Third Party Technology Contracts
Understand the Risk

Presented by

Brian W. Vitale, President

Compliance Advisory Services, LLC

COMPLIANCE ADVISORY SERVICES

Intelligence Cycle

Planning and Development

[4] Disseminate

[1] Collect

[3] Analyze

[2] Process

COMPLIANCE ADVISORY SERVICES

Purpose

A Risk Assessment:

- Drives Policy and Procedures
- Strategic Allocation of Resources
- Establishes Credibility in both What and How

The What

A Risk Assessment:

- Primary Internal Control and Roadmap
- Not Static
- A ‘Living’ Document

The How

A Risk Assessment:

- Qualifies and Quantifies the Risks
- Establishes Enterprise Priorities
- Influences the Nature, Scope and Frequency of Third-Party Monitoring

No Risk Assessment?

COMPLIANCE ADVISORY SERVICES

Math

$$12 < 2 \times 6 < 6 \times 2$$

Top Risks / Supervisory Priorities 2016

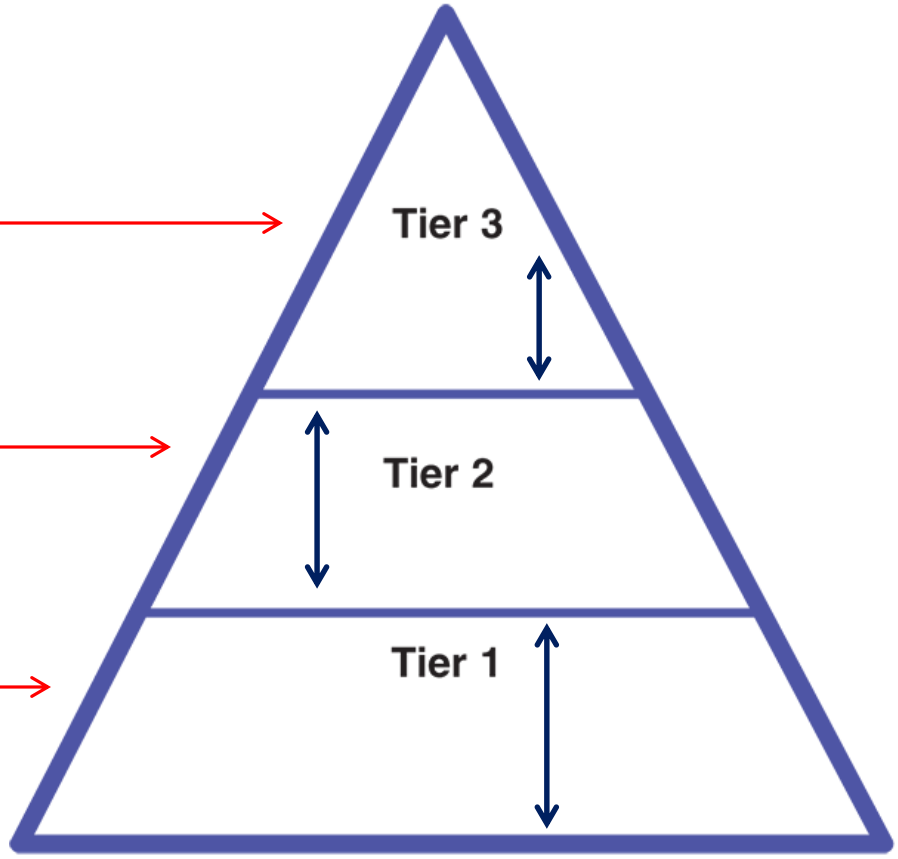
- NCUA Letter to Credit Unions 16-CU-01
  - Cybersecurity Assessment (2015 Priority)
  - Response Programs for Unauthorized Access to Member Information
- OCC Report: Top Risks Facing National Banks and Federal Savings Associations (December 2015)
  - Cyber threats, reliance on service providers, and resiliency planning remain industry concerns, particularly in light of increasing global threats

Types of Risk

- Inherent (Existing Risk)
  - ➢ Prior to Control Implementation
- Residual (Exposure Risk)
  - ➢ Post Control Implementation

Tiers of Risk (Quantitative)

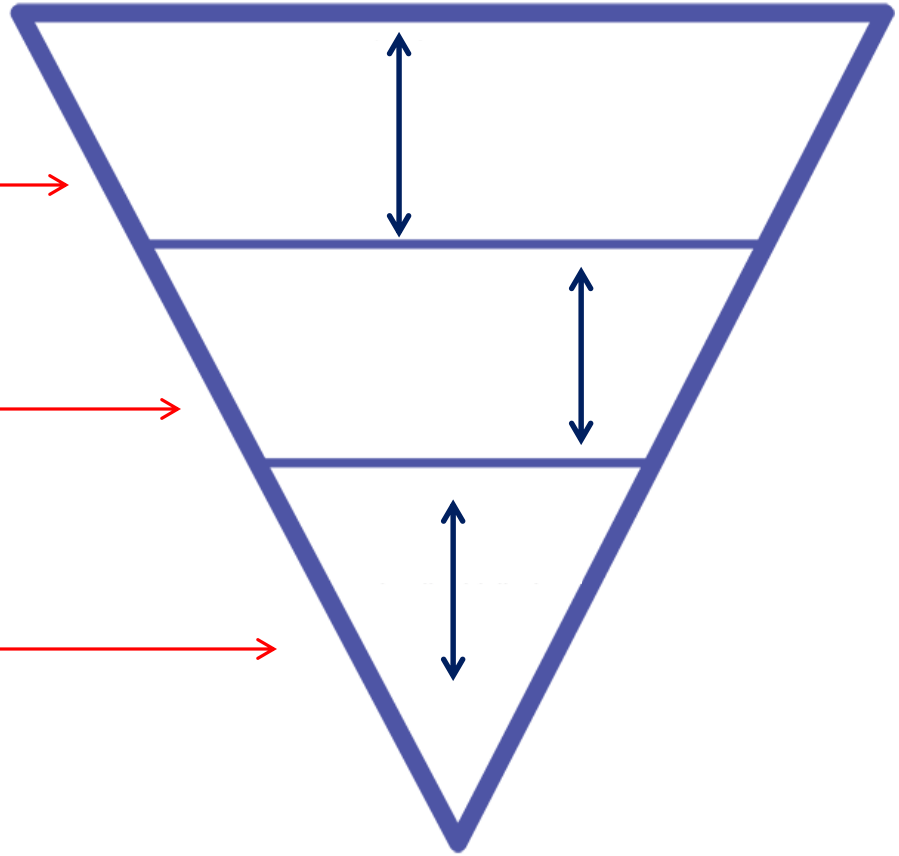
- High
- Moderate
- Low



COMPLIANCE ADVISORY SERVICES

Tiers of Risk (Qualitative)

- Strong
- Satisfactory
- Weak



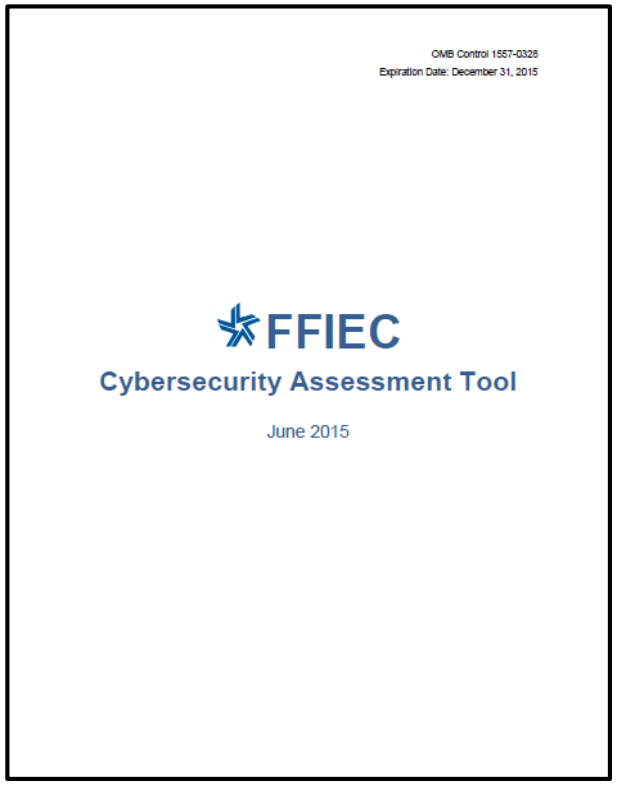
COMPLIANCE ADVISORY SERVICES

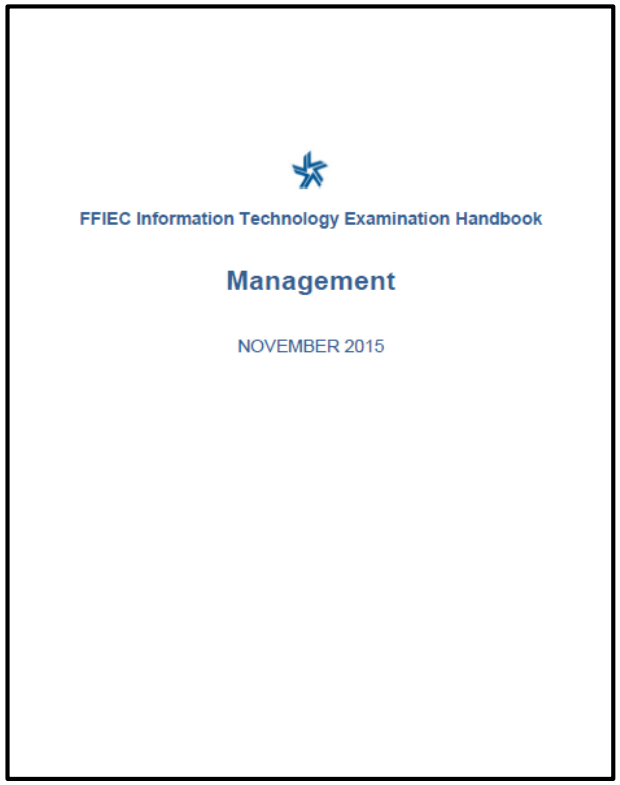
FFIEC IT Examination Handbook InfoBase

The Federal Financial Institution Examination Council (FFIEC) is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions…

The FFIEC Examiner Education Office created the FFIEC InfoBase, which is a vehicle that enables prompt delivery of introductory, reference, and educational training material on specific topics of interest to field examiners from the FFIEC member agencies. The IT Handbooks are updated and maintained electronically using the InfoBase vehicle.

Source References





http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_OutsourcingTechnologyServices.pdf

http://ithandbook.ffiec.gov/media/210375/managementbooklet2015.pdf

http://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_June_2015_PDF2.pdf

COMPLIANCE ADVISORY SERVICES

2004 Expectations

FFIEC's "Outsourcing Technology Services Booklet provides guidance and examination procedures to assist examiners and bankers in evaluating a financial institution's risk management processes to establish, manage, and monitor IT outsourcing relationships."

Risk Appetite

COMPLIANCE ADVISORY SERVICES

FFIEC: Five Inherent Risk Categories

- Technologies and Connection Types
- Delivery Channels
- Online/Mobile Products and Technology Services
- Organization Characteristics
- External Threats

FFIEC: Five Cybersecurity Domains

- Cyber Risk Management and Oversight
- Threat Intelligence and Collaboration
- Cybersecurity Controls
- **External Dependency Management**
- Cyber Incident Management and Resilience

4th Cybersecurity Domain

External Dependency Management

Domain 4 **External Dependency Management** External dependency management involves establishing and maintaining a comprehensive program to oversee and manage external connections and third-party relationships with access to the institution's technology assets and information.	
Assessment Factors	**Connections** incorporate the identification, monitoring, and management of external connections and data flows to third parties. **Relationship Management** includes due diligence, contracts, and ongoing monitoring to help ensure controls complement the institution's cybersecurity program.

COMPLIANCE ADVISORY SERVICES

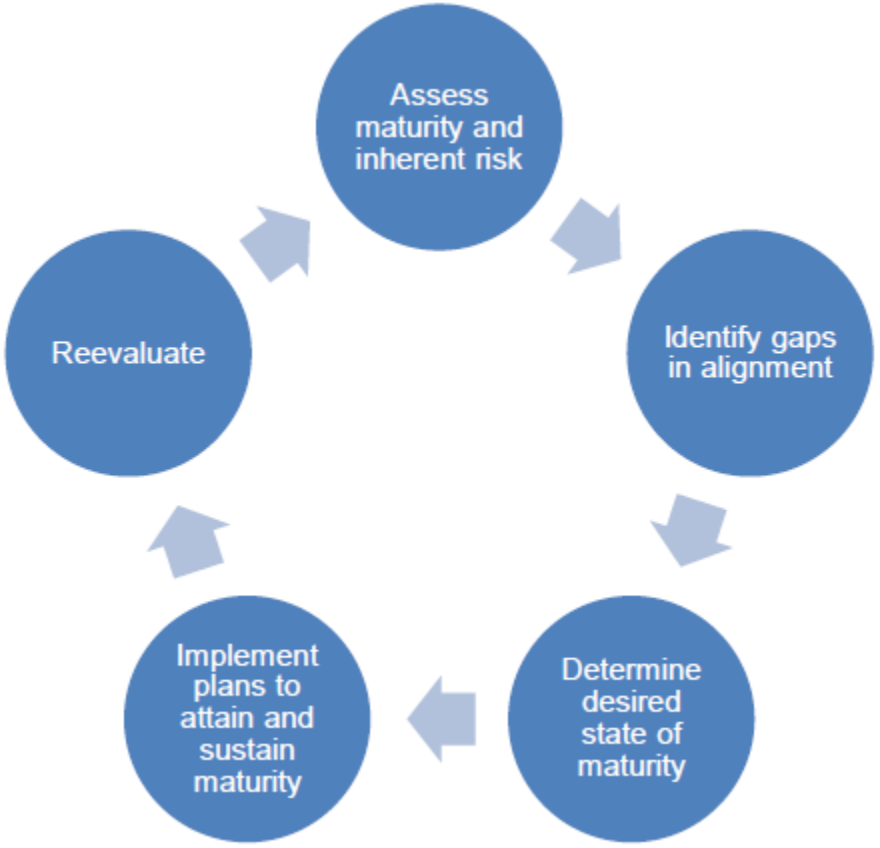
4th Cybersecurity Domain

- Connections
- Due Diligence
- **Contracts**
- Ongoing Monitoring

4th Cybersecurity Domain (Baseline)

- Formal contracts that address relevant security and privacy requirements are in place for all third parties that process, store, or transmit confidential data or provide critical
- Contracts acknowledge that the third party is responsible for the security of the institution's confidential data that it possesses, stores, processes, or transmits.
- Contracts stipulate that the third-party security controls are regularly reviewed and validated by an independent party.
- Contracts identify the recourse available to the institution should the third party fail to meet defined security requirements.
- Contracts establish responsibilities for responding to security incidents
- Contracts specify the security requirements for the return or destruction of data upon contract termination.

Domain Dominance Process



COMPLIANCE ADVISORY SERVICES

Third-Party Management

Action Summary

As part of a financial institution's third-party management program, management should ensure that third-party providers effectively provide support by doing the following:

- Negotiating clear and comprehensive contracts with appropriate terms that meet the institution's requirements.
- Ensuring receipt of audited financial statements from third-party providers at least annually.
- Reviewing results of independent audits of IT controls at third-party providers.
- Monitoring the responsiveness of third-party provider's customer service, including client user group support.

IT Management Handbook – Page 34

Third-Party Management

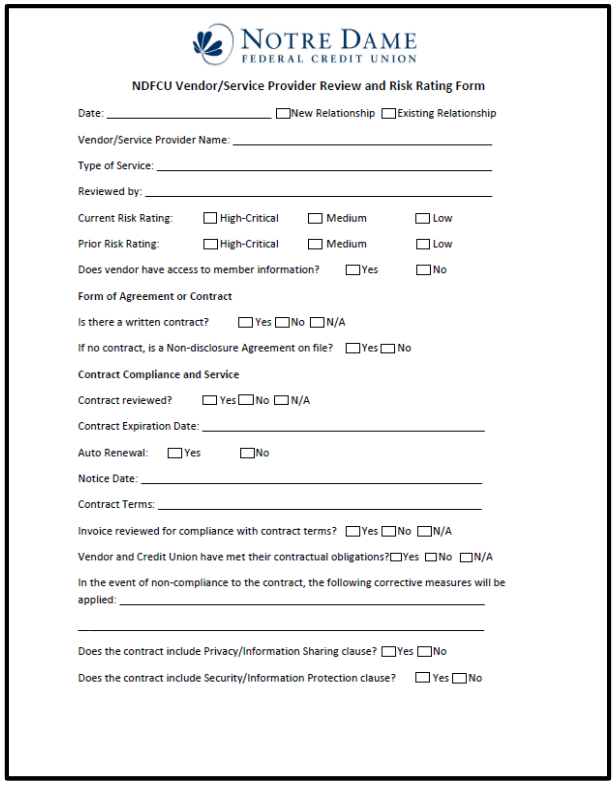
Action Summary

Financial institution management should ensure satisfactory monitoring and reporting of IT activities and risk. These practices should include the following:

- Developing metrics to measure performance, efficiency, and compliance with policy.
- Developing benchmarks for reviewing performance.
- Establishing and reviewing service level agreements (SLA) with critical third-party providers.
- Developing, implementing, and monitoring a process to measure IT compliance with established policies, standards, and practices.
- Evaluating the effectiveness of mitigation strategies and controls.
- Implementing a quality control or quality assurance program to monitor and test systems and applications.
- Implementing timely and effective reporting processes.

IT Management Handbook – Page 36

Due Diligence / Risk Rating Form



NOTRE DAME
FEDERAL CREDIT UNION

NDFCU Vendor/Service Provider Review and Risk Rating Form

Date: _____ ☐New Relationship ☐Existing Relationship

Vendor/Service Provider Name: _____

Type of Service: _____

Reviewed by: _____

Current Risk Rating: ☐High-Critical ☐Medium ☐Low

Prior Risk Rating: ☐High-Critical ☐Medium ☐Low

Does vendor have access to member information? ☐Yes ☐No

Form of Agreement or Contract

Is there a written contract? ☐Yes ☐No ☐N/A

If no contract, is a Non-disclosure Agreement on file? ☐Yes ☐No

Contract Compliance and Service

Contract reviewed? ☐Yes ☐No ☐N/A

Contract Expiration Date: _____

Auto Renewal: ☐Yes ☐No

Notice Date: _____

Contract Terms: _____

Invoice reviewed for compliance with contract terms? ☐Yes ☐No ☐N/A

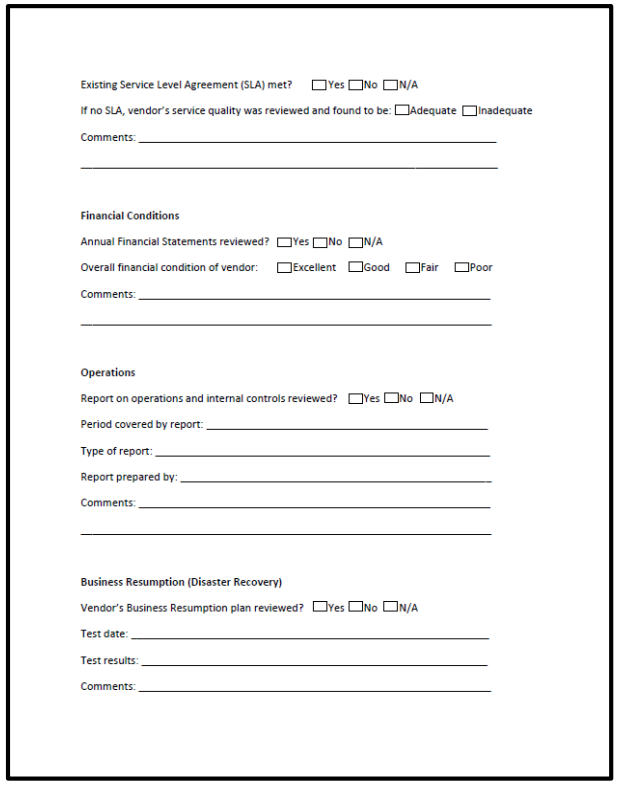
Vendor and Credit Union have met their contractual obligations? ☐Yes ☐No ☐N/A

In the event of non-compliance to the contract, the following corrective measures will be applied: _____

_____

Does the contract include Privacy/Information Sharing clause? ☐Yes ☐No

Does the contract include Security/Information Protection clause? ☐Yes ☐No



Existing Service Level Agreement (SLA) met? ☐Yes ☐No ☐N/A

If no SLA, vendor's service quality was reviewed and found to be: ☐Adequate ☐Inadequate

Comments: _____

_____

Financial Conditions

Annual Financial Statements reviewed? ☐Yes ☐No ☐N/A

Overall financial condition of vendor: ☐Excellent ☐Good ☐Fair ☐Poor

Comments: _____

_____

Operations

Report on operations and internal controls reviewed? ☐Yes ☐No ☐N/A

Period covered by report: _____

Type of report: _____

Report prepared by: _____

Comments: _____

_____

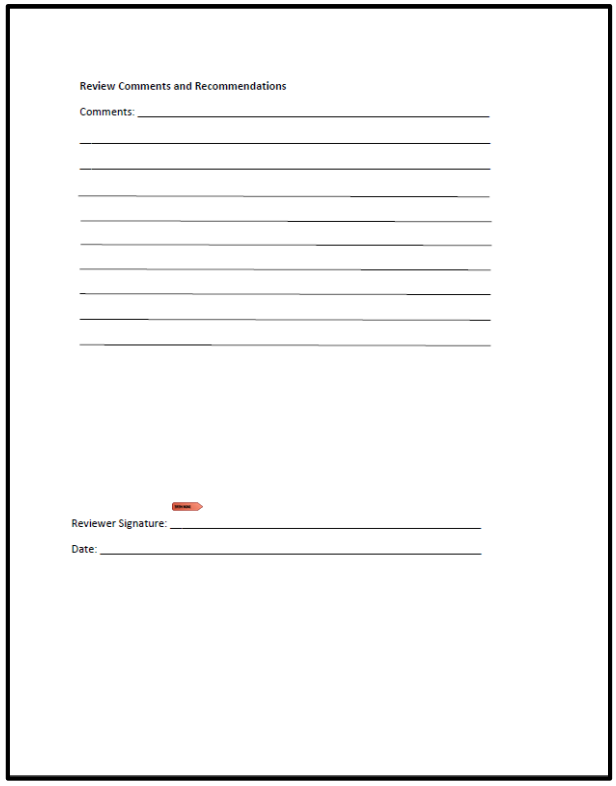
Business Resumption (Disaster Recovery)

Vendor's Business Resumption plan reviewed? ☐Yes ☐No ☐N/A

Test date: _____

Test results: _____

Comments: _____



Review Comments and Recommendations

Comments: _____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Reviewer Signature: _____

Date: _____

COMPLIANCE ADVISORY SERVICES

Vendor Management

Question	Answer	Weight
Would Loss of Service Create a Regulatory Exposure?	Yes	3
Would Loss of Service Create a Regulatory Exposure?	No	0
Would Loss of Service Create a Regulatory Exposure?	Possibly	2
Business Impact	Disruption in service would cause nominal business impact	1
Business Impact	Disruption in service would cause significant, but non-critical	2
Business Impact	Disruption in service would cause critical impact	3
Information Confidentiality	Contract contains privacy/confidential clause or no member information shared	1
Information Confidentiality	Contract includes privacy/confidentiality clause or addendum	2
Information Confidentiality	Contract lacks privacy/confidentiality clause	3
Expenditure Amount	Capital expenditure is less than $10,000	1
Expenditure Amount	Capital expenditure is between $10,000-$50,000	2
Expenditure Amount	Capital expenditure exceeds $50,000	3
Contract Term	Less than 1 Year	1
Contract Term	Between 1 and 3 Years	2
Contract Term	Greater than 3 years/Continuous	3
Information Sharing	No member information shared	1
Information Sharing	Only public information will be shared	2
Information Sharing	Non-public member information will be shared	3

Critical Contract Items

SLA = Service Level Agreement

RTO = Recovery Time Objective

RPO = Recovery Point Objective

Critical Contract Items

- Preventative
- Detective
- Corrective

Combination of the above should define exit strategy within third-party contract

COMPLIANCE ADVISORY SERVICES

Critical Contract Items

Gramm-Leach-Bliley Act (GLBA)

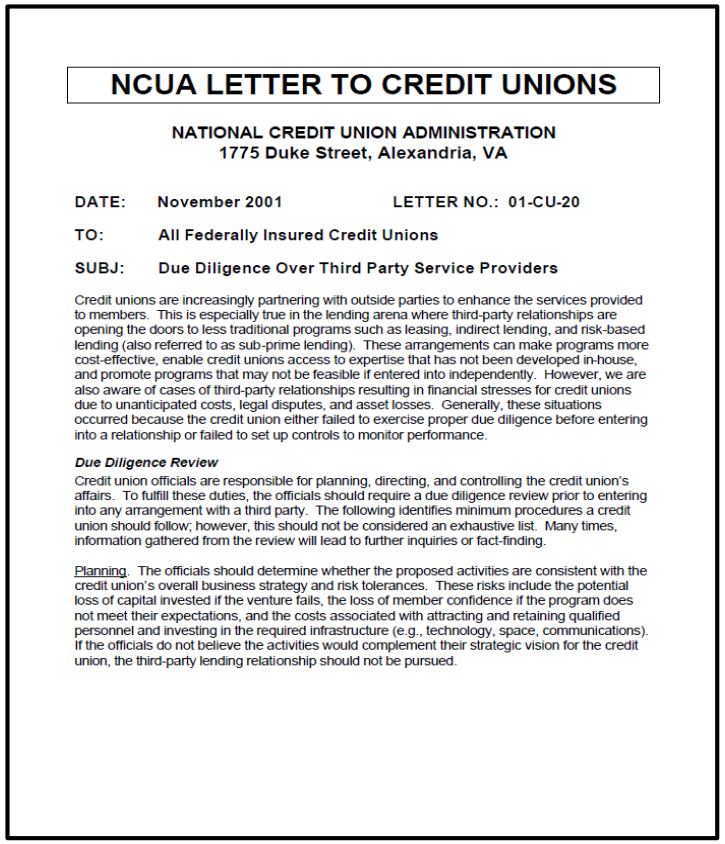
[Q] How will third-party safeguard member data? This should be enumerated within the contract. No accountability without language enumerating expectation.

Where to Start?

- NCUA Letter(s) To Credit Unions is a good place to start.
- Ultimate risk (legal, regulatory, reputational, etc.) rests with what entity, vendor or credit union?

NCUA Governing Guidance

Outsourcing Technology Services Appendix B: Laws, Regulations, and Guidance



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

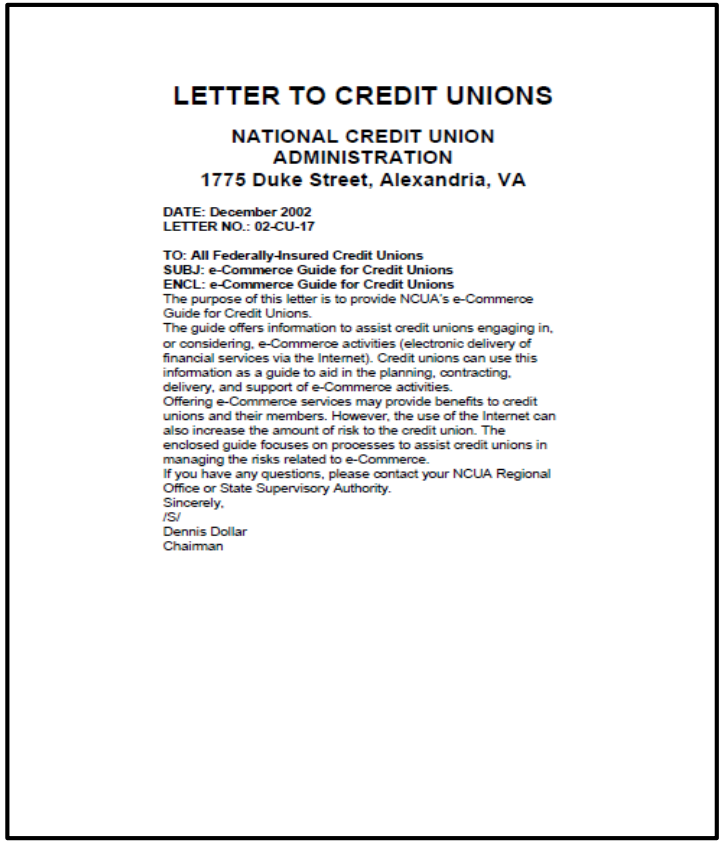
Credit unions are increasingly partnering with outside parties to enhance the services provided to members. This is especially true in the lending arena where third-party relationships are opening the doors to less traditional programs such as leasing, indirect lending, and risk-based lending (also referred 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.

http://ithandbook.ffiec.gov/media/resources/3554/ncu-01-cu_20_duedil_over_3rd_party_serv_providers.pdf



LETTER TO CREDIT UNIONS

NATIONAL CREDIT UNION ADMINISTRATION
1775 Duke Street, Alexandria, VA

DATE: December 2002
LETTER NO.: 02-CU-17

TO: All Federally-Insured Credit Unions
SUBJ: e-Commerce Guide for Credit Unions
ENCL: e-Commerce Guide for Credit Unions

The purpose of this letter is to provide NCUA's e-Commerce Guide for Credit Unions.

The guide offers information to assist credit unions engaging in, or considering, e-Commerce activities (electronic delivery of financial services via the Internet). Credit unions can use this information as a guide to aid in the planning, contracting, delivery, and support of e-Commerce activities.

Offering e-Commerce services may provide benefits to credit unions and their members. However, the use of the Internet can also increase the amount of risk to the credit union. The enclosed guide focuses on processes to assist credit unions in managing the risks related to e-Commerce.

If you have any questions, please contact your NCUA Regional Office or State Supervisory Authority.

Sincerely,

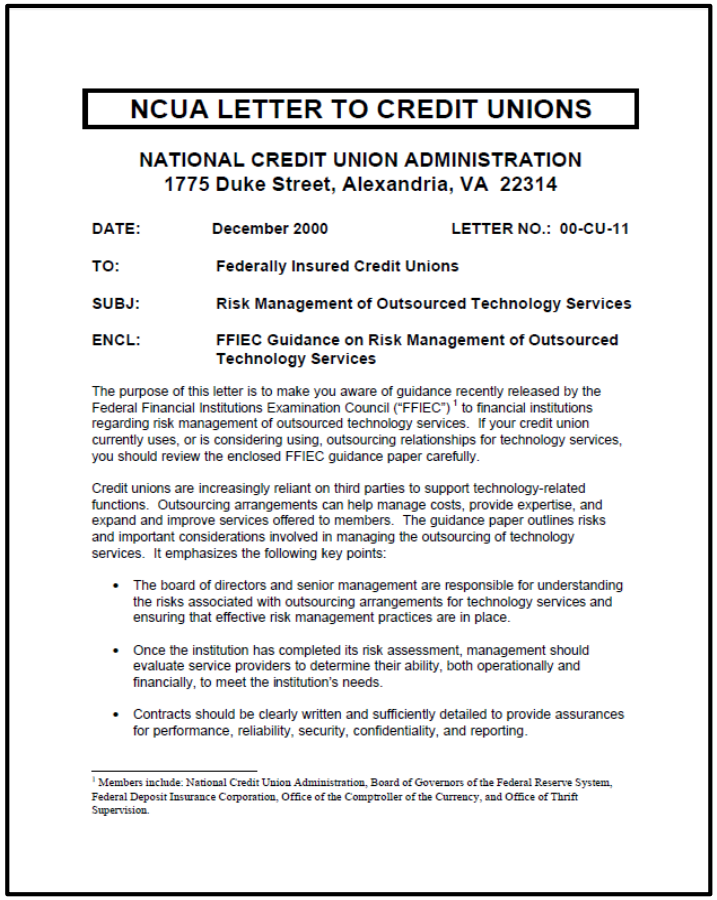
/S/
Dennis Dollar
Chairman

http://ithandbook.ffiec.gov/media/resources/3553/ncu-02-cu-17-e-comm_guide_credit_unions.pdf

COMPLIANCE ADVISORY SERVICES

NCUA Governing Guidance

FFIEC Information Technology Examination Handbook: Management (November 2015)



NCUA LETTER TO CREDIT UNIONS

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

DATE: December 2000 **LETTER NO.: 00-CU-11**

TO: Federally Insured Credit Unions

SUBJ: Risk Management of Outsourced Technology Services

ENCL: FFIEC Guidance on Risk Management of Outsourced Technology Services

The purpose of this letter is to make you aware of guidance recently released by the Federal Financial Institutions Examination Council ("FFIEC")[1] to financial institutions regarding risk management of outsourced technology services. If your credit union currently uses, or is considering using, outsourcing relationships for technology services, you should review the enclosed FFIEC guidance paper carefully.

Credit unions are increasingly reliant on third parties to support technology-related functions. Outsourcing arrangements can help manage costs, provide expertise, and expand and improve services offered to members. The guidance paper outlines risks and important considerations involved in managing the outsourcing of technology services. It emphasizes the following key points:

- The board of directors and senior management are responsible for understanding the risks associated with outsourcing arrangements for technology services and ensuring that effective risk management practices are in place.
- Once the institution has completed its risk assessment, management should evaluate service providers to determine their ability, both operationally and financially, to meet the institution's needs.
- Contracts should be clearly written and sufficiently detailed to provide assurances for performance, reliability, security, confidentiality, and reporting.

[1] Members include: National Credit Union Administration, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency, and Office of Thrift Supervision.

Included within the new FFIEC IT Management Handbook, yet not within governing guidance for 'Outsourcing Technology Services'.

https://www.ncua.gov/Resources/Documents/LCU2000-11.pdf

COMPLIANCE ADVISORY SERVICES

Takeaway

“Risk comes from not knowing what you're doing.”

–Warren Buffett

- What you don’t know can hurt you
- What you know and don’t act on will hurt you
- Gap Identification Expectation = Zero Defects

COMPLIANCE ADVISORY SERVICES

Additional Resources

NCUA Examiner's Guide - Chapter 6 – Information Systems and Technology
https://www.ncua.gov/Legal/GuidesEtc/ExaminerGuide/Chapter06.pdf

FFIEC Business Continuity Planning (February 2015)
http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_BusinessContinuityPlanning.pdf

FFIEC Business Continuity Planning - Appendix J: Strengthening the Resilience of Outsourced Technology Services
http://ithandbook.ffiec.gov/it-booklets/business-continuity-planning/appendix-j-strengthening-the-resilience-of-outsourced-technology-services.aspx

Questions?

Brian W. Vitale, CAMS-Audit, NCCO

Compliance Advisory Services, LLC

bvitale@complianceadvisoryllc.com

(574) 309-1757

COMPLIANCE ADVISORY SERVICES