Bridging the gap between risk assessment and transaction monitoring

A robust money laundering/terrorist financing (ML/TF) risk assessment is the cornerstone of a sound compliance program. With more reliance on automated transaction monitoring systems, it is more important than ever to ensure that your transaction monitoring program is properly configured and aligned to the ML/TF risk profile of your institution.

On June 30, 2016, the New York Department of Financial Services (NYDFS) issued final rule part 504 requiring senior officers or board of directors to certify the effectiveness of anti-money laundering (AML) and Office of Foreign Assets Control (OFAC) transaction monitoring and filtering programs. The final rule goes on to state that an institution’s transaction monitoring program should be reasonably designed based on the risk assessment of the institution and appropriately matches BSA/AML/OFAC risks to the institution’s businesses, products, services and customers/counterparties.

While conducting ML/TF risk assessments is not a new practice, it is the first time that ML/TF risk assessments are a written requirement for NYDFS-regulated institutions. This article will provide best practices for bridging identified ML/TF risks to your transaction monitoring program.

Identifying ML/TF risks within your institution

The board of directors and management set the risk appetite and are responsible for creating a culture of compliance to ensure staff adherence to the financial institution’s compliance program. A robust risk assessment will help your financial institution to promptly and accurately identify risks and apply appropriate controls to mitigate risk or identify unacceptable risks to avoid. A sound risk assessment will identify potential events that might impact compliance objectives and should employ a combination of qualitative and quantitative risk assessment methodologies. The risk assessment should be utilized for the purpose of driving policy, procedures, controls and independent testing.

The risk assessment process has four main steps:

1. Identify the ML/TF inherent risks
2. Analyze the mitigating controls
3. Evaluate residual risk
4. Determine the direction of risk

Inherent risk is the risk that is present without regard to mitigating controls. Per the Federal Financial Institutions Examination Council’s (FFIEC) BSA/AML Examination Manual, a risk assessment should include an assessment of the financial institution’s products, services, customers, entities, transactions and geographic locations. A sound risk assessment should include gathering relevant customer and transaction data and interviews of business line leaders. The composition of a complete customer and transaction database is the first step in understanding where the ML/TF risks are within your institution. It is best practice to include at least two years of customer and transaction data within your database as this helps identify potential trends utilized for determining the direction of risk.

The final rule applies to banks that are chartered or licensed by New York, as well as nonbanks, such as money services businesses.

The interview process is essential to obtaining a tailored and effective risk assessment and can assist with providing a qualitative assessment of the customer and transaction data. The interview process can identify ML/TF risks that were not previously identified and can help foster a line of communication between each business line and the compliance department. In addition, the interview process can help promote a culture of compliance by breaking down the silos of a traditional financial institution by encouraging information sharing and looking at ML/TF risks across the financial institution.

For each ML/TF risk identified throughout the risk assessment process, it is important to cross reference the institution’s policies and procedures to ensure that there are policy statements and controls in place to mitigate the ML/TF risk. This helps financial institutions determine whether there is a potential gap in the policy and procedures and the ongoing monitoring of the particular ML/TF risk.

How to establish a risk assessment methodology for assessing ML/TF risk

One of the biggest shortcomings with ML/TF risk assessments is the lack of a well-defined risk assessment methodology. The risk assessment process should follow a well-defined methodology, which should be fully described in your risk assessment report and supporting documents. The risk assessment methodology should provide: 1) measurement of inherent risks accounting for the principals of impact and likelihood; 2) an assessment of the effectiveness of the mitigating controls; 3) an evaluation of the residual risks that exist after consideration of the mitigating controls; 4) a determination of the direction of risk for each risk; and 5) a process for determining the overall inherent and residual risk rating of the institution.

In addition, the risk assessment should incorporate new and emerging risks within the industry such as the FinCEN guidance FIN-2016-A005 on cyber-enabled crime and on how documenting cyber risk impacts a financial institution’s ML/TF risk profile. It is important to remember that the risk assessment should be tailored for each institution and allow for the application of specialized knowledge/professional judgment by the compliance officer. The professional judgment factor can allow for an accurate reflection of the financial institution’s risk profile based on intricate knowledge held by the compliance officer and/or stakeholders.

While risk assessments are typically conducted on an annual basis, it is often forgotten that it should be updated when a “major event” occurs as well. A major event is generally interpreted as: 1) a merger or acquisition; 2) exponential growth in a new market area; 3) introduction of a new product or service; and 4) significant changes in the regulatory environment that impacts the financial institution. It is recommended that each financial institution define in its institution’s policy what may necessitate an event-driven risk assessment. Furthermore, it is
important to note that a supplemental risk assessment and/or mini-
risk assessment can be completed in lieu of a full risk assessment
when a major event occurs. Failure to have a well-defined method-
ology tailored to the financial institution that also incorporates
recent trends and/or regulatory guidance can expose the financial
institute to undue scrutiny from the independent auditors and/or
regulators.

### Aligning your ML/TF risk to your transaction monitoring program

Over the past 18 months, one of the most commonly cited areas of
examiner AML criticism is the concept of sound model risk manage-
ment and inadequate enterprise-wide risk assessments. Regulatory
agencies have shifted resources and attention to assessing how
institutions set up their automated transaction monitoring and high-
risk customer management programs.

Financial institutions rely heavily on automated systems to identify
potential suspicious activity but have been inundated with high
levels of false positives, which have taken time and resources away
from the ML/TF risks that require the most attention. Scenarios
principally based on judgmental and quantitative considerations
should be tailored to the institution’s specific ML/TF risk profile.

### A sound enterprise-wide risk assessment is the key to bridging the gap to effectively identify and monitor ML/TF risks within your financial institution

Conceptual soundness is the foundation for setting up an auto-
mated transaction monitoring model commensurate with your institu-
tion’s ML/TF risk profile. Conceptual soundness involves
assessing the quality of the model design and construction, as well
as a review of documentation and empirical evidence supporting
the methods used and variables selected for the model.1 In setting
up your transaction monitoring system, you should ensure that
judgment exercised in model design and construction is well
informed, carefully considered and consistent with published
research and with sound industry practice.

When setting up your scenarios or rules to be utilized in the auto-
mated transaction monitoring system, you should map the areas
with higher ML/TF inherent risks to scenarios or rules to ensure
there is coverage of such risks. When setting the thresholds for your
scenarios or rules, it is important to consider conducting some level
of statistical analysis of the percentage of coverage (i.e., customer
transactions that would be captured by the scenario) to deter-
mine whether the scenario will identify those customers and/or
transactions that present the highest risk. When setting your pro-
duction scenario or rule thresholds, it is important to consider the
results of below-the-line scenarios as there may be potential

### Suspicious activity below your threshold that may warrant the threshold of the scenario to be reduced to include suspicious activ-
ity that may have gone undetected.

In addition, you should consider historical suspicious activity expe-
rience within your financial institution. Also, it is important to
remember that all scenarios and settings should be reviewed in a
“test” environment before moving them into production to ensure
that scenarios are operating as designed.

Once you have implemented your transaction monitoring scenarios
or rules, it is important to maintain key performance indicators
(KPIs), such as an alert to information request percentage, an alert
to investigation percentage and an alert to suspicious activity report
percentage, as this will assist the institution in determining the
effectiveness of each scenario or rule on an ongoing basis.

Some common pitfalls that may occur when reviewing automated
monitoring systems are:

- Inaccurate or incomplete model documentation
- New ML risks to the institution are not considered part of the
  transaction monitoring model
- Misaligned alerts to ML/TF risk profile (i.e., focus of scenarios or
  rules are for areas identified as low risk to the institution)
- High-risk jurisdiction alerts do not consider all countries
  involved with a transaction and redundant alerts or scenarios
  (i.e., looking at the same activity multiple times)

Financial institutions should look for opportunities to monitor trans-
action activity by customer peer grouping. This will allow for a more
tailored transaction monitoring approach and it will allow an insti-
tution to benchmark customers against their peers and identify out-
liers that may present heightened ML/TF risk to the institution.

In the near future, at a minimum, institutions will need to consider
creating a Model Governance Committee responsible for oversight
of the institution’s model, risk management program. Your financial
institution should conduct an AML model inventory documenting all
the systems utilized to monitor ML/TF risks within the institution.
The Model Governance Committee should determine and document
the frequency of any calibration and validation efforts.

In summary, a sound enterprise-wide risk assessment is the key
to bridging the gap to effectively identify and monitor ML/TF
risks within your financial institution. By setting up your compli-
ance program in a manner commensurate with the institution’s
ML/TF risk profile, you will be able to focus your attention and
resources on those areas that present the highest risk to your
financial institution.

Jason Chorlins, CAMS, principal, Kaufman Rossin, Miami, FL, USA,
jchorlins@kaufmanrossin.com

---