

# CFO STRATEGIES

Jim Vilker, NCCO, CAMS  
VP of Professional Services  
CU\*Answers

**AuditLink**

# AGENDA

- Supervisory Priorities
- AuditLink 2017
  - Concentration on internal controls
  - Audit Plans
  - Fraud management
- Next phase of vendor management
  - Primer on assessment process
  - 10 clients

# Supervisory Priorities for 2017

NATIONAL CREDIT UNION ADMINISTRATION  
1775 Duke Street, Alexandria, VA 22314

DATE:	January 2017	LETTER No.:	17-CU-01
TO:	Federally Insured Credit Unions		
SUBJ:	Supervisory Priorities for 2017		

Dear Board of Directors and Chief Executive Officer:

This letter is intended to assist you in preparing for your next NCUA examination. NCUA field staff will continue to use the streamlined small credit union exam program procedures for credit unions with assets up to \$50 million and CAMEL ratings of 1, 2, or 3. For all other credit unions, field staff will conduct risk-focused examinations, which concentrate on the areas of highest risk, new products and services, and compliance with federal regulations. In 2017, NCUA is implementing an extended exam cycle, which is discussed in more detail in NCUA Letter to Credit Unions 16-CU-12, [Risk Based Examination Policy](#).

NCUA's primary areas of supervisory focus in 2017 are described below.

# CYBERSECURITY



FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL  
*Promoting uniformity and consistency in the supervision of financial institutions*

[Home](#) | [Site Index](#) | [Disclaimer](#) | [Privacy Policy](#) | [Accessibility](#)

[About the FFIEC](#)

[Contact Us](#)

[Search](#)

[Press Releases](#)

[Enforcement Actions](#)

[What's New](#)

[Consumer Compliance](#)

[Reports](#)

[Consumer Help Center](#)

[Financial Institution Info](#)

[Examiner Education](#)

[Supervisory Info](#)

[Cybersecurity Awareness](#)

[Federal Register](#)

[Freedom of Information Act](#)

[EGRPRA \(Economic Growth and Regulatory Paperwork Reduction Act of 1996\)](#)

## Cybersecurity Assessment Tool

In light of the increasing volume and sophistication of cyber threats, the Federal Financial Institutions Examination Council (FFIEC) developed the Cybersecurity Assessment Tool (Assessment) to help institutions identify their risks and determine their cybersecurity preparedness. The Assessment provides a repeatable and measurable process for financial institutions to measure their cybersecurity preparedness over time.

The following resources can help management and directors of financial institutions understand supervisory expectations, increase awareness of cybersecurity risks, and assess and mitigate the risks facing their institutions.

[Overview for Chief Executive Officers and Boards of Directors](#) (PDF)

[Cybersecurity Assessment Tool](#) (PDF)

- [User's Guide](#) (PDF)
- [Inherent Risk Profile](#) (PDF)
- [Cybersecurity Maturity](#) (PDF)

### Additional Resources

- [Appendix A: Mapping Baseline Statements to the FFIEC IT Handbook](#) (PDF)
- [Appendix B: Mapping to NIST Cybersecurity Framework](#) (PDF)
- [Appendix C: Glossary](#) (PDF)

[Print all documents at once](#) (PDF)

FFIEC Cybersecurity Assessment Tool Presentation [View Slides](#) (PDF) | [View Video](#)

# CYBERSECURITY

- Increasing emphasis for the third straight year
- Adopting a risk based approach
  - <https://www.ncua.gov/Resources/Documents/IST/examguide.pdf>
- Use of the tool is not required but expected
- IS&T exams..... Every exam in Michigan
  - Concentration on vendor management

# RESOURCES

<https://www.ncua.gov/regulation-supervision/Pages/policy-compliance/resource-centers/cyber-security.aspx>

<https://www.cuanswers.com/resources/risk-assessment-center/>



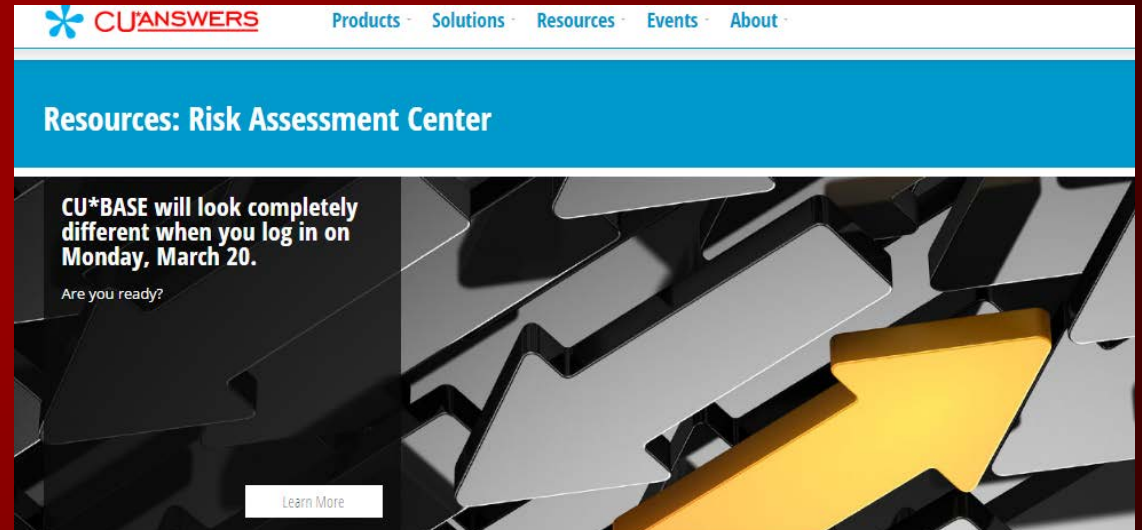
## CYBER SECURITY RESOURCES

NCUA recognizes the importance of cybersecurity and using the web safely and securely.

The information on this page is offered as resources for research and informational purposes. It may not reflect all of the requirements or guidance in this area and should not be construed as requirements except as noted. NCUA does not endorse any vendor, service, or product.

When you access the links below, you might leave NCUA's site.

NCUA Regulations and Guidance	Federal Government Requirements and Guidelines	Information Sharing Forums on Cyber Threats
		



**CU\*ANSWERS** Products · Solutions · Resources · Events · About

### Resources: Risk Assessment Center

**CU\*BASE will look completely different when you log in on Monday, March 20.**

Are you ready?


[Learn More](#)

Resources · Documentation · Risk Assessment Center

#### Risk Assessment Center

This website is designed to assist credit unions in completing their Internet Banking risk assessment as required by the "Guidance on Authentication in Internet Banking Environment" (NCUA [letter 05-CU-18](#)). You'll find technical information and business considerations related to It's Me 247 Online Banking. This page also includes links to additional resources.

**SHARE WITH YOUR PARTNERS!**  
HAVE YOU DEVELOPED A RISK ASSESSMENT FORMAT THAT YOU BELIEVE WORKS WELL AND SATISFIES THE NCUA REQUIREMENTS?  
SHARE YOUR FORMAT WITH YOUR CUSO PARTNERS!  
SUBMIT A COPY OF YOUR RISK ASSESSMENT



# BSA

- Emphasis on MSB's
  - <https://www.ncua.gov/regulation-supervision/Pages/policy-compliance/communications/letters-to-credit-unions/2014/10.aspx>
- BSA exam checklist for every exam
  - <https://www.ncua.gov/regulation-supervision/Pages/bank-secrecy-act.aspx>
- Concentration on evaluation on on-going monitoring of high risk accounts
- Heavy concentration on credit unions CIP
- Incorporating beneficial ownership

# INTEREST RATE RISK

- NCUA Letter to Credit Unions
  - <https://www.ncua.gov/regulation-supervision/Pages/policy-compliance/communications/letters-to-credit-unions/2016/08.aspx>

**Revised Interest Rate Risk Supervision**

**NCUA LETTER TO CREDIT UNIONS**  
NATIONAL CREDIT UNION ADMINISTRATION  
1775 Duke Street, Alexandria, VA 22314

DATE:	October 2016	LETTER No.:	16-CU-08
TO:	Federally Insured Credit Unions		
SUBJ:	Revised Interest Rate Risk Supervision		
ENCL:	(1) <a href="#">Fact Sheet: Revised Interest Rate Risk Supervision</a> (2) <a href="#">Revised Examiners Guide</a> (3) <a href="#">Interest Rate Risk Review Procedures Workbook</a> (4) <a href="#">Guide to Using NCUA's Interest Rate Risk Exam Procedures Workbook</a>		

Dear Board of Directors and Chief Executive Officer:



# INTEREST RATE RISK

Key changes to NCUA's interest rate risk supervision include:

- The development of the *Interest Rate Risk Review Procedures Workbook*;
- The updating of interest rate risk tolerance thresholds in the *Net Economic Value Supervisory Test*
- The creation of an estimated net economic value tool for credit unions with total assets of \$50 million or less; and
- The revision of the interest rate risk chapter in the *Examiner's Guide*.

# COMMERCIAL LENDING AND CONSUMER COMPLIANCE

- NCUA's revised **Part 723, Member Business Loans; Commercial Lending**, is effective January 1, 2017. NCUA field staff will evaluate a credit union's commercial loan policies and procedures and assess the risk management processes associated with managing a commercial loan portfolio. Credit union officials should be prepared to provide documentation to support management's ability to effectively monitor and manage its commercial loan portfolio.
- Given changes to the Military Lending Act that have gone into effect recently, as well as additional changes that will go into effect in October 2017, NCUA field staff will evaluate credit unions' compliance with the Act. For more information on the Military Lending Act, see NCUA Letter to Credit Unions 16-CU-07, **Military Lending Act Examination Approach**.
- Field staff will also review compliance with the Service members' Civil Relief Act. For additional consumer compliance tools and resources, visit NCUA's **Consumer Compliance Regulatory Resources website**.

# INTERNAL CONTROLS

- Credit unions with limited staff may be more susceptible to insider fraud as a result of inherent challenges maintaining adequate separation of duties. NCUA field staff will continue to evaluate the adequacy of credit union internal controls, as well as overall efforts to prevent and control fraud.
  - Employee security
  - File maintenance
  - Transaction monitoring
  - Fee reversals
  - Suppression of transactions
  - Misc check cutting
  - ACH distributions
  - New account review
  - Cash handling
  - Dormancy monitoring

VENDOR MANAGEMENT  
101 (COMPILATION OF A YEAR OF WORK)

# POLICY

- Completed using the words “risk based approach”
- Describe those individuals responsible for managing vendor relationships and what duties that entails
- Outline what should be included in contract review
- Outline what documents may be requested for ongoing due diligence
- If using a third party outline their responsibilities and the fact you are not subrogating your own duties
- Outline reporting structure and frequency (NCUA says monthly)
- <https://www.ncua.gov/Resources/DocumentsGrants/THIRD%20PARTY%20VENDOR%20REVIEW%20CHECKLIST.pdf#search=vendor%20management>

# ORIGINAL SELECTION OF VENDORS

(NO, NOT THE ENTIRE ACCOUNTS PAYABLE)

- Include accounting and have someone on your team familiar with the accounts payable
- Include all significant contracts
- Give a brief description of what the vendor does for the credit union
- Ask the right questions of department leads..examples:
  - What does the vendor do for you... be detailed
  - If member data.... what member data
  - Is the relationship significant and long term
  - If there is connectivity to the network.... Where is the connectivity

# ASSESSMENT PROCESS

- Document your process and mythology
- Understand what risks you are trying to control
  - Reputational
  - Financial
  - Compliance
  - Strategic

*If possible, put mitigating controls in place to keep them off the monitoring lists*

# ASSESSMENT PROCESS

- Have a standard set of variables when assessing risk
  - Extent to which the vendor has access to non-public member information
  - Extent to which the vendor stores non-public member information
  - Extent to which the vendor has access to the credit union's physical location
  - Extent to which the vendor has access to the credit union's IT infrastructure
  - Extent to which the service provided by the vendor is intolerant (disaster recovery/business resumption) to the disruption of member services
  - Extent to which the service provided is vital to the organization and financially woven into the strategies of the organization



# CATEGORIZATION

- According to the level of risk
- Tiers should be developed and utilized for grouping types of vendors from the most critical (risky) to the least
- Tiers should be tied to the amount of ongoing due diligence including the review of some or all of the following
  - Financials
  - Disaster recovering tests
  - Control audits
  - Insurance/bonding coverages
  - News reports
  - Performance standards

# MONITORING AND REPORTING

- Continuously not annually (truthfully requiring automated processes)
- Develop process for onboarding and evaluating new vendors
- Annual reviews of non-critical vendors to determine if the status must be changed
- Reporting should be completed for four audiences
  - Vendor management manager or department head
  - Senior management
  - Board of Directors
  - Regulators

# ***NEW* “OCC SUPPLEMENTAL EXAM PROCEDURES”**

## **JANUARY 23<sup>RD</sup>, 2017**

<https://www.occ.gov/publications/publications-by-type/comptrollers-handbook/pub-third-party-exam-supplemental-procedures.pdf>

### **Supplemental Examination Procedures for Risk Management of Third-Party Relationships**

---

#### **Scope**

These procedures are designed to help examiners tailor the examinations of national banks and federal savings associations (collectively, banks) and determine the scope of the third-party risk management examination. This determination should consider work performed in related areas by internal and external auditors, risk and compliance functions, and examiners. Examiners need to perform only those objectives and steps that are relevant to the scope of the examination as determined by the following objectives. Seldom will every objective or step of the expanded procedures be necessary.

#### **Life Cycle Phase 4—Ongoing Monitoring**

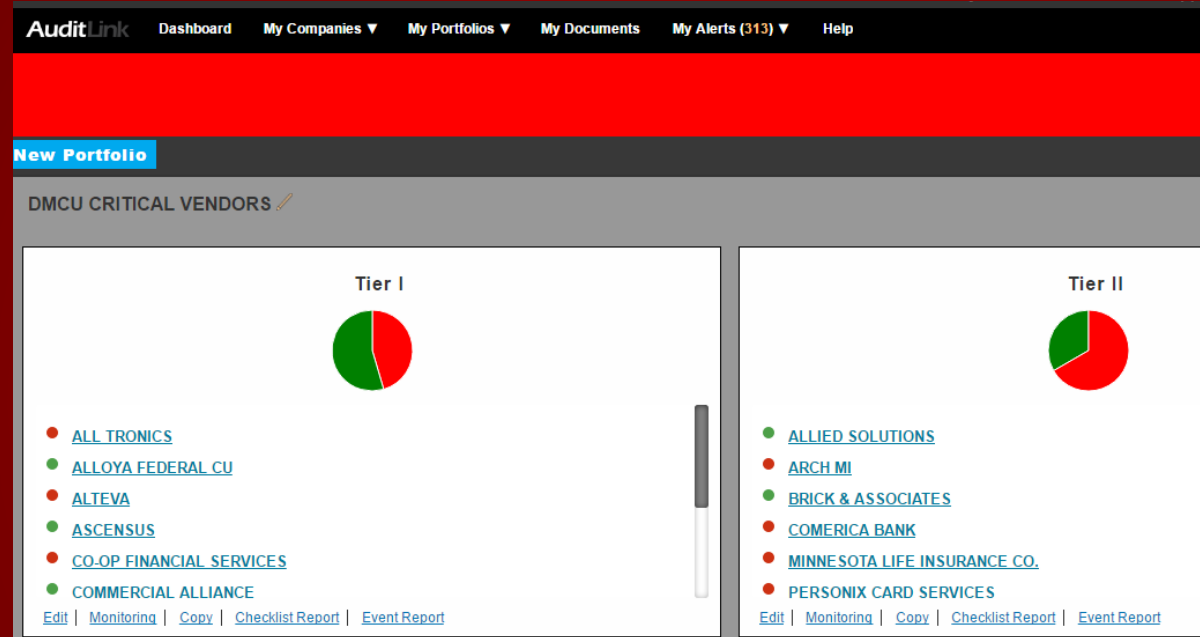
1. Assess whether management periodically reviews third-party relationships to determine if the nature of the activities is critical.
2. Determine whether management has dedicated sufficient staff with the necessary expertise, authority, and accountability to oversee and monitor the third party in a manner commensurate with the level of risk and complexity of the relationship. Consider whether there is sufficient monitoring of the
  - quality and sustainability of the third party’s controls.
  - third party’s ability to meet service-level agreements, performance metrics, and other contractual terms, and to comply with legal and regulatory requirements.

# AUDITLINK VM

- AuditLink is partnering with Trust Exchange and began performing vendor management for CU\*Answers in January of 2016
- End to end with a dynamic monitoring process
- 10 credit unions have signed with another 10 in consideration phase
- Service includes:
  - Assessment of vendor criticality
  - Creating and categorizing them on the monitoring system
  - Creating critical event tables with real time monitoring
  - Daily monitoring including communicating with vendors directly
  - Full contract management platform for credit unions with archival and notification of critical dates

[https://auditlinksuite.com/wp-content/uploads/auditlink\\_G2\\_partnership.pdf](https://auditlinksuite.com/wp-content/uploads/auditlink_G2_partnership.pdf)

# AND THE RESULT OF A YEAR OF EFFORT



[Click here](#)

QUESTIONS??

