KB1

CONTRACTS

Vendor's Keeper

How to Make Sure Your Third-Party Vendors Aren't Creating a Compliance Nightmare

OVERVIEW

1. Third-Party Vendors & Compliance Risk
2. Vendor Compliance Failures
3. Assessing Vendor Compliance
4. Reducing Vendor Compliance Risk
5. Guarding Against Vendor Data Breaches
6. Examiners & Vendor Compliance Oversight

Slide 1

KB1 Kimberly Boatwright, 10/26/2021

Third-Party Vendors & Compliance Risk

Vendor Management is Important

"Board and management are responsible for understanding the risks associated with outsourcing arrangements and ensuring that effective risk management practices are in place."

NCUA Letter 07-CU-13

"The use of service providers does not relieve a financial institution's board of directors and senior management of their responsibility to ensure that outsourced activities are conducted in a safe and sound manner in compliance with applicable laws and regulations... ...Senior management is responsible for ensuring that board-approved policies for the use of service providers are appropriately executed..."

Federal Reserve -SR-13-19

"An institution's board of directors and senior management are ultimately responsible for managing activities conducted through third-party relationships, and identifying and controlling the risk arising from such relationships, to the same extent as if the activity were handled within the institution."

FDIC-FIL-44-2008

"The bank's board of directors(or a board committee) and senior management are responsible for overseeing the bank's overall risk management processes. The board, senior management, and employees within the lines of businesses who manage the third-party relationships have distinct but interrelated responsibilities to ensure that the relationships and activities are managed effectively..."

-OCC Bulletin 2013-29

Vendor Management: Specific Guidance

- Latest Guidance:
  - FRB – December 2013
  - OCC – Guidance October 2013,
    - FAQ for Vendor Management, March 2020
  - FDIC – Guidance 08-44; Examiners guidance updated March 2017
  - NCUA – Guidance October 2007

What's New

July 2021

- Proposed Interagency Guidance on Third-Party Relationships: Risk Management

August 2021

- Conducting Due Diligence on Financial Technology Companies: A Guide for Community Banks

Compliance – Outsourcing

Any outsourced activity means the financial institution is responsible for making sure vendor is compliant with laws, regulations, rules, etc.

THAT INCLUDES…

- Business resiliency/ continuity
- Data privacy (GLBA, state laws, GDPR)
- UDAAP
- Fair lending
- Cybersecurity
- BSA/AML
- Debt collection
- Disclosures
- Flood insurance

Areas of Increased Third-Party Compliance Risk

Compliance risk is elevated when third-party:

- Services, or systems aren't properly reviewed for compliance;
- Operations are inconsistent with laws, regulations, ethical standards, or
  - FI's policies and procedures;
- Products or services unfair, deceptive, or abusive;
- Using technology that violates intellectual property rights;
- Not in compliance with BSA or OFAC;
- Lacks appropriate audit and control features (especially for new or expanded activities)

Areas of Increased Third-Party Compliance Risk

Compliance risk is elevated when:

- Activities are further subcontracted;
- Activities are conducted in foreign countries;
- Customer and employee data is transmitted to foreign countries;
- Conflicts of interest aren't appropriately managed;
- Transactions aren't adequately monitored for compliance; and
- Missing appropriate controls to protect consumer privacy and customer and bank records.

Vendor Compliance Failures

COSTLY VENDOR COMPLIANCE VIOLATIONS

- Morgan Stanley (2020) - $60 million civil money penalty, vendor hired to decommission two data centers left unencrypted data on some of the machines
- Citibank (2020) - $1.5 million Flood Act penalty, vendor failed to force place insurance within required timeframe
- Mortgage servicer (2019) - $236k fines & restitution, vendor failed to create escrow account so property taxes and insurance premiums not paid on time
- GreenSky (2021) – $11.5 million fine & penalties, third-party UDAAP violations

DATA BREACHES

Financial Services Data Breaches

Accellion (2021) – Exposed FI data after cyber attack

Kaseya (2021) – Data breach due to ransomware attack

Case Study

A History of Violations:

- A Florida Community bank (2018) – $4.75 million – deposit account add on products not delivered
- A Nebraska Bank (2016) - $35 million fine – deceptive add on services for credit cards
- OCC regulated bank (2017) – Cease & desist order – vendor not in compliance with mortgage products

Case Study

Vendor Management Oversights

- Did the bank know about the vendor's history?
- Did the bank assess the risk of working with the vendor?
- What kind of controls did it have in place?

Assessing Vendor Compliance

How Do You Know Vendors Are Compliant?

Vendor Management

- The ongoing process of monitoring a vendor, beginning with due diligence before a new contract is signed and continual monitoring throughout the duration of the relationship.

Compliance Management System (CMS):

The method used by a FI to:

- Learn about compliance requirements
- Train business units
- Ensure processes are compliant
- Review operations to ensure requirements are carried out
- Take corrective action

THE VENDOR MANAGEMENT LIFE CYCLE

- Pre-screening
- Onboarding
- Contract structuring and review
- Ongoing monitoring (risk assessments)

How Do You Know Vendors Are Compliant?

Prescreening

Goal: Identify high-risk vendors.

- Access to sensitive information or expose the bank to risky consumer protection regulations.
- Identify all applicable consumer laws and regulations to ensure compliance.
- Assess the risks/rewards of outsourcing activity.
- Determine if vendor activities may be "viewed as predatory, discriminatory, abusive, unfair, or deceptive to consumers."
- Does it align with FI's strategic plan?
- Does the FI have resources to oversee relationship?

How Do You Know Vendors Are Compliant?

Prescreening

Goal: Understand the vendor's financials, experience, legal and regulatory knowledge, reputation, operations, and controls.

Includes:

- Legal and regulatory compliance
- Financial condition
- Business experience and reputation
- Fee structure and incentives
- Principals
- Risk management
- Information security
- Management of information systems
- Resilience
- Physical security
- Human resource management
- Subcontractors
- Insurance coverage
- Incident-reporting and management programs

How Do You Know Vendors Are Compliant?

Contract Structuring & Review

Goal: Specifically outline rights and responsibilities.

Includes:

- Nature and scope of arrangement
- Performance measures and benchmarks
- Reporting
- Audit and remediation
- Compliance
- Cost and compensation
- Ownership and license
- Confidentiality and integrity
- Indemnification, insurance & liability
- Dispute resolution
- Default
- Termination
- Customer complaints
- Subcontracting
- Foreign-based third parties
- OCC supervision
- Business resumption and contingency plans

How Do You Know Vendors Are Compliant?

Ongoing Monitoring (Risk Assessments)

Goal: Ensures vendor is meeting contractual obligations.

Focus on:

- Quality and sustainability of vendor's controls
- Ability to meet service-level agreements
- Performance metrics and other contractual terms
- Controls should be regularly tested.
- Compliance with legal and regulatory requirements, including newly applicable requirements
- Monitor vendor for legal and regulation violations in connection with its other clients.
- Deal with any findings promptly and thoroughly.
- Significant findings should be shared with management/board.

How Do You Know Vendors Are Compliant?

3 CMS Elements

Board and Senior Management Oversight

- Culture of Compliance
- Understand Compliance Responsibilities

A Compliance Program

- Policies & Procedures
- Tailored Training
- Monitoring & Testing
- Consumer Complaint Resolution

Violation of Law and Consumer Harm

- Root Cause of Violations
- Severity of Harm
- Duration of Violation
- Pervasiveness of Violation

How Do You Know Vendors Are Compliant?

Compliance Management Program

Preventative

- Policies & Procedures
- Training

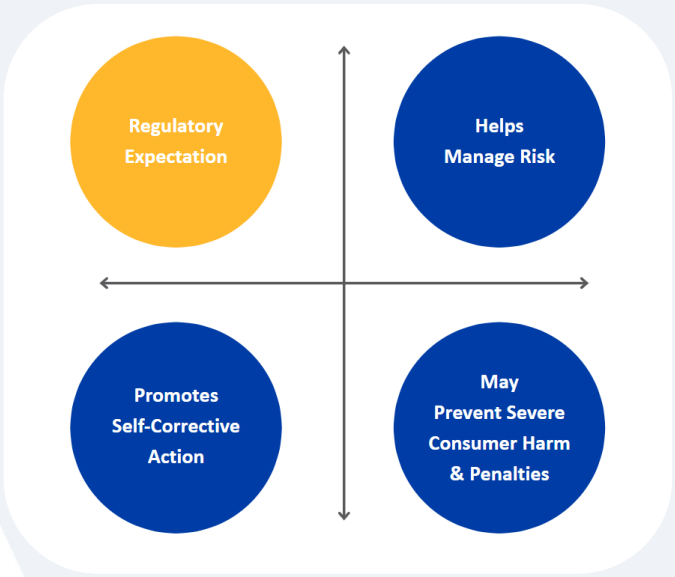
Detective

- Monitoring
- Testing
- Independent Audits

Corrective

- Complaint Resolution
- Error & Violation Resolution

A CMS IS IMPORTANT BECAUSE...



How Do You Know Vendors Are Compliant?

Board & Management Oversight

- **Board.** The board oversees both vendor management and compliance. It approves significant vendor agreements and reviews material changes. It must show knowledge and commitment to the CMS.
- **Management.** Management periodically reviews vendor risk and performance. There should be systems for identifying emerging compliance risks across the FI.

Management should consult the CMS to ensure ongoing vendor compliance with consumer protection laws and regulations plus internal policies and procedures.

Reducing Vendor Compliance Risk

Ensuring Third-Party Compliance

Third-party offerings must comply with consumer protection laws and regulations (including marketing, processing, and servicing).

- Review all marketing materials prepared by third parties.
- Collect documentation of service-level standards, including consumer complaints.
- Consumer compliance committee.
- Board oversight of the bank's compliance risk management program.
- Sufficient compliance resources.

Ensuring Third-Party Compliance

- How does the relationship fit with the bank's strategic plan?
- Compliance risk assessments as part of vendor due diligence
- Appropriate controls to ensure vendor updates policies and internal controls to keep pace with regulations
- Due diligence reports and audit results.
- Follow up on audit and exam findings.

How to Deal with Vendor Compliance Problems

Be proactive in uncovering compliance issues with:

- A system for handling customer complaints.
- Clear in-house reporting requirements for vendor issues.
- Knowing which vendor, employee, or department to report issues to.
- Following up on resolution.

Fourth-Party Risk

Protect against fourth-party compliance violations by:

- Including an assignment clause in vendor contracts to track outsourcing.
- Conducting proper due diligence.
- Reviewing SSAE 18 to assess whether third-party vendors use good vendor management.

Guarding Against Vendor Privacy & Data Breaches

Assessing Vendor Cyber Risk

FFIEC Cybersecurity Assessment Tool (CAT)/ NCUA Automated Cybersecurity Examination Tool (ACET)

- Designed to determine a financial institution's overall cyber risk and preparedness.
- Ensures preparedness aligns with an FI's risk appetite and reveals where controls or control enhancements are needed.
- Approximately 10% of these questions address external dependencies (aka vendors)
- Example: "Contracts establish responsibilities for responding to security incidents?"

Cyber Risk Due Diligence

Identify high-risk activities.

A vendor poses a greater cyber risk—and requires increased management oversight—when it meets any of these conditions:

- Housing confidential data in a cloud-based system
- Housing or outsourcing confidential data offshore
- Outsourcing sensitive activities and/or a number of critical operations
- Using web-based services to conduct business transactions with customers
- Permitting access of confidential data to third-party providers

Cyber Risk Due Diligence

- **Controls from the top.** The vendor's board or a committee should oversee cybersecurity controls, monitoring, protocols and risk assessment.
- **Protect systems.** Both physical access and systems controls should be logged and monitored. Email and customer data should be secure.
- **Incident response.** Third-party vendors must have an incidence response policy.
- **Internal controls.** Vendors must implement controls to prevent or mitigate the severity of a cybersecurity attack.

Cyber Risk Due Diligence

- **Business continuity.** Vendors must implement and test their business continuity program.
- **Human resources**. Access controls should be role-based and granted based upon job function. Personnel should be screened before hiring and employees should undergo data safety training.
- **Data security.** There should be protocols and multi-factor authentication during data transmissions and storage and protocols for securely destroying data.
- **Cloud risk.** Vendors that rely on a cloud-based system require additional scrutiny.

Negotiating Controls in Contract

Negotiating controls in the contract

- Notice of breach clauses (include definition and timeline).
- Right to audit, giving you access to a vendor's internal processes, including the vendor's cyber resilience, patching and updates procedures, and testing results and reports.
- Policies to protect customer data and limit its usage.
- Design the contract so it can evolve with regulatory and technological changes instead of benchmarking it to a standard or rule that can become outdated.
- **Oversight.** Maximize the value of your controls by using them to monitor and mitigate risk. Audits and reports do little good if you don't carefully review them to see if the vendor is living up to its expectations and keeping data and systems safe.

Oversight

Maximize the value of your controls by using them to monitor and mitigate risk.

Audits and reports do little good if you don't carefully review them to see if the vendor is living up to its expectations and keeping data and systems safe.

Vendor Cyber Monitoring

- Ongoing monitoring of your vendors' cybersecurity controls to detect vulnerabilities before there is an issue and take action if an issue is uncovered.
- Assessing your vendors' ability to effectively identify and resolve incidents.
- Comprehensive documentation of activity regarding your vendors' cybersecurity program.
- A system for recording incidents and resolutions regarding your vendors' cybersecurity issues so you can document due diligence for regulators, seek remediation if a vendor has violated its service level agreement and uncover patterns.
- Ensuring a vendor's cyber risk aligns with your institution's appetite for cyber risk.

Examiners & Vendor Compliance Oversight

What Examiners Want to See

- Documented processes.
- Identification of compliance risks.
- Vendor management and compliance risk management are ongoing.
- Justification for decisions, including how risk is identified, managed and mitigated.
- Resources to analyze reports and carefully negotiate and track contracts.
- Vendor management ties into the CMS.
- Evidence of board and management oversight.
- Understanding of how vendor selection ties into ERM.

Questions?


CONTRACTS
Contact Us
Learn more about our integrated, comp ions
www.ncontracts.com
Subscribe to our blog for risk and compliance management insights
www.ncontracts.com/nsight-blog