Vendor Management: Software Considerations

By: Leah Hamilton, ProBank Austin

When it comes to managing third party risk, software vendors should top the list. However, due to the size of core providers, we often minimize the risk because, after all, they are a core provider and are examined by the federal prudential regulators as well. Our software systems comprise of much more than core software – there are specialty platforms such as account opening, loan applications, loan servicing, as well as numerous interfaces to our core system.

Even with all of the bells and whistles that software providers offer and promise compliance, software can only enable us to be compliant. In other words, human input will be required – whether it is establishing or verifying parameter settings, user profiles, setting up our products and services and so much more. Moreover, we cannot simply defer to or otherwise delegate our compliance responsibilities to the third party; ultimately, the institution is responsible for meeting any applicable regulatory requirements. As such, each institution must identify, control and manage its compliance risks with any software it leverages for providing its banking products and services.

Whether the software is new to the institution or has been in place for several years, system validation testing is a critical component to managing and controlling risk. The first step is to identify what products and services are offered or provided, what are the regulatory requirements for those products and services, and which software are utilized. Next comes collaborating with the head of Information Technology (IT) as IT should have a road map of the software used and how they are interfaced to deliver the product or service.

By identifying a road map of the required or leveraged software, the products/services and the compliance requirements, an institution will be able to identify the inherent and residual risks as software cannot eliminate all risk – software is a control that is leveraged to mitigate inherent risk (that risk posed without any controls) coupled with additional controls (e.g., policies, procedures and training) to identify the residual risk (what exposures still exist despite controls in place – and what is the probability of such exposure).
When assessing the software against the regulatory requirements, the keys to successfully identifying, controlling and managing compliance risk is to ask questions and to document our business-decisioning of who, what, where, when, why and how. Examiners will ask the same or similar types of questions – and want to know the institution’s business-decisioning. The following is an example of this process in reviewing Bank Secrecy Act/Anti-money Laundering (BSA/AML) software.

During a BSA/AML examination, examiners will expect that the institution has conducted system validation testing to ensure that the software function consistent with regulatory requirements, safe and sound practices, and the institution’s business strategy and appetite for risk. One component of BSA/AML system validation testing includes a review of the parameter settings and user profiles. For example, what parameters or threshold values can the institution customize to address its risk, did it use them, and who is overseeing the input, throughput and output? In turn, questions that may arise include:

• Is an individual assigned oversight of the software? If not, why? If so, what is the individual’s knowledge and understanding of the platform?

• What are the values or thresholds established by the institution within the software?

• What was the business-decisioning process in determining the appropriate values or thresholds established to ensure that the software is effective in carrying out those protocols? Do the thresholds or values meet or exceed regulatory requirements, institution objectives, appetite for risk?

• For this monitoring platform specifically, what are the data sources – what is the original source of input of the data? How does the institution know that the platform is importing and ultimately translating accurate data? Does the institution understand its regulatory requirements in validating the data?

• What reports are available through the software? Which ones does the institution use and why? If the software can generate 100 different reports, what was the decisioning process for selecting only 30 reports? Why do the other 70 reports not apply or contribute to effective BSA/AML monitoring for this institution?

• How does the institution leverage and utilize the output from the system (e.g., reports, red-flags, etc.) to manage its risk, identify suspicious activity, etc.?

• Are there written procedures demonstrating how this institution utilizes the software? Are they consistent with the vendor’s recommendations? If not, why? Are they consistent with the institution’s products, services, strategy, risk appetite?
• Are parameters/thresholds periodically verified to ensure that they still reflect the values that were established and entered?

These are but a few of the multitude of questions institutions address in assessing software solutions to assist in identifying, controlling and managing compliance risk.

An institution cannot simply rely on the guarantee or other promises a software provider may extend as the institution is ultimately responsible for ensuring its own compliance with the regulations as well as ensuring it operates in a safe and sound manner.

For more information on managing third party risk, each of the federal prudential regulators have issued various guidance over the years that institutions should leverage to ensure it is identifying, controlling and managing its third-party compliance risk.