

## **EVALUATING THIRD PARTY RELATIONSHIPS REPEATABLE INTERNAL AUDIT PROGRAM**

### **AUDIT NAME:**

### **OBJECTIVE:**

To assess the credit union's compliance efforts with NCUA's October 2007 Letter to Credit Unions 07-01, Evaluating Third Party Relationships. This letter is intended 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. This letter sets forth supervisory principles derived and adapted from guidance issued by NCUA and other federal regulatory agencies.

### **SCOPE:**

Limited to interview, observation, and review of key (high risk) vendor contracts to assess management's vendor oversight controls (see Risk Measurement, Monitoring, and Control elements of NCUA's Evaluating Third Party Relationships Questionnaire).

### **POPULATION / SAMPLE SIZE:**

To be determined by auditor-in-charge

### **AUDIT PROCEDURES:**

#### **THIRD PARTY / VENDOR MANAGEMENT**

1. Interview key management to determine if they have any key (high-risk) third party relationships. (i.e. the third party vendor is providing a service on behalf of the credit union. For example; lending services, auditing and management consulting services, asset liability management, BSA and OFAC, data processing, and internet banking services).

#### **RISK ASSESSMENT AND PLANNING**

2. For key third party relationship(s) identified in step #1, assess management's level of planning and initial risk assessment. The NCUA has stated that it expects credit unions to carefully evaluate the risks that the relationship imposes and how the services provided relate to or compliment the credit union's overall mission and philosophy. Factors that should be considered include:

- Credit Union Expectations – What needs of the credit union is the third party relationship expected to fill?
- Importance of the Relationship – How important is the relationship of the third party to the credit union? Is the function the third party will perform one the absolutely must be performed by someone, or is it one that is less important?
- Staff Expertise – Are there individuals on the credit union's staff who can perform the services if the risk or working with the third party proves greater than the credit union would like? Is credit union staff qualified to manage and monitor the third party relationship? How much reliance on the third party will be necessary?
- Cost-Benefit Relationship – Does the potential benefit of the arrangement outweigh the potential risks or costs? Will this change over time?

## **EVALUATING THIRD PARTY RELATIONSHIPS REPEATABLE INTERNAL AUDIT PROGRAM**

- Impact on Membership – How will management gauge the positive or negative impacts of the arrangement on credit union members? How will they manage member expectations?
- Credit Union's Insurance Coverage – Does the credit union's insurance policy provide adequate protection if the credit union gets sued because of the acts of a third party?
- Exit Strategy – If the relationship goes poorly, can the credit union withdraw from the relationship? Is there another party who can take over if need be?
- Financial Projections – Do financial projections align with the credit union's overall strategic plan and Asset/Liability Management framework?

### **VENDOR DUE DILIGENCE**

3. For key third party relationship(s) identified in step #1, assess management's level of due diligence. Did management perform an investigation of its third party vendor prior to entering into a relationship? Due diligence processes should be tailored to the complexity of the relationship.

The following are potential avenues of investigation:

- Background Check – References, prior performance, licensing and certification, key individuals, legal proceedings.
- Business Model
- Cash Flows – Can management explain how cash flows (both incoming and outgoing) move between the member, the third party, and the credit union?
- Financial and Operational Control Review – SAS 70's, independent audit results, and/or regulatory reports.
- Contractual Provisions and Legal Review
- Accounting Considerations – Have potential accounting complexities been adequately considered by those qualified, such as a CPA?

### **RISK MEASUREMENT, MONITORING, AND CONTROL**

4. Document management's processes in place for ongoing monitoring of the relationship. Management should establish ongoing expectations and limitations, compare program performance to expectations, and ensure all parties to the arrangement are fulfilling their responsibilities. To the extent that management relies on the third party to provide measurement information, clear controls should be contractually established and subject to periodic independent testing to ensure the accuracy of the information.

Note: Some contracted vendors may have clauses that allow them to retain agents to provide services to GI on behalf of the contracted vendor. Credit Union Management must conduct due

## **EVALUATING THIRD PARTY RELATIONSHIPS REPEATABLE INTERNAL AUDIT PROGRAM**

diligence to determine the adequacy of relevant controls at the agent (e.g., obtain description of controls, information security policy, privacy policy, hiring policy, and/or SAS 70 report), as appropriate.

The following are possible due diligence procedures management can perform. Keep in mind this is not a comprehensive list. Management may choose these items, or others they deem necessary, to monitor the relationship. The number of due diligence procedures, and nature of the procedures will be guided by management's assessed level of risk and the importance and complexity of the relationship:

### Monitor Financial Condition and Vendor Internal Controls over Critical Processes and Information

- Evaluate the service provider's financial condition periodically.
- Periodically review audit reports (e.g., SAS 70 reviews, security reviews) as well as regulatory examination reports if available, and evaluate the adequacy of the service providers' systems and controls including resource availability, security, integrity, and confidentiality.
- Periodically review the service provider's policies relating to internal controls, security, systems development and maintenance, and back up and contingency planning to ensure they meet the institution's minimum guidelines, contract requirements, and are consistent with the current market and technological environment.
- Monitor changes in key service provider project personnel allocated to the institution.
- Review and monitor the service provider's insurance policies for effective coverage.
- Perform on-site inspections in conjunction with some of the reviews performed above, where practicable and necessary.

### Assess Quality of Service and Support

- Regularly review reports documenting the service provider's performance. Determine if the reports are accurate and allow for a meaningful assessment of the service provider's performance.
- Review system update procedures to ensure appropriate change controls are in effect, and ensure authorization is established for significant system changes.
- Evaluate the provider's ability to support and enhance the institution's strategic direction including anticipated business development goals and objectives, service delivery requirements, and technology initiatives.
- Determine adequacy of training provided to its employees.
- Periodically meet with contract parties to discuss performance and operational issues.

## **EVALUATING THIRD PARTY RELATIONSHIPS REPEATABLE INTERNAL AUDIT PROGRAM**

### Monitor Contract Compliance

- Periodically review invoices to assure proper charges for services rendered, the appropriateness of rate changes and new service charges.
- Periodically review the service provider's performance relative to service level agreements, determine whether other contractual terms and conditions are being met, and whether any revisions to service level expectations or other terms are needed given changes in the institution's needs and technological developments.
- Maintain documents and records regarding contract compliance, revision and dispute resolution.

### Maintain Business Resumption Contingency Plans

- Review the service provider's business resumption contingency plans to ensure that any services considered mission critical for the institution can be restored within an acceptable timeframe.
- Review the service provider's program for contingency plan testing. For many critical services, annual or more frequent tests of the contingency plan are typical.
- Ensure service provider interdependencies are considered for mission critical services and applications.

### **BSA, OFAC, Red Flags**

**5.** Determine if the contract business owner is outsourcing any processes related to the Bank Secrecy Act/Anti-Money Laundering Requirements, Office of Foreign Assets Control Requirements and/or Red Flags – Identity Theft Rules Requirements.

**6.** If the answer is affirmative for any of the processes in Step 5, determine the adequacy of management's oversight of the vendor in relation to these processes.

**7.** Determine if the contractual agreement includes adequate language in regards to the service provider's compliance with the above laws and regulations. If necessary, request assistance from the Corporate Compliance Officer.

### **Resources**

NCUA letter 07-CU-13

NCUA Letter 08-CU-09

NCUA Letter 08-CU-09, Appendix A

NCUA Questionnaire for Examiners

CUNA's - Third Party Management Guide

Managing Vendor Relationships (BCG)