business continuity plan for the service organization that is tested at least on an annual basis and provisions for coordinating joints tests of the *user organization's* disaster recovery plan with that of the service organization. In addition, roles and responsibilities and key contact personnel should be clearly delineated in the SLA.

Appendix D: BDO Seidman, LLP— Guidance For Selecting Vendor Management Software

Christopher Tower, Assurance Partner, BDO Seidman, LLP
Costa Mesa, Orange County, California
(714) 668-7320

Craig Linnell, IS Assurance Partner, BDO Seidman, LLP
Costa Mesa, Orange County, California
(714) 668-7360

Guidance For Selecting Vendor Management Software

Christopher Tower, Assurance Partner, BDO Seidman, LLP
Costa Mesa, Orange County, California
(714) 668-7320

Craig Linnell, IS Assurance Partner, BDO Seidman, LLP
Costa Mesa, Orange County, California
(714) 668-7360

I. Overview

Due to the increasing use of third party vendors by CUNA members to support credit union operations and IT systems, there is a growing need for members to consider the use of third party software packages to help manage and monitor vendor services, risks and contracts. While the use of software to manage the vendors does not appear to be wide spread in our industry, members should be aware that many software products on the market can be an effective tool to help manage vendor risk.

II. Evaluating and Selecting Third Party Software

Members should work closely with their respective IT personnel to evaluate and select a software package that best meets their needs. In evaluating their needs each member needs to carefully consider the following:

A. Identify and Assess System Needs

Each member should carefully identify the specifics needs of the desired software package and ensure potential users of the software are actively involved in the system selection process. IT personnel and users should work closely to select a package that meets member needs and objectives.

B. Define System Requirements

Members need to identify the system requirements of the software and rank the requirements in order of priority. The requirements should also be categorized into those that are absolutely required and those that are “nice to haves”.

C. Identify Software Solutions and Evaluate Products

In evaluating the various software solutions members should consider the following:

- Does the product support the member’s vendor management needs and requirements?
- What are the hardware specifications needed to support the software product?

- Will the product be vendor maintained and supported or will it be supported in-house? If maintained by the vendor, are clients involved with testing the application changes?
- What are the product costs including initial purchase costs, implementation costs and ongoing maintenance costs?
- What type of reporting is provided with the system and will it meet the needs of the member organization?
- Was the software package developed using current technology?
- Have software reviews been published, if so, were they positive or negative?
- What security features are provided with the application to maintain proper security over access to the system (i.e., restricting access based on groups/roles/menus, administrative functions, etc.)?
- Is the software vendor well known with a strong reputation in the marketplace?
- Is the vendor able to address all of the questions and concerns that were presented?
- How knowledgeable and experienced is the vendor in the industry?
- Is the vendor financially strong?
- Are other credit unions or financial institutions currently using the vendor? If so, solicit input as to their experience with the vendor.
- Does the package come with user manuals and is the application user friendly?
- Does the package need to be compatible with other software products within the member organization and, if so, what are the compatibility requirements and does it appear compatible?
- Will the vendor provide a software demonstration?

D. Perform Post-Implementation Review

Once a software solution has been selected and implemented, each member should solicit feedback from its respective users of the software and assess whether the product is meeting its needs.

In assessing the software solution, members should consider the following:

- Does the software provide the functionality as stated and meet member expectations? If not, what are the limitations?
- Are users satisfied with the system and have they been properly trained in its use?
- Did users easily adapt to the application (i.e., user friendliness, etc.)?
- Was the product implemented on schedule and within the cost estimates?
- Have there been any significant issues with training or system availability?
- Does the vendor provide support as needed and in a timely fashion?
- What issues were faced during the system implementation and roll-out? How were they resolved?

III. List of Selected Software Products

The following is a list of vendor software solutions that may be considered to support member needs. These products are listed only as an initial starting point and each member organization needs to identify and select a software product that meets their respective needs, which may not be provided by the vendors noted below:

A. CUNA Strategic Services/TraceSecurity Vendor Management

CUNA Strategic Services (CSS) and Trace Security have developed a vendor management system specifically for credit unions ("VendorTrack™"). VendorTrack is supported by CUNA and CSS through an alliance relationship with TraceSecurity.

CUNA Strategic Services/TraceSecurity Vendor Management (Release Date: December 2008)	
Vendor	**CUNA Strategic Services and TraceSecurity**
Contact	Debbie Bergenske, Product Manager, CSS, (800)356-9655, ext. 4340.
Architecture	Web-based
Features	▪ Provides a centralized solution for vendor management that allows credit unions to securely upload and store vendor information such as the policies, procedures, financials, SAS 70 and other critical due diligence information. ▪ Create and maintain a list of current vendors and identify the criticality of each vendor relationship. ▪ Upload third-party contracts and receive email notifications to track critical contract dates. ▪ Access vendor due diligence files that contain responses to CSS' due diligence questionnaires or credit unions can upload their own due diligence files and information. ▪ Receive email notifications for timely due diligence updates. ▪ Provides an easy-to-use resource to prospect and compare potential new third-party relationships. ▪ Utilize other due diligence resource information including RFPs, business plan and risk management templates.
Costing	The basic functionality of VendorTrack will be available for credit unions at no cost with no contract commitment. The only charge a credit union could incur is associated with the purchase of pre-populated vendor file information, which is based on the following schedule. If a credit union is already a customer of one of CSS' Strategic Alliance Providers, there will be no cost associated with the access a strategic alliance provider's due diligence information.

	▪ $100 per vendor file (access for 1 year) ▪ Volume discounts block available if purchased at the same time. – 5 vendor credits for 3% off or $485 – 10 vendor credits for 5% off or $950 – 20 vendor credits for 10% off or $1800 – 50 vendor credits for 15% off or $4250 Note: Credits do not expire. If a credit is used to purchase a vendor file, the credit union will have access to those files for one year.

The following vendor management products and services were compiled by a third-party consultant and are listed for your information only. These products and services are not endorsed or recommended by CUNA or any of its affiliates. Neither CUNA nor any of its affiliates make any express or implied warranty as to the accuracy, completeness or usefulness of this information.

B. VendorPoint Software

VendorPoint	
Vendor	**Fortrex Technologies, Inc.**
Contact	(877) 367-8739
Architecture	Web-based
Features	▪ Provides complete, customizable program policy templates ▪ Contains extensive due diligence questionnaires ▪ Centralizes the document repository for vendor information ▪ Tracks vendor issues and trending ▪ Ranks vendor and provides trend reporting ▪ Provides full automation ▪ Configurable for centralized or decentralized operations ▪ Generates extensive reporting ▪ Provides online independent third party security assessments ▪ Add-ons for additional privacy module
Costing	▪ Based on asset size ranging from $0 - $5 billion. Note: The vendor was unwilling to provide further details on pricing for the various levels of asset size. ▪ Minimum 3 year contract ▪ Initial start up fee of $3,000 which includes walkthrough of the product via phone and training, help desk support and upgrades. ▪ Annual licensing fee starting at $5,000 to $20,000 (range varies based

	on asset size) per year for 15 user licenses (Co-op discount of 15% through the end of 2008, may become 10% for the start of 2009). Note: Based on discussions with the vendor, discount arrangements can be made through co-op financial services or company relationships.

C. Vendor Relationship Management (VRM)

Vendor Relationship Management (VRM)	
Vendor	**BMC Software**
Contact	(800) 841-2031
Architecture	Web-based
Features	▪ Single source for vendor information ▪ Manages the vendor relationship life cycle-from initial evaluation and selection to management of ongoing activities, issue management, obligation management, performance scorecards and management, and vendor consolidation ▪ Tracks vendors according to basic business classification, number of employees, contacts, agreements, and vendor status ▪ Alerts can be associated with commitments and key milestones such as maintenance contract expiration dates ▪ Integrates with other enterprise systems, such as purchasing and accounts payable
Costing	▪ The vendor was unwilling to provide detailed pricing information but stated that costs are based on an individual client basis.

D. VendorXpert

VendorXpert	
Vendor	**Sydel Corporation**
Contact	(305) 569-0400
Architecture	Web-based
Features	▪ Enables due diligence in vendor selection using predefined vendor categories with specific requirements and approval workflow ▪ Analyzes mathematical risk to find areas of exposure with the usage of a vendor and more importantly the termination or disappearance of that vendor

	▪ Maintains internal control documentation including personnel, financial and operational risk mitigation strategies ▪ Maintains vendor agreement, maintenance agreements and escrow requirements ▪ Supervises and monitors vendors using a risk-based model with proactive alerts of contract expiration dates, insurance requirements and required documents supporting the agreement ▪ Tracks payments versus agreement terms to ensure payments are within tolerances for the approved agreement
Costing	**Banking & Credit Union Purchase Model:** ▪ Greater than $1 billion in assets o License Fee: $25,000 ▪ $1 billion to $100 million in assets o License Fee: $14,900 ▪ Less than $100 million in assets o License Fee: $7,500 **Banking & Credit Union Financing Model** *3 Years* ▪ Greater than $1 billion in assets o Initiation Fee: $1,200 o Monthly Fee: $1,111 ▪ $1 billion to $100 million in assets o Initiation Fee: $900 o Monthly Fee: $ 662 ▪ Less than $100 million in assets o Initiation Fee: $700 o Monthly Fee: $ 333 *5 Years* ▪ Greater than $1 billion in assets o Initiation Fee: $1,200 o Monthly Fee: $833 ▪ $1 billion to $100 million in assets o Initiation Fee: $900 o Monthly Fee: $497 ▪ Less than $100 million in assets o Initiation Fee: $700 o Monthly Fee: $250 *7 Years* ▪ Greater than $1 billion in assets o Initiation Fee: $1,200 o Monthly Fee: $ 714 ▪ $1 billion to $100 million in assets o Initiation Fee: $900 o Monthly Fee: $426 ▪ Less than $100 million in assets o Initiation Fee: $700

	○ Monthly Fee: $214 ***Notes on Financial Breakdown:*** ▪ Sydel includes the following items in the licensing fees at no additional charge: ○ Software installation fee for the user licenses ○ Software implementation ○ Software training up to 16 hours, as needed ○ Assistance in creating an initial load of vendors ○ Crystal Reports run time license ▪ Pricing presented above is for up to five(5) concurrent user licenses ▪ Pricing does not include the cost of the escrow service, which is invoiced separately to the customers that elect to receive the escrow protection at $800 per year ▪ Yearly maintenance fee of 20% of the license fee will be billed on the anniversary of the agreement date, including free product upgrades as they are distributed to all financial institutions. NOTE - Maintenance fee is included in the Financing Model ***Optional Services may be requested and added at any time:*** ▪ Vendor download interface development included ▪ Payment interface development included ▪ Additional training per day: $1,000 ▪ Additional user license: $1,500

E. Archer Vendor Management

Archer Vendor Management	
Vendor	**Archer Technologies**
Contact	(913) 851-9137
Architecture	Multi-tenant
Features	▪ Aggregates all vendor information, including vendor profiles, contacts, facilities, contracts and projects ▪ Provides an enterprise view of corporate vendor documentation, services and utilization that is categorized by relationship manager, tier or any other data element ▪ Enables vendor relationship managers to minimize and manage risk associated with vendor relationships by tracking key performance indicators and the status of deliverables ▪ Assesses vendor risk using various assessment types and

	a library of questions based on best-practice standards, such as the Shared Assessments Program ▪ Derives risk and compliance ratings from assessment results using easily configurable and flexible risk scoring formulas ▪ Measures and report vendor compliance with all relevant company policies, procedures and regulatory requirements ▪ Tracks and address areas of non-compliance identified in the vendor assessment process ▪ Monitors the overall vendor management program through powerful executive dashboards
Costing	▪ Annual, enterprise-wide licensing structure (unlimited user base) ▪ Vendor Management Solution = $50,000/year (only for the Vendor Management module and includes maintenance, standard care maintenance and version upgrades. Other client care plans are available for an additional fee.) ▪ Calculated Fields Extension = $15,000/year (extension to the Archer SmartSuite Framework provides the ability to create formulas for dynamically computing a value for a field using a library of functions and operators) ▪ Data-Driven Events Extension = $15,000/year (extension to the Archer SmartSuite Framework provides the ability to drive actions with the system based on data input in an Archer module. Supported actions include filtering available options, requiring field input and generating email based on date information) ▪ SmartStart Installation = $10,000 one-time fee (includes installation and basic configuration services) ▪ Archer Certified Professional (ACP) course and exam = $3,000 per person (includes 5 day course and exam for primary administrators of application) ▪ Archer's Professional Services team is also available at $270.00/hour (a formal statement of work would be drafted prior to each project to provide the credit union with the number of hours estimated to complete). Based on the size of the organization and the solutions interested in licensing, Archer can provide a customized proposal. Archer does not have, at this time, pricing details for mid-size organizations (they work with Fortune 1000 companies, with 45% being in the financial industry).

Copyright