Third party management process includes the following:

Friday, August 16, 2024 1:55 PM

Third-Party Management Checklist with Compliance to Appendix A to Part 748, Title 12

Section 1: Vendor Management Policy

- **[ ] Vendor Management Policy Documented and Approved**
  - **Reference: Appendix A to Part 748, Section III(C)(1)(c)** – Ensure vendors implement safeguards for member information.
- **[ ] Policy includes vendor categories (e.g., critical, non-critical)**
  - **Reference: Appendix A to Part 748, Section III(A)(1)** – Vendors must be categorized based on their access to critical systems or sensitive data.
- **[ ] Procedures for vendor selection, risk assessment, and monitoring**
  - **Reference: Appendix A to Part 748, Section III(A)(2)** – Requires appropriate vendor risk assessments and ongoing monitoring.
- **[ ] Annual review and approval by the board or designated committee**
  - **Reference: Appendix A to Part 748, Section III(C)(2)(b)** – Board oversight of vendor management policies.

Section 2: Due Diligence Process

- **[ ] Documented Due Diligence Process**
  - **Reference: Appendix A to Part 748, Section III(A)(2)** – Due diligence is required when selecting and managing vendors.
- **[ ] Includes initial due diligence and ongoing monitoring**
  - **Reference: Appendix A to Part 748, Section III(C)(1)(c)** – Continuous evaluation of third-party service providers.
- **[ ] Background checks and financial stability assessments**
  - **Reference: Appendix A to Part 748, Section III(A)(2)** – Financial and operational stability reviews of vendors.
- **[ ] Security posture evaluations**
  - **Reference: Appendix A to Part 748, Section III(A)(1)** – Ensure vendor security controls align with safeguarding member information.
- **[ ] Documentation of due diligence for critical vendors**
  - **Reference: Appendix A to Part 748, Section III(A)(5)** – Proper documentation is necessary for compliance and audits.

Section 3: Critical Vendor and Contract Listing

- **[ ] Updated List of Critical Vendors and Contracts**
  - **Reference: Appendix A to Part 748, Section III(A)(1)** – Maintain an up-to-date list of vendors with access to sensitive information.
- **[ ] Vendor List Completeness**
  - **Reference: Appendix A to Part 748, Section III(A)(5)** – Ensure all critical vendors are accounted for in vendor lists.

Section 4: Information Security in Service Provider Contracts

- **[ ] Contract Clauses for Information Security**
  - **Reference: Appendix A to Part 748, Section III(C)(1)(c)** – Contracts must include security and confidentiality clauses.
- **[ ] Data protection, confidentiality, and security standards**
  - **Reference: Appendix A to Part 748, Section III(A)(3)** – Ensure that service providers protect member data.

Section 5: Incident Notification in Contracts

- **[ ] Contract Clause for Incident Notification**
  - **Reference: Appendix A to Part 748, Section III(A)(2)** – Vendors must notify institutions of security incidents in a timely manner.
- **[ ] Historical Incident Review**
  - **Reference: Appendix A to Part 748, Section III(C)(1)(d)** – Ensure that past incidents were properly notified and addressed.

Section 6: Service Specifications in Contracts

- **[ ] Contracts Define Service Frequency, Format, and Specifications**
  - **Reference: Appendix A to Part 748, Section III(A)(1)** – Service provider contracts should define the services provided, ensuring compliance with business continuity plans.
- **[ ] Monitoring of Vendor Performance Against Specifications**
  - **Reference: Appendix A to Part 748, Section III(A)(4)** – Continuously monitor vendor performance and compliance.

Section 7: Oversight of Third-Party Technology Providers

- **[ ] Documented Process for Managing Technology Providers**
  - **Reference: Appendix A to Part 748, Section III(C)(1)(c)** – Ensure that critical technology service providers are subject to proper oversight.
- **[ ] Oversight Committee Review**
  - **Reference: Appendix A to Part 748, Section III(C)(2)(b)** – Board or committee review of third-party technology management.

Section 8: Monitoring Information Security Measures

- **[ ] Audit and Test Results from Service Providers**
  - **Reference: Appendix A to Part 748, Section III(C)(1)(c)** – Ensure vendors' security controls are regularly audited.
- **[ ] Regular Security Review Process**
  - **Reference: Appendix A to Part 748, Section III(A)(4)** – Implement a regular process for reviewing security measures of third-party providers.

Section 9: Service Level Agreements (SLAs)

- **[ ] Adequate and Measurable SLAs in Contracts**
  - **Reference: Appendix A to Part 748, Section III(A)(3)** – Contracts must define clear performance measures to ensure service providers comply with security and operational standards.

Section 10: Compliance with Laws and Regulations

- **[ ] Third-Party Compliance with Laws and Regulations**
  - **Reference: Appendix A to Part 748, Section III(A)(2)** – Vendor contracts must include clauses to ensure compliance with relevant regulations.

Section 11: Insurance Coverage in Contracts

- **[ ] Insurance Requirements in Contracts**
  - **Reference: Appendix A to Part 748, Section III(A)(2)** – Contracts should specify adequate insurance coverage for vendors handling sensitive data.

Section 12: Vendor Risk Assessment

- **[ ] Regular Vendor Risk Assessments**
  - **Reference: Appendix A to Part 748, Section III(A)(2)** – Regular risk assessments of vendors, especially those with access to critical systems, must be documented and reviewed.

Section 13: Vendor Financial Information Review

- **[ ] Financial Statement Review for Critical Vendors**
    - **Reference: Appendix A to Part 748, Section III(A)(2)** – Regular review of vendor financial stability to assess risks.

Section 14: Authorization to Monitor Compliance in Contracts

- **[ ] Contracts Include Monitoring Authorization**
    - **Reference: Appendix A to Part 748, Section III(C)(1)(c)** – Contracts should allow for regular monitoring of vendors to ensure compliance with security standards.

Section 15: Independent Validation of Security Controls

- **[ ] Independent Security Control Validation Requirement**
    - **Reference: Appendix A to Part 748, Section III(C)(1)(c)** – Service providers must submit to independent security validations such as SOC reports.

Section 16: Software Escrow Clause in Contracts

- **[ ] Software Escrow Clause in Contracts**
    - **Reference: Appendix A to Part 748, Section III(A)(2)** – Vendor contracts should include a software escrow clause for critical systems to ensure business continuity in the event of vendor failure.

Section 17: Legal Review of Contracts

- **[ ] Legal Counsel Review Process**
    - **Reference: Appendix A to Part 748, Section III(C)(2)(b)** – Ensure that legal reviews of third-party contracts are conducted, particularly for contracts involving sensitive data handling.

Section 18: Independent Security Reviews (e.g., SOC Reports)

- **[ ] Obtain SOC Reports or Equivalent**
    - **Reference: Appendix A to Part 748, Section III(C)(1)(c)** – Require independent security reviews from service providers, including SOC reports.

Section 19: Addressing Material Exceptions in Independent Security Reviews

- **[ ] Material Exception Handling**
    - **Reference: Appendix A to Part 748, Section III(A)(5)** – Ensure material exceptions in vendor security reviews are addressed promptly.

Section 20: Verifying Credit Union's Performance of Complementary User Entity Controls

- **[ ] Review SOC Reports for Complementary Controls**
    - **Reference: Appendix A to Part 748, Section III(C)(1)(c)** – Confirm that complementary controls are in place and regularly reviewed for third-party risk management.

Issues

Thursday, September 19, 2024 3:42 PM

Potential Findings for the Third-Party Management Checklist

Section 1: Vendor Management Policy

1. **Vendor Management Policy Not Documented or Approved**
   - **Impact:** Lack of a formal policy increases the risk of inconsistent vendor management practices, especially for vendors handling sensitive data.
   - **Reference: Appendix A to Part 748, Section III(C)(1)(c)**
2. **Policy Does Not Include Vendor Categories**
   - **Impact:** Without categorizing vendors (e.g., critical, non-critical), the organization may fail to appropriately prioritize risk assessments and monitoring.
   - **Reference: Appendix A, Section III(A)(1)**
3. **Lack of Annual Review and Approval**
   - **Impact:** Outdated vendor policies can leave risks unaddressed, especially if significant changes to vendor relationships or services occur.
   - **Reference: Appendix A, Section III(C)(2)(b)**

Section 2: Due Diligence Process

1. **Due Diligence Process Not Documented**
   - **Impact:** Inconsistent due diligence efforts may result in selecting vendors with inadequate security controls or unstable financial conditions.
   - **Reference: Appendix A, Section III(A)(2)**
2. **Due Diligence Not Performed for Critical Vendors**
   - **Impact:** Lack of due diligence increases the risk of selecting vendors who may be unable to meet security and compliance requirements.
   - **Reference: Appendix A, Section III(A)(1)**
3. **Ongoing Monitoring Process Not Implemented**
   - **Impact:** Vendors' security postures and financial health may degrade over time without proper monitoring, increasing risk to the credit union.
   - **Reference: Appendix A, Section III(C)(1)(c)**

Section 3: Critical Vendor and Contract Listing

1. **Outdated Vendor and Contract Lists**
   - **Impact:** Incomplete or outdated vendor lists may lead to missed risk assessments or oversight for critical service providers.
   - **Reference: Appendix A, Section III(A)(1)**
2. **Critical Vendors Omitted from the List**
   - **Impact:** Omitting critical vendors from risk management and monitoring processes exposes the credit union to heightened risk from unmonitored third parties.
   - **Reference: Appendix A, Section III(A)(1)**

Section 4: Information Security in Service Provider Contracts

1. **Missing Information Security Clauses**
   - **Impact:** Contracts lacking security, confidentiality, or data protection clauses can result in poor enforcement of vendor obligations to safeguard member data.
   - **Reference: Appendix A, Section III(C)(1)(c)**
2. **Security Clauses Not Reviewed or Negotiated**
   - **Impact:** Failure to negotiate appropriate security terms can leave the credit union exposed to risks, as vendors may not have adequate security measures in place.
   - **Reference: Appendix A, Section III(A)(3)**

Section 5: Incident Notification in Contracts

1. **Missing Incident Notification Clauses**
   - **Impact:** Without notification requirements, vendors may delay reporting security breaches, increasing the risk of harm to member information.
   - **Reference: Appendix A, Section III(A)(2)**
2. **No Evidence of Historical Incident Notification**
   - **Impact:** Failure to document or follow up on past incidents suggests weaknesses in the incident response process, leading to delayed or inadequate responses.
   - **Reference: Appendix A, Section III(C)(1)(d)**

Section 6: Service Specifications in Contracts

1. **Service Specifications Not Clearly Defined in Contracts**
   - **Impact:** Vague or poorly defined service specifications can result in misunderstandings about vendor performance expectations, leading to service failures.
   - **Reference: Appendix A, Section III(A)(1)**
2. **No Regular Monitoring of Vendor Performance**
   - **Impact:** Without monitoring performance against specifications, service quality may degrade without detection, affecting business operations.
   - **Reference: Appendix A, Section III(A)(4)**

Section 7: Oversight of Third-Party Technology Providers

1. **No Formal Oversight Process for Technology Providers**
   - **Impact:** Without a documented oversight process, critical technology providers may not be effectively monitored for compliance with security and operational standards.
   - **Reference: Appendix A, Section III(C)(1)(c)**
2. **No Oversight Committee Involvement**
   - **Impact:** Lack of committee involvement reduces accountability and may result in vendors not receiving sufficient oversight.
   - **Reference: Appendix A, Section III(C)(2)(b)**

Section 8: Monitoring Information Security Measures

1. **Audit and Test Results Not Collected or Reviewed**
   - **Impact:** Vendors may not be meeting required security standards if audit results are not reviewed, increasing the risk of vulnerabilities and breaches.
   - **Reference: Appendix A, Section III(C)(1)(c)**
2. **No Regular Security Review Process**
   - **Impact:** Inconsistent security reviews increase the risk of undetected vulnerabilities within vendors' environments.
   - **Reference: Appendix A, Section III(A)(4)**

Section 9: Service Level Agreements (SLAs)

1. **SLAs Not Clearly Defined**
   - **Impact:** Without clear and measurable SLAs, the credit union may not have recourse if the vendor fails to meet performance expectations.
   - **Reference: Appendix A, Section III(A)(3)**
2. **No Process for Monitoring SLA Performance**
   - **Impact:** Without SLA monitoring, vendors may consistently underperform without corrective actions being taken.
   - **Reference: Appendix A, Section III(A)(4)**

Section 10: Compliance with Laws and Regulations

1. **Compliance Clauses Missing from Vendor Contracts**
   - **Impact:** Vendors may fail to comply with regulatory requirements if contractual obligations to do so are not clearly stated.
   - **Reference: Appendix A, Section III(A)(2)**
2. **Vendor Compliance Certifications Not Obtained**
   - **Impact:** Failure to collect vendor certifications may result in non-compliance with applicable laws and regulations, leading to fines or penalties.
   - **Reference: Appendix A, Section III(A)(2)**

Section 11: Insurance Coverage in Contracts

1. **Missing or Inadequate Insurance Clauses**
   - **Impact:** Vendors may not have adequate insurance coverage to cover potential damages or breaches, increasing the financial risk to the credit union.
   - **Reference: Appendix A, Section III(A)(2)**

Section 12: Vendor Risk Assessment

1. **No Regular Vendor Risk Assessments**
   - **Impact:** Failure to conduct regular vendor risk assessments may result in undetected risks associated with vendor relationships.
   - **Reference: Appendix A, Section III(A)(2)**
2. **Incomplete or Outdated Risk Assessments**
   - **Impact:** Outdated risk assessments may fail to reflect current vendor risks, particularly after changes in services or technology.
   - **Reference: Appendix A, Section III(A)(2)**

Section 13: Vendor Financial Information Review

1. **Financial Stability Not Reviewed for Critical Vendors**
   - **Impact:** Financially unstable vendors pose a risk of service interruptions or inability to fulfill contractual obligations.
   - **Reference: Appendix A, Section III(A)(2)**

Section 14: Authorization to Monitor Compliance in Contracts

1. **No Authorization to Monitor Vendors in Contracts**
   - **Impact:** Without a monitoring clause, the credit union may lack the ability to ensure vendor compliance with security and performance requirements.
   - **Reference: Appendix A, Section III(C)(1)(c)**

Section 15: Independent Validation of Security Controls

1. **No Independent Validation of Vendor Security Controls**
   - **Impact:** Vendors may not meet necessary security standards if independent validation is not required or reviewed.
   - **Reference: Appendix A, Section III(C)(1)(c)**

Section 16: Software Escrow Clause in Contracts

1. **No Software Escrow Clause in Contracts**
   - **Impact:** The credit union risks losing access to critical software in the event of vendor failure without an escrow agreement.
   - **Reference: Appendix A, Section III(A)(2)**

Section 17: Legal Review of Contracts

1. **Contracts Not Reviewed by Legal Counsel**
   - **Impact:** Without legal review, contracts may not adequately protect the credit union's interests, particularly regarding compliance and liability.
   - **Reference: Appendix A, Section III(C)(2)(b)**

Section 18: Independent Security Reviews (e.g., SOC Reports)

1. **SOC Reports or Independent Security Reviews Not Obtained**
   - **Impact:** The credit union may not be aware of vulnerabilities within vendors' systems if independent reviews are not conducted or obtained.
   - **Reference: Appendix A, Section III(C)(1)(c)**

Section 19: Addressing Material Exceptions in Independent Security Reviews

1. **Material Exceptions Not Handled Properly**
   - **Impact:** Failure to address exceptions identified in security reviews may leave the credit union exposed to security risks.
   - **Reference: Appendix A, Section III(A)(5)**

Section 20: Verifying Credit Union's Performance of Complementary User Entity Controls

1. **Failure to Implement Complementary User Entity Controls**
   - **Impact:** If the credit union fails to perform its responsibilities, critical security gaps may remain unresolved.
   - **Reference: Appendix A, Section III(C)(1)(c)**

Remediation

Thursday, September 19, 2024 4:08 PM

Mitigation Strategies for Third-Party Management Findings

Section 1: Vendor Management Policy

1. **Vendor Management Policy Not Documented or Approved**
   - **Mitigation:** Develop a formal vendor management policy that includes processes for selecting, monitoring, and evaluating vendors. Get the policy reviewed and approved by senior management or the board. Ensure it is updated regularly.
   - **Action:** Assign a dedicated team to develop the policy with input from key departments (IT, legal, compliance). Schedule an annual review process.
   - **Reference: Appendix A to Part 748, Section III(C)(1)(c)**
2. **Policy Does Not Include Vendor Categories**
   - **Mitigation:** Define vendor categories such as critical and non-critical. Implement procedures that align vendor risk with the level of oversight.
   - **Action:** Create categories based on vendors' access to sensitive information or the criticality of the service they provide.
   - **Reference: Appendix A, Section III(A)(1)**
3. **Lack of Annual Review and Approval**
   - **Mitigation:** Establish a regular review and approval process by the board or relevant committee to ensure vendor management policies stay current.
   - **Action:** Create a calendar for policy reviews and assign responsibility to a compliance or risk officer.
   - **Reference: Appendix A, Section III(C)(2)(b)**

Section 2: Due Diligence Process

1. **Due Diligence Process Not Documented**
   - **Mitigation:** Document the due diligence process, including the selection, evaluation, and monitoring of vendors. Specify criteria such as financial stability, security practices, and compliance with regulations.
   - **Action:** Use a checklist to standardize the due diligence process across all vendor engagements.
   - **Reference: Appendix A, Section III(A)(2)**
2. **Due Diligence Not Performed for Critical Vendors**
   - **Mitigation:** Prioritize due diligence for critical vendors, including comprehensive security assessments and financial reviews.
   - **Action:** Ensure a thorough risk assessment for critical vendors, and document findings and approvals.
   - **Reference: Appendix A, Section III(A)(1)**
3. **Ongoing Monitoring Process Not Implemented**
   - **Mitigation:** Implement an ongoing monitoring process that includes periodic risk assessments, audits, and performance reviews for all critical vendors.
   - **Action:** Schedule regular vendor reviews and set up automated alerts for key performance or compliance thresholds.
   - **Reference: Appendix A, Section III(C)(1)(c)**

Section 3: Critical Vendor and Contract Listing

1. **Outdated Vendor and Contract Lists**
   - **Mitigation:** Regularly update the list of critical vendors and contracts. Ensure that the list is integrated with procurement and financial data to stay current.
   - **Action:** Implement automated systems to ensure vendor data is updated in real-time whenever new vendors are onboarded or contracts are renewed.
   - **Reference: Appendix A, Section III(A)(1)**
2. **Critical Vendors Omitted from the List**
   - **Mitigation:** Conduct a full audit of all vendor relationships to identify missing critical vendors. Ensure they are included in the vendor management program.
   - **Action:** Perform an inventory check of vendors and cross-reference them with the organization’s critical systems.
   - **Reference: Appendix A, Section III(A)(1)**

Section 4: Information Security in Service Provider Contracts

1. **Missing Information Security Clauses**
   - **Mitigation:** Review and update vendor contracts to include specific information security clauses that cover data protection, breach notification, confidentiality, and compliance with relevant laws.
   - **Action:** Engage legal and compliance teams to review existing contracts and ensure security terms meet regulatory requirements.
   - **Reference: Appendix A, Section III(C)(1)(c)**
2. **Security Clauses Not Reviewed or Negotiated**
   - **Mitigation:** Ensure all new and existing vendor contracts include a security clause review. Negotiate stronger security terms where necessary.
   - **Action:** Establish a standard security addendum for all contracts and negotiate with vendors to include this in agreements.
   - **Reference: Appendix A, Section III(A)(3)**

Section 5: Incident Notification in Contracts

1. **Missing Incident Notification Clauses**
   - **Mitigation:** Add incident notification clauses in contracts that require vendors to notify the credit union of security breaches, data leaks, or other incidents within a specific time frame.
   - **Action:** Work with legal counsel to amend existing contracts and ensure future contracts include incident notification requirements.
   - **Reference: Appendix A, Section III(A)(2)**
2. **No Evidence of Historical Incident Notification**
   - **Mitigation:** Review the incident history for each vendor and document whether the notification requirements were met. Implement tracking to ensure timely notifications in the future.
   - **Action:** Set up a system to log and track all vendor notifications related to incidents.
   - **Reference: Appendix A, Section III(C)(1)(d)**

Section 6: Service Specifications in Contracts

1. **Service Specifications Not Clearly Defined in Contracts**
   - **Mitigation:** Update contracts to clearly define service frequency, format, and specifications. Include measurable performance metrics.
   - **Action:** Work with vendors to clarify service expectations and document them in contracts.
   - **Reference: Appendix A, Section III(A)(1)**
2. **No Regular Monitoring of Vendor Performance**
   - **Mitigation:** Establish a process for regularly monitoring vendor performance against the service specifications outlined in the contract.
   - **Action:** Implement performance management tools to track vendor service levels and take corrective actions if SLAs are not met.
   - **Reference: Appendix A, Section III(A)(4)**

Section 7: Oversight of Third-Party Technology Providers

1. **No Formal Oversight Process for Technology Providers**
    - **Mitigation:** Develop a formal oversight process for technology providers, including a governance structure that defines roles and responsibilities for monitoring third-party technology services.
    - **Action:** Establish an oversight committee to review and monitor technology provider performance.
    - **Reference: Appendix A, Section III(C)(1)(c)**

Section 8: Monitoring Information Security Measures

1. **Audit and Test Results Not Collected or Reviewed**
    - **Mitigation:** Ensure regular collection and review of third-party audit reports (e.g., SOC reports) and security test results.
    - **Action:** Set up automated requests for security audits from vendors and schedule reviews with the internal risk team.
    - **Reference: Appendix A, Section III(C)(1)(c)**

Section 9: Service Level Agreements (SLAs)

1. **SLAs Not Clearly Defined**
    - **Mitigation:** Review and update SLAs in contracts to ensure they are specific, measurable, and enforceable.
    - **Action:** Engage stakeholders to define measurable service levels and amend contracts where necessary.
    - **Reference: Appendix A, Section III(A)(3)**
2. **No Process for Monitoring SLA Performance**
    - **Mitigation:** Implement tools and processes to regularly track vendor performance against SLAs, including alerts for SLA breaches.
    - **Action:** Automate SLA tracking and create a reporting process for vendor performance reviews.
    - **Reference: Appendix A, Section III(A)(4)**

Section 10: Compliance with Laws and Regulations

1. **Compliance Clauses Missing from Vendor Contracts**
    - **Mitigation:** Ensure all vendor contracts include clauses that require compliance with relevant laws and regulations.
    - **Action:** Engage legal and compliance teams to review and update contracts as necessary to ensure regulatory compliance.
    - **Reference: Appendix A, Section III(A)(2)**
2. **Vendor Compliance Certifications Not Obtained**
    - **Mitigation:** Implement a process to request and review compliance certifications from vendors (e.g., PCI-DSS, HIPAA, SOC 2).
    - **Action:** Ensure compliance certifications are updated annually and stored for audit purposes.
    - **Reference: Appendix A, Section III(A)(2)**

Section 11: Insurance Coverage in Contracts

1. **Missing or Inadequate Insurance Clauses**
    - **Mitigation:** Update contracts to require vendors to maintain appropriate insurance coverage based on the level of risk they pose.
    - **Action:** Require vendors to provide certificates of insurance, and review them regularly for adequacy.
    - **Reference: Appendix A, Section III(A)(2)**

Section 12: Vendor Risk Assessment

1. **No Regular Vendor Risk Assessments**
    - **Mitigation:** Establish a schedule for regular risk assessments of all vendors, especially those that handle critical systems or sensitive data.
    - **Action:** Use a risk assessment framework to evaluate vendors on an annual basis and track risk mitigation measures.
    - **Reference: Appendix A, Section III(A)(2)**

Section 13: Vendor Financial Information Review

1. **Financial Stability Not Reviewed for Critical Vendors**
    - **Mitigation:** Regularly review the financial statements of critical vendors to ensure they remain stable and capable of fulfilling their contractual obligations.
    - **Action:** Incorporate financial reviews into your ongoing vendor risk assessment process.
    - **Reference: Appendix A, Section III(A)(2)**

Section 14: Authorization to Monitor Compliance in Contracts

1. **No Authorization to Monitor Vendors in Contracts**
    - **Mitigation:** Amend vendor contracts to include clauses allowing for the regular monitoring of compliance and performance.
    - **Action:** Work with legal counsel to update contracts and ensure monitoring provisions are included.
    - **Reference: Appendix A, Section III(C)(1)(c)**

Section 15: Independent Validation of Security Controls

1. **No Independent Validation of Vendor Security Controls**
    - **Mitigation:** Require all critical vendors to submit to independent security audits (e.g., SOC 2, ISO 27001) and review the results.
    - **Action:** Include independent validation requirements in new contracts and review existing contracts for compliance.
    - **Reference: Appendix A, Section III(C)(1)(c)**

Compliance

Thursday, September 19, 2024 4:09 PM

1. Establish a Vendor Management Policy

- **Develop and Approve a Vendor Management Policy:** Draft a comprehensive vendor management policy that details procedures for selecting, evaluating, and monitoring third-party vendors. Ensure the policy is reviewed and approved by the board or a designated committee.
- **Include Vendor Risk Categorization:** Define categories for vendors (e.g., critical and non-critical) based on the sensitivity of data accessed and the criticality of services provided.

Reference: Appendix A, Section III(C)(1)(c) – Vendors must be contractually required to maintain appropriate security safeguards.

2. Conduct Due Diligence on Vendors

- **Initial Vendor Risk Assessments:** Perform thorough due diligence on all third-party service providers before entering into a contract. Assess vendors' security posture, financial stability, and ability to comply with your institution's information security standards.
- **Ongoing Monitoring:** Implement a process for ongoing monitoring of vendors, especially those with access to sensitive member information. This should include periodic assessments, audits, and reviews.
- **Key Areas to Review:**
  - Vendor's financial health
  - Security controls and certifications (e.g., SOC reports)
  - Data protection measures
  - History of security incidents or breaches

Reference: Appendix A, Section III(A)(2) – Institutions must conduct due diligence in selecting and managing service providers.

3. Implement Strong Contractual Safeguards

- **Include Security Clauses in Contracts:** Ensure that contracts with third-party vendors include specific security requirements. These should cover the following areas:
  - Data protection and encryption
  - Access control measures
  - Confidentiality of member information
  - Breach notification timelines
- **Right to Audit:** Ensure contracts give the institution the right to audit vendors' security practices and review their security assessments.
- **Service Level Agreements (SLAs):** Define measurable SLAs for service performance, security standards, and breach response times. Ensure that non-compliance with SLAs triggers corrective actions or penalties.

Reference: Appendix A, Section III(C)(1)(c) – Vendors must be contractually required to implement and maintain appropriate security measures.

4. Conduct Regular Risk Assessments of Vendors

- **Ongoing Risk Assessment:** Conduct regular risk assessments for third-party vendors, especially critical service providers. Assess their security measures, operational stability, and compliance with your information security policies.
- **Focus on Critical Vendors:** Pay particular attention to vendors that have access to sensitive member information or that provide critical services. Ensure that the risks they present are regularly monitored and mitigated.
- **Vendor Risk Monitoring Tools:** Use automated tools to continuously monitor vendor risks, including financial health and cybersecurity posture.

Reference: Appendix A, Section III(A)(2) – Ongoing monitoring and assessment of third-party risks must be implemented.

5. Ensure Incident Notification and Response Procedures

- **Incident Notification Clauses in Contracts:** Ensure all third-party contracts require vendors to notify your credit union of any security incidents, data breaches, or significant disruptions in a timely manner. Define clear timelines for notification (e.g., within 24 hours of detection).
- **Review Historical Incidents:** Regularly review whether vendors have met incident notification requirements and track how incidents were handled.
- **Include Vendors in Your Incident Response Plan (IRP):** Ensure that vendors, especially those managing sensitive data, are included in your incident response plans. Clearly define the roles and responsibilities of each vendor in the event of an incident.

Reference: Appendix A, Section III(C)(1)(d) – Incident response plans must address unauthorized access or breaches involving third-party vendors.

6. Vendor Training and Awareness

- **Provide Training for Vendors:** Ensure that third-party vendors receive regular training on your institution's security policies, standards, and regulatory requirements.
- **Verify Vendor Staff Competency:** Ensure that vendors' employees who handle sensitive member information are trained in cybersecurity best practices, data protection, and incident response.

Reference: Appendix A, Section III(C)(1)(b) – Vendors must be aware of and comply with your institution's security procedures and standards.

7. Monitor Vendor Performance and Compliance

- **Regular Vendor Audits:** Implement a regular audit process to review vendor security practices, performance against SLAs, and compliance with contractual obligations. Use external or independent auditors when necessary (e.g., SOC 2 audits).
- **Review Independent Security Assessments:** Require vendors to provide regular independent security assessments, such as **SOC 1**, **SOC 2**, or **ISO 27001** certifications. Review the results of these assessments to ensure vendors meet security expectations.
- **Conduct Performance Reviews:** Periodically review vendor performance against SLAs, especially those related to security and incident response. Document all findings and ensure corrective actions are taken when performance falls short.

Reference: Appendix A, Section III(B)(3) – Regular testing and review of controls and safeguards should be part of the vendor management process.

8. Ensure Board Oversight of Third-Party Management

- **Annual Reports to the Board:** Provide the Board of Directors or an oversight committee with regular updates on the status of third-party management, including vendor risk assessments, contract reviews, security audits, and incidents involving third parties.
- **Board Involvement in Policy Development:** Ensure that the board or designated committee is involved in the approval of vendor management policies and practices.
- **Board-Approved Action Plans:** Present action plans to the board for addressing any third-party vendor risks or incidents.

Reference: Appendix A, Section III(C)(2)(b) – The board must oversee the implementation and effectiveness of the vendor management program.

9. Maintain Comprehensive Documentation

- **Document All Vendor Management Activities:** Keep records of all due diligence, risk assessments, security audits, and incident response activities related to third-party vendors. These records will demonstrate compliance and assist in regulatory audits.
- **Track Vendor Contracts and SLAs:** Maintain an updated list of all vendor contracts, including detailed service specifications, SLAs, and compliance clauses.
- **Ensure Audit Trails:** Document all monitoring activities, including audit results, vendor performance reviews, and corrective actions taken.

Reference: Appendix A, Section III(C)(2)(c) – Ensure proper documentation of the third-party management program is maintained to demonstrate compliance.

10. Regularly Review and Update Vendor Policies

- **Annual Review of Vendor Management Program:** Schedule an annual review of the vendor management program to ensure that it continues to meet the credit union's needs and complies with evolving regulatory requirements.
- **Adjust Vendor Categories:** Review vendor categories annually to ensure they remain appropriate based on the risk they pose to the institution.
- **Update Contracts and SLAs:** Ensure that vendor contracts and SLAs are updated as necessary to reflect changes in the services provided, regulatory requirements, or risk profile.

Reference: Appendix A, Section III(C)(1)(a) – The vendor management program must be updated regularly to reflect changes in business processes or vendor relationships.

11. Ensure Compliance with Relevant Laws and Regulations

- **Ensure Compliance with GLBA:** Ensure that vendors comply with the **Gramm-Leach-Bliley Act (GLBA)**, which governs the protection of nonpublic personal information (NPI). Vendors handling sensitive member information must follow GLBA standards for safeguarding data.
- **Monitor Regulatory Changes:** Implement a process for tracking changes in applicable laws and regulations and ensure that vendor contracts are updated accordingly.

Reference: Appendix A to Part 748 – Vendor management policies must ensure compliance with the Gramm-Leach-Bliley Act and other relevant regulations.

Contracts

Friday, August 16, 2024 2:06 PM

Contract Review Criteria

1. Scope of Services
- **[ ] Service Description**: Is the scope of services clearly defined, including specific deliverables, tasks, and responsibilities?
- **[ ] Service Specifications**: Are the quality, frequency, and format of the services or products provided clearly outlined?
- **[ ] Service Location**: Is it clear where the services will be performed or where products will be delivered?

2. Service Level Agreements (SLAs)
- **[ ] Performance Metrics**: Are the performance standards and metrics measurable and clearly defined?
- **[ ] Response Times**: Are response and resolution times specified for issues or service disruptions?
- **[ ] Penalties for Non-Performance**: Are there penalties or remedies in place for failure to meet SLAs?

3. Information Security and Data Protection
- **[ ] Data Handling**: Are data protection and handling requirements explicitly stated, including data storage, transmission, and access controls?
- **[ ] Compliance Requirements**: Does the contract mandate compliance with relevant data protection laws (e.g., GDPR, HIPAA)?
- **[ ] Incident Reporting**: Is there a clear process and timeline for reporting security incidents or breaches?
- **[ ] Confidentiality Clauses**: Are there strong confidentiality provisions protecting sensitive information?

4. Legal and Regulatory Compliance
- **[ ] Regulatory Compliance**: Does the contract require the third party to comply with all applicable laws, regulations, and industry standards?
- **[ ] Audit Rights**: Does the contract grant the institution the right to audit the third party for compliance with regulatory and contractual obligations?
- **[ ] Termination Clauses**: Are there clear provisions for terminating the contract if regulatory compliance is not maintained?

5. Financial Terms
- **[ ] Pricing Structure**: Is the pricing structure transparent, including all costs, fees, and payment terms?
- **[ ] Invoicing and Payment Terms**: Are the invoicing procedures and payment terms clear, including due dates and penalties for late payments?
- **[ ] Budget Impact**: Have potential cost fluctuations (e.g., due to service scope changes) been assessed and included?

6. Risk Management
- **[ ] Indemnification**: Does the contract include indemnification clauses protecting the institution from losses due to third-party actions?
- **[ ] Limitation of Liability**: Are the limitations of liability reasonable, and do they align with the risks involved?
- **[ ] Insurance Requirements**: Does the contract specify required insurance coverage (e.g., cyber liability, general liability) to be maintained by the third party?
- **[ ] Force Majeure**: Are there provisions for handling unforeseen events (force majeure) that may impact the third party's ability to deliver services?

7. Contract Governance
- **[ ] Dispute Resolution**: Are the mechanisms for dispute resolution clearly defined, including arbitration or litigation procedures?
- **[ ] Change Management**: Is there a clear process for managing changes to the contract, including amendments and scope changes?
- **[ ] Review and Renewal**: Are the review, renewal, and termination processes clearly outlined, including notice periods and conditions?

8. Intellectual Property (IP)
- **[ ] IP Ownership**: Is the ownership of intellectual property (e.g., software, data) created under the contract clearly defined?
- **[ ] License Terms**: Are the licensing terms for any third-party IP clearly stated?
- **[ ] IP Infringement**: Does the contract address IP infringement and the responsibilities of each party?

9. Business Continuity and Disaster Recovery
- **[ ] Continuity of Services**: Are there provisions for ensuring the continuity of services during disasters or disruptions?
- **[ ] Disaster Recovery Plans**: Does the third party have a documented and tested disaster recovery plan?
- **[ ] Notification Requirements**: Are there requirements for notifying the institution of any business continuity or disaster recovery incidents?

10. Termination and Exit Strategy
- **[ ] Termination Conditions**: Are the conditions under which the contract can be terminated by either party clearly stated?
- **[ ] Exit Strategy**: Does the contract outline an exit strategy, including the return or destruction of data and IP, and the continuation of critical services during the transition?
- **[ ] Post-Termination Support**: Are there provisions for post-termination support to ensure smooth transition to another vendor or back in-house?

11. Third-Party Monitoring and Reporting
- **[ ] Reporting Requirements**: Are the reporting requirements, including frequency and content of reports, clearly stated?
- **[ ] Performance Monitoring**: Does the contract define how the institution will monitor the third party's performance?
- **[ ] Review of Security Controls**: Are there requirements for the periodic review of the third party's security controls, including independent audits and assessments?

12. Review by Legal Counsel
- **[ ] Legal Review Process**: Has the contract been reviewed by legal counsel for compliance with internal policies and applicable laws?
- **[ ] Documentation of Legal Review**: Is there documentation confirming the legal review and any recommendations provided?
- **[ ] Incorporation of Legal Feedback**: Have legal recommendations been incorporated into the final contract?

Pitfalls

Friday, August 16, 2024 2:07 PM

Common Contract Review Pitfalls

1. Inadequate Definition of Scope
- **Vague or Ambiguous Service Descriptions**: Failing to clearly define the scope of services, deliverables, and responsibilities can lead to misunderstandings and disputes. This can result in unmet expectations or additional costs.
- **Missing Details on Service Specifications**: Not specifying the quality, frequency, or format of services/products can lead to subpar performance without clear grounds for recourse.

2. Weak or Unenforceable SLAs
- **Lack of Specificity in SLAs**: Service Level Agreements (SLAs) that are too broad or vague make it difficult to hold the vendor accountable for performance issues.
- **Absence of Penalties for SLA Breaches**: Without clearly defined penalties for failing to meet SLAs, vendors may have little incentive to adhere to agreed-upon standards.

3. Insufficient Focus on Data Protection and Security
- **Overlooking Data Handling and Security Requirements**: Failing to include robust data protection and information security clauses can expose the organization to data breaches, regulatory fines, and reputational damage.
- **Inadequate Incident Response Provisions**: Contracts that do not specify how and when the vendor must report security incidents can leave the organization vulnerable to delayed responses.

4. Neglecting Legal and Regulatory Compliance
- **Ignoring Regulatory Requirements**: Contracts that do not explicitly require compliance with relevant laws and regulations can result in legal liabilities for the organization.
- **Omitting Audit Rights**: Without the right to audit the vendor's compliance with contractual and regulatory obligations, the organization may be unable to verify adherence to critical standards.

5. Incomplete Financial Terms
- **Unclear or Unfavorable Pricing Structure**: Complex or ambiguous pricing terms can lead to unexpected costs and budget overruns. Failure to clarify payment terms can also cause disputes over invoices.
- **Lack of Cost Controls for Scope Changes**: Contracts that do not address potential cost increases due to changes in the scope of work can lead to significant financial risk.

6. Inadequate Risk Management Provisions
- **Missing Indemnification Clauses**: Without indemnification provisions, the organization may be exposed to significant liabilities arising from the vendor's actions.
- **Overly Broad Limitation of Liability**: Allowing the vendor to limit their liability too broadly can leave the organization with little recourse in the event of significant losses.
- **Insufficient Insurance Requirements**: Failing to require adequate insurance coverage from the vendor can leave the organization exposed to financial risks if the vendor's actions result in a loss.

7. Poor Contract Governance
- **Lack of Clear Dispute Resolution Mechanisms**: Contracts that do not outline how disputes will be resolved can lead to prolonged and costly legal battles.
- **Absence of Change Management Provisions**: Without a clear process for managing contract changes, amendments can be made haphazardly, leading to inconsistencies and confusion.
- **Neglecting Contract Renewal and Termination Processes**: Contracts that do not specify renewal and termination terms can result in unwanted automatic renewals or difficulties in exiting the agreement.

8. Overlooking Intellectual Property (IP) Rights
- **Unclear IP Ownership Clauses**: Failing to clearly define IP ownership can lead to disputes over who owns the work or products created under the contract.
- **Inadequate IP Protection**: Contracts that do not protect the organization's IP rights can result in unauthorized use or loss of valuable intellectual property.

9. Weak Business Continuity and Disaster Recovery Clauses
- **Lack of Continuity of Services Provisions**: If the contract does not address how services will continue during a disaster or vendor failure, the organization may face significant operational disruptions.
- **Unspecified Disaster Recovery Plans**: Failing to require and review the vendor's disaster recovery plan can leave the organization unprepared for emergencies.

10. Inadequate Termination and Exit Strategy
- **Overlooking Termination Clauses**: Contracts without clear termination clauses can make it difficult for the organization to exit the agreement, even if the vendor fails to perform.
- **No Defined Exit Strategy**: Without a clear exit strategy, including data return or transfer provisions, the organization may face challenges in transitioning services to another provider.

11. Insufficient Monitoring and Reporting
- **Lack of Ongoing Monitoring Provisions**: Contracts that do not specify how the organization will monitor the vendor's performance and compliance can lead to undetected issues and risks.
- **Inadequate Reporting Requirements**: Without regular reporting, the organization may be unaware of the vendor's performance issues, security concerns, or other risks.

12. Incomplete Legal Review
- **Skipping Legal Review**: Failing to have contracts reviewed by legal counsel increases the risk of missing critical legal, regulatory, and compliance issues.
- **Incorporating Legal Feedback**: If legal recommendations are not properly incorporated into the final contract, the organization may still be exposed to legal risks.

Mitigating These Pitfalls

To avoid these pitfalls, organizations should:
- Establish a standardized contract review process that includes input from legal, compliance, finance, and operational teams.
- Use detailed checklists to ensure all critical areas are covered.
- Regularly train staff involved in contract management on best practices and common pitfalls.
- Engage legal counsel early in the contract negotiation process to ensure all potential risks are addressed.

By being vigilant and systematic in the contract review process, organizations can better protect their interests and reduce the risk of unfavorable outcomes.

SOC reports

Friday, August 16, 2024 2:10 PM

System and Organization Control (SOC) reports are critical tools for evaluating the effectiveness of a service organization's internal controls, particularly when it comes to security, confidentiality, and data integrity. However, relying on SOC reports without fully understanding their limitations and potential issues can lead to significant risks. Here are some common issues to be aware of when reviewing SOC reports:

Common SOC Report Issues

1. Misinterpretation of the Scope of the Report

- **Understanding the Scope**: Not all SOC reports cover the same scope. For example, a SOC 1 report focuses on financial reporting controls, while SOC 2 and SOC 3 reports cover security, availability, processing integrity, confidentiality, and privacy. Misunderstanding the scope can lead to reliance on controls that are not relevant to your organization's needs.
- **Incomplete Scope**: The SOC report may not cover all relevant systems or controls. For example, it might exclude certain subcontractors or critical systems that could impact the security and availability of the service provided.

2. Time Period Coverage Issues

- **Outdated Reports**: SOC reports cover a specific time period, typically six months to a year. If the report is outdated, it may not reflect the current control environment, leaving you unaware of recent changes or issues.
- **Gaps in Coverage**: If there are significant gaps between the end of the period covered by the SOC report and the present, recent control failures or changes may not be reflected.

3. Inadequate Review of Complementary User Entity Controls (CUECs)

- **Neglecting CUECs**: SOC reports often include Complementary User Entity Controls (CUECs) that the service organization expects the user entity (your organization) to implement. Failing to review and implement these controls can lead to gaps in the control environment.
- **Assuming Completeness**: Some organizations mistakenly assume that the service organization is responsible for all controls, leading to an incomplete implementation of necessary security measures.

4. Limited Insight into Subservice Organizations

- **Carve-Out Method**: Some SOC reports use the "carve-out method," where the service organization's controls over subservice organizations are excluded. This means you might not have visibility into how critical third parties (subservice organizations) are managed and whether their controls are effective.
- **Insufficient Detail**: Even when subservice organizations are included, the SOC report may provide limited information on the controls these organizations have in place, making it difficult to assess the full risk.

5. Over-Reliance on Control Descriptions

- **Assuming Control Effectiveness**: Just because a control is described in the SOC report doesn't mean it is effective. It's important to review the auditor's findings to understand whether controls were operating as intended during the review period.
- **Ignoring Control Failures**: SOC reports typically include a section on control failures or deviations. Overlooking or underestimating the significance of these failures can lead to unaddressed vulnerabilities.

6. Not Considering the Type of Report

- **SOC 1 vs. SOC 2**: SOC 1 reports focus on internal controls relevant to financial reporting, while SOC 2 reports focus on controls related to security, availability, processing integrity, confidentiality, and privacy. Using the wrong type of report for your assessment needs can lead to inadequate evaluation of relevant controls.
- **SOC 2 Type I vs. Type II**: SOC 2 Type I reports evaluate the design of controls at a specific point in time, while SOC 2 Type II reports evaluate both the design and operating effectiveness of controls over a period of time. Relying on a Type I report when ongoing control effectiveness is crucial can be risky.

7. Incomplete or Ambiguous Reporting

- **Vague Control Descriptions**: Some SOC reports may include control descriptions that are too vague or general, making it difficult to assess their relevance or effectiveness.
- **Unclear Findings or Recommendations**: Reports that do not clearly articulate control failures or recommendations for improvement can lead to misunderstandings about the service organization's control environment.

8. Ignoring Material Exceptions and Auditor's Opinions

- **Downplaying Exceptions**: Material exceptions or deviations identified by the auditor should be taken seriously. These exceptions indicate that certain controls did not operate effectively, which could expose your organization to risks.
- **Qualified Opinions**: If the auditor issues a qualified opinion, indicating that there were significant issues with the controls, this should be a red flag. Ignoring or underestimating the impact of a qualified opinion can lead to unaddressed risks.

9. Failing to Align SOC Reports with Internal Risk Assessments

- **Not Integrating with Risk Management**: SOC reports should be integrated into your organization's broader risk management framework. Failing to do so can lead to gaps in your understanding of how third-party risks impact your overall risk profile.
- **Overlooking Context**: The risks and controls highlighted in a SOC report should be considered in the context of your specific operations, regulatory requirements, and risk appetite.

10. Lack of Ongoing Monitoring and Review

- **One-Time Review**: Treating SOC reports as a one-time checklist rather than part of an ongoing monitoring process can lead to a false sense of security. Regularly reviewing updated reports and maintaining an ongoing dialogue with the service provider is crucial.
- **Neglecting Follow-Up on Findings**: If issues are identified in a SOC report, it is essential to follow up with the service provider to ensure that corrective actions are taken. Failure to do so can result in unresolved risks.

Mitigating SOC Report Issues

To mitigate these issues:

- **Understand the Scope and Limitations**: Always review the scope, period coverage, and limitations of the SOC report to understand what is included and excluded.
- **Evaluate Complementary Controls**: Ensure that Complementary User Entity Controls (CUECs) are understood and implemented within your organization.
- **Review Material Exceptions and Auditor Opinions**: Pay close attention to any control failures or material exceptions noted in the report, and consider their potential impact.
- **Incorporate SOC Reports into Risk Management**: SOC reports should be part of a broader third-party risk management strategy, aligned with your organization's risk profile and regulatory obligations.
- **Maintain Ongoing Monitoring**: SOC reports should be reviewed regularly as part of an ongoing vendor management process, not just during the initial vendor assessment.

By being aware of these common issues and taking proactive steps to address them, organizations can more effectively use SOC reports to manage third-party risks.

Risk Management

Friday, August 16, 2024 2:16 PM

1. Categorize Vendors by Type

- **Critical Vendors**: Vendors whose failure or compromise would have a significant impact on your organization's operations, reputation, or compliance. Examples include cloud service providers, payment processors, and cybersecurity vendors.
- **High-Risk Vendors**: Vendors that handle sensitive data, perform essential services, or operate in high-risk regions. Examples include data processors, IT infrastructure providers, and suppliers in politically unstable regions.
- **Moderate-Risk Vendors**: Vendors that provide important but non-critical services or products. Their failure would cause disruption but not necessarily a catastrophic impact. Examples include office supply vendors, HR software providers, and general service contractors.
- **Low-Risk Vendors**: Vendors whose services or products have minimal impact on your organization's operations. Examples include catering services, janitorial services, and some office equipment suppliers.

2. Assess Vendor Risk Factors

- **Data Sensitivity**: Assess the level of access the vendor has to your sensitive data, including personal, financial, or proprietary information.
- **Regulatory Requirements**: Determine if the vendor is subject to regulatory requirements or if your organization must ensure compliance through the vendor (e.g., GDPR, HIPAA).
- **Financial Stability**: Evaluate the financial health of the vendor to ensure they can continue providing services without interruption.
- **Operational Impact**: Assess how critical the vendor's services or products are to your core operations and whether there are viable alternatives.
- **Geopolitical Risk**: Consider the risks associated with the vendor's location, including political instability, natural disasters, or supply chain vulnerabilities.
- **Security Posture**: Review the vendor's cybersecurity practices, including their history of breaches, security certifications, and adherence to best practices.
- **Reputational Risk**: Assess the potential for reputational damage if the vendor were to experience a breach, fail to deliver services, or become involved in a scandal.
- **Service Criticality**: Determine how critical the vendor's services are to your daily operations. This can include whether the vendor is involved in key processes or supports critical infrastructure.

3. Score Vendors Based on Risk

Develop a scoring system to quantify the risk associated with each vendor. Assign weights to each risk factor based on your organization's priorities and tolerance for risk. For example:

- **Data Sensitivity**: 25%
- **Regulatory Compliance**: 20%
- **Operational Impact**: 20%
- **Financial Stability**: 15%
- **Security Posture**: 10%
- **Reputational Risk**: 5%
- **Geopolitical Risk**: 5%

Score each vendor on a scale (e.g., 1 to 5) for each risk factor, then calculate an overall risk score by multiplying each score by its respective weight and summing the results.

4. Prioritize Vendors Based on Risk Score

Rank vendors based on their overall risk scores from highest to lowest. This will help you identify which vendors require the most immediate attention and ongoing monitoring.

5. Implement Risk Mitigation Strategies

- **High-Risk Vendors**:
  - Conduct regular risk assessments and audits.
  - Implement strict contractual requirements, including robust service level agreements (SLAs) and security obligations.
  - Establish contingency plans for vendor failure.
  - Monitor for changes in the vendor's risk profile.
- **Moderate-Risk Vendors**:
  - Perform periodic risk assessments.
  - Ensure contractual agreements address key risks, including data security and compliance requirements.
  - Monitor vendor performance and compliance with agreed-upon terms.
- **Low-Risk Vendors**:
  - Conduct initial due diligence to ensure basic compliance and operational reliability.
  - Review contracts to include general terms for data security and performance.
  - Perform periodic reviews but with less frequency than higher-risk vendors.

6. Continuous Monitoring and Review

- **Ongoing Monitoring**: Regularly review vendor performance, security incidents, and changes in the vendor's operational environment that could affect their risk profile.
- **Update Risk Assessments**: Reassess vendor risk profiles at least annually or when significant changes occur (e.g., mergers, new regulations, or security incidents).
- **Adjust Prioritization**: Update your vendor prioritization list based on the latest risk assessments, and adjust resource allocation accordingly.

7. Communication and Reporting

- **Internal Reporting**: Regularly report on high-risk vendors to senior management and relevant stakeholders, highlighting key risks and mitigation efforts.
- **Vendor Communication**: Communicate risk management expectations and findings to vendors, and collaborate on risk mitigation strategies.

8. Documentation

- Maintain detailed records of all vendor risk assessments, scoring methodologies, monitoring activities, and risk mitigation efforts. Ensure this documentation is readily accessible for audits and compliance reviews.

1. Vendor Identification and Classification

- **Identify Vendor**: Record the vendor's name, contact information, and key representatives.
- **Classify Vendor**:
  - Critical Vendor
  - High-Risk Vendor
  - Moderate-Risk Vendor
  - Low-Risk Vendor

2. Initial Due Diligence

- **Company Background**:
  - Verify the vendor's legal entity status (e.g., registration, incorporation).
  - Check the vendor's reputation (e.g., customer reviews, industry standing).
  - Assess the vendor's financial stability (e.g., credit ratings, financial statements).
- **Experience and Expertise**:
  - Review the vendor's experience in the industry.
  - Evaluate the vendor's expertise in the required services/products.
- **References**:
  - Obtain and review references from other clients.
  - Check for any past incidents, lawsuits, or disputes.

3. Regulatory Compliance

- **Regulatory Requirements**:
  - Identify any industry-specific regulations that apply to the vendor.
  - Verify that the vendor complies with relevant laws and regulations (e.g., GDPR, HIPAA, PCI DSS).
- **Certifications**:
  - Review the vendor's certifications (e.g., ISO 27001, SOC 2).
  - Verify the validity and scope of certifications.

4. Information Security and Data Privacy

- **Security Controls**:
  - Assess the vendor's cybersecurity policies and practices.
  - Review the vendor's data encryption methods (both in transit and at rest).
  - Verify the vendor's incident response and breach notification procedures.
- **Access Controls**:
  - Evaluate the vendor's access control mechanisms (e.g., role-based access, multi-factor authentication).
  - Determine how the vendor manages privileged accounts.
- **Data Handling**:
  - Assess how the vendor collects, processes, and stores data.
  - Review the vendor's data retention and destruction policies.
- **Third-Party Subcontractors**:
  - Identify any subcontractors the vendor uses.
  - Ensure subcontractors are subject to similar security and compliance requirements.

5. Business Continuity and Disaster Recovery

- **Business Continuity Plan (BCP)**:
  - Review the vendor's BCP and ensure it aligns with your organization's needs.
  - Verify the frequency of BCP testing and updates.
- **Disaster Recovery Plan (DRP)**:
  - Assess the vendor's DRP, including recovery time objectives (RTOs) and recovery point objectives (RPOs).
  - Ensure the vendor has documented procedures for disaster recovery.
- **Redundancy and Resilience**:
  - Determine if the vendor has redundant systems and data centers.
  - Assess the vendor's ability to maintain service continuity during disruptions.

6. Contractual Obligations and Legal Considerations

- **Contract Review**:
  - Ensure the contract includes clear terms for data security, confidentiality, and privacy.
  - Verify the inclusion of service level agreements (SLAs) with measurable metrics.
  - Check for provisions on audit rights and vendor performance monitoring.
  - Review termination clauses and conditions for contract exit.
- **Legal Compliance**:
  - Ensure the contract includes clauses for compliance with applicable laws and regulations.
  - Verify that the contract addresses the vendor's responsibility for regulatory changes.
- **Liability and Indemnity**:
  - Review liability and indemnity clauses to ensure appropriate risk allocation.
  - Verify that the contract includes provisions for breach notification and remediation.

7. Risk Assessment and Scoring

- **Risk Factors**:
  - Data Sensitivity: Assess the level of sensitive data handled by the vendor.
  - Operational Impact: Determine the impact of vendor failure on your operations.
  - Financial Stability: Evaluate the financial health of the vendor.
  - Regulatory Compliance: Assess the vendor's adherence to relevant regulations.
  - Security Posture: Review the vendor's security controls and incident history.
  - Reputational Risk: Consider potential reputational damage from vendor association.
- **Scoring Methodology**:
  - Assign scores to each risk factor based on the vendor's responses and findings.
  - Calculate an overall risk score to prioritize the vendor.

8. Ongoing Monitoring and Review

- **Performance Monitoring**:
  - Establish a schedule for regular performance reviews (e.g., quarterly, annually).
  - Monitor vendor performance against SLAs and other contractual obligations.
- **Security Audits**:
  - Schedule regular security audits or assessments of the vendor.
  - Review audit reports, including SOC 2, ISO 27001, and other relevant certifications.
- **Incident Reporting**:
  - Ensure the vendor has a process for reporting incidents in a timely manner.
  - Verify that the vendor provides root cause analyses and remediation plans for incidents.
- **Compliance Monitoring**:
  - Monitor the vendor's ongoing compliance with regulatory requirements.
  - Ensure the vendor provides updates on any regulatory changes that may impact the relationship.

9. Documentation and Reporting

- **Assessment Documentation**:
  - Maintain detailed records of all assessments, findings, and risk scores.
  - Document any issues identified and the actions taken to address them.
- **Reporting**:
  - Provide regular reports to senior management and relevant stakeholders on vendor risks.
  - Include updates on high-risk vendors and any changes in risk profiles.
- **Contractual Updates**:
  - Review and update contracts as necessary based on changes in risk or regulatory requirements.
  - Ensure any changes are documented and communicated to all relevant parties.

10. Training and Awareness

- **Employee Training**:
  - Provide training for employees involved in vendor management on risk assessment procedures.
  - Ensure employees are aware of the importance of third-party risk management.
- **Vendor Awareness**:
  - Communicate risk management expectations to vendors.
  - Collaborate with vendors on improving security controls and compliance.

11. Remediation and Contingency Planning

- **Remediation Plans**:
  - Develop and implement remediation plans for identified risks.
  - Monitor the progress of remediation efforts and reassess risks as necessary.
- **Contingency Planning**:
  - Prepare contingency plans for vendor failure or breach.
  - Ensure backup vendors or alternative solutions are available if needed.

References

Friday, August 16, 2024 2:18 PM

Strong	Satisfactory	Less Than Satisfactory	Deficient	Critically Deficient
☐ Formal risk-based vendor management program has been implemented to monitor service provider and vendor relationships; ☐ Monitoring of service level agreement (SLA) compliance; ☐ Monitoring of internal/external audit reports; ☐ Monitoring of incident response and monitoring of business continuity program, including integrated testing; ☐ Addresses foreign-based risks when applicable (including OFAC and SDN)	☐ Formal risk-based vendor management program has been implemented to monitor service provider and vendor relationships; ☐ Monitoring of service level agreement (SLA) compliance; ☐ Monitoring of internal/external audit reports; ☐ Either no monitoring of incident response or no monitoring of business continuity program, including integrated testing; ☐ Foreign-based risks are not consistently considered, when applicable.	☐ Informal risk-based vendor management program has been implemented to monitor service provider and vendor relationships; ☐ Monitoring of service level agreement (SLA) compliance; ☐ No monitoring of internal/external audit reports; ☐ No monitoring of incident response and business continuity program, including integrated testing; ☐ Foreign-based risks are not considered, when applicable.	☐ Informal risk-based vendor management program has been implemented to monitor service provider and vendor relationships; ☐ No monitoring of service level agreement (SLA) compliance; ☐ No monitoring of internal/external audit reports; ☐ No monitoring of incident response and business continuity program, including integrated testing; ☐ Foreign-based risks are not considered, when applicable.	☐ No risk-based vendor management program has been implemented to monitor service provider and vendor relationships.

https://ithandbook.ffiec.gov/it-booklets/development-and-acquisition/introduction.aspx

From <https://ithandbook.ffiec.gov/it-booklets/outsourcing-technology-services/risk-management/contract-issues.aspx>

Strong	Satisfactory	Less Than Satisfactory	Deficient	Critically Deficient
☐ Due diligence process in place; ☐ includes copy and review of key vendor's audited financial statements; ☐ includes copy and review of key vendor's internal controls, information security, privacy protections, and audit coverage; ☐ includes copy or review of key vendor's insurance coverage; ☐ includes copies and review of key vendor's BCP, use of subcontractors, and record retention practices.	☐ Due diligence process in place; ☐ includes copy and review of key vendor's audited financial statements; ☐ includes copy or review of key vendor's insurance coverage; ☐ includes copy and review of key vendor's internal controls, information security, privacy protections, and audit coverage. ☐ Does not include copies and review of key vendor's BCP, use of subcontractors, and record retention practices.	☐ Due diligence process in place; ☐ includes copy and review of key vendor's audited financial statements; ☐ includes copy or review of key vendor's insurance coverage; ☐ does not include copy or review of key vendor's internal controls, information security, privacy protections, and audit coverage. ☐ Does not include copies and review of key vendor's BCP, use of subcontractors, and record retention practices.	☐ Due diligence process in place, but not risk based; ☐ does not include copy or review of key vendor's audited financial statements; ☐ does not include copy or review of key vendor's insurance coverage; ☐ does not include copy or review of key vendor's internal controls, information security, privacy protections, and audit coverage. ☐ Does not include copies and review of key vendor's BCP, use of subcontractors, and record retention practices.	☐ No due diligence process in place.

Strong	Satisfactory	Less Than Satisfactory	Deficient	Critically Deficient
☐ Contracts with key vendor or vendors are in place ☐ include specifications of the service or product to be provided and measurable service level agreements; ☐ include a requirement to comply with laws; ☐ include insurance coverage requirements; ☐ include confidentiality and security of information; ☐ include timely notification of breach and incident requirements; ☐ include provisions for third party to subcontract or use another party to meet its obligations.	☐ Contracts with key vendor or vendors are in place; ☐ include specifications of the service or product to be provided and measureable service level agreements; ☐ include a requirement to comply with laws; ☐ include insurance coverage requirements; ☐ include confidentiality and security of information; ☐ include timely notification of breach and incident requirements; ☐ do not include provisions for third party to subcontract or use another party to meet its obligations.	☐ Contracts with key vendor or vendors are in place; ☐ include specifications of the service or product to be provided and measureable service level agreements; ☐ include a requirement to comply with laws; ☐ do not include insurance coverage requirements; ☐ do not include confidentiality and security of information; ☐ do not include timely notification of breach and incident requirements. ☐ Does not include provisions for third party to subcontract or use another party to meet its obligations.	☐ Contracts with key vendor or vendors are in place; ☐ do not specifications of the service or product to be provided and measureable service level agreements; ☐ do not include a requirement to comply with laws; ☐ do not include insurance coverage requirements; ☐ do not include confidentiality and security of information; ☐ do not include timely notification of breach and incident requirements. ☐ Does not include provisions for third party to subcontract or use another party to meet its obligations.	☐ Contracts with key vendor or vendors are not in place.

Examiner Finding

Thursday, December 12, 2024 4:27 PM

Finding: Vendor Management Policy Enhancements Needed

The credit union's Vendor Management Policy demonstrates a strong foundation in managing third-party relationships. However, several areas require enhancements to fully align with regulatory expectations and best practices as outlined in Stmt 9. The following gaps were identified:

1. **Contract Provisions:**
    - Contracts for critical vendors do not include **software escrow clauses** (Stmt 9.17), leaving the credit union vulnerable in the event of vendor insolvency or failure.
    - Provisions addressing the credit union's role in **complementary user entity controls** (Stmt 9.21) are not clearly defined, potentially impacting the institution's ability to meet its responsibilities in SOC reports.
2. **Oversight Processes:**
    - The policy lacks detailed procedures for the **management and oversight of critical third-party technology service providers** (Stmt 9.7), which may result in inconsistent accountability and monitoring practices.
3. **Financial Review and Risk Monitoring:**
    - The review of **vendor financial condition and operational controls** (Stmt 9.10, 9.14) is not robust enough to ensure timely detection of financial instability or operational risks.
    - Processes for addressing **exceptions in periodic independent security reviews** (Stmt 9.20) are not defined, increasing the risk of unresolved vulnerabilities.
4. **Legal and Contractual Oversight:**
    - While legal reviews of contracts are performed (Stmt 9.11, 9.18), there is insufficient documentation of how recommendations from legal counsel are incorporated into final agreements.
5. **Board Reporting:**
    - Reporting to the board on **vendor performance and compliance with SLAs** (Stmt 9.15) needs to be standardized to ensure consistent oversight and informed decision-making.

Recommendation for Resolution:

To address these findings, the credit union should implement the following measures:

1. **Update Contracts:** Include software escrow clauses and clearly define complementary user entity controls in contracts with critical vendors.
2. **Enhance Oversight:** Develop and implement detailed procedures for managing and overseeing critical third-party technology service providers.
3. **Strengthen Financial and Risk Monitoring:** Establish quarterly reviews of vendor financial conditions and create a framework for resolving exceptions in SOC reports.
4. **Legal Integration:** Document the incorporation of legal counsel's

recommendations into all contracts and ensure periodic reviews align with regulatory updates.

5. **Board Reporting Improvements:** Create standardized templates and schedules for reporting vendor performance, SLA compliance, and risk assessments to the board.

Notes

Tuesday, September 3, 2024 6:46 AM

To validate the Vendor Management Program, it was ensured that a comprehensive policy was in place outlining procedures for vendor selection, evaluation, and monitoring, including board approval and risk categorization based on data sensitivity and service criticality. Thorough due diligence was conducted for all vendors before engagement, assessing their financial stability, security posture, and compliance, with ongoing monitoring through periodic assessments, audits, and reviews of SOC reports, data protection measures, and incident histories. Contracts were verified to include robust security requirements such as data protection, encryption, access controls, breach notification timelines, rights to audit, and enforceable SLAs. Regular risk assessments were conducted, prioritizing critical vendors, and automated tools were used to monitor financial health and cybersecurity risks. Incident notification clauses in contracts were reviewed, past vendor responses to incidents were evaluated, and vendors were integrated into the institution's incident response plan. Vendors received regular training on the institution's security standards and best practices, and it was confirmed that their staff were competent in data protection and incident response. Vendor performance was monitored through audits, independent security assessments, and SLA reviews, with corrective actions documented for deficiencies. The board received regular updates on vendor management activities, including risk assessments, contract reviews, and incidents, and participated in policy approval and risk mitigation. Comprehensive documentation of all vendor management activities was maintained, including updated inventories of contracts and audit trails. The program was reviewed annually to align with institutional needs and regulatory updates, with adjustments made to vendor categories, contracts, and SLAs as required. Lastly, compliance with applicable laws, including the GLBA, was ensured, and processes were maintained to monitor and address regulatory changes.