Vendor's Keeper:

Top Tips for Making Sure Your Third-Party Vendors Aren't Creating a Compliance Nightmare

NCONTRACTS
The Upside of Risk

VENDOR'S KEEPER:
TOP TIPS FOR MAKING SURE YOUR THIRD-PARTY VENDORS AREN'T CREATING A COMPLIANCE NIGHTMARE

It's no secret that third-party vendors represent a compliance risk for financial institutions. Regulators hold FIs responsible for the activities of their vendors, and third-party offerings must comply with consumer protection laws and regulations, including marketing, data security, processing, and servicing. They also need to follow a FI's internal policies and procedures.

How can you be sure your FI is doing everything it can to ensure third-party vendors are actively compliant?

Read on for top tips and best practices for vendor management and compliance.

Assessing vendor compliance requires cooperation among two key functions: Vendor management and compliance.

THE DREAM TEAM:
VENDOR MANAGEMENT & COMPLIANCE

Vendor management is responsible for overseeing the vendor relationship, including ensuring the vendor engages in compliant behavior. Compliance keeps tabs on the latest regulatory developments and hot-button compliance issues (and has a vested interest in vendor management since it's a regulatory requirement). These two areas naturally overlap as a FI considers how a vendor's activity will impact compliance.

It's an issue that goes straight to the top. The board is required by regulators to oversee both vendor management and compliance. It approves significant vendor agreements and reviews material changes. It must also show knowledge and commitment to the compliance management system (CMS).

Management periodically reviews vendor risk and performance and is responsible for ensuring there are systems for identifying emerging compliance risks across the FI. When vendor management and compliance work in tandem, it cuts down on the work necessary to reduce vendor compliance risk while making an institution safer. For the best results, make sure your vendor management program ties into your compliance management system.

3 WAYS
TO ENSURE VENDORS ARE COMPLIANT

When it comes to third-party vendor compliance, these three activities are essential to evaluating and enforcing vendor compliance.

1 Prescreening

The goal of prescreening is to identify high-risk vendors, including those with access to sensitive information and those that engage in activities regulated by consumer protection regulations.

It starts internally by identifying all applicable consumer laws and regulations to ensure compliance. Determine if vendor activities may be "viewed as predatory, discriminatory, abusive, unfair, or deceptive to consumers." Consider whether the activity aligns with the FI's strategic plan and if the FI has the resources to oversee the relationship. Once information is collected, the FI can assess the potential risks and rewards of outsourcing an activity.

Once an activity has been prescreened, move on to the vendor. Research the vendor's financials, experience, legal and regulatory knowledge, reputation, operations, and controls to get an idea of its compliance culture.

Areas to ask about include:

- 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

If the inherent risk of working with a vendor is high, there needs to be strong controls in place to ensure ongoing compliance.

continued...

2 Contract Structuring & Review

The goal of this step is to specifically outline rights and responsibilities. Cost shouldn't be the only concern. The contract should define the nature and scope of arrangement and include performance measures and benchmarks, reporting, audit and remediation, and compliance.

Beyond ownership and license, the contract should address indemnification, insurance and liability, dispute resolution, default, termination for cause, customer complaints, and business resumption and contingency plans. Another key area is the right of the vendor to subcontract to other vendors, including foreign-based parties. If not specifically prohibited by the contract, vendors are allowed to subcontract.

3 Ongoing Monitoring

(Risk Assessments)

Ongoing monitoring is important because it helps a FI ensure that a vendor is meeting its contractual obligations. This includes the quality and sustainability of the vendor's controls and its ability to meet service-level agreements (SLAs), performance metrics, and other contractual terms. Controls should be regularly tested.

It's important to assess whether the vendor is in compliance with legal and regulatory requirements, including newly applicable requirements, and keep an eye out for legal and regulatory violations in connection with the vendor's other clients. All marketing materials prepared by the third-party should be reviewed. Findings should be dealt with promptly and thoroughly, and significant findings should be shared with management and the board.

If the inherent risk of working with a vendor is high, there needs to be strong controls in place to ensure ongoing compliance.

ELEVATED RISK AHEAD:

12 WARNING SIGNS

How do you know when a vendor presents elevated compliance risk? Be on the lookout for signs that:

1. Third-party products, services, or systems aren't properly reviewed for compliance.
2. Third-party operations are inconsistent with laws, regulations, ethical standards, or FI's policies and procedures.
3. Third-party implements or manages a product or service in a manner that is unfair, deceptive, or abusive.
4. Licensing or using technology from a third party that violates intellectual property rights.
5. Third party doesn't comply with BSA or OFAC.
6. FI oversight lacks appropriate audit and control features (especially for new or expanded activities).
7. Activities are further subcontracted.
8. Activities are conducted in foreign countries.
9. Customer and employee data is transmitted to foreign countries.
10. Conflicts of interest aren't appropriately managed.
11. Transactions aren't adequately monitored for compliance.
12. Missing appropriate controls to protect consumer privacy and customer and bank records.

HOW TO DEAL WITH

VENDOR COMPLIANCE PROBLEMS

Vendors make mistakes. We all do. Make sure you have plans in place to ensure that when vendor mistakes are uncovered they are dealt with promptly and properly. That includes:

A system for handling customer complaints. Make sure your institution has policies and procedures in place for handling customer complaints related to a vendor. That's not just a potential vendor management issue. It's a regulatory expectation.

Clear in-house reporting requirements for vendor issues.

Make sure you have procedures for passing along information about vendor issues and train staff on what to do. Make it clear who information should be reported to and how it should be reported. Include follow-up procedures to ensure nothing gets lost.

Knowing which vendor, employee, or department to report issues.

If you encounter a security flaw or other issue, make sure you know exactly who to contact at the company. Don't just send an email to a generic email box. Also ask for estimates for how long before the problem will be fixed, what will be done to solve the problem in the short term, and how you will be updated with developments.

Tracking findings.

Use findings management to ensure vendor issues are logged and tracked to document that they are remediated promptly and properly—or that they remain outstanding.

Taking action.

With good incident management logs and findings tracking, you'll have the evidence you need to demonstrate non-compliance and show the vendor exactly where it's falling short of contract expectations. That can give you leverage in negotiating a new contract, collecting financial penalties, or even exiting the relationship, if necessary. It also demonstrates to examiners that your FI is working proactively to correct the problem.

Make sure you have plans in place to ensure that when vendor mistakes are uncovered they are dealt with promptly and properly.

FOURTH-PARTY RISK

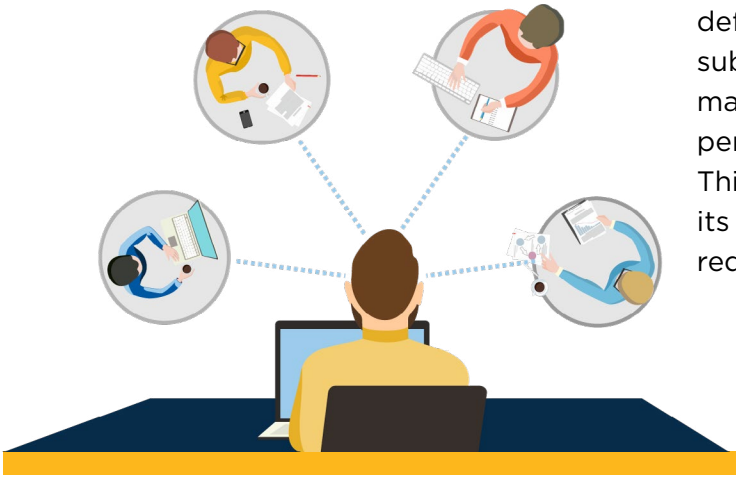
& HOW TO MITIGATE IT

As mentioned earlier, vendors are legally allowed to subcontract to other vendors (also known as fourth parties). Just as with third-party vendors, FIs are responsible for the work that fourth-party vendors do on their behalf.

Fourth-party relationships complicate vendor management, introducing another level of risk. Manage that risk by:

Including an assignment clause in vendor contracts to track outsourcing.

Assignment clauses are important elements in critical vendor contracts. The assignment clause should require your third-party vendor to provide you with notice and consent before subcontracting to another vendor. This way your FI is aware of who is working on its behalf. The assignment section can also include standards for any subcontractors like business continuity plans, data security, incident response, and similar provisions.



Conducting proper due diligence.

An assignment clause is important, but isn't worth much without vendor due diligence. Make sure your FI is provided with promised outsourcing information and engages in due diligence to understand the risks and controls of fourth-party relationships. If you don't trust your vendor's oversight of subcontractors, you may need to engage in due diligence of fourth-party vendors yourself.

Reviewing SSAE 18s to assess whether third-party vendors use good vendor management.

The Statement on Standards for Attestation Engagements 18 (SSAE 18) includes a vendor management section that requires a vendor to define the scope and responsibilities of all its subcontractors. It also documents its vendor management process, including subcontractor performance reviews, audits, and monitoring. This document can give an FI confidence in its vendor's vendor management and helps reduce the burden of vendor management.

GUARDING AGAINST
VENDOR DATA BREACHES

Cyberattacks and data breaches are a growing problem that requires additional attention during the vendor due diligence process. From identifying increased risk to mitigating it, here's what you need to do.

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.

How do you know if a vendor is prepared to meet these challenges? The answer is cyber risk due diligence. Just as you engage in due diligence to ensure a vendor is financially strong, compliant, and capable of delivering promised products and services, vendor cyber risk due diligence lets you know if the vendor has the policies, procedures, and controls needed to guard against cyber risk.

LOOK FOR:

- **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 incident response policy.
- **Internal controls.** Vendors must implement controls to prevent or mitigate the severity of a cybersecurity attack.
- **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.

Negotiate controls in the contract.

Your FI can't understand and mitigate its risk exposure if it doesn't have insight into the vendor's security practices. A carefully negotiated contract can give you this information.

Notice of breach clauses let your FI know how quickly it will learn of security incidents like breaches and attempted breaches. You also need the 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. Ensure there are 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 and vendor cyber monitoring.

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.

Engage in vendor cyber monitoring on an ongoing basis to detect vulnerabilities before there is an issue and take action if an issue is uncovered. Make sure your monitoring system can provide:

- Assessments of 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.
- Assurances that a vendor's cyber risk aligns with your institution's appetite for cyber risk.

The FFIEC Cybersecurity Assessment Tool (CAT) can help your FI assess its overall cyber risk and preparedness, including vendor relationships. Approximately 10 percent of its questions address external dependencies (aka vendors) with questions like "Contracts establish responsibilities for responding to security incidents?"

The CAT will ensure your FI's preparedness aligns with its risk appetite and reveal where controls or control enhancements are needed.

8 VENDOR MANAGEMENT PRACTICES

EXAMINERS ARE LOOKING FOR

Regulators recognize that third-party vendors play a critical role in delivering products and services and take compliance with vendor management regulations very seriously. What are they looking for?

1 **Documented processes.**

Vendor management isn't an ad hoc activity. It's a thoughtful, strategic exercise in keeping your financial institution and the customers, members, and consumers it serves safe. Examiners expect to see a documented plan for managing vendors and ensuring they remain compliant.

2 **Identification of compliance risks.**

It's hard to guard against a risk if you don't know it exists.

3 **Ongoing vendor management and compliance risk management.**

Just because a vendor is compliant today doesn't mean it will be compliant tomorrow. There needs to be ongoing monitoring of vendors to determine if anything has changed that would impact its ability to remain compliant—including keeping up with regulatory change.

4 **Justification for decisions, including how risk is identified, managed, and mitigated.**

Why did the FI decide to outsource? Why are vendor management and the compliance management system structured the way they are? It's not enough to simply have policies and procedures. Examiners want to see the logic behind it. If you can't make a good business case for your decisions, it can call your whole program into question.

5 **Resources to analyze reports and carefully negotiate and track contracts.**

One of the reasons FIs outsource to vendors is because they don't have the internal resources to accomplish a task—but that doesn't mean an FI won't need to expend any resources on that activity. When calculating the costs and benefits of outsourcing to a third-party vendor, don't forget to include the resources necessary to oversee the vendor and analyze reports as well as track and negotiate contracts. These resources are essential to a compliant vendor relationship.

6 Vendor management ties into the CMS.

Vendor management and the compliance management system work best as a pair. Compliance wants to be certain that vendors are compliant. Vendor management wants to know the rules and regulations vendors need to be following. If the two areas aren't linked, they can end up duplicating each other's work—or an important element may get lost in the shuffle.

7 Evidence of board and management oversight.

Vendor management is such an important issue that the board and management need to be involved, especially when it comes to critical vendors. Make sure you document board meetings, minutes, and reports dealing with vendor management.

8 Understanding of how vendor selection ties into ERM.

Outsourcing to a vendor isn't just a question of resources and convenience. It's about strategy. Risk plays an important role in ensuring that an institution's mission, vision, and values influence an institution's strategy, strategic plan, and ultimately its strategic success. Selecting a vendor is about aligning the benefits of the vendor relationship with the FI's risk tolerance.

NCONTRACTS: YOUR VENDOR MANAGEMENT, RISK & COMPLIANCE PARTNER

VENDOR

Nvendor is a secure, feature-rich, online vendor and contract management solution that enables financial institutions to achieve and maintain regulatory compliance in their third-party vendor relationships. Spend less time on vendor management while gaining deeper insights into third-party risk with Nvendor.

COMPLY

Ncomply is a secure, centralized compliance management system (CMS) that eliminates manual processes and allows departments to share information. Designed by a compliance officer, it's an efficient, effective solution that saves time and money while protecting your organization from compliance risk.

CONTRACTS
The Upside of Risk

About Ncontracts

Ncontracts provides integrated risk management and compliance software to a rapidly expanding customer base of nearly 1,400 financial institutions located in all 50 states and US territories. The company's powerful combination of software and services enables financial institutions to achieve their risk management and compliance goals with an integrated, user-friendly cloud-based solution suite that encompasses vendor risk, organizational risk, audit risk, and compliance risk management. The company was recently named to the Inc. 5000 fastest-growing private companies in America for the 2nd consecutive year.

For more information visit www.ncontracts.com or follow the company on LinkedIn and Twitter.