Educator
Maleka Ali, CAMS–AUDIT
Director of Consulting/Education
Banker’s Toolbox, Inc.

Consultant
Robert Casares, CAMS
Managing Director
SentryNet, LLC

Financial Institution
Myrna Olvera, CAMS
SVP/Operations Risk Manager
City National Bank

Examiner
Elizabeth Slim, CAMS
SVP/BSA Officer
1st Enterprise Bank

AML Program Validation
From different prospective
Data Validations / Program Evaluations

Maleka Ali, CAMS-AUDIT
Director of Consulting & Education
Banker’s Toolbox, Inc.
maleka@bankerstoolbox.com
Current Environment

- Tough exams
- Tougher expectations
Last Year:

- Senate Banking Committee examined state of affairs following a string of large-bank BSA violations.
- Since then regulators are under pressure to improve BSA/AML regime.
- “This pattern of violations is disturbing. . . To address this threat we must understand how banks’ safeguards malfunction and assess the way the government enforces our AML rules.”
Emphasis on Efficiency

How well are you equipped?

Processes and Procedures and Systems

How are those tools working?

Are they being used properly?

Are they making an impact?
Does it work?—Are you using it?

- Area of growing attention & expense—is BSA/AML data validation
- Examiners suggest audits on BSA/AML activity monitoring systems to ensure they are performing correctly—producing reliable alerts & accurate reports of potential criminal activity
- Data integrity from end to end is one concern, but there’s more to the validation process
Many institutions have proactively had efficiency reviews/evaluations done before exams to catch issues before examiners visit.

Examiners want to see what banks have done with the systems they purchased

- Automation brings you powerful tools, but are they all turned on?
- If they have been, have the rules of the system been kept up-to-date in recognition of evolving money-laundering patterns?
Under Transaction Monitoring:
- “Management should periodically evaluate the appropriateness of filtering criteria and thresholds used in the monitoring process. Each bank should evaluate and identify filtering criteria most appropriate for their bank. The programming of the bank’s monitoring systems should be independently reviewed for reasonable filtering criteria.”

Under Surveillance Monitoring:
- “Management should also periodically review the filtering criteria and thresholds established to ensure that they are still effective. In addition, the monitoring system’s programming methodology and effectiveness should be independently validated to ensure that the models are detecting potentially suspicious activity.”
Program Evaluations

Evaluate/identify filtering criteria most appropriate for your institution

“Is your program sufficient for the risk level of your institution”
Program Evaluation

- Review & test system capabilities & thresholds on a periodic basis
- Focus on specific parameters or filters in order to ensure that suspicious or unusual activity will be captured

Understanding the filters in your system and how your system works is critical to assessing the effectiveness of your monitoring program
Program Evaluation

- Consider higher-risk products & services, customers & entities, & geographies

  • Filters should be based on what is reasonable & expected for each type of account
FFIEC BSA/AML Examination Manual

OCC 2011-12 Guidance on Model Risk
What is a Model

Quantitative method, system, or approach

That applies statistical, economic, financial, mathematical theories, techniques and assumptions

To process input data into quantitative estimates
Model Components

- Information/Input
- Processing
- Reporting
Model Governance

- Development
- Implementation
- Use
- Validation
The Risk of Models

- Fundamental Design & Implementation Errors
- Data Quality
- Applicable Data Inputs
- Incorrect or Inappropriate Data
- Optimization
Components of Model Validation

Conceptual Soundness
- Does Model logic properly account for institutional risk?
- Are assumptions sound and appropriate for the environment?
- Assumptions may have to be tested

Syntax Validation
- Does the code capture data without errors?
- Testable through code replication or control data

Data Quality & Integrity
- Is data completely & accurately passed to monitoring platform
- Review of controls or analysis of data extracts

Model Performance
- Is the model performing as intended (i.e. capturing the desired behavior?)

Validation & Sustainability
- Is proper governance in place to manage approval process and model changes?
- Validation cycle?
- Out of cycle?
When is a Rule/Scenario Effective?
- Effective is measured by “meaningful” investigations
- A “meaningful” investigation could result in a “no-SAR” decision
- Effectiveness will differ based on intended purpose of the scenario
  - Results driven by individual scenario threshold testing
Approval of your Model?

- Authority to establish or change filters should be clearly defined
- Should require approval of BSA officer or senior management
- Document and be able to explain filtering criteria, thresholds used, & how both are appropriate for your risks
Expectations

Examiner evaluation of scenarios
  ◦ System capabilities
    • Scenarios available
    • Transaction/data feeds in the system

Scenarios selected by Financial Institution
  ◦ Criminal Typologies
  ◦ Incorporation of the Risk Assessment
    • Higher Risk Customers
Criticisms

- Use of Default Settings
- No below/above the line testing
- Lack or Insufficient documentation supporting scenarios or thresholds
- Scarce Evidence of threshold Validation
- Unsupported Sampling Methodology
- Exclusion of Customers, Products, Services
The Myth of Validation

- Validation is a living and breathing lifecycle which has matured with age and doesn’t have to be cumbersome
- Industry has moved into taking a risk based approach to validation and this makes perfect sense; adopt a proficient risk management methodology
The Myth of Validation

- For years many institutions took the approach that in order to satisfy regulatory expectations, everything should be validated all of the time, this is simply not the case.
- In most instances validating everything, every-time is just a waste of time, money, human resources and the various rain forests of the world.
- Take a Risk Based Approach
- Determine what information is important
- And focus on quality
What is enough?

- Not all institutions are the same
- Just like your BSA program—your validation should also be risk based
Can I expect to catch everything?
## Risk Based Validation

### High Level Assessment

### Full Model Validation

#### 1. Conceptual Soundness of AML Models

| Qualitative analysis of the current rule set to assess risk coverage; analysis of rules to assess model logic. Analysis and testing of underlying model assumptions to establish validity |
|---|---|
| - Assess documentation around the genesis of the rule set and the underlying model assumptions | - Analyze rule set to assess risk coverage and industry conformance. Conduct formal hypotheses tests of assumptions |
2. Assessment of Data Integrity and Quality

Assess the data requirements of the AML models and assist the Bank in determining whether these requirements are fully met or whether any relevant information appears lost or corrupted in the data flow from source systems to monitoring systems.

- Review documentation on systems, intermediate warehousing, and transformations for data feeds, and assess quality of controls in place to determine effectiveness of the data inputs.
- Perform testing of sample data obtained from all source systems to assess the integrity of all data feeds.
- Perform data quality and comprehensive testing for all critical elements.
## 3. Syntax Validation of Current Transaction Monitoring Systems

Assess the accuracy of the code used to implement the scenarios

<table>
<thead>
<tr>
<th>N/A</th>
<th>Validate rules syntax by code review</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Validate rules by independent replication</td>
</tr>
</tbody>
</table>
## 4. Model Performance (in Production)

<table>
<thead>
<tr>
<th>High Level Assessment</th>
<th>Full Model Validation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Evaluation of the performance of the Model in production to 1) enhance the rules set through changes in its composition, 2) enhancements in the threshold sets to reduce false positives, &amp; 3) ensure to a reasonable level that the model is not missing an excessive amount of suspicious activity as defined by bank policy.</td>
<td></td>
</tr>
<tr>
<td>Qualitative assessment of appropriateness of thresholds and parameters with respect to transactional activity of customers. Assessment of potential benefits of segmentation, if not already being applied, within the transaction monitoring process.</td>
<td></td>
</tr>
<tr>
<td>• Sample &amp; investigate alerts around parameter values to determine the relative quality and effectiveness of alerts generated under the new parameters. • Re–analysis of Historical Alerts &amp; SARs • Analyze historical performance of rules. • Analyze the distributions &amp; statistical properties of the Bank’s customers &amp; transactions • Assess quality/appropriateness of current client segmentation. • Conduct below the line analysis</td>
<td></td>
</tr>
</tbody>
</table>
## 5. Assessment of Model Governance and Sustainability

<table>
<thead>
<tr>
<th>High Level Assessment</th>
<th>Full Model Validation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assess the data requirements of the AML models and assist the Bank in determining</td>
<td>Governance policies and procedures for model risk management clearly delineating</td>
</tr>
<tr>
<td>whether these requirements are fully met or whether any relevant information appears</td>
<td>authorities and controls, as well as standard re-validation cycles.</td>
</tr>
<tr>
<td>lost or corrupted in the data flow from source systems to monitoring systems</td>
<td>– Identify key trigger events &amp; stability metrics to specify conditions when re-</td>
</tr>
<tr>
<td>– Review the current processes and procedures that govern the change management</td>
<td>validations should be conducted.</td>
</tr>
<tr>
<td>process for the transaction monitoring model &amp; make recommendations for potential</td>
<td>– Governance policies and procedures for model risk management clearly delineating</td>
</tr>
<tr>
<td>improvements based on industry practices.</td>
<td>authorities and controls, as well as standard re-validation cycles.</td>
</tr>
<tr>
<td></td>
<td>– Identify key trigger events &amp; stability metrics to specify conditions when re-</td>
</tr>
<tr>
<td></td>
<td>validations should be conducted.</td>
</tr>
</tbody>
</table>
Other Things to Consider

- Case Investigation, Escalation, and Alert Triage processes may also be subject to “validation”
  - Statistical tests/evaluations of potential biases in the resolution of cases
  - Analysis and validation of alert triage and scoring models used for case prioritization or case closure.
Part One- Program Efficiency Review

- Evaluate rules, thresholds, filtering criteria, & parameters used to generate reports (manually or to generate alerts), to ensure they are reflective of the client’s risks.
- Review parameters & reports to eliminate redundancies & increase synergies between the different reports.
- Determine whether Client has documented & is able to explain rationale behind existing rules & thresholds, & that filtering criteria & parameters are reflective of risk.
- Provide recommendations on optimization of rules & documentation of respective rationales to ensure effective monitoring going forward based on the client’s risk profile.
- Evaluate all management reports designed to measure the effectiveness of specific rules.
- Provide recommendations where appropriate.
Part Two- Data Validation

- Obtain overview of core banking systems & transaction activity to understand institutions business & systems feeding into software
- Cross check Transaction Code lists in software to institution lists
- Obtain sample accounts & data to be validated
- Transaction Testing comparison between data importing into software & original data sources
- Review existing data integrity tests performed by Client that would validate that relevant customer, transaction, other data elements are being captured by software. Evaluate the scope & frequency of existing reconciliation tests to ensure accuracy & completeness.
- Ascertain controls are in place to ensure appropriate access to software
- Report each exception including recommendations where appropriate
Other Things to Consider

- It makes sense!
  - More rigorous evaluation of systems/models leads to:
    - Better risk management
    - Better decisions
Garbage in Data Management System Bad Decisions

Accurate Data in Data Management System Good Decisions
Data Validation

- You rely on the data in your reports to help you detect suspicious activity
- Important to ensure you are not missing significant data in your monitoring reports
- And that your information is accurate
- You never want your examiners to find suspicious activity that you missed!
2 Types of Data Validation

- Daily
- Annual or other periodic basis
Daily Data Validation

- What will you validate?
- What dollar amounts?
- Risk Based Decision
- Document your procedures
- *Will you really miss identifying suspicious activity if that $22 item is not researched and validated?*
Annual Data Validation

- On at least an annual basis, perform a more comprehensive data validation that includes trancodes, verifying mapping of critical information and transaction testing.
The Real Risk is doing Nothing.......
Data Validation—Consultant’s Viewpoint

Robert Casares, CAMS
Managing Director
SentryNet, LLC
Rcasares@sentrynetllc.com
When to consider a Data Validation

- Core System Changes
  - Significant Core upgrade
  - Change to one or all data feeds
- Acquisitions
  - Converting new bank data on to bank’s existing platform
- Other Significant events
- Annually
  - Examiner recommended
  - Peace of mind
- All warrant validation of Core and AML data
Data Validation Approach

1. Obtain overview of core banking systems & transaction activity to understand institutions business & systems feeding into software
   - FIS
   - Jack Henry
   - Fiserv
   - Harland (D+H)
   - Mom & Pop solutions –
Data Validation Approach

2. Obtain overview of banks AML system
   - Yellow Hammer (Jack Henry)
   - Patriot Officer (Global Vision)
   - BAM + (Bankers Toolbox)
   - NICE Actimize
   - AML Manager (Fiserv)
   - Verafin -
Data Validation Approach

3. Obtain overview of banks Data Feeds
   - Teller
   - ATM
   - ACH
   - RDC
   - Wires (Domestic & International)
   - Monetary Instruments -
What I Need from You

System Access:

◦ Access to AML system – Administrator Level
◦ Access to Core Banking System
What I Need from You

Pertinent Core Information:

- List of Product Codes & Descriptions (Loans and Deposits) – from the Core
- List of Accounts Type Codes & Descriptions – from the Core
- List of Transaction Codes & Descriptions, including the Teller System transaction codes – from the Core
- List of all Country Codes & Descriptions – from the Core
- List of all TIN Codes used in the Core. Any codes being used to identify NRAs as well.
- List of BSA Risk Codes populated at Account Opening and stored in the Core.
- List of all Exempt Accounts (Name, Account Number, Date of Exemption). -
What I Need from You

Pertinent Account & Transaction Information:

- Wire source documents (Incoming & Outgoing) for 5 days. If using Fedline or a correspondent bank, a report (or excel spreadsheet) of wires will be sufficient. If using a different channel/correspondent for foreign wires, please include them in the population. The report should list all fields and their contents.

- List of 5 accounts for each of the following categories (Name, Account Number, TIN/SSN, Account Type/Product Type). Need either a full statement or access to the system to view the statement. Need CIS record for each account and signer, or access to the system to review the owner/signer records. Personal Checking Account
  - Business Checking Account (can include NOW)
  - Personal Savings/MMDA Account
  - Business Savings/MMDA Account
  - Personal CD/IRA
  - Business CD
  - Personal Loan
  - Business Loan -
What I Need from You

Pertinent Account & Transaction Information:

- Incoming ACH report, listing all incoming ACH transactions, account number, amount, transaction date, transaction description, SEC code)
- Incoming IAT (transaction date, account number, amount, description, SEC code) – rec’d. Run IAT in AML System.
- ATM settlement report (account type, account number, transaction date, amount, description)
- Teller cash transaction report (transaction date, account number affected, amount, description, teller, branch, transaction code).
- Monetary Instrument report – from Teller system or source system (transaction date, amount, source account number, transaction code, description, payer/payee). This is not the MIL for BSA purposes, but the record of all monetary instruments sold and redeemed.
- CTR candidate/suspect report, from the Core system/Teller system (the system and reports that you rely upon to determine CTR reporting candidates)
- Closed account report (most current report) -
What do I Validate?

**Codes and Tables**
- Transaction Codes
- Business Type Codes (NAICS)
- Product Codes
- TIN Codes
- Country Codes
- CTR Exemptions

**CIS**
Compare CIS Information in Core to Data captured in software for:
- CIS #
- TIN
- Name and Signers
- Account Number
- Account Type
- Open/Closed Date

**Transactions**
Compare Transaction Data in Core to data captured in software for:
- Tran Dates
- Tran Type
- Tran Amounts
- Descriptions
- Matching
Other Transaction Testing

- Do at least a 2-3 day comparison
- Are variances acceptable for risk

**Source Data**

<table>
<thead>
<tr>
<th>Date</th>
<th>Transaction Type</th>
<th>#</th>
</tr>
</thead>
<tbody>
<tr>
<td>12/21/13</td>
<td>Cash</td>
<td>795</td>
</tr>
<tr>
<td>12/21/13</td>
<td>Wire</td>
<td>341</td>
</tr>
<tr>
<td>12/21/13</td>
<td>ACH</td>
<td>21,923</td>
</tr>
<tr>
<td>12/21/13</td>
<td>ATM</td>
<td>5,904</td>
</tr>
<tr>
<td>12/21/13</td>
<td>Monetary Instruments</td>
<td>33</td>
</tr>
</tbody>
</table>

**Software Data**

<table>
<thead>
<tr>
<th>Date</th>
<th>Transaction Type</th>
<th>#</th>
</tr>
</thead>
<tbody>
<tr>
<td>12/21/13</td>
<td>Cash</td>
<td>793</td>
</tr>
<tr>
<td>12/21/13</td>
<td>Wire</td>
<td>341</td>
</tr>
<tr>
<td>12/21/13</td>
<td>ACH</td>
<td>21,910</td>
</tr>
<tr>
<td>12/21/13</td>
<td>ATM</td>
<td>5,899</td>
</tr>
<tr>
<td>12/21/13</td>
<td>Monetary Instruments</td>
<td>33</td>
</tr>
</tbody>
</table>
What I Typically Find

- Number of files imported from core system doesn’t match with what’s imported into AML system
- Missing or improperly coded tran codes
- Excessive non-posted items that don’t properly validate in AML system
- Lack of address or country information in wires.
- Incomplete IAT information deriving from core system -
Help Me Help You

- Report issues as I go
- Allows for you to correct problems or issues while on-site
- Make recommendations that may require attention from product vendor or core processor
- Sum everything up in a comprehensive report along with supporting documentation
Data Validation
The Financial Institution’s Viewpoint

Myrna Olvera, CAMS
Senior Vice President & Operations Risk Manager
City National Bank
myrna.olvera@cnb.com
Who, Where & Whom do we Serve
Our Early Beginnings

City National Bank is California’s Premier Private and Business Bank\textsuperscript{SM}, providing entrepreneurs and professionals, their businesses and their families with complete financial solutions on \textit{The way up\textsuperscript{®}}.

Serving successful entrepreneurs and professionals since 1954
Where We Are

$30.8 Billion in Assets

- 77 offices, including 16 full-service regional centers
- 11 California counties from San Diego to San Francisco
- Four Nevada counties from Las Vegas to Reno
- Expanded private and commercial banking capabilities in New York City
- New Nashville and Atlanta offices to better serve the music industry
- New Daytona Beach office to support Motorsport Industry - NASCAR
Who We Serve

Understanding the unique needs of...

- Manufacturers
- Non-Profits
- Professional Firms
- Apparel
- Real Estate
- Affluent Individuals
- Restaurants & Franchises
- Importers & Exporters
- Entrepreneurs
- Agriculture
- Technology
- Entertainment
- Distributors
Managing Data

All of our data is grossly inaccurate... but I need data in order to manage.

If I concentrate hard enough I can forget that the data is bad, then I can use it.

I have to give him credit; managing is harder than it looks.
Case Study

- Getting Started
- Request for Proposal
- Model Assessment
- Data Validation
- Scope of Work
- Reports
- Action Plan
Request For Proposal

- Describe the work
- Site regulatory guidance
- Describe your organization and responsibilities
- Identify system and modules – description
- Additional software or tools
- Extra conditions, dependencies or the use of advisory services
- Vendors invited to participate in a conference call
Scope of Services

- Key Activities
- Conduct interviews with model owners
- Review data and process
- Model assumptions
- Model sensitivity, performance and stability test results
- Sample review of the data structure and documentation
- Spot check of data quality and data completeness
- Sample AML vendor’s data tables for comparison to source system
- Sample AML rules thresholds and compare to customer account activity
- Identify sample accounts and clients meeting AML rule alerting criteria and verify generation of system alerts
- Verify key data inputs align with institutional risk considerations
- Model change control process and permissions
- Perform and verify model development calculations
- Code associated with quantitative modelling processes
Prepare for Independent Review

Involve the appropriate colleagues – IT, H.R.

Background check for consultants

Setup PC and/or internet connections, system access

How to transmit sensitive data

Collect and assemble relevant documentation

Set up Kick-off and subsequent meetings

Communicate frequently, ask questions, clarify the observations

BE FLEXIBLE!!!
Model Assessment

- Conceptual Soundness
  - Documentation and testing
  - Qualitative and judgmental assessments

- Documented methodology of model choices

- Risk Assessment – Products/Services Coverage

- Plan for using results of quantitative testing
Data Validation

- Pre-Designed Test Scripts
- Transaction Code Mapping
- Sampled Data – transaction types, dates
- Transaction Coverage – Reconciled from AML to Core Systems
- Transactional Activity – Record count matches, check data to source system
- Description – expected results vs. actual results
System Validation

Testing includes validation of the following:

- Data completeness – data field populated correctly, source type and NULL values
- Data Integrity – sample period, transaction types reflected in right columns, negative values and nonsensical values
- Data Security

- Validate that system monitoring and interfaces are functioning appropriately as configured
Results

- Executive Summary
- Overview – model, validations, summary findings
- Conceptual Soundness and Development Evidence – validation work, observations, findings, key assumptions and data inputs
- Model Implementation – overview & Technology Platform Security & Control
- Outcomes Analysis and Ongoing Monitoring
- Appendix
Lessons Learned

Documentation, Documentation, Documentation?
- Right documentation includes methodology, assumptions and quantitative analysis to support decisions (out-of-box parameters)
- Written policies and procedures (wiggle room)

Risk Assessment Matrix to include all products/services to determine AML monitoring coverage

Colleague(s) with sufficient knowledge of AML System

This is a journey with continuous process improvement along the way...
Communicate, communicate and communicate
Teach, train and solicit feedback from end-users
Know your client data
Learn the terminology
Understand the risks
Setup an internal process to capture new product/service transactions
Test, test and test before making changes
Controls in place for parameter changes
Decision alerts in a timely manner
Consistency in alert review and analysis
Data Validation Examiner/Regulator Expectations

Elizabeth Slim, CAMS
Senior Vice President/BSA Officer
1st Enterprise Bank
Regulators Expectations and Review...

2 Rationales that alert settings are too low:

1. Percentage of auto/closed alerts exceeds 50%, is an indication the system is not generating meaningful alerts.

2. Percentage of alerts being escalated or cases being opened for further investigations is low indicates analysts are spending too much time reviewing meaningless alerts.
Regulators Expectations and Review...Validate Alert Settings

- Test if alert settings are set too high
  - Establish baseline: current alerts setting and number of alerts generated.
  - Review frequency of occurrence threshold and dollar amount threshold for each alert (# of alerts generated)
Regulators Expectations and Review...Validate Alert Settings

When each threshold setting is changed, it changes the number of alerts generated (in both dollar & frequency alerts).

- Lower threshold setting:
  - Will increase number of alerts
  - Must review additional new alerts generated (are alerts meaningful?)
  - If no meaningful alerts in the new review sample, it means that your alert threshold was set too high.
Regulators Expectations and Review...Validate Alert Settings

When each threshold setting is changed, it changes the number of alerts generated (in both dollar & frequency alerts).

- Increase threshold setting:
  - Will decrease number of alerts
  - Review the alerts that are dropped from the baseline population.
  - If no meaningful alerts in the review sample of dropped alerts, keep increasing the threshold setting upward until you find a meaningful alert in the new review sample to establish new threshold.
Regulators Expectations and Review…Alert Analytics Report

- Alert Management Analytic Report should be reviewed in conducting quality control and will indicate the following:
  - Number of times each alert is triggered
  - Number of each type of alert resulting in auto-closed
  - Number of each type of alert that is suppressed
  - Percentage of each type of alert that is being escalated or a case is opened for further investigations
  - Aging of alerts being worked in terms of work days
  - Work efficiency of each analyst based on number of alerts he/she reviews
Regulators Expectations and Review...

- A bank’s automated AML program system should be independently validated:
  - every one or two years
  - when there is a significant change in operations or merger or acquisition
  - to ensure alerts covers all products, services and activities
If alert threshold settings are adjusted on an ongoing basis, management should implement some type of quality control process in between validation cycles to ensure that settings are properly set.

- Document threshold setting process to justify decisions made
THANK YOU