Due Diligence

Monday, October 28, 2024 9:23 AM

1. Due Diligence and Planning

- **Risk Assessment (Stmt 23.1)**: Review the credit union's vendor risk assessment, ensuring it covers factors from the Planning/Risk Assessment section of the Job Aid: Third-Party Relationships. Verify documentation of AI vendor-specific risks.
- **Evaluation of Support Costs (Stmt 23.2)**: Analyze documented costs associated with monitoring and supporting third-party programs, covering staff, technology, and capital expenditures.
- **Strategic Business Plan (Stmt 23.3)**: Ensure the credit union's strategic plan includes measurable goals, authority levels, and responsibilities for third-party relationships.
- **Cost-Benefit Analysis (Stmt 23.4)**: Verify that the credit union performed a documented financial analysis evaluating the reward versus the risk of the proposed third-party relationship.

2. Vendor Selection and Qualification

- **Vendor Selection (Stmt 23.5)**: Confirm that the credit union considered multiple third-party vendors before establishing the relationship.
- **Experience and Legal Concerns (Stmt 23.6)**: Ensure that vendor selection included assessment of their industry experience and any potential legal issues, especially for AI vendors who may handle sensitive member data.
- **Mission Alignment (Stmt 23.7)**: Confirm the selected third-party vendor(s) align with the credit union's mission and philosophy, with a focus on compliance and security.
- **Business Model Understanding (Stmt 23.8)**: Document the credit union's understanding of the vendor's business model and how it aligns with services provided.
- **Income and Conflict Analysis (Stmt 23.9)**: Ensure the credit union reviewed the vendor's income sources, expenses, and any potential conflicts of interest.

3. Financial and Legal Review

- **Financial Analysis (Stmt 23.10)**: Confirm that a financial review of the vendor and any affiliates demonstrates their ability to fulfill contractual commitments.
- **Contract Review (Stmt 23.11)**: Verify that contracts address due diligence, contractual, and legal issues outlined in the Job Aid: Third-Party Relationships.
- **Legal Opinion (Stmt 23.12)**: Ensure the credit union obtained an independent legal opinion for services provided by the third party, specifically for high-risk or AI-related services.

4. Regulatory and Compliance Assurance

- **Regulatory Compliance Verification (Stmt 23.13)**: Confirm that the vendor complies with relevant laws and regulations (e.g., Regulation B, Z, HMDA, BSA/AML) and is contractually bound to compliance.
- **Accounting Infrastructure (Stmt 23.14)**: Verify the credit union's accounting system can

accurately track and classify transactions with the third party per GAAP.

- **Monthly Activity Reporting (Stmt 23.15)**: Ensure monthly reports on third-party activity are accurate and comprehensive enough for performance monitoring.

5. Oversight and Monitoring

- **Risk Summary Reports (Stmt 23.16)**: Confirm that senior management or the board receives risk summary reports related to third-party vendors regularly.
- **Staff Oversight (Stmt 23.17)**: Verify that qualified staff members are assigned to monitor third-party performance and contract compliance.
- **Transaction Verification (Stmt 23.18)**: For vendors handling member transactions, ensure a process is in place to verify these transactions with members.
- **Account Servicing Reports (Stmt 23.19)**: If the vendor services member accounts, confirm that regular activity reports are reviewed by the credit union.
- **Account Verification Control (Stmt 23.20)**: Ensure there are controls to manage member account verification between the credit union and the vendor.

6. Accuracy and Remittance Verification

- **Report Accuracy (Stmt 23.21)**: Review the accuracy verification process for vendor-provided reports.
- **Loan Servicing Compliance (Stmt 23.22)**: Confirm that when vendors service loans, member payments are remitted per contract terms.

7. Infrastructure and Internal Controls

- **Monitoring Infrastructure (Stmt 23.23)**: Ensure adequate infrastructure (staff, equipment, technology) is in place to monitor third-party relationships.
- **Internal Controls (Stmt 23.24)**: Review internal controls to ensure adherence to policy guidelines for managing third-party relationships.
- **Third-Party Policies (Stmt 23.25)**: Validate that policies address third-party relationship management comprehensively, including vendor performance expectations and compliance with data handling and security.
- **Activity Limits (Stmt 23.26)**: Ensure policies define clear limits on third-party activity levels.
- **Approved Party List (Stmt 23.27)**: Confirm that an approved list of third-party vendors is maintained and regularly updated.

8. Secure Data Transmission

- **Data Security (Stmt 23.28)**: Review the methods for secure data transmission between the credit union and third-party vendors, ensuring encryption or secure transfer mechanisms are in place (e.g., VPNs, encrypted email, secure fax).

Questions

Monday, October 28, 2024 9:24 AM

1. Due Diligence and Planning

Risk Assessment

- Has a risk assessment been completed for each third-party vendor, including AI vendors, based on factors in the Planning/Risk Assessment section of the Job Aid for Third-Party Relationships?
- Are risk assessments for vendors periodically reviewed and updated?

Support Costs

- Has the credit union evaluated the total costs of supporting third-party relationships, including AI-related programs, for staffing, capital, communications, and technology?
- Are these costs aligned with budget and resources available?

Strategic Business Plan

- Does the strategic business plan outline clear, measurable objectives and responsibilities for managing third-party relationships?
- How does the plan integrate third-party relationships within the credit union's overall strategic goals?

Cost-Benefit Analysis

- Has a cost-benefit analysis been conducted to assess if the rewards justify the risks of each third-party relationship?
- Was this analysis documented and reviewed by relevant stakeholders?

2. Vendor Selection and Qualification

Vendor Selection Process

- Were multiple third-party vendors considered before finalizing a contract with the chosen vendor?
- What criteria were used to evaluate and compare potential vendors, including those offering AI solutions?

Experience and Legal Review

- Was the vendor's industry experience, including any legal concerns, evaluated?
- Has management documented the vendor's qualifications and any legal or compliance risks identified during the review?

Mission Alignment

- Does the vendor's service align with the credit union's mission and values?
- How does the vendor's work support or enhance the credit union's goals?

Understanding the Business Model

- Can the credit union confidently describe the vendor's business model, revenue sources, and cost structure?
- Were any potential conflicts of interest between the vendor and the credit union identified, and if so, how are they managed?

3. Financial and Legal Review

Financial Analysis

- Were the financial statements of the vendor and its affiliates reviewed to verify their financial stability?
- Was this review sufficient to ensure the vendor's ability to meet contractual obligations?

Contract Review

- Do contracts include all necessary provisions regarding due diligence, compliance, and legal requirements as per the Job Aid for Third-Party Relationships?
- Has legal counsel reviewed each contract for adequacy and regulatory compliance?

Independent Legal Opinion

- Was an independent legal opinion obtained, especially for high-risk or AI-related services?
- Are there documented justifications for any services not requiring an independent opinion?

4. Regulatory and Compliance Assurance

Regulatory Compliance Verification

- How does the credit union verify that vendors comply with federal and state laws (e.g., BSA/AML, Regulation B)?
- Is this compliance requirement clearly stated in contracts?

Accounting Infrastructure

- Does the credit union's accounting system effectively track, identify, and classify transactions with each third party according to GAAP?
- Are there controls to ensure accurate reporting and classification of vendor-related transactions?

Monthly Activity Reporting

- Are monthly reports on vendor activities generated and reviewed to monitor performance effectively?
- Do these reports provide sufficient data for informed decision-making?

5. Oversight and Monitoring

Risk Summary Reports

- Are regular risk summary reports on third-party relationships, including AI vendors,

provided to senior management or the board?

- Do these reports contain actionable insights to guide risk management?

Assigned Oversight Staff

- Are specific staff members assigned to monitor each third-party relationship, and do they have the expertise required for effective oversight?
- How often is their performance in this oversight role reviewed?

Transaction Verification

- Is there a process to verify member transactions initiated by third-party vendors to ensure accuracy and accountability?
- Are any discrepancies documented and resolved promptly?

Account Servicing Reports

- Are reports on third-party account servicing activities regularly reviewed by the credit union?
- What processes are in place to address any issues identified in these reports?

Account Verification Control

- How does the credit union control the verification of member accounts processed by third parties?
- Are there regular audits to ensure accuracy and security in account verification?

6. Accuracy and Remittance Verification

Report Accuracy

- Is there a process to verify the accuracy of reports received from vendors?
- How often are these reports audited for discrepancies?

Loan Servicing Compliance

- For vendors involved in loan servicing, does the credit union verify that all member payments are remitted according to contract terms?
- Are any inconsistencies documented and addressed in a timely manner?

7. Infrastructure and Internal Controls

Monitoring Infrastructure

- Does the credit union have sufficient infrastructure (staff, technology) to monitor third-party performance and compliance?
- Are there plans to enhance monitoring capabilities as the credit union expands its vendor relationships?

Internal Controls

- Are internal controls in place to ensure adherence to third-party management policies?

- How often are these controls tested and updated?

Policy Coverage for Third-Party Relationships

- Do current policies comprehensively cover third-party relationship requirements, performance expectations, and data handling?
- Are these policies reviewed and updated regularly?

Activity Limits

- Are there defined activity limits for third-party vendors?
- How does the credit union ensure compliance with these limits?

Approved Vendor List

- Is there a maintained list of approved third-party vendors?
- How often is this list reviewed and updated?

8. Secure Data Transmission

Data Transmission Security

- What secure methods are used to transmit data between the credit union and vendors (e.g., encrypted email, VPN)?
- Are there documented policies mandating secure data transmission, and how is compliance verified?

Periodic Reviews of Data Transmission Practices

- Are data transmission practices regularly reviewed to adapt to evolving security standards?
- How does the credit union ensure that data transmission with vendors remains compliant and secure?

Answers

Monday, October 28, 2024 9:24 AM

1. Due Diligence and Planning

Risk Assessment

- **Positive Response**: The credit union performs a comprehensive risk assessment for each third-party vendor, including AI vendors, considering factors like financial stability, data security, regulatory compliance, and operational reliability. Assessments are updated periodically to address new risks.
- **Negative Response**: No formal risk assessment process is in place, or it lacks specific criteria for evaluating third-party vendors. Risk assessments are irregular, outdated, or fail to account for unique risks associated with AI vendors.

Support Costs

- **Positive Response**: The credit union has thoroughly evaluated and budgeted for all costs associated with third-party oversight, including staffing, technology, and communications. Allocations align with resources, enabling effective monitoring and support.
- **Negative Response**: Costs for supporting third-party programs are not fully considered, leading to under-budgeting. There may be insufficient resources allocated for adequate monitoring and support, particularly for high-risk vendors like AI providers.

Strategic Business Plan

- **Positive Response**: The credit union's strategic plan integrates clear, measurable goals and roles for third-party management, aligning vendor performance with organizational objectives and compliance.
- **Negative Response**: The strategic plan either does not address third-party relationships or lacks specific goals, roles, and accountability measures, reducing oversight effectiveness.

Cost-Benefit Analysis

- **Positive Response**: A documented cost-benefit analysis is performed for each vendor, balancing potential rewards against risks. Stakeholders regularly review these analyses.
- **Negative Response**: No cost-benefit analysis is conducted, or it is superficial, lacking sufficient consideration of risks. Stakeholders may not be fully informed on potential vendor impacts.

2. Vendor Selection and Qualification

Vendor Selection Process

- **Positive Response**: Multiple vendors were assessed against clear criteria before selection, ensuring that chosen vendors meet quality and compliance standards.
- **Negative Response**: Vendor selection is limited or based solely on convenience, with little comparison of alternatives. This could lead to risks from unvetted providers.

Experience and Legal Review

- **Positive Response**: The vendor's experience and legal history were thoroughly evaluated,

with all findings documented. Legal counsel reviewed the risks associated with AI vendors.

- **Negative Response**: Little or no due diligence was conducted on the vendor's experience or legal history, increasing potential compliance and legal risks.

Mission Alignment

- **Positive Response**: The vendor's services support the credit union's mission, enhancing member service quality and aligning with strategic goals.
- **Negative Response**: The vendor's services do not align well with the credit union's mission or could pose reputational risks if misaligned.

Understanding the Business Model

- **Positive Response**: The credit union understands the vendor's business model, including sources of revenue and cost structure, minimizing conflicts of interest.
- **Negative Response**: Lack of understanding of the vendor's business model creates potential for conflicts of interest and financial misalignment.

3. Financial and Legal Review

Financial Analysis

- **Positive Response**: Vendor financials, including affiliates, were reviewed, showing adequate resources to meet obligations. Documentation supports a well-informed decision.
- **Negative Response**: Financial analysis was either not conducted or inadequate, leading to potential risks if vendors cannot fulfill their contracts.

Contract Review

- **Positive Response**: Contracts address all necessary provisions for due diligence, compliance, and risk management, having been reviewed by legal counsel.
- **Negative Response**: Contracts lack essential clauses or are not reviewed by legal counsel, potentially exposing the credit union to legal and compliance risks.

Independent Legal Opinion

- **Positive Response**: Independent legal opinions were obtained for high-risk arrangements, particularly with AI vendors, ensuring compliance.
- **Negative Response**: Legal opinions were not sought, raising risks if the vendor arrangement fails to comply with legal standards or presents unforeseen liabilities.

4. Regulatory and Compliance Assurance

Regulatory Compliance Verification

- **Positive Response**: Vendors are contractually bound to comply with all relevant federal and state regulations, with regular verification procedures in place.
- **Negative Response**: Contracts lack specific regulatory requirements, or compliance verification is inadequate, potentially resulting in regulatory penalties.

Accounting Infrastructure

- **Positive Response**: The credit union's accounting system accurately tracks vendor-related transactions per GAAP, with regular reviews to ensure integrity.
- **Negative Response**: Accounting infrastructure is inadequate or lacks controls for accurate vendor transaction tracking, risking financial misstatements.

Monthly Activity Reporting

- **Positive Response**: Monthly reports on vendor activities are reviewed, providing actionable insights for risk management and performance monitoring.
- **Negative Response**: Reports are infrequent or lack sufficient detail, hampering the credit union's ability to oversee vendor activities effectively.

5. Oversight and Monitoring

Risk Summary Reports

- **Positive Response**: Regular, detailed risk reports are provided to senior management, enabling informed oversight of vendor risks.
- **Negative Response**: Reporting is inconsistent or lacks depth, limiting the credit union's visibility into potential third-party risks.

Assigned Oversight Staff

- **Positive Response**: Trained staff oversee vendor relationships, with regular performance evaluations to ensure effective monitoring.
- **Negative Response**: Oversight is insufficient due to lack of dedicated staff or expertise, impacting monitoring and risk response capabilities.

Transaction Verification

- **Positive Response**: Verification processes ensure all transactions initiated by vendors are accurately reflected, with discrepancies promptly addressed.
- **Negative Response**: No formal verification process exists, increasing the risk of errors and fraud in member transactions.

Account Servicing Reports

- **Positive Response**: Account activity reports from vendors are reviewed to ensure compliance with service standards.
- **Negative Response**: Reports are not reviewed or lack essential details, affecting the credit union's ability to ensure quality service.

Account Verification Control

- **Positive Response**: Controls are in place to manage vendor access to member accounts, regularly audited for accuracy and security.
- **Negative Response**: Verification controls are weak or untested, raising risks of unauthorized access and data inaccuracies.

6. Accuracy and Remittance Verification

Report Accuracy

- **Positive Response**: Processes are in place to verify vendor reports for accuracy, with periodic audits to identify and resolve discrepancies.
- **Negative Response**: Verification of vendor reports is limited or absent, increasing the risk of errors or data integrity issues.

Loan Servicing Compliance

- **Positive Response**: Loan payments handled by vendors are verified against contract terms, with immediate actions taken on any discrepancies.
- **Negative Response**: No verification exists for loan servicing, increasing the risk of compliance failures and financial inaccuracies.

7. Infrastructure and Internal Controls

Monitoring Infrastructure

- **Positive Response**: Adequate resources and infrastructure support comprehensive monitoring of all third-party relationships.
- **Negative Response**: Insufficient monitoring resources hinder the credit union's ability to effectively oversee vendors.

Internal Controls

- **Positive Response**: Internal controls are regularly reviewed and align with policy guidelines for managing third-party relationships.
- **Negative Response**: Internal controls are inadequate, inconsistently applied, or untested, resulting in potential policy violations.

Policy Coverage for Third-Party Relationships

- **Positive Response**: Policies are comprehensive, regularly updated, and cover all necessary third-party management requirements.
- **Negative Response**: Policies are outdated, incomplete, or do not sufficiently address third-party relationship management.

Activity Limits

- **Positive Response**: Policies define and enforce activity limits for vendors, ensuring operations remain within agreed-upon boundaries.
- **Negative Response**: Lack of defined activity limits risks vendors overstepping or conducting unauthorized activities.

Approved Vendor List

- **Positive Response**: A current, approved list of vendors is maintained, with regular updates reflecting vendor performance and risk.
- **Negative Response**: No formal vendor approval process exists, increasing risk from unvetted third-party relationships.

8. Secure Data Transmission

Data Transmission Security

- **Positive Response**: Data transmitted to and from vendors is securely encrypted, with established policies ensuring data protection.
- **Negative Response**: Secure transmission policies are absent or inconsistently applied, raising risks of unauthorized data access.

Periodic Reviews of Data Transmission Practices

- **Positive Response**: Data transmission practices are periodically reviewed and updated to meet evolving security standards.
- **Negative Response**: Reviews are infrequent, leaving potential vulnerabilities in secure data transmission protocols.

Compliance

Monday, October 28, 2024 9:25 AM

1. 12 CFR Part 748 - Security Program, Report of Suspected Crimes, Suspicious Transactions, Catastrophic Acts and Bank Secrecy Act Compliance

- **748.0** – *Security Program*: This section mandates that credit unions must implement a written security program, which includes protecting against unauthorized access and ensuring third-party relationships do not expose the credit union to unnecessary risks.
- **748.1** – *Filing Requirements*: Credit unions must report suspicious activity, particularly related to third-party breaches, compliance issues, or financial risks involving vendors.
- **Appendix A to Part 748** – *Guidelines for Safeguarding Member Information*: This appendix emphasizes the need for robust third-party due diligence and oversight to safeguard member information when shared with vendors.

2. Appendix B to Part 748 - Guidelines for Response Programs for Unauthorized Access to Member Information and Member Notice

- **Vendor Risk and Data Protection**: This appendix outlines that credit unions must have a response program for unauthorized access, including with third-party relationships. It also mandates that credit unions ensure vendors follow standards that protect member information.

3. 12 CFR Part 749 - Records Preservation Program and Appendices – Catastrophic Act Preparedness Guidelines

- This part requires credit unions to have a records preservation program and disaster recovery plan, especially when vendor relationships involve critical data management. Vendors handling sensitive information must adhere to these requirements, ensuring records and data continuity in case of catastrophic events.

4. 12 CFR Part 741.201 - Minimum Security Devices and Procedures

- Credit unions are required to implement appropriate security devices and procedures, which extend to third-party relationships. Vendors with access to physical or digital resources are expected to comply with the same security requirements as the credit union.

5. Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. §§ 6801-6809 - Privacy of Consumer Financial Information

- **Section 6801** – *Protection of Nonpublic Personal Information*: GLBA mandates that financial institutions, including credit unions, ensure that vendors handling sensitive information adhere to privacy protections.
- **Section 6805(b)** – *Enforcement*: Outlines enforcement mechanisms for GLBA violations, which include oversight on vendor compliance with data protection requirements.

6. Federal Financial Institutions Examination Council (FFIEC) Guidance

- **Outsourcing Technology Services**: FFIEC's guidance on outsourcing technology services provides a detailed framework for managing risks related to third-party relationships, specifically for vendors handling IT and security functions.
- **Cybersecurity and Third-Party Relationships**: FFIEC's Cybersecurity Assessment Tool (CAT) and associated guidance address risks and requirements for third-party management,

especially for vendors with access to sensitive or member-specific data.

7. Bank Service Company Act (BSCA), 12 U.S.C. §§ 1861-1867

- This act applies to third-party service providers performing core services on behalf of credit unions. It requires that such vendors are subject to regulation and examination by the National Credit Union Administration (NCUA) and that credit unions implement oversight to mitigate risks associated with these relationships.

8. NCUA Letters and Supervisory Guidance

- **NCUA Letter 07-CU-13** – *Evaluating Third-Party Relationships*: This letter emphasizes the importance of vendor due diligence, oversight, and management, particularly for relationships involving member data.
- **NCUA Supervisory Letter 17-CU-09** – *Cybersecurity Guidance and Standards*: Provides standards for credit unions to assess and manage cybersecurity risks with third-party vendors, especially those handling critical IT infrastructure.