Robert Bondy is a partner at Plante Moran.

Brad Birkholz is a senior manager at Plante Moran.

RISK MANAGEMENT

Rightsize Your BSA/AML Model

Many bank executives have questions about the April Interagency Statement on Model Risk Management for Bank Systems Supporting Bank Secrecy Act/Anti-Money Laundering Compliance. Here, we share some key takeaways and steps to take.

Prudent Risk Management

While the recent statement doesn't change existing Bank Secrecy Act/anti-money laundering (BSA/AML) requirements, or establish new ones, financial institutions must still ensure "prudent risk management" for automated transaction monitoring systems. This includes periodic review and testing of filtering criteria and thresholds for effectiveness, and independent validation of the monitoring system methodology to ensure its effectiveness in detecting potentially suspicious activity. This applies even if the systems might not meet the definition of a model.

That said, it's incumbent that banks understand whether or not their BSA/AML monitoring systems qualify as models and how that qualification opinion impacts platform governance.

Tailoring Risk Management Procedures

The supervisory guidance covering model risk management doesn't have the force and effect of law, and it's not a set of testing procedures. Rather, banks should view the guidance as a resource as they tailor the institution's approach to risk management for the particular BSA/AML systems they use. The risk management procedures should:

- Fit the chosen system.
- Fit how the institution currently uses the system.
- Fit how that use impacts the institution's BSA/AML risk profile.

Keep in mind that practices might need to differ between internal and third-party models when tailoring your risk management procedures. Banks must employ sound vendor management practices, both when entering into a relationship with a third-party model provider, as well as periodically during the ongoing relationship.

Using a third-party model doesn't absolve banks from the duty of knowing how the model works, and it doesn't relieve them of needing to implement a plan to manage the model risk.

Inadequate Management, Wasted Resources

Often, we encounter institutions that believe their BSA/AML systems don't meet the definition of a "model" and don't subject the system to adequate risk management practices when, indeed, they do meet the definition. We recently worked with a client in this situation who was remediating a long-standing processing issue. We helped them strengthen their risk management processes to align with the uniqueness of the model, which enabled them to proactively address potential issues.

We also see institutions allocating too many resources to validate systems that don't meet the definition of a model. For these institutions, it's important to adjust expectations and system management, which allows BSA/AML and other personnel to reallocate time and energy.

Steps to Take Now

First, determine if your financial institution is satisfied with how it classifies its BSA/AML system in light of the new statement.

Next, review your risk management practices. They shouldn't be a carbon copy of practices used to manage other systems, since some risks are unique to BSA/AML systems. Are your risk management practices commensurate with your bank's use of the system and your BSA/AML risk profile? Even if two financial institutions are the same size and use the same BSA/AML system, the way they use their individual systems and their different BSA/AML risk profiles should influence their respective risk management practices.

Finally, if your institution has employed a third-party model, you should have a sufficient understanding of how the system works and be able to articulate this to regulators. You also need to ensure your vendor management program is tailored to address vendor risks specific to your BSA/AML system. Create a process to monitor your BSA/AML system vendor on a "go-forward" basis, not only at implementation.

Banks that don't implement risk management frameworks with clear model definitions and their associated review, testing, and validation, are opening the door for examiner scrutiny.

Protect your institution. Gaining greater clarity around risk management frameworks and taking these steps can help ensure that your bank gains as much benefit as possible from the software platform you've selected.