CUNA MUTUAL GROUP

Vendor Due Diligence

a Risk & Compliance Solutions Webinar

A vendor relationship involves more than just signing on the dotted line.

Today's Expert Panelists

Carlos Molina **Jim Bullard**

Risk & Compliance Solutions • 800.637.2676 • RiskConsultant@cunamutual.com

What's On Tap?

- Vendor Management Policy
- Ownership / Responsibility
- Outsource vs. In-house
- Due Diligence & Contracts
- Measuring, Monitoring & Controlling Risk

and more...

Vendor Management Program

- Scope
- Risk & Criticality Assessments
- Due Diligence
- Vendor Selection & Contract Management
- Monitoring
- Termination & Exit Strategies
- Executive Management / Board Support

CUNA MUTUAL GROUP

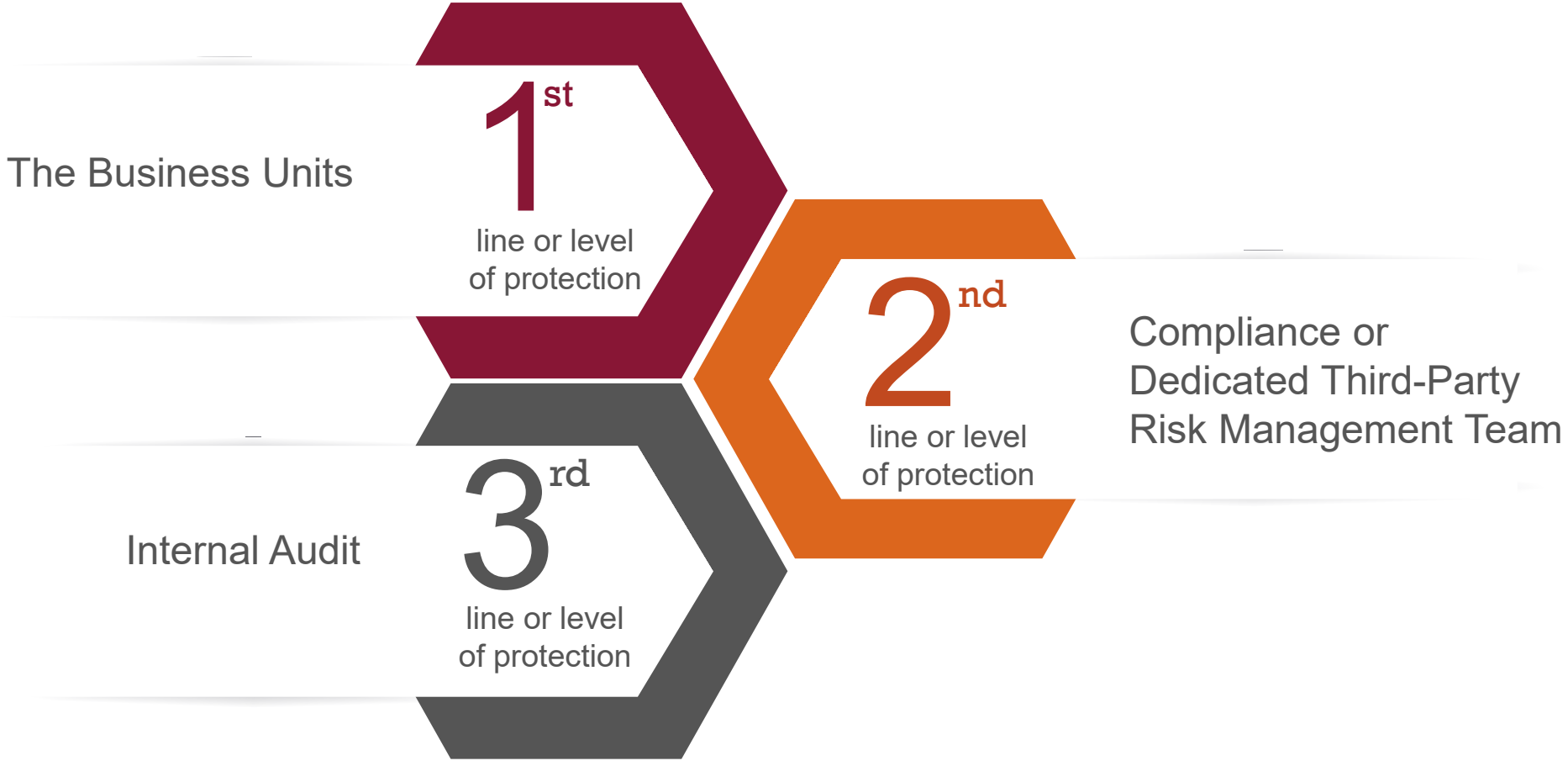
Vendor Management Policy Components

- Policy Statement
- Purpose
- Responsibilities
- Risk Assessment Process
- Vendor Classifications
- Risk Categories
- Due Diligence Requirements
- Contract Review
- Monitoring

Who owns the vendor management process?

CUNA MUTUAL GROUP

Vendor Management Ownership



Best Practices for Relationship Owners

Strong internal knowledge of subject matter

Decision-maker or access to a decision-maker

Outsource to a vendor management service

Clear focus of credit union strategy

- Financial Review
- Insurance Coverage
- Customer Experience / Complaints
- Business Continuity Plan / Disaster Recovery Testing Results
- SOC Audit & IT Audit Reports
- Contract Documentation

Prior to vendor onboarding

CUNA MUTUAL GROUP

When executing a contract…

- Ensure the contract clearly defines the rights and responsibilities of both parties;
- Ensure the contract contains adequate and measurable service level agreements;
- Ensure contracts with affiliates clearly reflect an arms-length relationship and costs and services are at least as favorable to the credit union as those available from a non-affiliated provider;
- Choose the most appropriate pricing method for the financial institution's needs;
- Ensure the contract does not contain provisions or inducements that may have a significant, adverse affect on the institution;
- Engage legal counsel to review the contract

Remember who created the contract form and who will benefit.

Are there any deal-breakers that we should lookout for?

Contractual Provision Considerations

Mandatory

- Scope of Service
- Performance Standards
- Schedule & Price
- Standard of Care
- Limitation of Liability
- Waiver of Consequential Damages
- Mutual Indemnification
- Security and Confidentiality
- Warranties
- Business Resumption / Contingency Plans

Nice-to-Have / Situational

- Vendor Personnel
- Notice of Breach
- Opportunity to Cure
- Reports, Records, Access, and Right to Audit
- Vendor Insurance Minimums
- Independent Contractor Relationship

Heightened Risk / Deal Breakers

- Legal Compliance
- Regulatory Requirements
- Force Majeure Exception (e.g., Covid-19)
- Performance / Key Deliverables

Vendor Risk Classification

Non-Essential

No access to member PII

No access to credit union's network

e.g., an office supplies vendor who never has direct access to your organization's facilities or information

Significant

Possible / minimal access to member PII and/or credit union's network

e.g., a networking consultant who is responsible for maintaining the internal network, which is important for operations, but only has intermittent access to some private information

Critical

Access to member PII

Access to credit union's network

e.g., a core provider or host, who is both responsible for private / customer information, and is vital to your operation

Performance Standards

- Monitoring compliance of contractually-agreed upon KPIs and SLAs
- Identifying areas where the vendor is not performing to expectations
- Partnering with the vendor to resolve low vendor performance
- Benchmarking the vendor's performance against similar vendors
- Resolving poor performance trends before they impact productivity
- Partnering with the business unit(s) to ensure they are engaged with and utilizing the vendor's services

What suggestions do you have for third-parties that won't negotiate?

Negotiation Tips

- ☐ 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 may mean vendor re-selection
- ☐ Understand your bargaining position
- ☐ Changes often require “legal” review by vendor which can add cost, delay
- ☐ Price and Term are usually negotiable
- ☐ Insist upon a clear contract statement of what the Product/Service is and is expected to do
- ☐ Privacy and Data Security must meet Minimum Compliance Standards
- ☐ Always be prepared to walk away

Stages of a Mature Vendor Management Program

1

Compliant

directed toward compliance with regulation and laws

2

Collaborative

aims to drive more engagement and opportunities for cost savings and opportunity

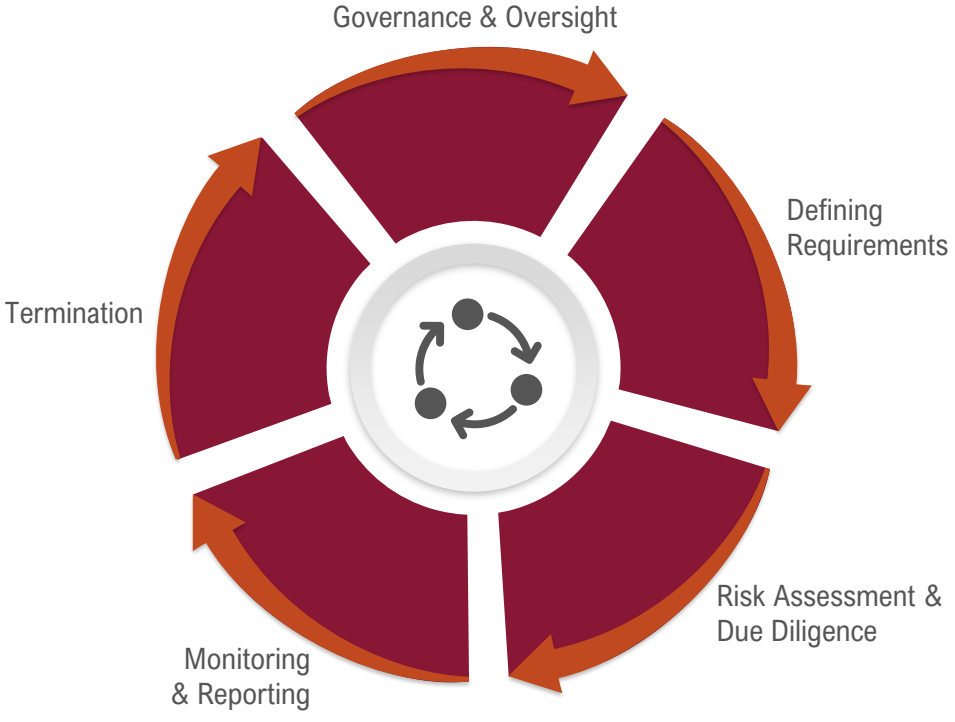
3

Strategic

relationships grow into strategic partnerships leading to additional growth, service and innovation

The goal should be to adopt an approach that is beyond simple compliance, that enhances vendor management capabilities within the credit union and maximize key vendor relationships

Key Elements for Mature Vendor Management Processes



The effectiveness and sophistication of a credit union's vendor management will depend on how they assemble and develop these elements

Decentralized

- Different vendor management teams per line of business
- Greater flexibility for individual line of business
- Misaligned objectives, distributed decision making

Centralized

- Management is consolidated, line of business responsible for execution
- Clear decision-making authority
- Lack of lob area knowledge leads to fractured strategies

Continuous vendor management improvement

Factors of effective measurement

- Performed timely
- Metrics are appropriate for the vendor type and credit union line of business
- Key stakeholders are engaged
- Aligned with service levels defined in contracts
- Establish improvement plans and actions

Examples of performance metrics

- Percentage or number of SLA nonconformance
- Escalation issues
- Price variances from contract
- Negative news or internal risks reported per quarter

How should credit unions handle fourth-party risks?

Examining Fourth Party Risk Issues

Fourth party outsourcing risks to consider.

Outsourcing Risks

- Financial
- Strategic
- Reputation
- Geolocation
- Credit
- Quality

Possible Implications

- Difficulties or failures
- Misalignment with objectives
- Brand / organizational impacts
- Consent orders, fines and penalties
- Sanctions due to country
- Inability to make payments
- Inability to deliver in line with SOW specs

Service-Level Risks

- Cyber
- Compliance
- Legal
- Intellectual Property
- Privacy
- Contractual
- Operational
- Resiliency

Can Result In

- Impacts to confidentiality, integrity or availability of information / services
- Non-alignment with standards / frameworks
- Failure to meet contract obligations
- Failures that impact operations
- Inability to provides services

A Fourth Party is your vendor's third party or subcontractor and is vulnerable to the same risk as your third parties.

Continuous vendor management improvement

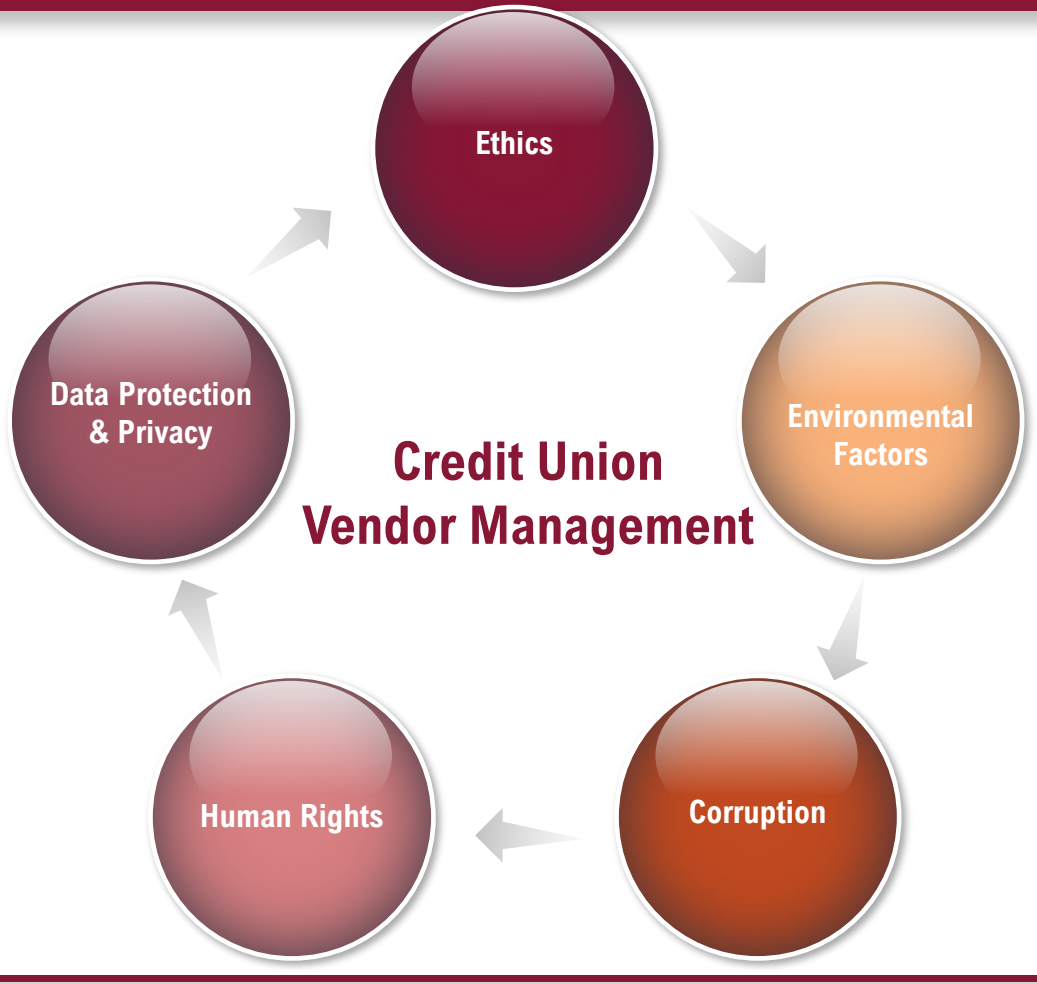
Risk Indicators

- Are all the mission critical third parties with fourth parties identified and risk assessed during the third-party selection phase?
- Are all parties that touch sensitive data identified and a risk assessment performed prior to gaining access?
- Are all parties that are consumer-facing (direct contact, mail/email or systems) identified prior to gaining access to the credit union's consumers?
- Do contracts define roles and responsibilities, including monitoring of specific risk factors and compliance with regulations?

Mitigation Tips

- Fourth party SLAs or contract template(s) that include requirement of a risk management program comparable to the outsourcer's third-party risk area requirements
- Automated collection of publicly accessible data (news, data collection and reporting agencies, management dashboard tool providers, etc.) that divulge fourth party relationships, even if the third-party provider has not divulged those to the outsourcer
- Security Information and Event Management (SIEM) documentation demonstrating follow through of reported material event(s)

Why ESG Factors Matter…



Help examine how an organization contributes to and performs on environmental, social, and ethical challenges, and the overall governance of the organization.

The vendor management program goal is to build greater understanding, vision, and insight into the extended enterprise and align the credit union's strategic and operational goals with any ESG initiatives

CUNA Mutual Group

Risk & Protection Response Center

800.637.2676

Select you're a credit union, then choose option 4

riskconsultant@cunamutual.com

Ask a Risk Manager interactive form

Facing risk challenges?

- Protection Resource Center
- RISK Alerts – **Warning** ◆ **Watch** ◆ **Awareness**
- RISK Alert Library
- Risk Insider: Emerging Risks
- Loss Prevention Library (risk overviews, checklists)
- On-Demand Webinars & Training Modules

Not receiving RISK Alerts? Sign-up today

"Great webinars - serious, important information delivered in a relaxed, 'we're among friends' way."

$9B credit union

Related Risk Resources

Vendor Management Risk Overview

Vendor Due Diligence Contract Provisions

Vendor Contract Provisions Checklist

Vendor Performance and Reporting Overview

Access more Risk Resources and RISK Alerts:

www.cunamutual.com/prc

CUNA MUTUAL GROUP

This presentation was created by the CUNA Mutual Group based on our experience in the credit union and insurance market. It is intended to be used only as a guide, not as legal advice. Any examples provided have been simplified to give you an overview of the importance of selecting appropriate coverage limits, insuring-to-value and implementing loss prevention techniques. No coverage is provided by this presentation/ publication, nor does it replace any provisions of any insurance policy or bond.

CUNA Mutual Group is the marketing name for CUNA Mutual Holding Company, a mutual insurance holding company, its subsidiaries and affiliates. Insurance products offered to financial institutions and their affiliates are underwritten by CUMIS Insurance Society, Inc. or CUMIS Specialty Insurance Company, members of the CUNA Mutual Group. Some coverages may not be available in all states. If a coverage is not available from one of our member companies, CUNA Mutual Insurance Agency, Inc., our insurance producer affiliate, may assist us in placing coverage with other insurance carriers in order to serve our customers' needs. For example, the Workers' Compensation Policy is underwritten by non-affiliated admitted carriers. CUMIS Specialty Insurance Company, our excess and surplus lines carrier, underwrites coverages that are not available in the admitted market. Cyber policies are underwritten by Beazley Insurance Group or other nonaffiliated admitted carriers.

This summary is not a contract and no coverage is provided by this publication, nor does it replace any provisions of any insurance policy or bond. Please read the actual policy for specific coverage, terms, conditions, and exclusions.

www.cunamutual.com