To Manage 3rd and 4th Party Risk, Think – and Act – Like a Regulator

by Sean Cronin, ProcessUnity

Regulatory bodies including the Office of the Comptroller of the Currency (OCC) have made clear that when a bank outsources functions to third parties, the bank is still responsible for managing risks associated with those functions. But what if the third party then outsources certain functions to yet another company? Is the bank now expected to manage risks associated with that company, which is now a fourth party vendor to the bank?

In a word, yes, and it so happens bank regulators make the same argument. "A bank's use of third parties does not diminish the responsibility of its board of directors and senior management to ensure that the activity is performed in a safe and sound manner and in compliance with applicable laws," says OCC Bulletin 2013-29, issued on Oct. 30, 2013. As one of the factors contributing to the number and complexity of bank relationships with third parties, the same document cites "contracting with third parties that subcontract activities to other foreign and domestic providers." One of the OCC's concerns is that banks enter into contracts "without assessing the adequacy of a third party's risk management practices."

Banks would do well to share those concerns and for the most part, they do. But the issue is a thorny one because it is indeed a complex task for banks to continually manage risk for all those third- and fourth-party vendors.

The operative word there is "continually," because risk management is an ongoing process. Any company performs due

diligence before contracting with a third-party service provider. But the key to effective risk management is ongoing follow-up, to ensure the controls that were in place when the relationship began remain in place over time, and change as necessary to manage new risks.

This level of risk mitigation requires a repeatable program that includes periodic inspection. “You don’t get what you expect, you get what you inspect,” as the saying goes.

At a minimum, inspection begins by identifying all fourth-party providers that are servicing your bank. You need to understand the type of information and services being outsourced, and what controls are in place to protect the bank’s interests.

The idea is to gain an understanding of the total risk across both third and fourth parties and what contingency plans are in place should an event occur. It makes sense to be proactive in this effort because banks will increasingly be under pressure from regulators and their own boards to prove a program is in place for managing both third- and fourth-party providers.

Such a program involves assessments that take a sampling of the controls that should be in place and asks vendors questions to ensure they are indeed in place and functioning as intended. But as banks continue to outsource more and more functions to cloud providers and others, the inspection process can become unwieldy at best and, at worst, untrustworthy.

To ease the burden, banks need to automate the process of conducting assessments and analyzing results. The program should be set up to follow risk tolerance guidelines and measurements that are well-defined and defensible to senior management and regulators. It should produce documentation that helps illustrate where you may need to take steps to

further reduce risk, such as diversifying to reduce exposure. In general, it should provide plenty of data elements and analytics to improve decision-making.

Besides the main benefit such an automated program provides – reducing your level of risk – this kind of proactive, self-policing program also gives banks a leg up in its meetings with regulators. It's like taking a test where you know the questions ahead of time and can prepare your answers. The regulators will be asking you the same questions you've been asking your third- and fourth-party providers because you've, in effect, been regulating them all along.

Automating your vendor risk management program also ensures risk assessments don't fall through the cracks because of overloaded internal auditors. What's more, it eliminates the appearance of subjectivity in vendor classifications and ensures the process is repeatable. Automation also brings a new level of intelligence, because an automated system can find trends and the proverbial needle in a haystack that may help you prevent a serious breach.

Being proactive and finding those needles will help any bank prove it's doing an effective job at regulating all of its service providers, both third and fourth party, all the while reducing its risk of exposure.

Moving to the Cloud: Why now?

For law firms and financial institutions, questions linger about the transition to cloud-based technology: is it safe? How does it benefit the existing infrastructure? Will new IT personnel need to be hired in order to manage it?

The simple answer is that cloud-based solutions are designed to be easier to deploy and more affordable to manage than comparative on-premise solutions. There is minimal set-up

involved in building a cloud database, and it’s managed by the vendor – not the IT department. Therefore, banks and law firms don’t need to invest in new IT staff to deploy a cloud-based solution, and as needs change, new applications can be deployed as required.

The less time that financial and legal organizations have to spend relying on manual tasks to control risk enables them to better allocate resources to focus on high-risk management activities. Cloud-based solutions augment that approach by simplifying the deployment process and shifting the maintenance onus to the vendor – typically with lower costs and infinite scalability.