Wolters Kluwer

Lien Solutions

# *CFPB asks: How compliant is your vendor?*



*By Sandra Langford, Senior Product Manager, Lien Solutions*

**Financial companies in the mortgage industry are often on the front lines when it comes to regulatory change. Staying abreast of evolving requirements, and proactively adapting to them, is key to ensuring compliance and mitigating risk.**

For example, in April 2012, the Consumer Financial Protection Bureau (CFPB) changed the relationship between lender and settlement service provider by releasing Bulletin 2012-03. This put lenders and service providers on notice that lenders will be held liable for the actions of their service providers.

Four years later, on October 26, 2016, the CFPB published a notice for a new bulletin in the Federal Register. This states: "The bureau is reissuing its guidance on service providers, formerly titled CFPB Bulletin 2012-03, Service Providers to clarify that the depth and formality of the risk management program for service providers may vary depending upon the service being performed — its size, scope, complexity, importance and potential for consumer harm — and the performance of the service provider in carrying out its activities in compliance with Federal consumer laws and regulations. This amendment is needed to clarify that supervised entities have flexibility and to allow appropriate risk management."

The addition of this language allows for some scalability for lenders and the title agents they work with, but questions remain about whether there is enough clarity for industry members to move forward with confidence.

One important way to be more sure about meeting your obligations is to work with a large, established vendor who is ready to provide a high level of assurance across a wide range of offerings.

## Greater Responsibility for Lenders

Risk mitigation is of utmost importance in an environment where lenders continue to be held to higher standards of accountability. As part of this, lenders must look not only to their own policies and procedures, but to those of the vendors with whom they work. It is the lender's responsibility to make sure a vendor is compliant. For larger lenders, that means actively auditing their vendors.

To make sure these audits go as smoothly as possible, it's necessary for a vendor to audit itself throughout the year. Of course, not every lender can audit every vendor; this makes it even more important to work with trustworthy, knowledgeable vendors who hold themselves responsible and work transparently within the guidelines.

Reviewing the audit capabilities of potential vendors has become an important consideration for lenders. Actively understanding and verifying the audit capabilities of vendors is an essential part of vetting, selecting and working with a vendor. Making sure that vendors have adequate controls in place is key to making informed business decisions and to mitigating risk. It's not just primary vendors who are of concern, either: sub-vendors count, too.

Lenders must also be sure of the ways that vendors select their own providers and manage their relationships with them. It's essential to make sure that the cascade of assurance extends down through all levels. So, selecting a vendor with its own strong vendor management program is also key.

> Risk mitigation is of utmost importance in an environment where lenders continue to be held to higher standards of accountability.

## The Bigger and Fewer, the Better

A vendor that has no audit measurements in place can represent an unacceptable risk to a lender. Conversely, the better equipped a vendor is with internal controls, the more confident a lender can be in engaging their services. Larger service providers are often better set up to conduct the right audits and quality controls. That's why it makes sense for a lender to select a vendor with a dedicated audit department, with team members trained and focused on audits and quality control.

Because a bigger vendor can do more for a lender, selecting a larger supplier can deliver the added benefit of working with fewer vendors. That can translate into lower costs and risks. Each additional vendor that a lender uses represents an additional layer of auditing that must be done. By consolidating work with fewer vendors, lenders can streamline the auditing process, which can translate to faster decision-making and decreased expense.

There's also less risk of error when there is only one entity handling the work: It's a basic rule of thumb that the more hands that touch something, the more chance there is for things to go wrong. And, fewer vendors can also increase accountability.

When mistakes do happen, it's not as hard to figure out where and by whom: Having just one vendor means you know who to call right away.

# *What to Look for When Selecting a Vendor*

## Audits and Related Practices

What sorts of specific safeguards should a lender look for in a vendor? First and foremost, consistent audit practices are essential.

Lenders should seek vendors who annually commission an SOC 1, Type 2 Audit for company products, conducted by RSM US, LLP. It's also wise to look for vendors with an Internal Control Office (ICO), which performs annual audits within the company.

In addition, vendors should have an Internal Control Framework (ICF) based on COSO (Committee of Sponsoring Organizations of the Treadway Commission) framework.

Audits should be announced and all results communicated with the lender. If required, the remediation of any identified findings should be tracked through the vendor's ICO.

## Other Important Practices

A range of other practices and procedures can also give a lender greater confidence in selecting a vendor.

### Business Continuity and Disaster Recovery Policies & Procedures

Programs of this kind help ensure that a vendor is ready to provide continuous, uninterrupted support to its customer base.

A comprehensive, executable, enterprise disaster recovery and business continuity program (BCP) supports customer-centric, value-added, mission-critical services. Lenders should look for vendors whose Enterprise Disaster Recovery (DR) and Business Continuity Program adheres to industry best practices for disaster recovery and business continuity services.

**A good Enterprise Program includes:**

- Oversight through the BCP/DR Steering Committee, sponsored and attended by members of senior management
- Local system recovery; e.g., Fault-tolerant and redundant system configurations, service center reciprocal agreements
- Data Center Disaster Recovery
- Data replication to standby data center
- Service Operations Business Continuity Support
- Business Resumption Planning

Prepared vendors can ensure that in the event of a temporary outage at service centers, order management and fulfillment can be dynamically re-configured to re-route orders to an alternate service centers. Vendors should test their recovery processes annually. In addition, appropriate managers and departments need to be involved. Senior Management should be required to identify and approve the testing of specific business recovery scenarios.

IT Management must be able to support all the recovery requirements of the approved business scenarios. To prepare for smooth implementation in the event of an emergency, test scenarios should be coordinated and documented through the use of a DR testing and "Lessons Learned" approach.

**Consistent Audit Practices for Vendors**



**Annually commissions a SOC 1, Type 2 Audit**

**Has an Internal Control Office (ICO) to conduct annual internal audits**

**Has an Internal Control Framework (ICF)**

**Communicates all audit results**

## 3rd Party Management Policies & Procedures

Access to information or IT resources by external or third parties is a necessary part of business activities. This can include physical and/or electronic access by customers, product vendors, outsourced data center operators or other managed service providers. In order to control this process, a 3rd Party Management program should be implemented to ensure that all contractual obligations including but not limited to operational support, security, business continuity and other areas have been identified and addressed. An effective program will include regularly scheduled scorecard monitoring and annual security assessments.

## Human Resources Policies & Procedures

A diligent vendor will outline requirements for employee, confidentiality/non-disclosure agreements, background checks, and termination procedures. Background checks should be required for all employees, contractors, and consultants.

Part of the termination process should include the return of all company assets (hardware, software, manuals) and internal, confidential, and restricted data. Employees should be provided an initial orientation upon hiring, to inform them of their obligations and introduce them to the culture and expectations of the company.

## Physical Security Policies & Procedures

A Physical Security Program encompasses aspects of employee, data, and equipment security. These include, but are not limited to, badge access readers, CCTV, Fire suppression systems, and supporting utilities. Network equipment and other sensitive equipment should be maintained in controlled areas, with access allowed only to authorized individuals.

## Access Control Security Policies & Procedures

Proper oversight includes the requirement of unique user IDs and passwords for access to systems and data. Segregation should be enforced through a management and resource owner authorization process. It's important to employ a comprehensive backup and recovery strategy for all server level applications and data. Encryption of data should be enforced through applications utilizing HTTPS/SSL.

## Data Management Policies & Procedures

It's important for vendors to have an information classification policy that outlines required protection measures, including reproduction and destruction of Public, Internal, Confidential, and Restricted data. Such a policy enforces commitment to ensure that discussions, hard copies of documents, and data are controlled and protected at the specified level.

## Intrusion Detection and Incident Response/ Notification Policies & Procedures

Vendors should monitor key systems and evaluate all security incidents. A corporate level CIRT team will promptly analyze potential security incidents to assess the impact, determine if there is an immediate risk to the corporation, and take immediate action to mitigate such damage.

Local incidents will be reported to the corporate level CIRT. Any employee found to have violated approved policies may be subject to disciplinary action, up to and including termination of employment.

## Network Security, Penetration Testing and Vulnerability Assessments

Network service agreements include security features, service levels, and management requirements. Firewalls are configured to protect all entry points into internal networks. Only approved network staff will be authorized to administer corporate firewalls, and firewall policies should be reviewed periodically. Remote access to networks and systems is achieved only through a Virtual Private Network (VPN) with multi-factor authentication, and Network Threat Protection should be deployed on all computers accessing the network.

Network Penetration Testing and Vulnerability Assessments ought to be performed on a recurring basis to ensure the utmost security of products and services. The results should be shared and discussed with senior level management to determine the best implementation plan to address any findings.

> It continues to be a top priority for financial companies to ensure compliance. That means lenders must look not only to their own operations, but to those of their vendors.

### Software Product Development Methodology

From a process perspective, new development should be based on the Scrum development framework, which has been shown to reduce project risk through its focus on short, iteration cycles and frequent customer collaboration. The process framework can be complemented with various technical practices such as test-driven development, test-automation, secure coding/scanning practices and adherence to object-oriented principles and design patterns coupled with regular code reviews. The methodology will ensure managed, incremental enhancements and bug fixes to achieve availability and quality targets.

### Quality Assurance and Quality Control

An appropriate QA/QC strategy is based on customer satisfaction achieved by meeting internal and external customer requirements. Conformance to customer's requirements and expectations is the responsibility of all employees.

Quality assurance and testing program procedures and practices ought to be developed, reviewed, and revised with the continuous participation of employees. The goal of a quality assurance and testing program is to ensure the continued improvement of a company's products in support of its customers and employees.

### Change Management Policies & Procedures

A vendor should employ a formal change management process to ensure that consistent and tested changes are deployed to the production environment, thereby reducing impacts to internal and external customers.

An appropriate change management process includes, but is not limited to, ensuring minimum disruption to services; ensuring that risks to the production system are identified, assessed and managed; and mandating that changes are scheduled for deployment through designated change windows.

## *Finding Confidence in Scale*

It continues to be a top priority for financial companies to ensure compliance. That means lenders must look not only to their own operations, but to those of their vendors. They must be ready to actively audit vendors and/or to make sure they work with trustworthy, knowledgeable vendors who are actively auditing themselves. This is important to the initial selection of a vendor and to the maintenance of an ongoing, healthy vendor relationship.

The larger and more established a vendor, the more likely it is to have sophisticated and comprehensive safeguards already in place. In addition to auditing, a range of factors help to make a vendor a safer choice for a lender.

From Human Resources policies to technology protocols, there are important signs across a vendor's operations that suggest whether it is a sound choice for a lender.

As regulations continue to place the onus on them, lenders can increase their confidence by selecting and working with established vendors who are prepared to offer a broader range of benefits, and hold themselves to the same high standards as lenders do.

## About the Author

**Sandra Langford** is a Senior Product Manager at Lien Solutions. A 19-year veteran of the company, she is responsible for the web-based iLienRED platform and Real Property Recording & Search services.

## About Lien Solutions

Wolters Kluwer's Lien Solutions is the leading technology and service provider of comprehensive lien management, debtor due diligence, monitoring, and risk management solution, to financial professionals. Through unmatched industry expertise and a service-oriented culture, we use the iLien suite of products – addressing solutions for asset-backed loans, real-estate, and vehicle title processing and management – to simplify complexity in lien lifecycle management, resulting in more confident lending decisions. Servicing clients across North America, Lien Solutions enables more secured transactions than any other company in the United States. Lien Solutions is a product suite of Wolters Kluwer, headquartered in Houston, Texas. For more information, visit the Wolters Kluwer Lien Solutions website, or follow @WKLienSolutions on Twitter.

Wolters Kluwer

*© 2017 C T Corporation System and its affiliates. All rights reserved.*

WKLS0004-RED-1-201703

*Lien Solutions is not a law firm and does not provide legal, accounting or other professional advice. Customers should consult with their legal counsel and other advisors regarding their use of the products and services offered by Lien Solutions.*