The FINE ART of Vendor Management

BY MICHAEL STEER

With today's regulatory risk, vendor management is an opportunity to strengthen your risk management program and invest in quality vendor partnerships. For many lenders, it appears vendor management is still an area that is not given sufficient resources and attention. This is understandable given today's compliance requirements. However, lenders need to make vendor management a priority as it can have an immediate impact on operations. Consider this: A vendor that is critical to your operations goes out of business tomorrow. Would you have a fully developed contingency plan so as to reduce business interruption? Probably not. Most owners and key executives I interviewed in the last five years are in the same boat. Like it or not, vendors are an extension of your business and many regulators take this position when assessing the vendors you select for your business. If a vendor you utilize suffers a data security breach, it may be your borrowers that are impacted leaving you ultimately

responsible. Does anyone remember the name of the vendor that suffered the security breach that leaked Target's customer information? I can't. However, I do remember Target's customers were affected. So, what do you do to mitigate this risk and how do you develop a program that creates value to your organization? That is the million-dollar question and one that many financial institutions and independent mortgage banks are challenged to solve.

The title of this article explains what vendor management is... an art, not a science. With various supervisory guidance publications and numerous articles on vendor management, one would think that developing and implementing a vendor management program would be simple, but it is not. Try reading CFPB Compliance Bulletin and Policy Guidance 2016-02 (formerly Bulletin 2012-03), OCC Bulletin 2013-29, Federal Reserve Guidance on Managing Outsourcing Risk December 5, 2013, FDIC FIL-44-2008, National Credit Union Letter 01-CU-20 and Supervisory Letter No. 07-01, or a number of other articles on the web. Although useful documents, they do not necessarily spell out how to develop a compliant and practical vendor management program. So, how is one supposed to interpret and apply the requirements of these directives into an effective vendor management program? Doing nothing is bad, doing something is probably okay, and doing everything will result in your business units knocking on your door questioning why they cannot get a new vendor partner approved.

Based on my experience, the best approach is to start off simple and grow from there. The following steps outline one approach that can be applied to create an effective vendor management program.

1. Define what you would like to accomplish with your vendor oversight program. Items for consideration may include, but are not limited to, compliance, privacy, and information security, as well as limiting financial and reputational risks.

2. Identify who your vendors are. Obtain a list of your paid vendors for the previous 12-24 months from Accounts Payable to determine which vendors your company utilizes.

3. Review your list of vendors and assign risk tiers based on various factors, such as risk, exposure to consumer nonpublic personal information (NPI), whether the vendor is considered a "critical vendor," etc.

a. Tier 1 vendors may be critical to your operations, have access to non-public personal information (NPI) or other confidential or proprietary information, may not be easily replaceable, or may be a high annual dollar spend.

b. Tier 2 vendors may be moderately critical to your operations, maintain company confidential or proprietary information, be moderately replaceable, and be a moderate annual dollar spend.

c. Tier 3 vendors will likely be your least risky vendors. However, these are not to be disregarded. As an example, many companies consider janitorial services to be Tier 3, but do not take into consideration that janitorial employees often have access to facilities after hours. Therefore, if your company does not follow clean desk procedures or the janitorial vendor does not run appropriate background checks on its employees, you may want to consider them in a different tier.

d. Transactional vendors, as it relates to the mortgage industry, are your settlement agents on individual loan files, and are often a time sensitive transaction; therefore, one must take into consideration time constraints in order to meet closing deadlines.

4. Locate all of your contracts (fully executed). It is likely that you will find that you do not have a centralized repository of stored and fully executed contracts, so this step may result in a scavenger hunt of sorts. While we are on this topic, you should work to implement a company-wide policy that prohibits unauthorized individuals, branches, and business units from engaging new vendors without appropriate Executive Management approval. While putting a policy in place may reduce the number of non-corporate approved vendors, company-wide training will aid in achieving better results.

5.   **Obtain, deposit, and track vendor information, such as contact information, applications and/or questionnaires, risk assessments, written contracts, and other due diligence materials from the vendor into a centralized location.** There are many technology solutions in the market that serve as a vehicle to automate parts of this process, in addition to serving as a centralized repository. Some of these solutions provide reporting features for ongoing monitoring and analysis. Spreadsheets, shared folders, and calendar reminders may work, but this is a manual process that can be cumbersome and inefficient.

6.   **Once you complete steps 1-5, you should be able to evaluate your vendors and create due diligence questionnaires and/or applications to collect information necessary to determine the vendor's residual risk exposure.** Understand what information and documentation you need based on the inherent risk of the vendor and the required controls. As an example, you probably do not want to ask your janitorial vendor how they develop software for you if all they are doing is cleaning your facilities. Taking the time to customize your questionnaires/applications will result in a higher return in terms of quality of answers and quantity of vendor responses. In any case, be prepared to follow up, follow up, follow up, and follow up some more. Did I mention that you will have to follow up with these vendors in order to obtain the information you need to appropriately evaluate them?

7.   **Review and assess the documentation and information collected through the due diligence effort.** Too often vendor management is viewed as a checkbox approach, but what does checking the box really do? Your team should review the documentation provided and instead of answering, "yes, the vendor has X, Y, or Z document," they should determine if the documentation is sufficient. Imagine receiving a Business Continuity Plan from your vendor that says, "in the event of a disaster, we pack up and head to happy hour and will return to work once everything is resolved"? While that sounds like fun for your vendor, if your approach to vendor management is to check the box you will be in trouble in the event the vendor actually suffers some type of disaster or business interruption. You will also need to set company policy on incomplete questionnaires, missing documents, issues with background checks, or if a vendor refuses to provide required documents, such as financials or insurance.

8.   **Lastly, determine the frequency for recertification and the depth of your assessment, which may include a site visit.** Site visits assess a vendor's adherence with its own policies and procedures and allow you to physically view and confirm their practices. A perfect clean desk policy on paper by your vendor is worthless if the vendor's employees have stacks of confidential material on their desks and do not utilize shred bins.

GSEs, regulators, warehouse banks, and investors are all beginning to become more focused on their counterparty's vendor management program. These types of agencies and companies are more likely to look under the hood on a more frequent basis. Low hanging fruit for these entities is the absence of a plan or neglecting to fully execute the program. While vendor management is becoming more common practice, it is still a challenge for lenders to ensure a streamlined, robust, and compliant process. As mentioned in the beginning of the article, vendor management is an art, not a science. You have to build your program to be somewhat flexible and evolve with the ever-changing regulatory environment.

Look for Part II in a future issue of Mortgage Compliance Magazine, which will highlight additional components for vendor management, such as incident tracking, contract review, performance reviews, IT assessments, and general best practices when performing an onsite review.

MCᴍ

Michael Steer serves as the President of Mortgage Quality Management and Research, LLC (MQMR) and can be reached at MSteer@MQMResearch.com.