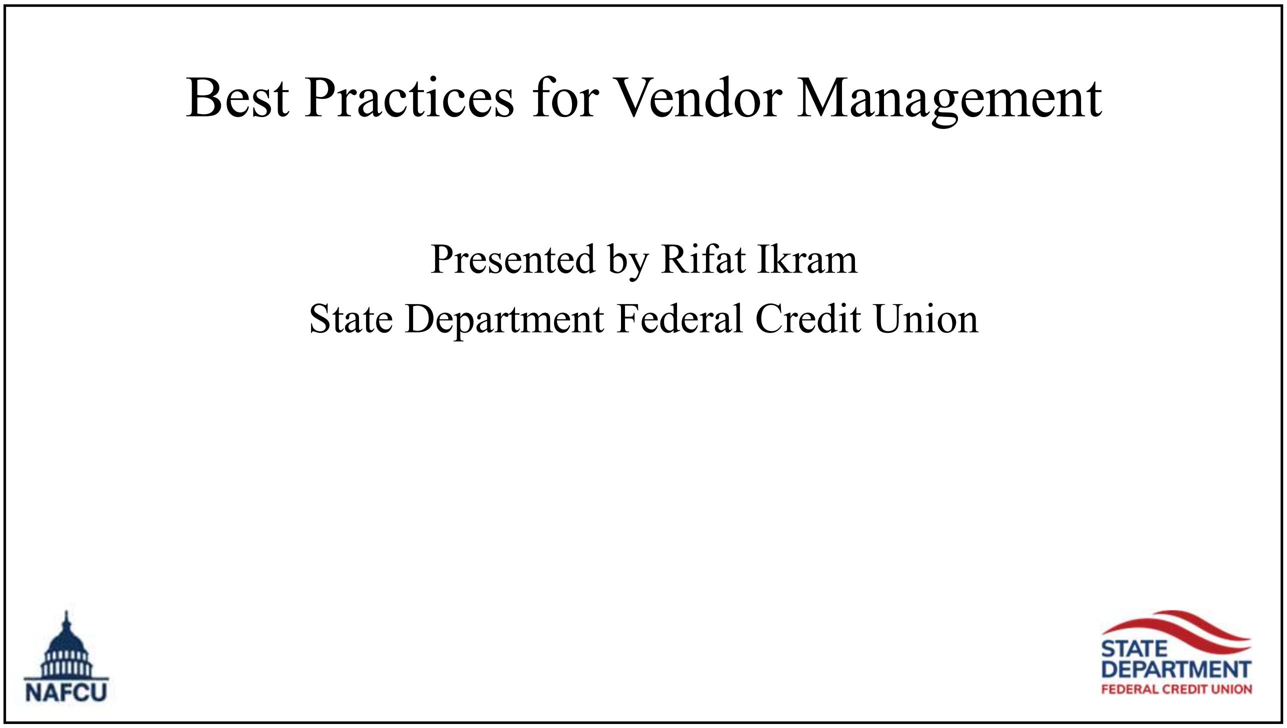
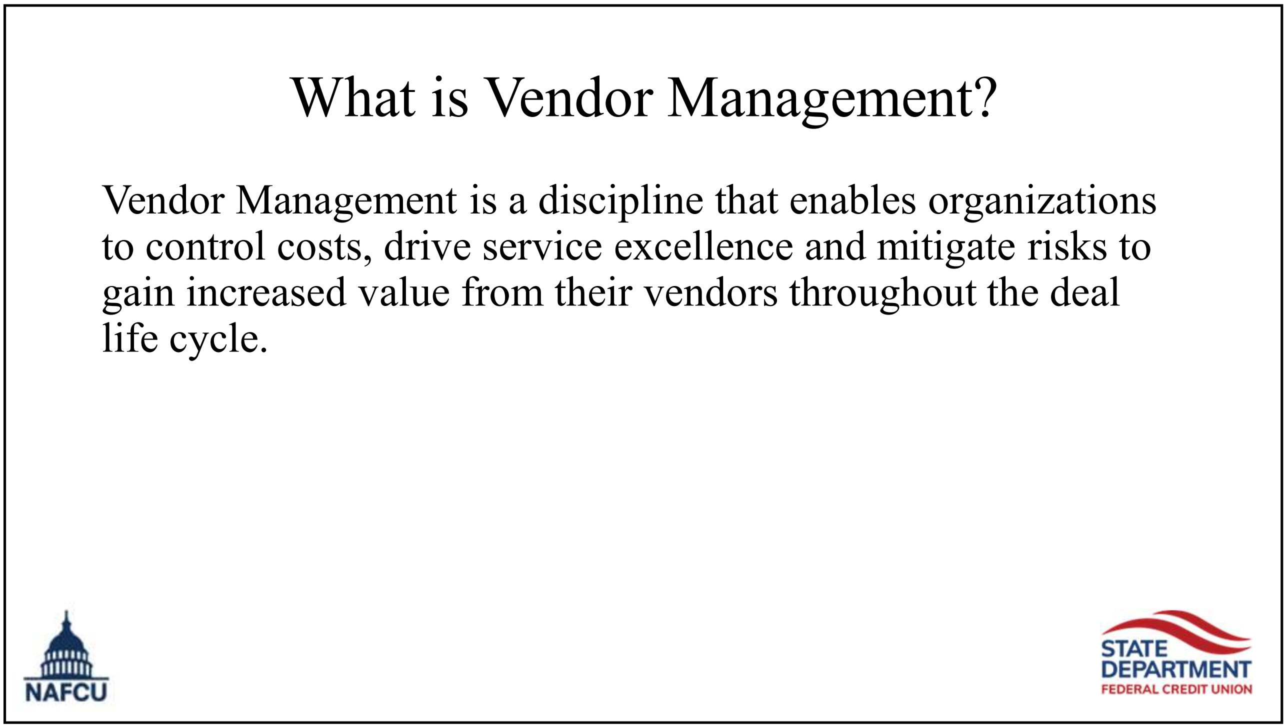


Best Practices for Vendor Management

Presented by Rifat Ikram

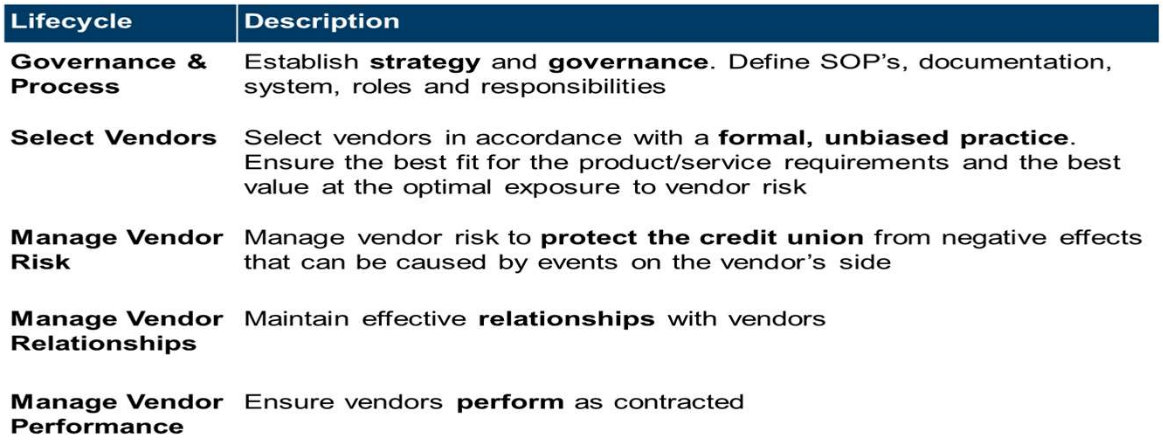
State Department Federal Credit Union



What is Vendor Management?

Vendor Management is a discipline that enables organizations to control costs, drive service excellence and mitigate risks to gain increased value from their vendors throughout the deal life cycle.

What is Vendor Management?



Lifecycle	Description
Governance & Process	Establish **strategy** and **governance**. Define SOP's, documentation, system, roles and responsibilities
Select Vendors	Select vendors in accordance with a **formal, unbiased practice**. Ensure the best fit for the product/service requirements and the best value at the optimal exposure to vendor risk
Manage Vendor Risk	Manage vendor risk to **protect the credit union** from negative effects that can be caused by events on the vendor's side
Manage Vendor Relationships	Maintain effective **relationships** with vendors
Manage Vendor Performance	Ensure vendors **perform** as contracted

Why is vendor management important for Credit Unions?

For most credit unions avoiding third-party service providers may not be an option. Service providers perform many key functions that can be critical to an credit union. A vendor management program can help a credit union mitigate the risks inherent in these relationships.

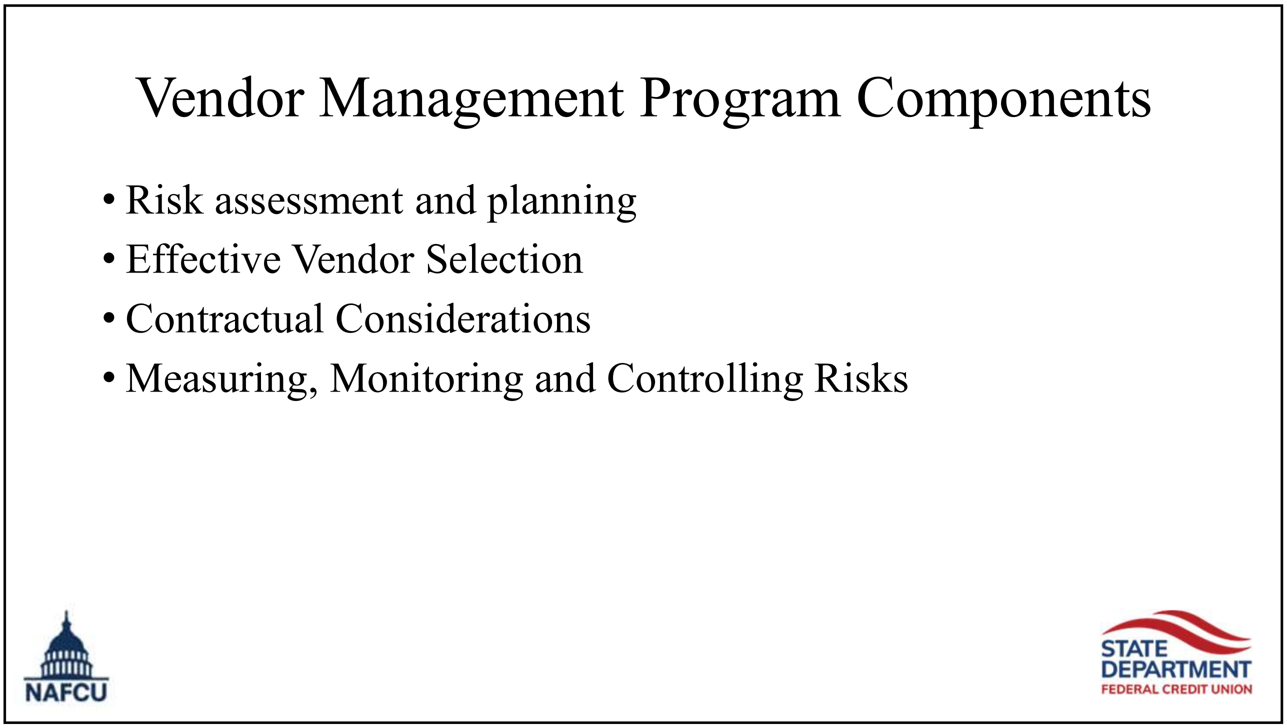
NCUA Minimum Scope

- Scope of arrangement, services offered and activities authorized;
- Responsibilities of all parties (including subcontractor oversight);
- 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.

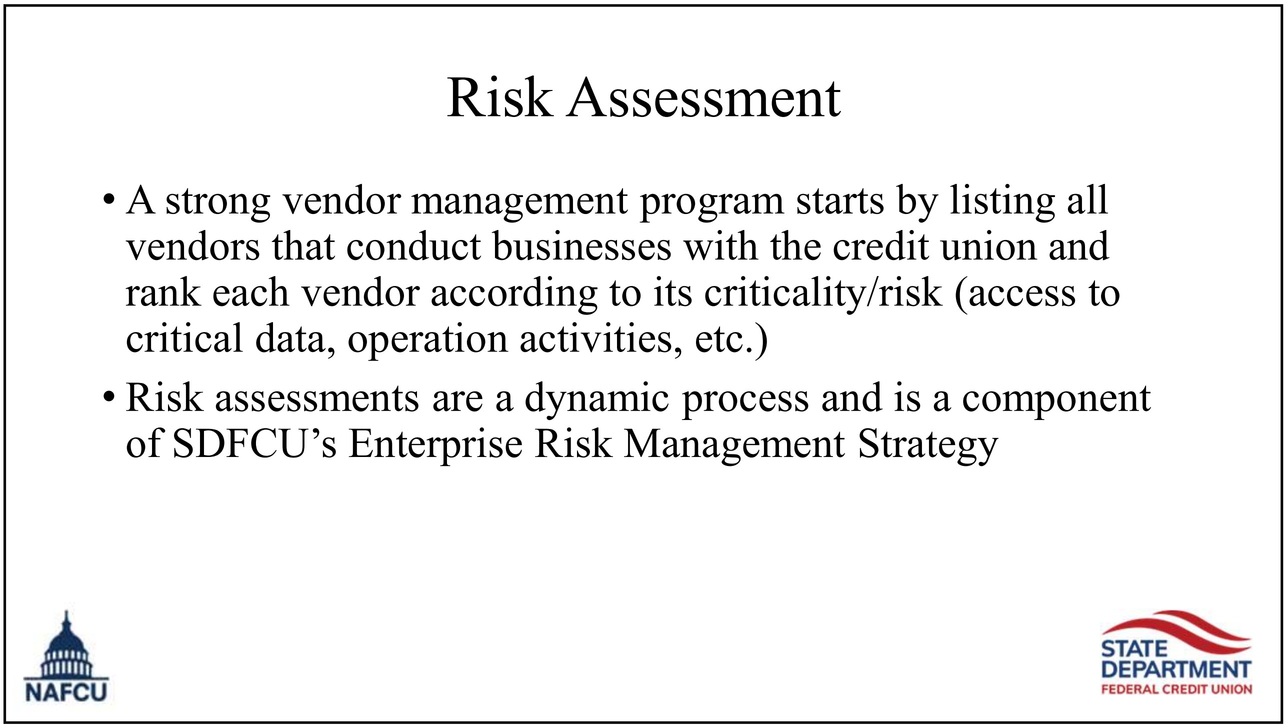
Risks Associated with Vendor Relationships

Strategic	Planning, implementation, scalability
Compliance	Legal and regulatory requirements
Reputational	Errors, delays, omissions, fraud, breaches
Interest Rate	Errors, inaccurate assumptions
Liquidity	Service disruptions, settlement delays
Cyber	Disruption, malware



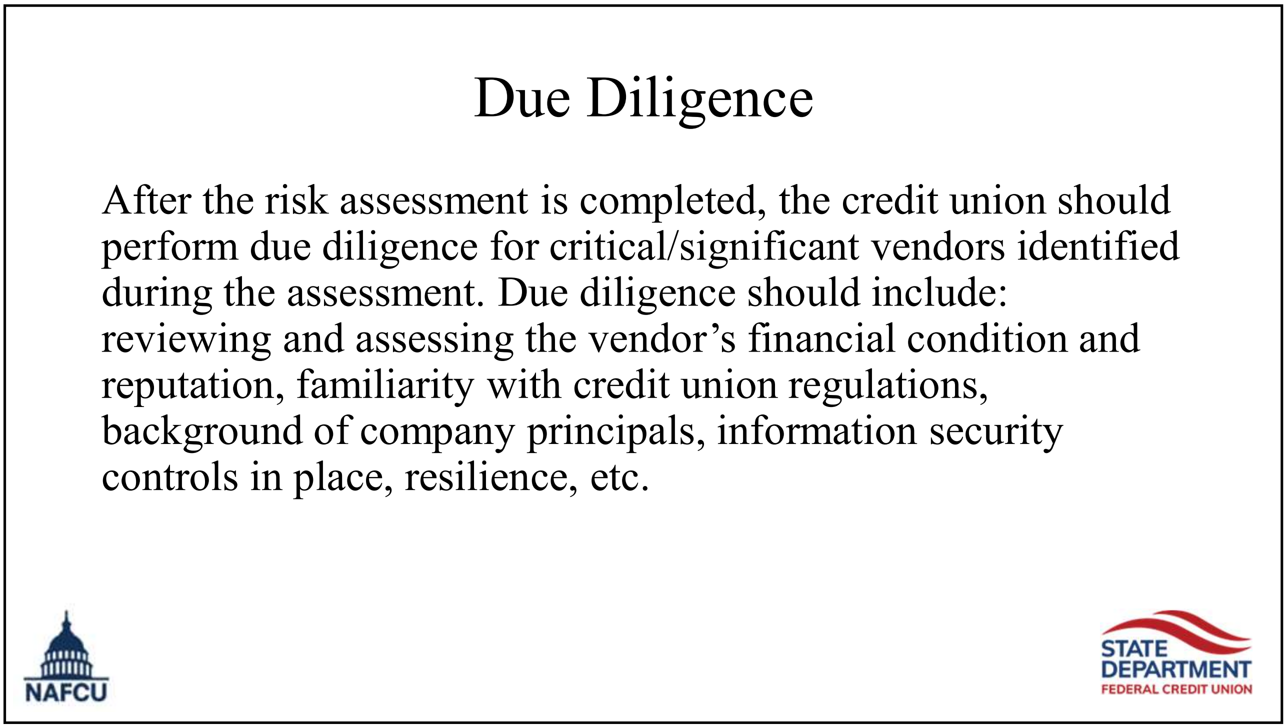
Vendor Management Program Components

- Risk assessment and planning
- Effective Vendor Selection
- Contractual Considerations
- Measuring, Monitoring and Controlling Risks



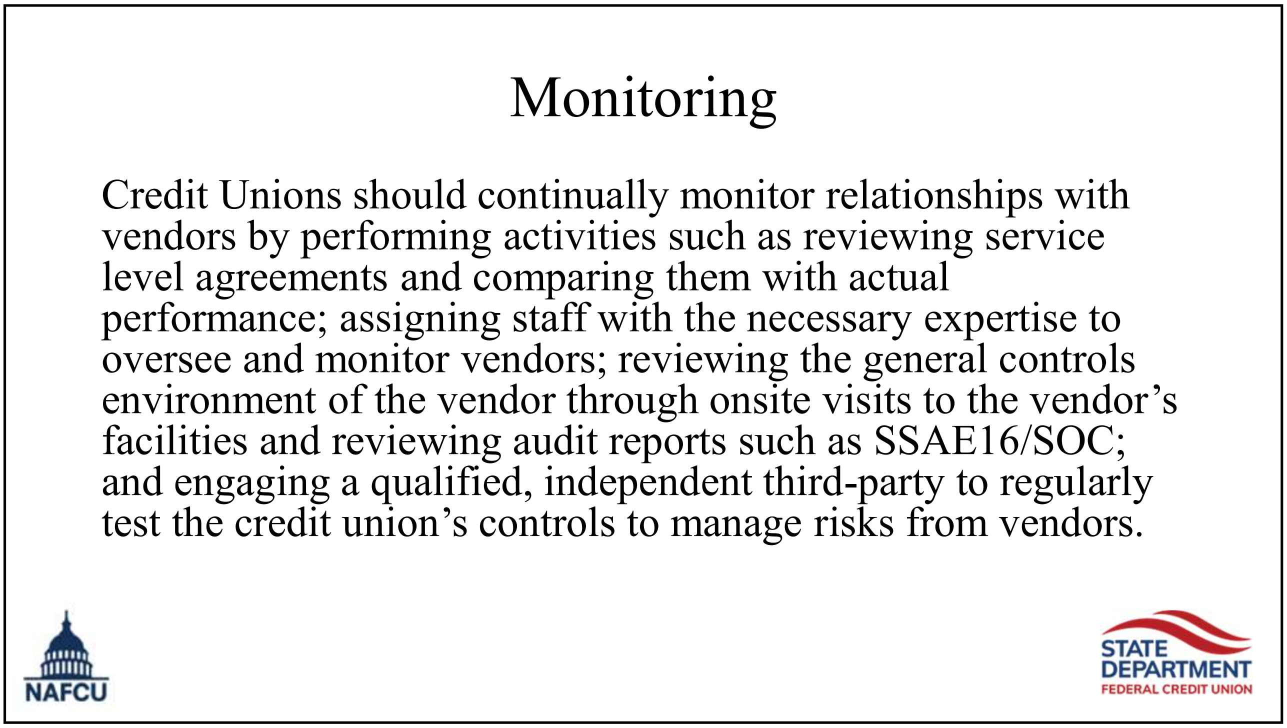
Risk Assessment

- A strong vendor management program starts by listing all vendors that conduct businesses with the credit union and rank each vendor according to its criticality/risk (access to critical data, operation activities, etc.)
- Risk assessments are a dynamic process and is a component of SDFCU's Enterprise Risk Management Strategy



Due Diligence

After the risk assessment is completed, the credit union should perform due diligence for critical/significant vendors identified during the assessment. Due diligence should include: reviewing and assessing the vendor’s financial condition and reputation, familiarity with credit union regulations, background of company principals, information security controls in place, resilience, etc.



Monitoring

Credit Unions should continually monitor relationships with vendors by performing activities such as reviewing service level agreements and comparing them with actual performance; assigning staff with the necessary expertise to oversee and monitor vendors; reviewing the general controls environment of the vendor through onsite visits to the vendor’s facilities and reviewing audit reports such as SSAE16/SOC; and engaging a qualified, independent third-party to regularly test the credit union’s controls to manage risks from vendors.

Documentation and Reporting

Credit unions should retain proper documentation to facilitate the accountability and monitoring of the vendor management program. That documentation may include: current inventory of vendors (IT and non IT), due diligence results, contracts, risk management reports, reports to the board of directors, and independent review reports.

Contracts

For data security reasons, credit unions should store a copy of vendor contracts off-site. Contracts should generally address the following:

- Nature and scope of services
- Duration of the contract
- Right to audit
- Cost
- Confidentiality and integrity
- Contingency plans.

Vendor Relationship Termination

Credit unions should also have processes in place regarding the transition or discontinuation of vendor activities when a relationship with a vendor ends.

Nondisclosure/Confidentiality Agreements

- Credit Union should have written nondisclosure/confidentiality agreement with vendors, especially if the vendor has access to the credit union's critical data in any form (written, verbal, or electronic).
- Vendors who fall into this category may include security guards, cleaning services and contractors who have unsupervised access to the credit union's facilities where critical data can be obtained.

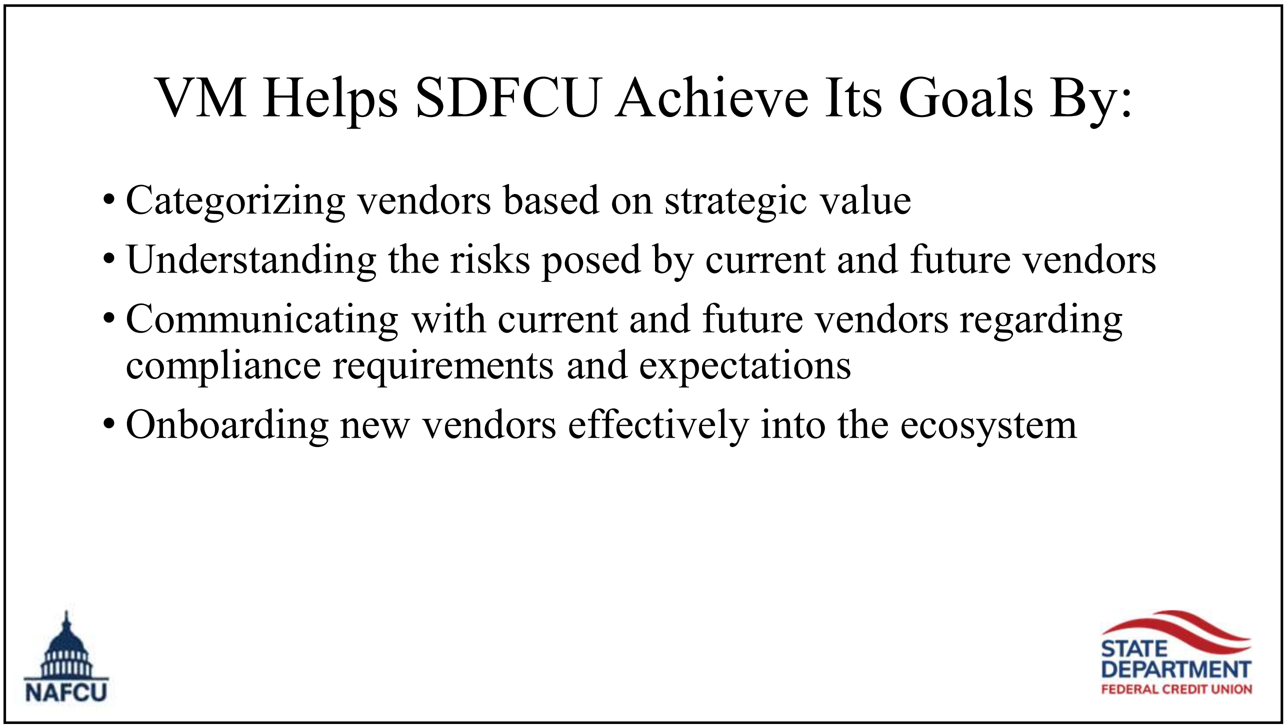
Challenges and Data Breaches

Ponemon Institute announced results of 2018 shows that 61% of companies experienced a Third-Party data breach, yet only 16% say they effectively mitigate third party risks

- Capital One
- Equifax

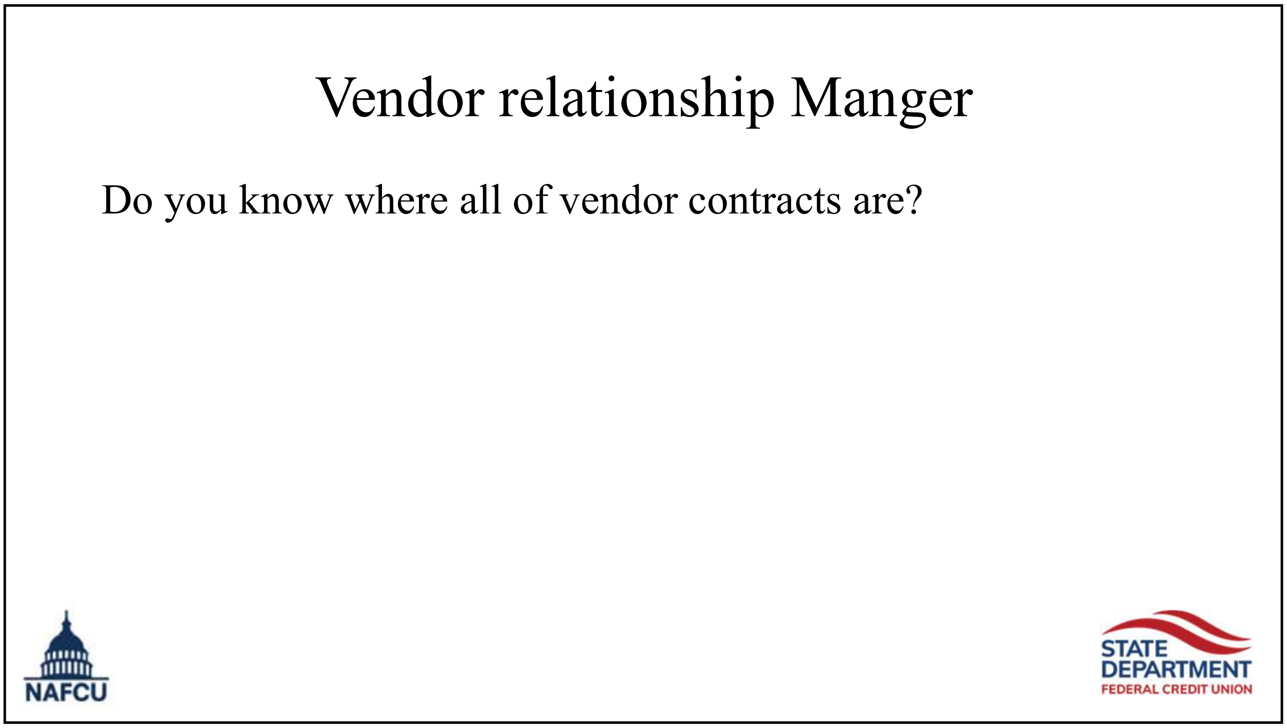
Who is responsible for Vendor Management at SDFCU?

- Compliance
- Information Technology
- Operations
- ??????????



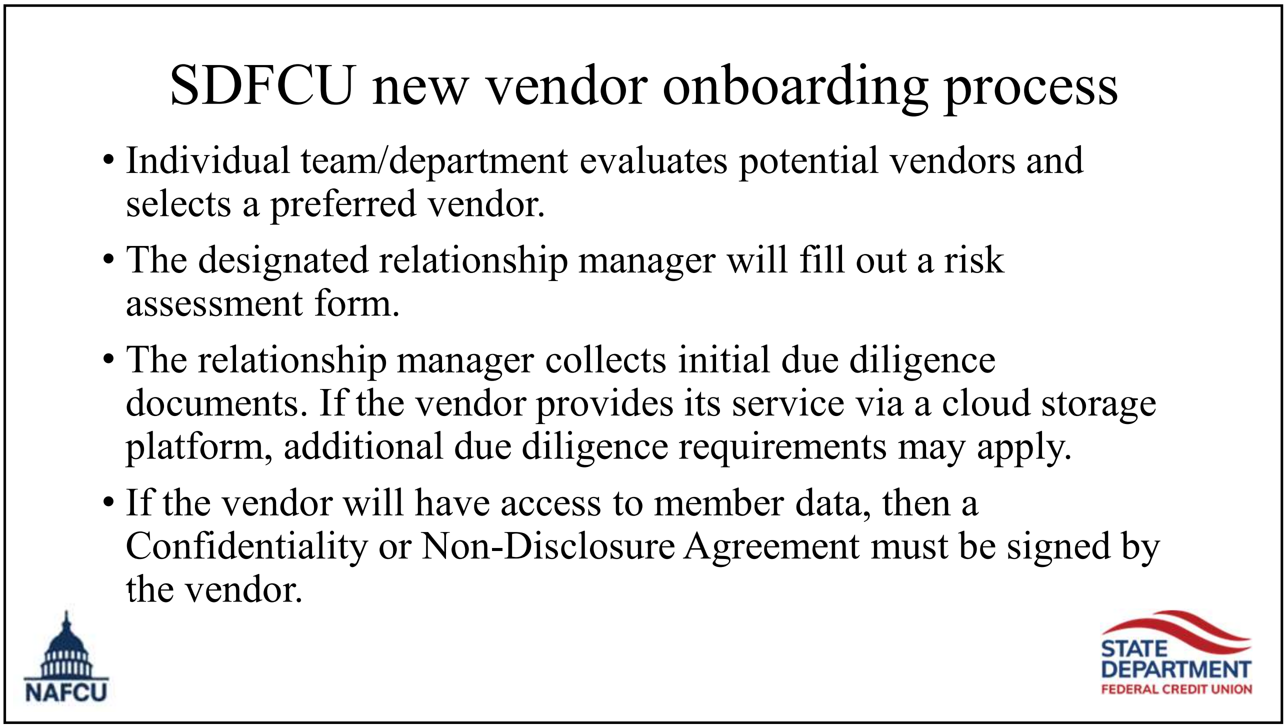
VM Helps SDFCU Achieve Its Goals By:

- Categorizing vendors based on strategic value
- Understanding the risks posed by current and future vendors
- Communicating with current and future vendors regarding compliance requirements and expectations
- Onboarding new vendors effectively into the ecosystem



Vendor relationship Manger

Do you know where all of vendor contracts are?

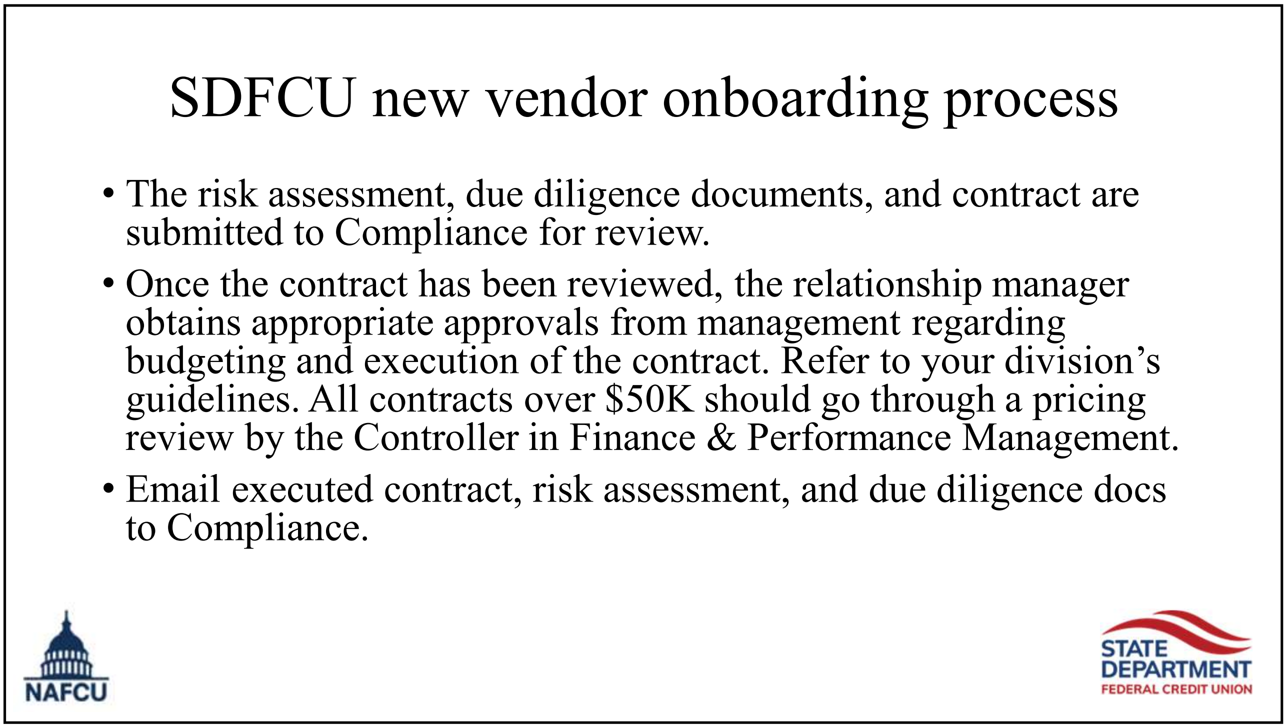


SDFCU new vendor onboarding process

- Individual team/department evaluates potential vendors and selects a preferred vendor.
- The designated relationship manager will fill out a risk assessment form.
- The relationship manager collects initial due diligence documents. If the vendor provides its service via a cloud storage platform, additional due diligence requirements may apply.
- If the vendor will have access to member data, then a Confidentiality or Non-Disclosure Agreement must be signed by the vendor.

NAFCU

STATE DEPARTMENT FEDERAL CREDIT UNION



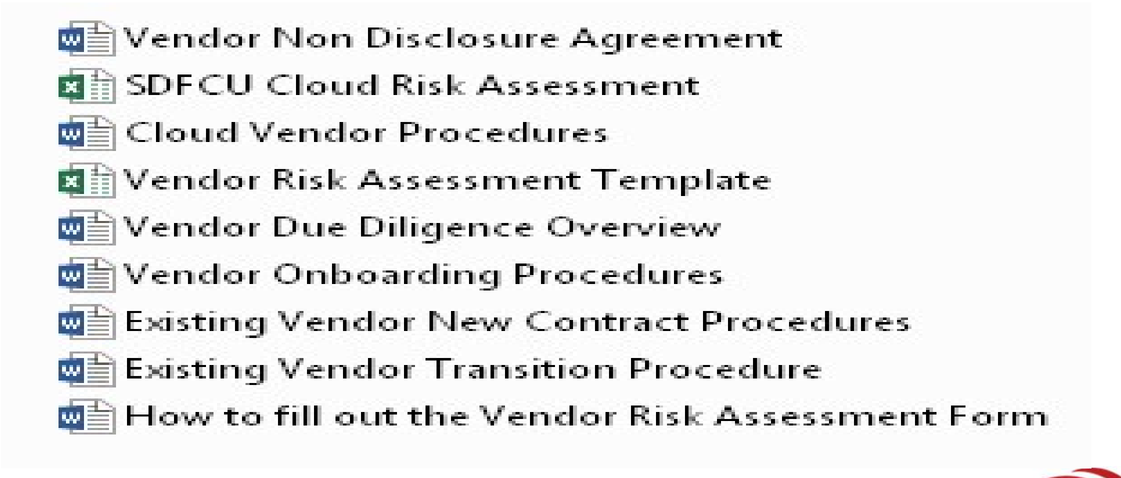
SDFCU new vendor onboarding process

- The risk assessment, due diligence documents, and contract are submitted to Compliance for review.
- Once the contract has been reviewed, the relationship manager obtains appropriate approvals from management regarding budgeting and execution of the contract. Refer to your division's guidelines. All contracts over $50K should go through a pricing review by the Controller in Finance & Performance Management.
- Email executed contract, risk assessment, and due diligence docs to Compliance.

NAFCU

STATE DEPARTMENT FEDERAL CREDIT UNION

SDFCU new vendor onboarding process



- Vendor Non Disclosure Agreement
- SDFCU Cloud Risk Assessment
- Cloud Vendor Procedures
- Vendor Risk Assessment Template
- Vendor Due Diligence Overview
- Vendor Onboarding Procedures
- Existing Vendor New Contract Procedures
- Existing Vendor Transition Procedure
- How to fill out the Vendor Risk Assessment Form

Takeaways

- Better understanding how vendors are currently being managed
- Familiarize yourself with the current information regarding your assigned vendors
- Regularly assess and monitor the effectiveness of your vendors, not just at the vendor selection stage

Vendor Relationship Manager Checklist

- I have read the contract, including all attachments and exhibits
- All terms and conditions of the contract conform with the final negotiations/agreements of the parties
- No supplementary verbal or written agreements were made
- All documents incorporated by reference in the contract, including exhibits and appendices, are attached
- The contract adequately describes all that the other party must do to make the project work

Vendor Relationship Manager Checklist

- Those carrying out the contract can meet the terms of the contract (e.g. the work can be completed, and it can be completed according to any time limits provided in the contract; we will be able to hire the personal specified in the contract etc.)
- Everyone necessary at the CU has signed off on the project
- This contract does not conflict with any other contracts, promises or obligations or the CU, e.g. exclusive use

What is a contract

- A contract is an agreement between two or more parties to do, not do, or promise something.
- Contracts can come in many forms- they can be oral or written, implied or express, and legally enforceable or not.
- The strongest contract, in terms of enforceability has an:
  - Offer,
  - Acceptance
  - Consideration for the exchange,
  - Cleary sets out the terms of the agreement without ambiguity, and
  - Is signed by the involved parties with proper capacity to enter into the contract.

Basic Contract Negotiation Tips

- Remember who created the contract form and who will benefit
- Get a copy of the contract as early as possible
- If the language works, keep using it
- If changes are agreed to, make SURE to put them into the contract
- Nothing sacred about “boilerplate” language
- Contract renewal means vendor re-selection.

Negotiating the Contract

- All Contracts involve Compromise- Vendor Due Diligence will give us a better understanding of what is available for service being purchased, the price and whether the vendor is reliable
- Understand your bargaining position
  - Changes often require “legal” review by vendor
  - Adds cost, delay
  - You will often hear- “legal won’t let us change it.”

Negotiating the Contract

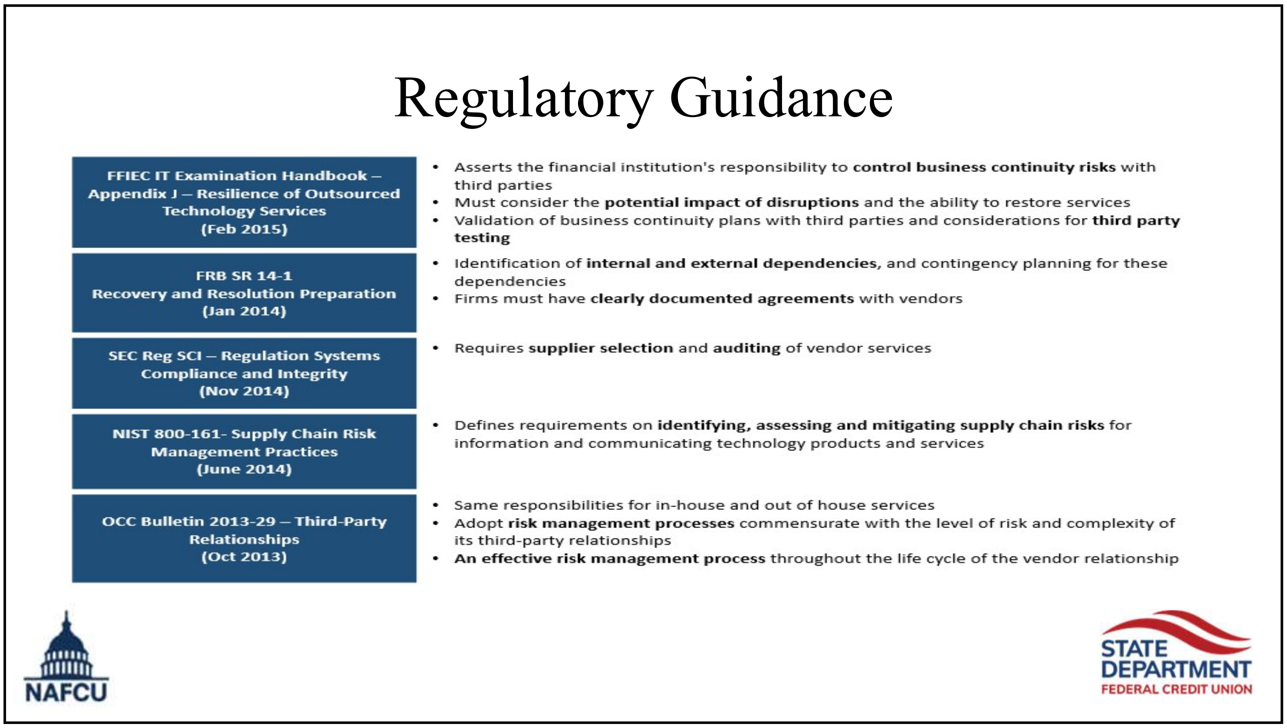
- Set Realistic Expectations
  - Price and Term usually negotiable
  - We deserve a clear statement in the contract of what the Product/Service is and is expected to do
  - Privacy and Data Security MUST meet Minimum Compliance Standards-aim high
  - Always be prepared to walk away

A Final Review

- Do your Vendor Due Diligence
- Keep a Complete File of Everything the Sales Rep Said and You Received from the Company
- Negotiate realistically
- Put Details in the proposal
- Get the Contract ASAP to begin the review

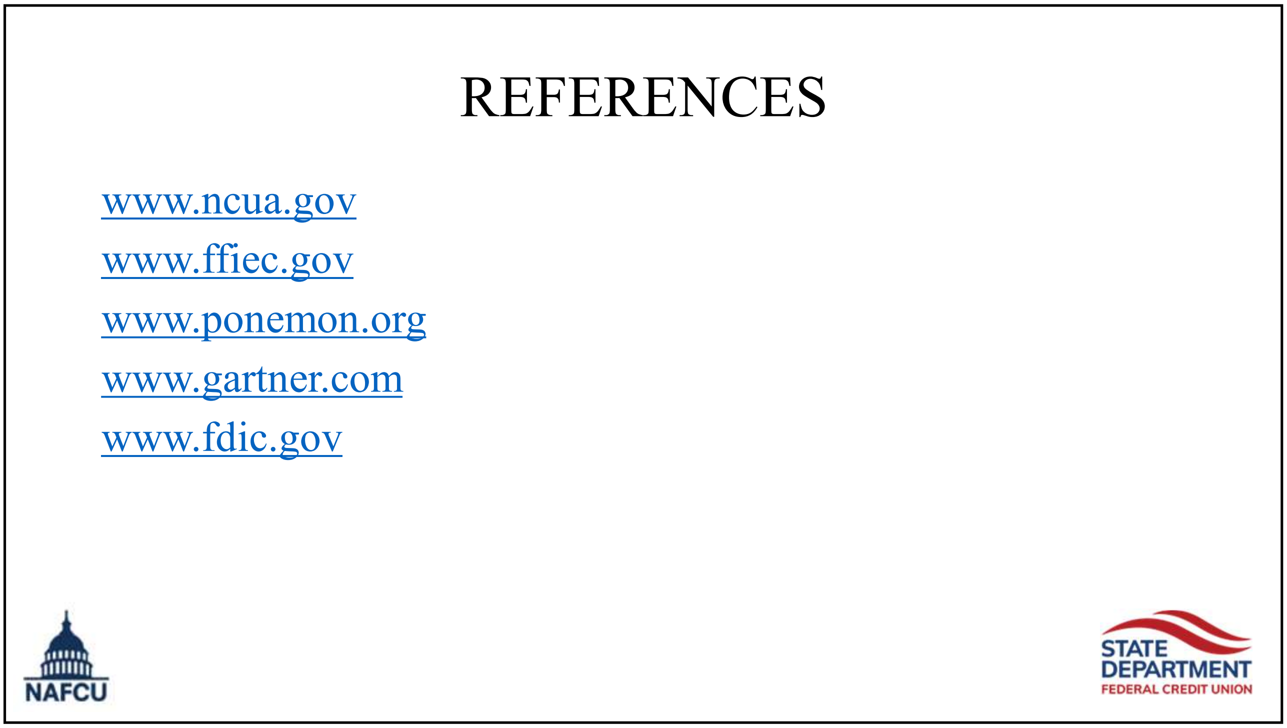
A Final Review

- Focus on Term, Price, Security and Contract Clarity- do the pieces fit?
- Lock Down Internal Accountability Issues
- Monitor Performance- Pounce on Nonperformance and document it
- Check the Invoices- Mitigate surprises
- Remember- Contract Renewal means renegotiation.



Regulatory Guidance

FFIEC IT Examination Handbook – Appendix J – Resilience of Outsourced Technology Services (Feb 2015)	• Asserts the financial institution's responsibility to **control business continuity risks** with third parties • Must consider the **potential impact of disruptions** and the ability to restore services • Validation of business continuity plans with third parties and considerations for **third party testing**
FRB SR 14-1 Recovery and Resolution Preparation (Jan 2014)	• Identification of **internal and external dependencies**, and contingency planning for these dependencies • Firms must have **clearly documented agreements** with vendors
SEC Reg SCI – Regulation Systems Compliance and Integrity (Nov 2014)	• Requires **supplier selection** and **auditing** of vendor services
NIST 800-161- Supply Chain Risk Management Practices (June 2014)	• Defines requirements on **identifying, assessing and mitigating supply chain risks** for information and communicating technology products and services
OCC Bulletin 2013-29 – Third-Party Relationships (Oct 2013)	• Same responsibilities for in-house and out of house services • Adopt **risk management processes** commensurate with the level of risk and complexity of its third-party relationships • **An effective risk management process** throughout the life cycle of the vendor relationship



REFERENCES

www.ncua.gov

www.ffiec.gov

www.ponemon.org

www.gartner.com

www.fdic.gov