Treliant

Risks and Controls for AML Monitoring Systems

December 3rd, 2018

Martin Jaundoo, Senior Manager

Version: Final
Release Date: 12/3/18
Classification: Public

Martin V. Jaundoo, CAMS

Senior Manager – Treliant, LLC

Martin Jaundoo, Senior Manager with Treliant, has over 18 years of experience working with large and small financial institutions, primarily focused on financial crimes compliance. He helps banks ensure Bank Secrecy Act/Anti-Money Laundering (BSA/AML) and USA PATRIOT Act compliance, fraud prevention, and adherence to the requirements of the Office of Foreign Assets Control (OFAC).

At Treliant, Martin has worked as part of an independent consultant and monitorship engagement team involved in the remediation of AML and sanctions compliance programs at global banks. He successfully led projects that optimized transaction monitoring tool rules and thresholds, increasing operational efficiency.

Before joining Treliant, Martin was a BSA/AML and fraud prevention consultant with the Capco professional services advisory firm. At Capco, he developed expertise in risk identification and assessment, automated transaction monitoring tools validation and rules threshold calibration/optimization, transaction monitoring/surveillance investigations (lookbacks), and enhancement of Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD) measures. His BSA program work included independent assessments and gap analysis, policy and procedure reviews, and risk model methodology development. Previously, he held Assistant Vice President roles in BSA/AML compliance with First Southern Bank and First Bank of Miami, and he was a Senior Investigator/Officer with Ocean Bank.

Among his accomplishments, Martin has contributed to regulator-enforced remediation actions involving enhancements to BSA/AML programs and reviews of correspondent banking and wire transfer transactions, leading to removal of the regulatory consent order. He has also automated manual monitoring processes for cost savings and operational efficiencies, trained investigators, and designed and documented risk models considering clients' various service offerings, customer characteristics, volume of activity, and geographic markets. Additionally, Martin has led a readiness and gap analysis addressing the New York State Department of Financial Services' (NYDFS) Part 504 transaction monitoring rule. He has significant experience with optimization and validation of a wide range of software tools for transaction monitoring system, sanctions watch-list filtering, and fraud prevention.

Martin received a BSc from Embry Riddle Aeronautical University in Professional Aeronautics with a minor in Aviation Safety and Management. He is a Certified Anti-Money Laundering Specialist (CAMS).

AML Monitoring Systems

AML Monitoring Systems are considered a “model” based on supervisory definition of a model.

Risk Management

AML monitoring systems invariably present a number of risks. These risks ranges from breakdowns in compliance controls (fundamental errors in the design may produce inaccurate output that fails to detect unusual activity) to reputational risks (consequence of not detecting and reporting suspicious activity resulting in regulatory penalties and negative press).

BSA/AML Penalties 2018 (YTD)

- U.S Bank - $598 million for BSA/AML failings.
- Capital One - $100 million for BSA/AML deficiencies.
- Bank of China NY Branch - $12.5 million for BSA/AML deficiencies.
- Aegis Capital - $1.3 million for SAR filing failures.

Selecting an AML Monitoring System

Risk

Selection did not analyze the system's ability to meet the business objectives resulting in system that did not satisfy business objectives and created transaction monitoring gaps.

Controls

Ability to satisfy regulatory requirements for transaction monitoring.

Scenario library provides adequate coverage for risks identified in institutions AML risk assessment.

Scenarios can be modified or new scenarios created by institution without vendor involvement.

Compatibility with existing source systems such as a trading platform.

Scenarios can be modified or new scenarios created by institution without vendor involvement.

Implementation of AML Monitoring System

Risk

Inadequate user acceptance testing (UAT) including failure to test all implemented system components that fail to identify system limitations, and incompatible components.

Controls

1. Test plan must cover all system components.
2. UAT personnel should be well trained on all system components.
3. UAT data is illustrative of institution's production environment data.

Implementation of AML Monitoring System

Continued

Risk

Unclear UAT goals and not defining expected results which failed to identify potential performance breakdowns.

Controls

Clear definition of expected results and comparing actual results with expectations. For example, defining expected number of alerts for a velocity scenario and comparing actual results.

Risk

System performance is compromised under stressed situations resulting in inaccurate calculations.

Controls

UAT should examine system's capability to perform required functions under stressed situations including handling extreme data values.

AML Monitoring Systems: Assumptions and Limitations

Risk

Failure to analyze system limitations and assumptions which compromise systems capability to satisfy business objectives.

Controls

Analyze all limitations to determine whether they compromise the systems performance and capability to achieve business objectives.

Analyze system overrides and data transformations to identify unacknowledged assumptions or limitations.

Implement a governance process to enforce limitations on system use.

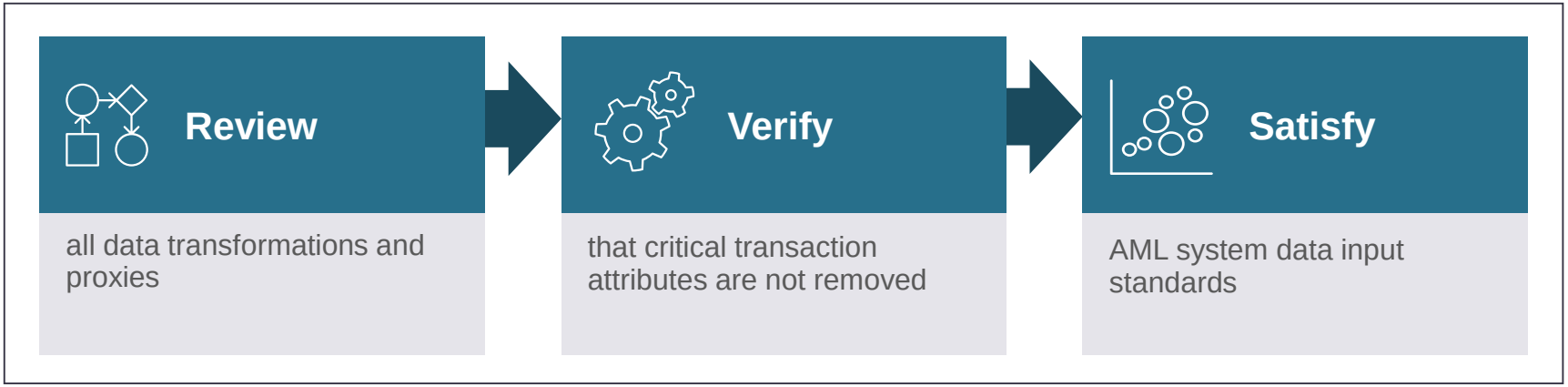
For example, if the system is unable to link customers by unique identifiers such as Tax ID, Social Security, transaction monitoring will be restricted.

Data Transformations

Risk

Data transformation to comply with AML system input requirements compromise data completeness resulting in ineffective transaction monitoring.

Controls



Treliant

Data Quality and Completeness

Risk

Failure to identify all data sources and critical data elements required for transaction monitoring creating transaction monitoring gaps.

Controls

1. Identify and document all internal and external data sources to ensure all critical sources are ingested in the system.
2. Review transaction code mapping document from source systems to AML system and verify all relevant transaction types are identified including CIP and transaction record.
3. Review data ETL process to ensure a complete and accurate transfer of data into the system.

Data Quality and Completeness

Continued

Risk

Frequency of data load from source systems to AML system create potential gap in transaction monitoring.

Controls

Review data load frequency and verify the loads are done at least daily to avoid potential transaction monitoring gaps. Example, if wire data is loaded weekly, there may be gaps when rules are triggered monthly, since the rule will only monitor 3 weeks of data.

Risk

Inadequate data security measures to prevent unauthorized access and modification of data resulting in data breach.

Controls

The AML system data should fall under a strict enterprise wide data security policy.

Data Quality and Completeness

Continued

Risk

Data reconciliation process failing to detect missing data which compromises the system's effectiveness.

Controls

Data reconciliation frequency must be adequate to detect missing data and ensure optimal system performance

Data reconciliation must include processes and controls to ensure the complete transaction universe is being monitored.

Data reconciliation should reconcile dollar amount and count of transactions loaded from source systems into system to verify relevant data are loaded.

Data Quality and Completeness

Continued

Risk

Inadequate controls for provisioning, recertification and revocation of system access rights resulting in access to confidential information by unauthorized users.

Controls

1. Responsibility of provisioning users should be assigned to IT
2. User rights separated by job function to prevent inadvertent access to SAR information.
3. Procedures to remove users when they are no longer part of compliance department.

Data Quality and Completeness

Continued

Risk

Inadequate disaster recovery measures resulting in significant downtime of AML system and potential backlog of alerts.

Controls

Implement disaster recovery measures to access system from alternate locations when necessary.

Initial Scenarios Implementation

Risk

Scenarios not aligned with typologies identified in AML risk assessment resulting in transaction monitoring gaps.

Controls

Create coverage assessment that maps risks identified in the risk assessment plus applicable money laundering typologies to the mitigating scenarios and manual transaction monitoring measures. Address any gaps with appropriate scenarios.

Risk

Scenario thresholds are not aligned with customer base resulting in over reporting or underreporting.

Controls

Statistical analysis of customer transactions to determine scenario thresholds to detect transaction anomalies. Document rationale for selected scenarios and thresholds.

Validation Risks and Controls

Risk

Inadequate documentation to support rationale for…
- System Selection
- UAT
- System Logistics and Methodology
- Limitations and Assumptions
- Data Transformations and Completeness

…which questions the integrity of the systems conceptual soundness

Controls

Robust documentation to support rationale for…
- System Selection
- UAT
- System Logistics and Methodology
- Limitations and Assumptions
- Data Transformations and Completeness

Ongoing Monitoring

Risk

Inadequate framework defining verification parties and their roles in the ongoing monitoring process leading to break in the ongoing monitoring process.

Controls

Framework with clear definition of parties, their role and frequency of periodic system verification.

Ongoing Monitoring

Continued

Risk

Inadequate ongoing monitoring and testing of data accuracy resulting in transaction monitoring gaps due to incomplete data.

Controls

1. Testing and verifying key data fields are used for transaction monitoring. Key data fields are in Appendix O of FFIEC BSA Exam manual.
2. Testing for completeness of data by executing queries for missing data fields and null entries in key data fields.
3. Selecting a judgmental sample of data fields in core systems and comparing to the AML System for a defined period and evaluate whether data was transferred completely and accurately. Examine judgmental sample to verify inclusion of the following: transaction types, dates, amounts, cash in/cash out, debit/credit, originator and beneficiary names and addresses, originator and beneficiary banks, monetary instruments purchaser and payee, etc.
4. Reconcile daily dollar amount and volume totals for each transaction type file from source systems to system for a defined time period to identify discrepancies.

Ongoing Monitoring

Continued

Risk

Insufficient effectiveness challenge and performance benchmarks failing to identify breakdown in system performance.

Controls

1. Implement performance benchmarks including any findings from independent reviews indicating transaction monitoring failure.
2. Effectiveness challenge include scenario effectiveness ratio, comparing number SARs filed from AML system and internal referrals. Comparing actual results to expected results and analyzing discrepancies.
3. Identify KPIs such as scenarios not producing alerts and investigate underlying reason.

Ongoing Monitoring

Continued

Risk

Failing to update AML risk assessment based on trends identified in ongoing monitoring process resulting in transaction monitoring gaps.

Controls

Implement procedures to update AML risk assessment based on unexplained changes in alert volumes related to certain geographic areas or activity types as indicators emerging risks.

Risk

Inadequate scenario tuning methodology and process resulting in significant number of false positives and operation inefficiencies.

Controls

Tuning methodology articulating trigger events, scenario effectiveness ratios, criteria for above the line, below the line, and rules decommissioning events. Tuning methodology including trends in KPIs, data analytics and capacity planning is part of the tuning process.

Outcomes Analysis (Back-Testing)

Risk

Inadequate sample of scenarios selected for testing failed to provide assurance system is operating as expected.

Controls

Scenarios selected should include:

1) Stable set of scenarios to confirm logical components are functioning as expected.

2) Scenarios implemented since most recent validation.

3) Scenarios generating alerts and those not generating alerts.

4) Cross-section of logical components, parameters and thresholds.

5) All customer types, risk class, businesses identified as high risk.

6) All transaction types.

7) Time periods consistent with timeframes defined in scenarios including longest timeframe for scenarios..

8) Testing period covering scenarios end of month cut-off.

Outcomes Analysis (Back-Testing)

Continued

Risk

Failure to adhere to transaction monitoring investigation procedures creating risk for possible late SAR filing.

Controls

1. Sample alerts to verify they are dispositioned within time frames consistent with expectations of the procedures.
2. Evaluate whether documentation to support alert disposition are consistent with procedures.
3. Whether alerts/case/SAR work flows are consistent with procedures.

Outcomes Analysis (Back-Testing)

Continued

Risk

Failure to adhere to transaction monitoring investigation procedures creating risk for possible late SAR filing.

Controls

1. Verify scenarios are correct in the system.
2. Test each logical component of scenarios selected for testing.
3. Perform back testing by reviewing a selection of alerts and trace alerted transactions to source systems and determine if all relevant transactions were captured in the alert.
4. Perform throughput testing by creating queries that mirror scenario syntax and executing queries against source system data. Evaluate whether results from throughput testing and system generated alerts are the same and resolve discrepancies.

Model Risk Management

Continued

Risk

No clear definition and identification of models according to the institution's policy resulting in a failure to identify all models and perform appropriate validations.

Controls

Clear definition of what is a model and model risk.

Risk

Model Risk Management policy does not detail scope and frequency of validation resulting in regulatory criticisms for incomplete and untimely validation.

Controls

Clear definition of all system components subjected to a validation cycle and a validation frequency consistent with regulatory expectations.

Model Risk Management

Continued

Risk

No clear definition of responsibilities within the MRM resulting breakdown of the model.

Controls

Clear definition of the roles and responsibilities of Model developer, Model owner, Model user, Internal Audit, Information Technology and Application Development and Third Party Vendor.

Risk

Ineffective change management implementing change without adequate testing resulting in undesirable system outputs.

Controls

Create a change management process that requires robust testing before implementation. Also, track all findings from validation with dates, roles, responsibilities, actions and resolutions.

Washington, DC Headquarters
1255 23rd Street NW
Suite 500
Washington, DC 20037
T. 202.249.7950

New York, NY
1133 Avenue of the Americas
Suite 3600
New York, NY 10036
T. 646.315.9430

Dallas, TX
2150 Lakeside Boulevard
Suite 250
Richardson, TX 75080
T. 469.802.4600

treliant.com