

KEY EXAMINATION ISSUES FOR 2008 WEBINAR FREQUENTLY ASKED QUESTIONS

This document contains Frequently Asked Questions (FAQs) which were posed by participants during the January 29, 2008 webinar conducted by NCUA Board Member Gigi Hyland.

Evaluating Third Party Vendors Presentation FAQs

1. Will the Letter to Credit Union 07-CU-13 and Supervisory Letter Number 07-01 be available for download on the NCUA website?

RESPONSE:

The Letter to Credit Union and Supervisory Letter are available on NCUA's website at the following address <http://www.ncua.gov/letters/2007/CU/07-CU-13.doc>.

2. Is NCUA making this presentation and the supporting material discussed and provided during this presentation available to credit unions?

RESPONSE:

The webinar and all the additional information presented and discussed is available to credit unions on NCUA's website (www.ncua.gov).

3. Why are third party vendors a concern of NCUA?

RESPONSE:

Third party vendors are a concern because they can provide critical products or services to members such as loan underwriting, loan servicing, and loan closing services. Credit unions which have not performed a comprehensive review (initial and periodic) of third party vendors, such as Credit Union Service Organizations (CUSO) or other third parties, have suffered financial loss, and reputation, credit, and operational risk. The effect on their operations could have been minimized if they understood the vendor's business plan initially and performed an ongoing evaluation of the service provided by the vendor.

4. Does NCUA have a recommended form or template to use when performing a risk assessment?

RESPONSE:

NCUA does not have a form or template to use when performing a risk assessment. NCUA provided guidance in a number of publications on the risk assessment process. The guidance is contained in NCUA IT Security Guide, Chapter III; Letter to Credit Union 02-CU-17 e-Commerce Guide for Credit Unions; and the FFIEC Information Security Booklet. The guidance is

on NCUA's website under Resources for Credit Unions
<http://www.ncua.gov/CreditUnionResources/index.htm>.

5. Some credit unions are being required by their auditors to have an enterprise wide risk assessment, covering internal and third party relationships and functions. The auditors are requiring the risk assessment be completed by a third party which is costly. What is NCUA's official opinion?

RESPONSE:

As outlined in Appendix A Section III B of Part 748 of the NCUA Rules and Regulations, credit unions need to assess risk in their operation. Therefore, credit unions need to perform a risk assessment. NCUA does not require credit unions to utilize an independent third party to complete the risk assessment. However, credit unions which perform the assessment of risk internally should have sufficient internal resources and expertise to perform the risk assessment of their operations.

6. What vendors and/or IT services do you consider higher risks?

RESPONSE:

The risk factors management should consider for all services provided by a third party, whether those services be Member Business Loans, Participation Loans, or IT services, vary based on the size, scale, complexity, and nature of the credit union and its activities. Some of the factors management should consider are: the business critical nature of the service; source of system access (internal or external); source of the application; number of credit union business units affected; sophistication of processing type (batch, real time, etc.); transaction volume and dollar value of transactions; sensitivity of data processed or used; impact to the data; experience level of management and staff stability; number of users; and changes in the legal, regulatory, or compliance environments.

7. Are there any additional risks for third party relationships which include the use of offshore or foreign companies?

RESPONSE:

There are additional risks for third party relationships which include the use of offshore or foreign companies. The risk in using offshore or foreign companies is exposure to "country risk," which is the risk that economic, social, and political conditions and events in a foreign country could adversely affect the ability of the offshore or foreign company to provide secure, accurate, and timely services to the credit union. The use of offshore or foreign based companies raises the level of compliance, contractual, reputation, operational, and strategic risks. For additional guidance on the use of offshore or foreign companies, refer to the FFIEC Outsourcing Technology Services IT Examination Handbook, Appendix C: Foreign-Based

Third-Party Service Providers. This Handbook can be accessed at http://www.ffiec.gov/ffiecinfobase/html_pages/it_01.html.

8. How does a credit union secure a copy of the vendor's business plan? Isn't that proprietary information?

RESPONSE:

Credit unions should request information on a vendor's business plan during the period when they are considering or negotiating with the vendor. A vendor may only provide their business plan information on the service the credit union is considering and that may be appropriate. The review of a vendor's business plan is especially important for a critical credit union product or service. If a vendor will not provide information on their business plan, the credit union should take this into consideration in their overall assessment of the relationship.

9. Who should perform the oversight of third party vendors at the credit union?

RESPONSE:

The board of directors and management of the credit union determine who should perform the oversight of third party vendors. This employee(s) should have sufficient knowledge and expertise to perform the oversight of the product or service secured from the third party vendor.

10. If a credit union has an existing relationship with a third party vendor, does the credit union need to complete an evaluation of the existing relationships?

RESPONSE:

The credit union does need to complete an evaluation of existing relationships and the evaluation for each vendor could include different components based on the duration and type of relationship. At a minimum, the due diligence review should take into account the critical nature of the service, the level of expertise exhibited by the vendor, staffing changes, economic and regulatory changes, and risk mitigation strategies associated with the vendor oversight.

11. Do vendors have to perform and produce a Type II SAS 70 report "annually"? If not, how often are they required to perform and produce a Type II SAS 70 report?

RESPONSE:

NCUA does not have any requirements which require a vendor to perform or produce a Type II SAS 70 report annually. However, a Type II SAS 70 Report provides credit unions with a description of the vendor's controls and tests those controls. A Type II SAS 70 Report should be secured on a periodic basis to provide the credit union with a description and test results of the controls.

12. How do credit unions review past legal concerns for a third party vendor?

RESPONSE:

Credit unions should request information from the credit union they contact for vendor reference and may also find information on past legal concerns by accessing information from organizations such as the Better Business Bureau, Federal Trade Commission, credit reporting agencies, state consumer affairs offices, and state attorney general offices. In addition, the credit union could request information in writing from the vendor which includes questions pertaining to past or current legal concerns.

13. Does NCUA or another agency maintain a list of vendors that have had legal, licensing, or other issues which could indicate vendor problems?

RESPONSE:

NCUA does not maintain a list of vendors which have had legal, licensing, or other issues which could indicate vendor problems nor is aware of another federal or state agency which maintains such a list.

14. Small credit unions rely on third party vendors to provide various services to members so they become the member's primary financial institution. However, the small size reduces their negotiating power. This is especially true with large vendors such as credit card processors or credit bureaus. How much cooperation can small credit unions realistically expect from these large vendors?

RESPONSE:

Securing information from vendors can be challenging. However, credit unions need to continue to press these vendors for information to meet their due diligence requirements as outlined in Appendix A of Part 748 of the NCUA Rules and Regulations. Credit unions can also form user groups to approach vendors. Vendors could be more receptive to inquires from groups who use their products or services.

15. Which vendors should credit unions include in their vendor due diligence review process?

RESPONSE:

Officials need to determine which vendors and the level of review for each based on the risk posed by the vendor. Officials should start this process by constructing a list of all third parties (vendors, CUSOs, etc.) and determining the critical nature of the service provided by the third parties. Third parties can be put into categories and officials can establish review requirements for each risk category.

16. The credit union leagues, CUNA, NAFCU, and other trade associations provide credit unions with a list of preferred partners for various products and services. Do credit unions need to perform an evaluation of the service providers on these groups preferred lists?

RESPONSE:

Officials and management are responsible for the evaluation of third parties utilized by their credit union. They can seek assistance in the evaluation process from outside sources, but officials and management are responsible to implement a sound evaluation process.

17. The Evaluating Third Party Vendors presentation discusses the need to address accounting and auditing issues. Who generally performs the accounting and auditing review?

RESPONSE:

The accounting and auditing review should be performed by someone who has sufficient knowledge and expertise in these areas. This individual could be an employee of the credit union, board member, or other official or the credit union could utilize their outside accounting firm.

18. There have been a number of reports in the media which identify breaches of non-public information at third party vendors. What information should be requested to determine if vendors have adequate controls to safeguard member information and other sensitive data?

RESPONSE:

There are a variety of reports credit unions can request from third party vendors to determine if they have adequate controls to safeguard member information. They range from reviews performed by independent third parties which assess the security and control environment of the vendor, executive summaries of penetration tests, and Payment Card Industry Data Security Standards Compliance Reports.

19. Does NCUA recommend that all third party contracts be reviewed by an attorney?

RESPONSE:

The type of relationship, risk parameters, and product and service provided should dictate the level of review required for third party contracts. The board of directors should establish guidelines on what contracts need to be reviewed and the level of review required.

20. Most of our vendor relationships are long term relationships. What due diligence does NCUA recommend we perform for these existing long term relationship?

RESPONSE:

The evaluation of vendors with which the credit union has a long term relationship could include different components based on the duration of the relationship. At a minimum, the due diligence review should take into account the critical nature of the service, the level of expertise exhibited by the vendor, staffing changes, economic and regulatory changes, and risk mitigation strategies associated with the vendor oversight.

21. Does a credit union need to have a written policy and procedure for evaluating third party vendors?

RESPONSE:

A credit union does need to have a written policy and procedure for evaluating third party relationships. A policy and procedure outlines the credit union evaluation requirements and provides management and employees with the guidelines the officials established to oversee the vendor relationship and operate the product and service in a safe and sound manner.

22. Does a credit union need a separate policy for evaluating vendor relationships or can this policy be included within other policies such as our Security Policy?

RESPONSE:

NCUA does not require credit unions to have a stand alone policy addressing the evaluation of third party vendors. This policy may be incorporated with other policies and procedures, but the credit union may determine it is prudent to have a stand alone policy.

23. Does a credit union vendor policy need to address general policy on selecting vendors, due diligence requirements, and monitoring, measuring and controlling risk?

RESPONSE:

A credit union vendor policy should address all aspects of the relationship. At a minimum, the policy should address the requirements for risk assessment and planning, the due diligence review requirements, and the measuring, monitoring, and controls requirements. The policy could be expanded further to document the review requirements for each of these areas for new and existing vendors. The requirement outlined for each should be based on the risk inherent in the prospective or existing relationships.

24. Will examiners review the process used by credit unions to evaluate their third party relationships during the examination process and what documentation should a credit union retain?

RESPONSE:

Examiners will be reviewing the process used by credit unions to evaluate their third party relationships during the examination process. Credit unions should retain a copy of all documentation secured to perform their review.

25. Why does NCUA not expand its review of third party vendors and make the information available to credit unions to assist in the evaluation process?

RESPONSE:

NCUA does not have direct regulatory authority over third party vendors. In addition, it is the responsibility of the credit union to evaluate third party vendors they utilize to provide products and services.

26. Will NCUA be providing a list of approved vendors or certifying vendor relationships like NCUA did during Y2K?

RESPONSE:

NCUA does not maintain an approved or certified list of vendors. It is the responsibility of each credit union to evaluate the third party relationship with each of the vendors the credit union is utilizing.

27. Are the Information Technology examination of vendors performed by NCUA and the other Federal Financial Insurance and Examination Council (FFIEC) agencies available to credit unions?

RESPONSE:

The Information Technology examinations conducted within the past twelve months by NCUA and the FFIEC agencies are available to credit unions. For a credit union to receive a copy of the IT examination, they must be a current client of the vendor. If a credit union is a current client, they can request a copy of the report, if available, through their Regional Office or State Supervisory Authority.

28. Does the AIREX Examination Program contain one questionnaire addressing evaluation of third party relationships or are there multiple questionnaires?

RESPONSE:

Currently there are a number of questionnaires contained in AIREX which provide additional guidance on evaluating third party relationships. The questionnaires are Outsourced Lending Relationships, Indirect Lending Controls, and IT Vendor Oversight. NCUA is in the process of constructing an AIREX Questionnaire which addresses the guidance contained in Letter to Credit Unions 07-CU-13, Evaluating Third Party Relationships.

29. Does the evaluation process contained in the Letter to Credit Unions and Supervisory Letter pertain to loan purchases/participation and Credit Union Service Organizations (CUSOs)?

RESPONSE:

Credit unions need to perform an evaluation of all third parties utilized by the credit union. The level of evaluation should be commensurate with the risk, critical nature, and type of the relationship.

Strategic Planning

30. Will examiners be looking for written strategic and business plans?

RESPONSE:

Examiners will be looking for written strategic and business plans and making an assessment of the effectiveness of the credit union's planning process when evaluating the credit union's CAMEL rating.

31. What are NCUA examiners looking for in a business plan?

RESPONSE:

The business plan should incorporate the following five steps: an assessment of the environment in which the credit union will operate over the medium term; a clear, written statement of key objectives; consistency with federal and state laws and NCUA regulations; communication of the plan's objectives to management and staff to assure adherence to both the business plan and strategic goals; and implementation of the plan.

32. What are the components of a good planning model? Is the annual budget considered a planning document?

RESPONSE:

The components of a good planning model are a strategic plan, a business plan, and an operating budget. The strategic plan considers the long-term allocation of resources and looks out about 3-5 years into the future. The business plan flows logically from the strategic plan and concentrates on the shorter-term allocation of resources. The budget should include projected revenues, expenses, and underlying assumptions (i.e. asset growth, loan growth, loan yield, etc.).

33. Should supervisory committee members or the compliance officer participate in planning sessions?

RESPONSE:

To be most effective, the planning process should be conducted by a planning team. The make up of the team will vary from credit union to credit union, but the team approach brings a variety of perspectives together, creates a sense of ownership, and facilitates cooperation to implement the plan.

34. How often should a credit union have a strategic planning session? Should the strategic plan be for a static period of time or on a rolling timeframe?

RESPONSE:

Consistent with the credit union's size and complexity, the board of directors should establish a strategic plan that documents management's course in assuring that the credit union prospers in the next three to five years, on a rolling timeframe, and should be reviewed and updated on a regular basis, most often annually.

35. We completed our business planning session and strategic plan already. Will we need to complete another before the 2008 exam to include the new requirements?

RESPONSE:

No. The strategic planning discussion on the webinar did not include any new requirements. Examiners have been evaluating the planning process of credit unions when assigning the Management component of CAMEL. NCUA is emphasizing planning in 2008 to highlight its importance and because NCUA is eliminating the use of the CAMEL Matrix in assigning CAMEL codes.

36. Is NCUA advocating a set process for planning? Are you going to mandate credit unions use a specific planning process?

RESPONSE:

We provided an example of a planning process that contains five major components, as shown on Slide 22 of the webinar. The planning process will vary depending on the size and complexity of the institution. As long as the credit union has a sound process in place for strategic planning and is taking an acceptable level of risk in implementing the products and services offered to its members, it should be suitable.

37. How does a small or low-income designated credit union request the services of an Economic Development Specialists (EDS)?

RESPONSE:

The best method to request the services of an EDS would be to contact your NCUA examiner and have a discussion with the examiner on what assistance is requested. The examiner will make the formal request for the credit union. In the case of a state-chartered credit union, contact your state supervisory authority.

38. What resources are available for small and low-income designated credit unions to find out more information on today's topics?

RESPONSE:

NCUA is offering 20 National Workshops in 2008, which include further discussion of some of today's topics. The dates, locations, agendas, and registration forms can be found on NCUA's website at this URL:
<http://www.ncua.gov/CreditUnionDevelopment/Events/Index.htm>.

A credit union could also contact their credit union league or association and other credit union trade organizations.

CAMEL/Courtesy Pay Questions

39. If NCUA is eliminating the CAMEL Matrix will this mean my credit union will no longer be assigned a CAMEL Rating?

RESPONSE:

For examination and supervision contacts with December 31, 2007, effective dates and thereafter, examiners will continue the risk focused examination practice to assign CAMEL component and composite codes. CAMEL was revised in December 2007, to eliminate the CAMEL Matrix as an optional examiner analysis tool. Examiners will assign the "C", "A", and "E" component ratings without a matrix following the approach currently used for assigning the "M" and "L" rating. The risk focused examination practice to disclose CAMEL component ratings and the overall rating in the examination report Overview will continue. When a CAMEL component or composite rating changes, examiners will inform management. Disclosing ratings facilitate understanding of NCUA's assessment of the credit union's overall operation. NCUA Letter to Credit Unions No. 07-CU-12-CAMEL Rating System provides detailed information on the CAMEL Matrix elimination.

40. Examiners and Supervisory Examiners are functional with reviewing components of credit unions, but few of them have management expertise. Where will they acquire the knowledge/ability to assess a strategic plan that requires a high-level of managerial expertise?

RESPONSE:

Strategic planning has been a part of the Management "M" component of CAMEL for a long-time. NCUA has provided and continues to provide Examiners and Supervisory Examiners training to properly evaluate strategic plans. Management has the responsibility to support the appropriateness of the strategic plan if questions arise during an examination.

41. This sounds like the examiner is going to be a lot more subjective than ever before. Is this a good idea for credit unions? The examiners have not managed a credit union.

RESPONSE:

The CAMEL Matrix applied to the C, A, and E components. The Matrix was an optional examiner tool since 1995. Subjectivity is a part of NCUA's CAMEL rating since it was implemented in 1987. Eliminating the Matrix does not increase subjectivity.

42. Do you see additional regulation on "courtesy pay" programs?

RESPONSE:

Congress can decide to propose legislation related to courtesy pay programs. For example, legislation could be proposed if courtesy pay practices are unsafe and unsound or if consumers need additional protection. NCUA's Board also has the authority to consider additional courtesy pay related rules and regulations.

43. NCUA has stated in various guidance documents that the capital ratio needed for each credit union is unique to each CU. But in actuality, I do not think it works that way. I have heard my examiner say the target is 10 percent. When a growing CU is guided to reduce member shares to reduce assets simply to increase capital, it seems counterproductive. Decreasing shares assumes funds are liquid and can be decreased at a positive margin. What is NCUA's official opinion?

RESPONSE:

The board of directors establishes and supports the credit union's strategic, business, and budget goals. Management needs to support net worth ratio goals are sound given the credit union's current and future risk exposure. Statutory net worth requirements must also be met. NCUA examiners may recommend a higher net worth ratio goal but should provide the basis for the recommendation. If the basis for a recommendation is not provided,

management should seek clarification about the recommendation. Individual credit unions may need net worth above regulatory requirements based on risk.

44. Can you comment on the role of the ALM Committee in this process?

RESPONSE:

The ALM Committee has different roles depending on a credit union's individual structure. The board of directors, through ALM policies, establishes the ALM Committee's role.

45. During the examination will the NCUA be looking through expenses incurred by the credit union for appropriateness?

RESPONSE:

Eliminating the CAMEL Matrix does not change NCUA's risk focused examination practices. Risk focused examination and supervision require examiners establish the examination scope based on risk. Expense review may be necessary to assess one or all of the seven risk areas (liquidity, interest rate risk, credit risk, strategic risk, transaction risk, reputation risk, and compliance risk). The seven risk areas are discussed in NCUA Letter to Credit Unions No. 02-FCU-09.

46. If the CAMEL rating is going away, how will this affect Reg-Flex credit unions? Is Reg-Flex going away as well?

RESPONSE:

NCUA is retaining the CAMEL rating. Only the CAMEL Matrix is being eliminated. No changes to Reg-Flex are required due to the CAMEL Matrix elimination.

47. What determines how often the NCUA examines a credit union?

RESPONSE:

NCUA Letter to Credit Unions 01-FCU-05-Risk-Based Examination Scheduling Policy addresses examination schedules.

48. Now that the CAMEL Matrix rode into the sunset, will the examiners use the rubrics system to evaluate our risk in all of the areas of risk performance?

RESPONSE:

NCUA is only eliminating the CAMEL Matrix. A rubrics system will not be included in the CAMEL Rating System. Examiners will continue to use The CAMEL Rating System to assign a rating. NCUA Letter to Credit Unions 02-FCU-09 includes criteria for the seven areas of risk (interest rate, credit,

liquidity, strategic, transaction, reputation, and strategic risk) evaluated in NCUA's risk focused examinations.

BSA Questions

49. What are the minimum qualifications you would expect for someone offering BSA/OFAC compliance audits?

We are a CPA firm specializing in serving credit unions. Our BSA/OFAC audits are managed by a certified BSA compliance officer (Sheshunoff program). However we see others offering that service with no verifiable credentials. How are the examiners evaluating those vendors?

RESPONSE:

The independent testing should be risk-based and evaluate the quality of BSA risk management and compliance for the overall credit union operations. Risk-based testing programs will vary depending on the credit union's size, complexity, scope of activities, risk profile, geographic diversity, etc. Each credit union must determine the qualifications needed for the auditor completing the BSA independent testing based upon the assessed risk of the credit union.

Independent testing may be conducted by the internal audit department, outside auditors, consultants or other third parties such as the Supervisory Committee or other persons who are not involved in the function being tested (auditor). The auditor conducting the BSA/AML testing should report directly to the board of directors or to a designated board committee comprised primarily or completely of outside directors. Examiners will evaluate whether the auditor is independent and reports directly to the board of directors or a designated committee.

The examiners review the independent testing to determine whether it adequately addresses the overall integrity and effectiveness of the BSA/AML compliance program, including policies, procedures and processes. This testing should include a review of the risk assessment, risk-based transaction testing, and a review of training. Examiners will also evaluate whether the independent testing reviewed the effectiveness of the suspicious activity monitoring systems, including the overall process for identifying and reporting suspicious activity.

For further information regarding the expectations of the independent testing, refer to the FFIEC BSA/AML Examination Manual. This manual may be accessed through NCUA's website or at www.ffiec.gov.