Auditing the Vendor

ACUIA- September 25, 2020

Third Party

Third Party is an Entity that has a business arrangement with the Credit Union. Generally, the relationship is memorialized with a formal contract.

Third party relationships may consist of traditional vendor or supplier relationships and non-traditional arrangements. Though, Third party relationships generally do not include members.

Typical Third Parties of the Credit Union

- Software Providers
- System Developers
- Hardware Providers
- Outsourced Loan Servicing
- Payment Processors
- Payroll Processors
- Outsourced Human Resources Consulting
- Statement and Mail services
- Consultants
- Suppliers
- Agents
- Cash Courier

Other Third Parties

Auto Dealers
Brokers
Correspondent Banks and Lenders
Affiliates
Joint Venture
Partners

© 2020 Crowe LLP

Polling Question #1

© 2020 Crowe LLP

Why Do Credit Unions Use Third Parties?

Process Data or Perform Services More Efficiently, Faster, Less Expensively

Expertise, Experience, and Knowledge

People

© 2020 Crowe LLP

What Risks Are Associated with Third Parties?

Third Parties may have the Credit Union's data, physical assets, money, and may interact with the Credit Union's members.

Risks

- Physical Information
- Data and Information Privacy
- Compliance including all applicable federal regulations, especially Fair Lending/Fair Banking, BSA/AML, and in some cases General Data Protection Regulation

More Risks

- Business Continuity and Recovery
- Business Recovery
- Financial Condition and Viability
- Fourth Parties

© 2020 Crowe LLP

What Risks Are Associated with Third Parties?

More, More Risks:

- Operations
- Customer complaints
- Fraud
- Credit
- Regulatory
- IT Security
- Privacy
- Legal
- Reputation and Negative News
- Strategic

© 2020 Crowe LLP

Polling Question #2

© 2020 Crowe LLP

Third Party Guidance

- FRB SR 2013 – 19: Guidance on Managing Outsourcing Risk CFPB
- FDIC FIL 44-2008: Guidance for Managing Third Party Risk
- FFIEC Appendix J (2015): Strengthening the Resilience of Outsourced Technology Services
- OCC Bulletin 2013 – 29: Risk Management Guidance

© 2020 Crowe LLP

Third Party Governance

- Board oversight
- Senior management TPRM Committee
- Structure
- Policy and Procedures
- Training
- Tools and Technology
- Reporting

© 2020 Crowe LLP

Credit Union Control Failures of Third Parties

Third party control failures attributed to financial institutions:

- Lack of Board oversight
- No policy and documented procedures
- No inventory of Third Parties and contracts
- No tracking and lack of contract requirements
- No one assigned to coordinate TPRM activities
- No risk rating of Third Parties
- No due diligence performed prior to signing contract
- No ongoing due diligence or audit of Third Parties
- No legal review or parameters for legal review
- Cost is not clearly articulated
- Don’t evaluate Third Parties against alternatives
- Everyone has access to add, delete, change of the TPRM system …….. etc

© 2020 Crowe LLP

Third Party Failures

Failures of Third Parties include:

Governance, service performance and quality, product quality

- Third Party does not have policy and procedures regarding the processes that they are required to perform.
- No oversight to ensure contract requirements are met.
- Third party does not comply with applicable regulations.
- Third party has not established governance.
- Third party does not have adequate resources.
- Third party has not provided quality service.
- Oversight of subcontractors.
- No controls over Credit Union system, data, information

© 2020 Crowe LLP

Polling Question #3

© 2020 Crowe LLP

3 Lines of Defense

First Line of Defense - Management implements TPRM processes and Independent Review

Second Line of Defense – Risk Management, Quality Control

Third Line of Defense – Internal audit reviews TPRM activities end to end for completeness, accuracy, compliance with regulatory requirements and risk profile

© 2020 Crowe LLP

Credit Union Third Party Key Controls

Inventory

Key Control: The Credit Union should have a process to determine the completeness of its Third Party inventory.

The Credit Union should consider accounts payable, executed agreements, contract repository of existing contracts, other real estate owned, collections and foreclosure activities, and inquiring of personnel to determine Third Party relationships not included in its inventory and identify gaps. Inventory should identify individual(s) responsible for each Third Party relationship.

© 2020 Crowe LLP

Credit Union Third Party Key Controls

Contract

Key Control: The Credit Union should have a contract for each significant Third Party relationship and the contract should include required language.

Each contract should identify the relationship, cost and compensation, specific performance required and compliance with laws and regulations, customer complaints, insurance, security breach, technology responsibilities, confidentiality. The Credit Union should seek Legal Counsel assistance to determine the clauses deemed necessary. Clauses that may be considered include right to audit and require remediation, having a current business continuity and resumption plan.

Key Control: All Third Party relationships should be assigned to an individual that is responsible for that relationship, its services, ensuring that the Vendor performs in accordance with the contract, and is responsible for evaluating and risk rating the Vendor ongoing.

© 2020 Crowe LLP

Credit Union Third Party Key Controls

Due Diligence

Key Control: The Credit Union should implement due diligence of evaluating Third Parties prior to executing contracts.

The Credit Union should perform due diligence of Third Party including but not limited to financial statements, site visits, insurance, risk management practices, Third Party's ability to comply with all applicable regulations and respond to incidents. Based upon information obtained, the Credit Union should risk assess each Third Party as it is setup on its Third Party system. This risk assessment will also drive ongoing monitoring.

© 2020 Crowe LLP

Credit Union Third Party Key Controls

Ongoing Monitoring

Key Control: The Credit Union should implement ongoing monitoring of Third Parties.

The Credit Union should implement ongoing monitoring. Such monitoring should include but not limited to financial condition, insurance coverage, business strategy, violations of compliance with laws and regulations, breach of and ability to, maintain confidentiality and security of data, customer complaints, business continuity and resumption plan, BSA/AML program, service lapses, periodic Third Party audits.

© 2020 Crowe LLP

Credit Union Third Party Key Controls

Ongoing Monitoring – Risk Assessment

Key Control: The Credit Union should risk assess each Third Party as it is setup on the Third Party system.

The Credit Union should establish risk assessment methodology for inherent and residual risk. Inherent risk should be based on type and significance of relationship, and number of services. Residual risk should incorporate effectiveness of controls, and inherent and residual risk ratings may be described as critical, high, moderate, and low.

© 2020 Crowe LLP

Credit Union Third Party Key Controls

Key Control: The Credit Union should formally develop and implement an ongoing monitoring program for risk assessed Third Parties. Such a program should assess financial viability, service/system performance completeness, accuracy, and quality,

The Credit Union should consider risk ratings in its ongoing monitoring of Third Parties. Critical and high residual risk rated Third Parties would be monitored more frequently and with greater effort. Third Party information obtained should include SOC 2 or SSAE18 independent audit reports. User control considerations noted in these reports should be reviewed and controls implemented at the Credit Union in response should be documented. Contract performance and adherence to service level agreement should be monitored.

© 2020 Crowe LLP

Polling Question #4

© 2020 Crowe LLP

Auditing the Vendor – Audit Program

Some audit procedures….

- Obtain the Credit Union's Third Party policy and determine whether the policy addresses inventory, vendors and subcontractors, contracts, due diligence, ongoing monitoring, termination, and governance.
- Based on the specific product or service provided, inquire of Vendor's processes to comply with policy, controls, applicable federal laws and regulations. Additionally, obtain audit, exam, internal audit reports and determine, by reviewing Credit Union records and onsite observation and evaluation as permitted by contract, whether Vendor is complying with policy, controls, applicable laws and regulations.
- Based on the service level or specific performance required in the contract determine, by reviewing Credit Union records and onsite observation and evaluation as permitted by contract, whether the Vendor is meeting the performance required.
- Obtain due diligence documentation for new Vendors and determine, whether all required documentation has been obtained, reviewed, approved, and maintained in the Third Party system. Additionally, determine if the relationship has been assigned to an individual responsible for that relationship.
- Obtain ongoing monitoring documentation for existing Vendors and determine whether all required documentation has been obtained, obtained timely reviewed, approved, and maintained in the Third Party system, in accordance with the Credit Union's Third Party policy and risk assessment of the Vendor.
- For Vendors that provide systems or processing services, obtain the Vendor's independent audit report and determine whether an unqualified opinion has been issued and whether any deficiencies have been noted.
- Inquire of Vendor and obtain policy for monitoring and managing sub-contractors.
- In addition to documentation provided by the Vendor, perform searches on internet via sites such as Google, Yahoo, Lexis Nexis, social media sites, etc.

© 2020 Crowe LLP

Thank you

Eileen Iles
Crowe LLP
eileen.iles@crowe.com

Niall Twomey
Crowe LLP
niall.twomey@crowe.com

Crowe LLP (www.crowe.com) is one of the largest public accounting, consulting and technology firms in the United States. Crowe uses its deep industry expertise to provide audit services to public and private entities while also helping clients reach their goals with tax, advisory, risk and performance services. Crowe serves clients worldwide as an independent member of Crowe Horwath International, one of the largest global accounting networks in the world. The network consists of more than 200 independent accounting and advisory services firms in more than 120 countries around the world.

In accordance with applicable professional standards, some firm services may not be available to attest clients.

This material is for informational purposes only and should not be construed as financial or legal advice. Please seek guidance specific to your organization from qualified advisers in your jurisdiction.
© 2018 Crowe LLP, an independent member of Crowe Horwath International crowehorwath.com/disclosure