



Risk & Compliance Solutions | Webinar

Improving your Vendor Oversight

Common risk themes & overlooked controls

Proprietary and confidential. Do not distribute.



Today's session



Brianda Rojas-Levering

Risk Consultant – Kentucky
TruStage™



Jim Bullard

Senior Risk Consultant – Georgia
TruStage™



→ | **What's on tap?**

Effective vendor oversight



- Act as a roadmap
- Clearly define roles, responsibilities and expectations
- Facilitate a positive relationship
- Ensure the quality and safety of the work it provides



Many organizations are still in the crawl stage of vendor management



Vendor management program maturity

- Documented processes for entire vendor lifecycle?
- Enterprise-wide understanding of vendor risk?
- Automated system for vendor onboarding?
- Automated data collection & monitoring system for critical vendors?
- Frequent and honest communication with critical vendors?
- Vendor scorecards to monitor performance?
- Ability to capture and analyze cost for all vendors?

7 challenging focus areas



Most overlooked items in vendor management?

 Meg in Indiana

- Conducting thorough due diligence
- Performing ongoing monitoring
- Adhering to regulatory compliance requirements
- Executing on promises - contract management, SLAs
- Protecting your data
- Ensuring business continuity
- Analyzing performance management & meeting expectations

While you can outsource the service; remember, you still own the responsibility of this critical business practice.





Due diligence


systematic, ongoing process of analyzing and evaluating strategies, programs, products, or operations. Governance and structure.

Key triggers:

- Changes in regulations
- Evolving risks
- Changes within credit union
- Changes with vendors and industries

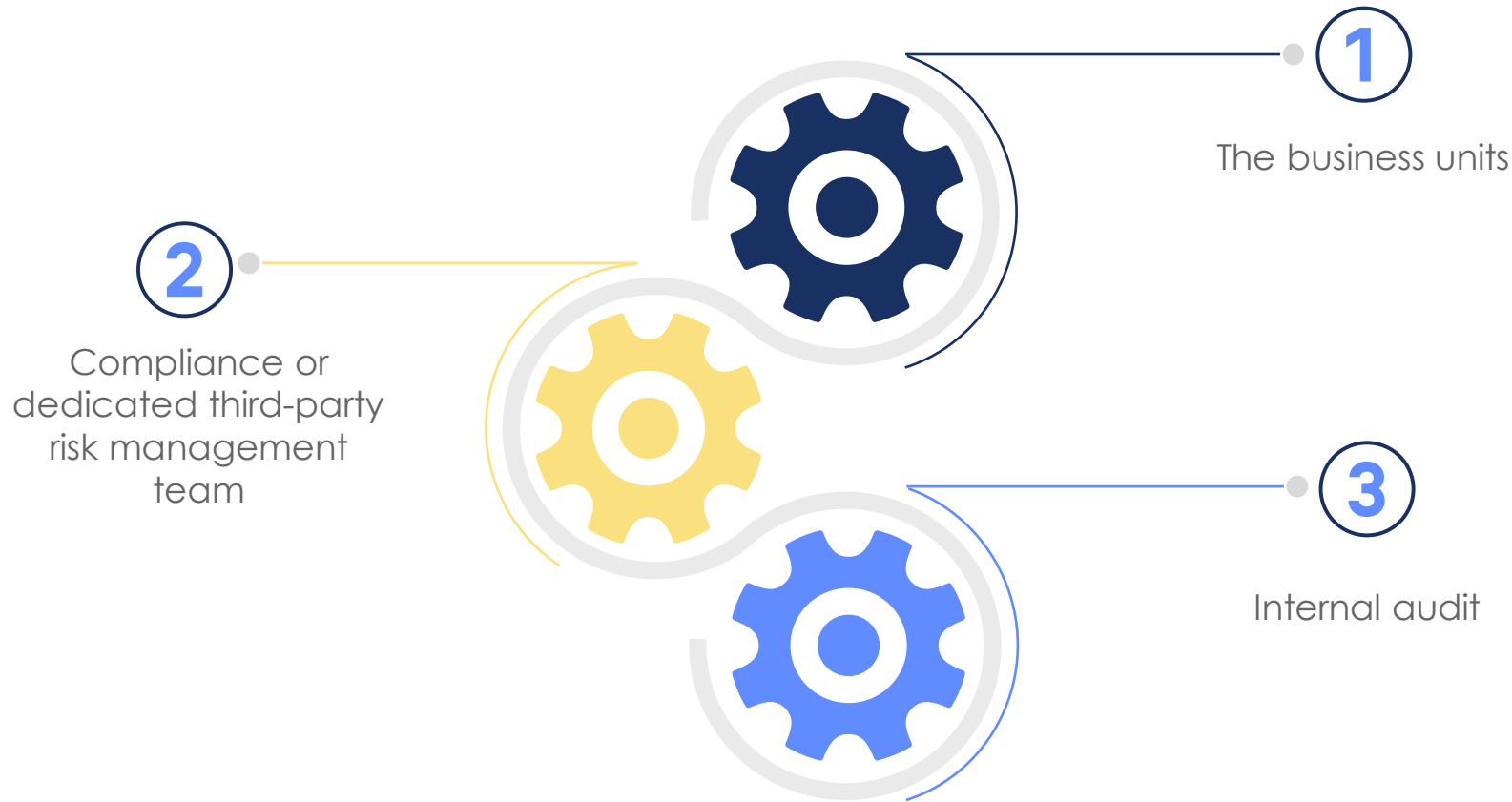


Who should be responsible for vendor oversight?

 Rosemarie in Pennsylvania

Vendor management ownership

Vendor management can seem like a daunting task



- Strong internal knowledge of subject matter
- Decision-maker or access to a decision-maker
- Outsource to a vendor management service
- Clear focus of organizational strategy



We struggle with defining critical vendors, and an adequate list of questions to help classify.

📍 Colleen in California

Criticality assessment



- Is the product or service essential to any credit union business process?
- Are there backup procedures, manual or alternative technology if this product or service fails?
- How easy is it to switch to another process or vendor?
- What is the timeframe to business resumption?
- Is the activity mission critical?
- If disruptions were to occur (loss or disruption of vendor/services/business), what would the impact be to your credit union? Impact to members?

Ongoing monitoring of service & performance

- 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

The goal should be to adopt an approach that is beyond simple compliance. Maximize vendors to enhance collaboration and grow strategic partnerships.





Regulatory compliance

- Examiners will look at response plans, incident documentation, as well as third-party contracts
- 72-hour rule

72-hour rule

All federally insured credit unions must notify the NCUA as soon as possible, and no later than 72 hours, after the credit union reasonably believes it has experienced a reportable cyber incident or received a notification from a third party regarding a reportable cyber incident.

- Contact your cyber insurance carrier and breach coach for guidance
- Document all incidents, regardless of whether they meet the reporting criteria. Documentation is essential and serves as a valuable resource for future incident response and reporting efforts. It also provides an audit trail to support reporting decisions.

To report:

- Call the NCUA at 1.833.CYBERCU (1.833.292.3728) and leave a voicemail; or
- Use the National Credit Union Administration Secure Email Message Center to send a secure email to cybercu@ncua.gov.²



In addition to contract basics like pricing, identify parties, disputes, terminations etc.

- Auto renewal
- Compliance requirements & regulatory expectations
- Right to audit
- Security/incident response obligations & requirements
- Ownership
- Licensing and certifications
- Disaster recovery, business continuity and resilience
- Indemnification clauses
- Insurance requirements
- Subcontracting (4th – nth parties)
- Termination/disputes
- Service Level Agreements (SLA) and other performance measures or benchmarks

Contract / SLA management

Protecting your data



Consider these vital steps for managing third-party relationships

- Know your vendors – maintain an easily accessible list of all third-party vendors and what type of access they have to your credit union and member data
- Take necessary steps to understand your vendors' data security standards
- Know your vendors' cybersecurity strategies. If your third-party vendors are entrusted with your credit union's member data, their cybersecurity strategy is just as important as your own
- Set expectations for your vendor relationships. When making relationships with new third-party vendors, make cybersecurity a part of the vetting process and ongoing monitoring
- Understand your risk. Establish processes to evaluate and manage associated third-party risks before entering, during, and even after the vendor relationship ends



How do we monitor our vendors to the nth degree?

 John in Virginia

Examining fourth/nth party risk issues



Assessment

- Develop a questionnaire to assess what services are performed, access to your organization, reliance by vendor, set a cadence of review by Vendor, and due diligence practices.
- 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 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?



Risk mitigation

- Use 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
- Automate the collection of publicly accessible data (news, data collection and reporting agencies, management dashboard tool providers, etc.) that divulges fourth party relationships, even if the third-party provider has not shared those with the outsourcer
- Ensure security information and event management documentation demonstrating follow through of reported material event(s)

Business resiliency issues

- Limited to IT disaster recovery
- Not updated or tested within the last 12 months
- Recovery Time Objectives and Recovery Point Objectives aren't defined or don't align with your recovery needs

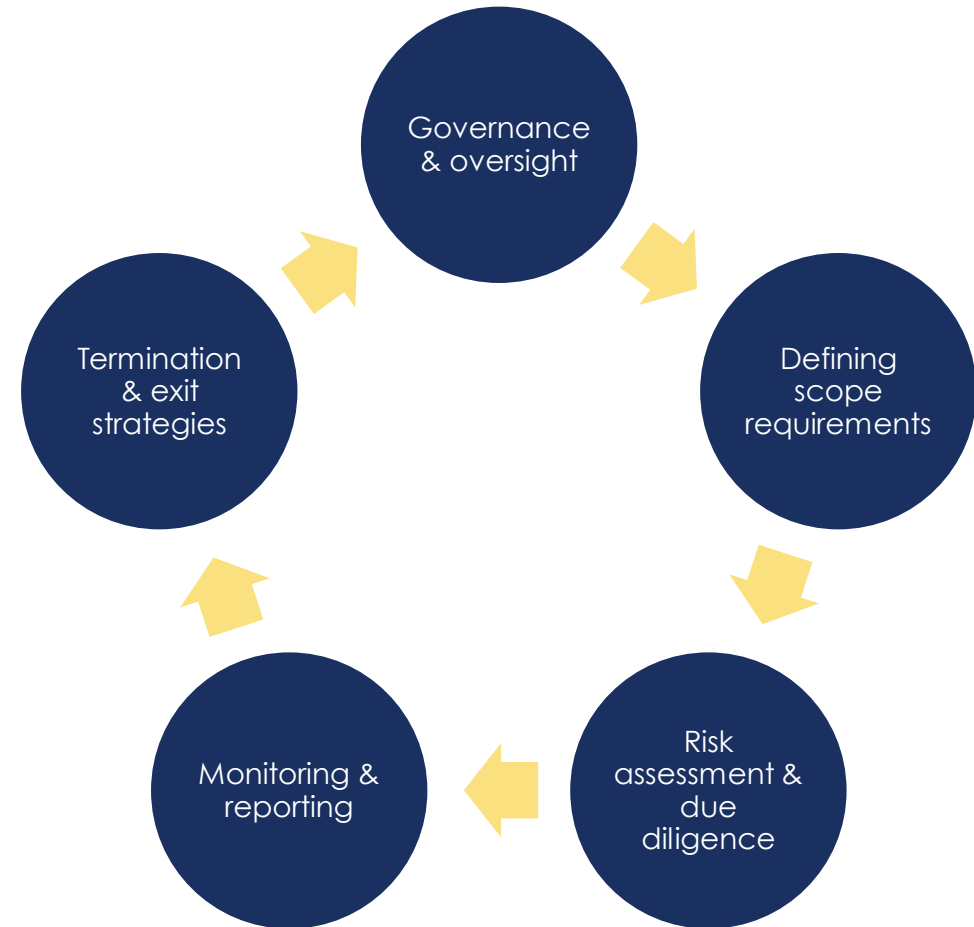
Proactive practices

- Assess vendor dependence
- Understand the vendor's role based on your criticality assessment
- Have business continuity plans reviewed by the vendor owner or subject matter expert
- Diversify and back-up critical vendors



Vendor 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
- Log, track, and monitor all vendor issues until resolved or remediated



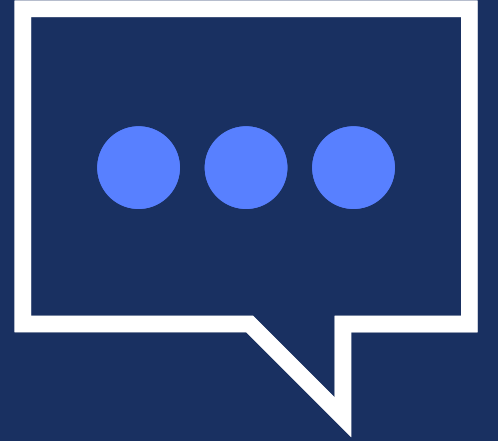
Performance management example

Vendor oversight scenario

- Credit union opted to have their collection functions performed by a vendor.
- Without notification, the vendor also outsourced a portion of the agreed upon services to a sub-contracted third party.
- Unfortunately, the sub-contractor continued to call a credit union member that filed bankruptcy resulting in a class action lawsuit and negative credit union publicity.
- During due diligence, the credit union did not clearly outline or confirm contract responsibilities regarding service-level expectations.

Oversight controls

- Be sure to inquire if they anticipate performing all the services or if they too will be outsourcing or subcontracting some services
- Clearly outline responsibilities in the contract
- Routinely confirm that the vendor is adhering to all service level expectations as part of their ongoing vendor due diligence efforts




Risk & Compliance Solutions

Q&A and wrap-up



What should we look for in SOC report, financials, disaster recovery documentation, etc.?

 Shelley in Michigan

What to do...

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
- 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

Obtaining necessary documentation

- Add a clause in the contract that would require documentation before a specified date
- Challenge the vendor to identify alternate methods of validating the controls
- Look for alternatives. Get creative and think of other sources that might provide you with similar information
- Request to see the document in person or virtually, without requiring that they hand over a physical or digital copy
- Ask for a waiver or exception if the vendor's reasoning for refusal is acceptable

Always be prepared to walk away.

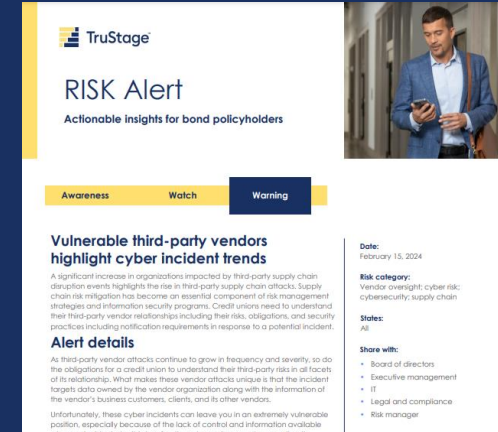
Risk resources

Business Protection Resource Center www.trustage.com/bprc

- RISK Alerts – warning | watch | awareness
- Loss prevention library
- risk overviews, checklists & whitepapers
- Emerging risks outlook
- Live webinars, risk forums & office hours
- On-demand learning & interactive training modules

“Great webinars - serious, important information delivered in a relaxed, ‘we’re among friends’ way.”

\$9B credit union



TruStage
RISK Alert
Actionable insights for bond policyholders

Awareness Watch **Warning**

Vulnerable third-party vendors highlight cyber incident trends

A significant increase in organizations impacted by third-party supply chain disruption events highlights the rise in third-party supply chain attacks. Supply chain risk mitigation has become an essential component of risk management strategies and information security programs. Credit unions need to understand their third-party vendor relationships including their risks, obligations, and security practices including notification requirements in response to a potential incident.

Alert details

As third-party vendor attacks continue to grow in frequency and severity, so do the obligations for a credit union to understand these third-party risks in all facets of its relationship. What makes these vendor attacks unique is that the incident targets data owned by the vendor organization along with the information of the vendor's business customers, clients, and its other vendors.

Unfortunately, these cyber incidents can leave you in an extremely vulnerable position, especially because of the lack of control and information available about the vendor's internal security practices.

Date:
February 15, 2024

Risk category:
Vendor oversight; cyber risk; cybersecurity; supply chain

States:
All

Share with:

- Board of directors
- Executive management
- IT
- Legal and compliance
- Risk manager



TruStage

Vendor management

Risk overview

Organizations today are not simply comprised of one internal team. Organizations, small and large alike, collaborate with partners, vendors, and other third parties. While you can outsource the service; remember, you still own the responsibility of this critical business practice.

Navigating vendor relationships

It's inevitable that your organization will work with vendors or third-party providers to deliver various products and services. Third-party vendors play an important role as you strive to become more competitive and expand member services.

But, partnering with these vendors doesn't come without risk. Managing risks associated with these relationships is a critical aspect to maintaining a successful operation.

Your decision to outsource a product or service should be dependent on a risk/reward, including cost benefit analysis. Before you begin the vendor selection process, it's important to determine if outsourcing is the right decision for your organization.

If your risk analysis points to outsourcing, consider classifying the product or service that you are looking to outsource. There are a few methods you can use - numerical designations or a high-medium-low scale. Classifying the risks allows you to rank the importance of the product or service, and in turn, determine the level of initial and ongoing due diligence necessary to maintain the relationship.

These activities should happen independent of the actual request for proposal and vendor selection process; and, instead are intended to help identify the level of risk associated with outsourcing an activity.

You should establish processes to evaluate and manage associated risks before entering, during, and even after the vendor relationship ends.

Remember, third-party and vendor risk management is an ongoing process. The initial data and information only provides you with a snapshot in time.

A risk/reward analysis can help determine the desirability of entering a relationship with a third party. It's important to consider both short-term, long-term costs, and risks along with benefits associated with outsourcing the function.



TruStage

Risk & Compliance Solutions | Presentation

Emerging risks outlook

Rethinking protection in an era of uncertainty

Proprietary and confidential. Do not distribute.



0:00:00



Contact us

800.637.2676

- riskconsultant@trustage.com
- [Ask a risk manager interactive form](#)
- [Schedule a 1:1 risk consultation](#)
- [Report a risk or scam](#)



Thank you.

Contact

riskconsultant@trustage.com

800.637.2676

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.

TruStage™ is the marketing name for TruStage Financial Group, Inc., its subsidiaries and affiliates. TruStage Insurance Products offered to financial institutions and their affiliates are underwritten by CUMIS Insurance Society, Inc. or CUMIS Specialty Insurance Company. 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. Please read the actual policy for specific coverage, terms, conditions, and exclusions.