RGS GLOBAL ADVISORS
1441 Broadway, Suite 6057, New York, NY 10018
390 North Orange Avenue, Suite 2300, Orlando, FL 32801

NCUA and Third-Party Risk Management

Regulatory Status

The National Credit Union Administration (NCUA) is seeking regulatory oversight authority related to third-party vendors who present additional cyber risks to the industry. In March 2022, the NCUA published a paper entitled, Third-Party Vendor Authority[1], in which it puts forth its case that without the statutory authority to examine third parties and enforce corrective actions, a regulatory blind-spot exists in the oversight of Credit Unions. This risk has increased because of greater reliance by the Credit Unions on Technology Service Providers (TSPs) as well as due to the adoption of Credit Union Service Organization (CUSO) rule in October 2021 which expanded the list of permissible activities through which CUSOs can serve Credit Unions[2]. Key risks discussed in the paper pertaining to outsourced services include:

- National Security risk caused by disruption to the financial system
- Cybersecurity risks and threat to data including ransom and fraud consequences
- Concentration risk meaning reliance across Credit Unions on the same vendors
- Reputation risk that compromises the confidence in Credit Unions
- Compliance risk with exposures to penalties, sanctions, and litigation
- Strategic risk that undermines the confidence in management.

Currently, NCUA relies on the federal banking agencies, who have authority over third-party vendors, for responding to a crisis at a third party. NCUA points out that granting this authority would bring parity with other federal banking agencies regarding third-party regulatory oversight. Despite NCUA's lack of supervisory authority over third-parties, it should be noted that it has provided supervisory guidance to credit unions concerning third-party relationships outlining risks and related controls.

The National Association of Federal Credit Unions (NAFCU) and the Credit Union National Association (CUNA) have lobbied on behalf of the industry against granting third-party statutory oversight to the NCUA citing the additional cost burden it will bring especially to smaller credit unions. However, given the ever- increasing rate of cybersecurity threats and data breaches, the NCUA is more likely than not to prevail and formerly add third-party vendor oversight as an oversight responsibility. Notably, the National Defense Authorization Act, recently passed by the House of Representatives, includes granting statutory authority to the NCUA to oversee third parties[3].

[1] https://www.ncua.gov/files/publications/regulation-supervision/third-party-vendor-authority.pdf
[2] https://www.ncua.gov/newsroom/press-release/2021/ncua-board-approves-final-rules-cusos-and-camels-rating-system-briefed-cybersecurity
[3] https://www.ncua.gov/newsroom/press-release/2022/ncua-statement-committee-passage-vendor-authority-and-underserved-areas-bills

@2022 RGS Global Advisors LLC

Competitive Forces

Digital transformation continues at a fast pace allowing for the increasingly rapid expansion by Banks and FinTechs into new products and services. As a result, Credit Unions face challenges for reciprocating to remain competitive and meet the evolving service expectations of members. Third-party vendors are, therefore, increasingly used by Credit Unions as they offer the most cost-effective solutions to provide products and technology across the financial service sector that are best equipped to support digital transformation efforts. However, the increasing use of third-party vendors add another layer of cybersecurity and privacy risk, and it is that aspect of risk management that requires further review.

Irrespective of the status of implementing a digital transformation strategy and engagement with third-party vendors, an institution should manage the process through a formalized program. A structured approach is vital to managing third-party risk and will help identify gaps and control deficiencies early and set in place mitigants to provide a sound control environment and oversight process.

Analysis of Risk and Controls

A key step forward is to determine the third-party risk exposures that exist in the operational environment by undertaking the following:

- Determine the status of policies and procedures including governance and reporting related to third-party relationships
- Perform an assessment of the third-party risks and a best practice gap analysis. The process should include performing an inventory and data update of all third-party providers and areas of service. This will establish a baseline to determine the third-party risk profile of the institution
- Review the controls in place to monitor and manage third party risk and how that is functionally structured. For example, is the process decentralized and managed in multiple silos or is there a centralized point of oversight and accountability.

Frequently Encountered Challenges

Completing an assessment that includes the above-mentioned criterion is important and will provide a more complete understanding of the landscape. The kinds of exposures that are flagged often include:

- Use of multiple vendors which invariably can lead to inefficiencies, duplication of effort and increased costs
- Legacy and manual intensive systems that do not provide real-time access to data limiting effective exception/red flag monitoring, and tracking of performance metrics

- Decentralization of oversight resulting in inconsistencies in standards and expectations of vendors
- Non risk segmentation amongst vendors resulting in inefficiencies in the risk management effort that may be applied uniformly across all vendors, even ones which do not need this level of scrutiny and oversight.

Mitigating Control Framework

Implementing a formal centralized program to manage third-party risk will provide multiple benefits including establishing a core platform that will allow for detailed analysis and review and should drive toward managing expectations and optimizing outcomes. Examples of positive outcomes include:

- Data access and reporting enhancements from vendors that can lead to better metrics and analysis and thereby supporting improved decision making within operational units
- Overall improved controls ensuring more confidence in the protection and integrity of data
- An improved governance structure that allows for more timely escalation of issues that arise and capabilities to monitor responses and resolutions
- Identification of areas of overcharging, or unnecessary elements of a service that can reduce overall cost and provide an opportunity for service consolidation or result in the elimination of any unnecessary or duplicative services
- Risk evaluation of vendors, enabling better use of time and resources in vendor management, resulting in a better vendor management program along with cost savings.

Conclusion

Credit unions increasingly use TSPs and CUSOs to support operations, introduce new products and services and enhance business models. These investments and strategies are key to the success and growth of credit unions and their ability to compete in the financial service marketplace. Accordingly, this reliance on TSPs and CUSOs will continue to increase. Inevitably, NCUA oversight will also expand with or without formalized legislation. As a result, credit unions and all financial service organizations will need to have structured vendor risk management programs that include specific processes and controls focused on their relationships with third-party vendors. The use of structured programs would enable Credit Unions in making effective use of their resources in managing and mitigating third-part risks and related cybersecurity risks.

RGS Global Advisors is a cost-effective provider of Technology Risk Management, BSA/AML/OFAC Compliance Consultancy and Internal Audit services to Financial Institutions.

For further guidance or assistance contact us at: info@RGSGlobalAdvisors.com