# The Ultimate Guide to Building an Exam-Proof Vendor Management Program

Continuity WHITE PAPER

Do you currently have a Vendor Management program?

**63% Yes**

Are you satisfied with your current Vendor Management process?

**42% No**

**Source:** Continuity Vendor Management Survey of 312 compliance and C-level banking executives.

# Executive Summary

It may seem like vendor management has just recently become a regulatory hot button – but the reality is that guidance on this topic was first issued nearly 15 years ago. Since then, any changes to the area have been limited to updates and clarifications. So, why does it feel like a flashpoint in the current regulatory climate?

Financial institutions (FIs) need only to look within their business operations to find the answer. Twenty years ago, the outsourcing of critical banking activities was uncommon among FIs and limited to a few providers. Most outsourcing initiatives fell under the oversight of IT and involved core banking systems. In this environment, a one-size-fits-all approach to managing vendors – often through checklists and spreadsheets – made sense.

Today, most FIs (especially community and regional) could not survive without a complex and long list of vendors – 40+ for the average community FI and many more times that for larger institutions. Nearly every aspect of banking is tech-enabled, and that's opened the door to thousands of vendors that provide solutions beyond the traditional core banking systems. These products and services are deeply entrenched into multiple facets of the business – lending, marketing, online banking, ATMs, IT security and so on.

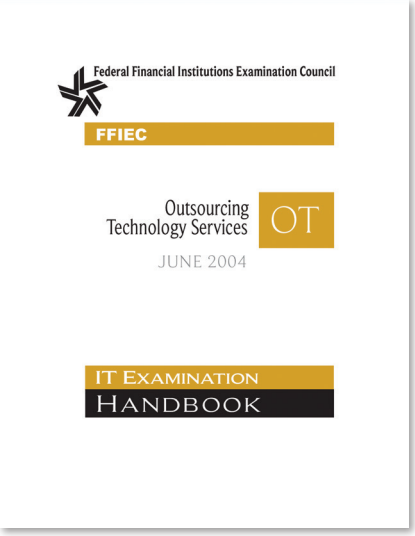
The interconnectedness of service providers across the banking organization, and the unique and multiple risks that each vendor introduces to the business, is just one aspect of concern. Over the past five years, there have been numerous enforcement actions where third parties have caused or contributed to compliance problems. Credit card add-on fees, deceptive marketing of student loans, improper mortgage servicing, inadequate audit scoping…these are just a few examples of the numerous areas where vendors have demonstrated poor understanding of compliance risk, and FIs have lacked the proper oversight to mitigate that risk accordingly. The result has been an increase in the number of vendor management-related enforcement actions against FIs, and even some directed towards specific vendors.

Changes in these dynamics have precipitated the need for a more formalized and standardized approach to vendor management. Many examiners have become frustrated at widespread negligence in this area of compliance, and the nature, number and scope of related enforcement actions bear this out. Vendor management has become too complex and too intricate for one person – or even a single department – to manage alone. FIs need a systematic approach that blends examiner expectations with business requirements and common sense.

**Whether** they like it or not, financial institutions are ultimately accountable for their vendors' work.

# Getting Clear on Agency Guidance and Examiner Expectations

Various agencies have issued vendor management guidance over the years. One example is the Federal Financial Institutions Examination Council's (FFIEC) Outsourcing Technology Services handbook, and there are numerous others. However, while each agency has its own take on vendor management, the major themes are consistent.




What is it? Vendor management provides a framework to identify, measure, monitor and control risks of outsourcing. The development of specific policies are required to govern the process consistently across the business, rather than confine the duty of vendor management to one silo or department.

Who oversees it? Oversight is the duty of the board and senior management, while the relationship manager should demonstrate sufficient expertise as it pertains to a particular vendor's focus.

What does it encompass? Regulators and examiners expect an end-to-end perspective on vendor management. That means well-defined, documented and repeatable processes for evaluating potential vendor relationships, establishing requirements, vendor selection, contract negotiation, monitoring the ongoing relationship, risk assessments, and changing terms or discontinuing the relationship.

What resources does it require? The time and resources devoted to managing outsourcing relationships should be based on the risk the relationship presents to the institution. While the process may be similar, the amount of oversight required to manage a landscaping service provider is very different than managing, let's say, an Internet security vendor.

Vendor management isn't just about compliance – it's about common sense. Your program must be defensible from a regulatory standpoint, but must also make sense as a prudent business practice.

# The Six Principles and Three Rules of Vendor Management

One of the biggest mistakes FIs make in vendor management is over-focusing on a checklist of activities and failing to understand the higher purpose of agency/examiner expectations. It's easy to get lost in the intricacies of due diligence and various agency requirements. Instead, FIs need to understand the common themes across different guidance sources, and build a program that incorporates compliance, common sense and business acumen.

Here are six key principles of sound vendor management practices:

1. Identify your reasons for outsourcing. FIs need to understand why they're outsourcing a particular responsibility, and show evidence that meaningful discussion and justification has taken place. This can be in the form of a memo or notes/minutes from a board or committee meeting.

2. Choose potential candidates who fill those needs. The focus here is on having multiple options, whether that means interviewing competing providers, or exploring different ways to meet the business's requirements (example: hiring a consultant versus buying a technology – in some cases these are both options for solving the business need).

3. Pick the right partners. This starts with clearly defining and communicating the FI's business and user requirements, then applying scrutiny to the capabilities of potential providers. It also requires FIs to hone in on areas of risk that need to be addressed.

4. Get things in writing. FIs need to ensure that terms, rights and obligations of the vendor relationship are spelled out and mutually agreed upon before entering an agreement. Remember, it's easier to negotiate the terms of an agreement at the beginning of the relationship than ad hoc when tensions may be higher.

5. Keep an eye on things. Ongoing monitoring is key to making sure that critical service level terms are being met, the use of the product/service is meeting the demands of the business, and that the FI can still justify the outsourcing arrangement. Most importantly, it lets the FI know when something needs attention – before it becomes a serious threat to compliance.

6. Change if changing makes sense. Every contract has a beginning and an end, even agreements with trusted vendors. FIs should have visibility into when vendor contracts are set to expire and use this opportunity to evaluate the need to continue the relationship. Do we still have the same business needs? Are they capable of meeting our requirements today and down the road? Do we need to bring in a new vendor? These are all questions that should be asked to determine if change will best serve the business.

**Don't overcomplicate vendor management – it's the enemy of effectiveness. Keep it simple, straightforward and – above all else – consistent.**

These six principles form the framework for a practical approach to vendor management, and should be guided by three rules of simplicity:

Centralize documentation. It's impossible to manage what the organization can't find, see or measure – much less demonstrate strong vendor management. FIs need a single repository for vendor information including: vendor contact information and identification data, proposals, contracts and addenda, due diligence documentation, and critical correspondence.

### Examiner Vendor Management Checklist

Financial Institutions need the following information at their fingertips when examiners ask for it:

- Who is this vendor? What products and services do they provide us?
- Why did we choose them? Who participated in that decision? What kind of due diligence did we perform to confirm they did and could continue to meet our needs?
- What risks do they expose us to? How do we manage and mitigate those risks?
- Do they rely on other third parties to carry out their business functions?
- When did we first contract with them? When does their contract expire?
- How far ahead of expiration do we want to review this contract? Who gets a say in whether we renew or terminate?
- Who is responsible for owning this relationship?
- Who is responsible for assuring performance under the contract?

Standardize the process. At the heart of strong vendor management is process standardization. This assures that every time work is completed – regardless by whom – it's clear, consistent and serves as solid evidence of the thought processes and work steps involved. It also affords ultimate flexibility in how resources are allocated. If the process is well documented and consistent, the work can be completed by virtually anyone.

### Process Standardization Checklist

According to the viewpoint of various regulatory agencies, there are several areas of process that need to be standardized:

- Vendor Turn-Up and Turn-Down – What are the processes used to onboard or wind down a vendor relationship?
- Third-Party Risk Management – How does the FI know when updates and adjustments need to happen to keep risk in check? These come in the form of policy reviews, policy updates and employee attestations.
- Vendor Risk Assessments – When, how and who needs to perform initial and ongoing risk assessments?
- New Vendor Due Diligence – What activities need to happen? Remember, the questions may change based on the vendor product or service, but the method remains consistent.
- New Contract Review – Who is responsible? When does legal need to be involved?
- Existing Contract/Performance Review – When does this take place and by whom?

Deputize those who know the vendors and their products best. It's important that FIs enlist the right staff to manage the vendor relationship. This person(s) should be closest to the concerns being addressed by the vendor, and be knowledgeable about the area. They are tasked with identifying and evaluating risks as well as helping determine strategies for mitigation. This approach brings an added layer of efficiency, accountability and continuity to the vendor management process.

# How to Jumpstart a Strong Vendor Management Program

Many FIs suffer from "analysis paralysis" as they aim to improve their vendor management program. The sheer number of vendors that need to be managed across myriad facets of the banking organization can be intimidating. Knowing which steps to take first is important to weeding through the chaos and achieving the goal of effective vendor management.

Step 1 – Perform a vendor inventory. Accounts payable records are a good starting point. Gather all vendor details and documentation into a single storage modality. Flag and separate significant/critical vendors to those with less impact to your business, and document the criteria for how this call is made.

Step 2 – Perform an initial risk assessment on significant vendors. Start by gathering six key pieces of documentation for each "key" vendor:

- Current identifying information required by your institution's customer identification program (CIP)
- Proof that an OFAC scan was performed, and its results
- Financial analysis
- Audited financial statements
- SSAE 16 report
- Vulnerability assessments (or network security reports)

FI's should also consult the FFIEC InfoBase and other guidance from relevant agencies to determine which questions need to be asked during the initial risk assessment.

Resources for Agency Guidance on Vendor Management

According to the viewpoint of various regulatory agencies, there are several areas of process that need to be standardized:

- OCC - Risk Management Guidance http://occ.gov/newsissuances/bulletins/2013/bulletin-2013-29.html
- FDIC - Guidance for Managing Third Party Risk https://www.fdic.gov/news/news/financial/2008/fil08044a.html
- FDIC - Technology Outsourcing: Information Tools https://www.fdic.gov/news/news/financial/2014/fil14013.html
- FRB - Guidance on Managing Outsourcing Risk http://www.federalreserve.gov/bankinforeg/srletters/sr1319a1.pdf
- NCUA - Evaluating Third Party Relationships http://www.ncua.gov/resources/documents/lcu2007-13enc.pdf

**Vendor** management cannot be a point-in-time event. It's continuous and dynamic.

Step 3 – Calendar ongoing review activities. FIs will need a schedule or "tickler" to remind them of the date of periodic risk assessments, periodic contract performance reviews, contract expiration, and pre-expiration review schedules.

Remember, programs should be built and records should be compiled to be examination-ready. They need to be able to be produced upon a minute's notice and be defensible in court, easily explained and updated frequently. The program and processes involved also need to be engineered to accommodate changing regulations and regulator expectations.

### Vendor Management Best Practices

Financial Institutions need to be able to explain and demonstrate:

- Who are the high-risk vendors, why they are higher risk, and what activities are performed differently to oversee and manage these relationships compared to non-high-risk vendors
- How overall risk exposures change over time – both in aggregate and by specific vendors
- Vendors ranked by risk profile and contract value
- When contracts expire and when performance was last reviewed
- The results of individual risk assessments PLUS an overall view of vendor risks among the various risk categories (e.g. a "heat map")
- How a particular vendor's risk profile has been modified over the last few cycles (why and by whom, with supporting evidence)
- How the FI stays on top of regulatory changes and incorporates them into monitoring processes
- Which management officials inside the FI are responsible for vendor relationships and contracts
- How the board stays apprised of vendor management issues and exercises appropriate oversight to the overall vendor management program

## Turning Vendor Management into a Byproduct of Effective Compliance Management

Regulatory compliance – including vendor management – is overwhelmingly time consuming and complex for most FIs. Yet, the answers are all there in the regulations if you know when and where to

*"The secret of change is to focus all of your energy not on fighting the old, but building the new."*

**Socrates**

find them. The problem is that the "book of answers" is *really, really big*. Even a single "chapter" or topic like vendor management can be frustrating to digest, interpret and enact. Regulators have realized the enormity of this problem and have advocated for the use of a compliance management system (CMS), or a framework to systematically and effectively "operational-ize" new rules and requirements.

So, what are the objectives of a strong CMS – one that can handle vendor management requirements alongside BSA, information security, lending and other rules? Guidance from various regulatory bodies and agencies points to six compliance management objectives:

1. Understand the regulations that apply to your financial institution
2. Keep up with regulatory changes that apply
3. Make sure everyone understands their regulatory responsibilities
4. Get regulatory requirements baked into your daily operations
5. Verify that you're on track on a routine basis
6. Have a reliable and transparent way to fix what breaks

These objectives are at the heart of the vendor management best practices, rules and steps outlined in this white paper. In fact, they're at the core of every area of compliance. The real challenge for FIs is coming up with an efficient way to meet these objectives. Traditional, checklist and spreadsheet-driven approaches to vendor management simply can't support the volume of vendors or the pace of regulatory change.

What the current state of compliance demands is a turnkey solution that combines automation, regulatory expertise and best practices to address the entire spectrum of regulatory requirements. Continuity has met these demands with the industry's first, turnkey CMS – the Compliance Core™. By leveraging deep, up-to-the-moment regulatory expertise and automation, the Compliance Core ensures requirements are interpreted and enacted correctly and quickly. It also gives FIs of all sizes the agility they need to respond to change, whether operational or at the regulatory level.

The burden of vendor management is only going to grow as banks and credit unions outsource more business activities. Having a way to centrally and easily manage this expanding area of compliance will be imperative to banks that want to accelerate growth and de-risk their business.

## Learn more about Continuity

Visit us at www.continuity.net/vendor to learn about how Continuity's Compliance Core™ provides a comprehensive vendor management solution as well as addressing your Integrated Mortgage Disclosures, HMDA and other critical regulatory compliance needs.