Model Validations “Demystified”

JUNE 2017

Presented by Southern California Chapter Board Members:
Maleka Ali, Arc-Serv, LLC
Melissa Triplett, Pacific Western Bank
Special Guest: Eric Holmquist, Managing Director-FIS
OCC 2011-12
Guidance on Model Risk

FFIEC BSA/AML Examination Manual
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
Current Environment
Changes the Game
New Reality:

Comptroller of the Currency Thomas J. Curry in speech to Institute of International Bankers:

- Focused extensively on BSA/AML compliance and highlighted bank regulators’ increased focus on BSA/AML compliance

Deputy Attorney General Sally Yates, ”Individual Accountability for Corporate Wrongdoing” (“the Yates Memorandum”).

- Expanded the threat of civil enforcement and civil penalties against individuals

Benjamin Lawsky, Former Superintendent of New York’s Financial Services Department (DFS):

- Bank executives should attest to adequacy of their institutions’ BSA/AML monitoring systems
Next Steps for Institutions

- Examiners taking aggressive approach
  - Review & enhance existing programs to ensure they are reasonably designed and risk-based
- Reviews should consider:
  - Gap analysis
  - Updated risk assessment
  - Enhanced documentation
  - Further testing & validation
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
- Exclusion of Customers, Products, Services
Optimization/Tuning

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
Risk Based Approach

Can I catch everything?
Garbage in Data Management System Bad Decisions

Accurate Data in Data Management System Good Decisions
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
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
The Risk of Models

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

- Information/Input
- Processing
- Reporting
Components of Model Validation

1. **Conceptual Soundness**
   - Model logic properly accounts for the risk

2. **Syntax Validation**
   - Code captures data without errors and is testable through replication or control data

3. **Data Quality & Integrity**
   - Data accurately passes to monitoring platform

4. **Model Performance**
   - Model performs as intended

5. **Validation & Sustainability**
   - Proper governance in place to manage approval process and changes
What is enough?

- Not all institutions are the same
- Just like your BSA program- your validation should also be risk based
3 Main Components to BSA Model Validation

- Program Efficiency Review
- Data Integrity Validation
- Rule/Algorithm Testing
Program Efficiency Review

Evaluate/identify filtering criteria most appropriate for your institution

“Is the filtering criteria sufficient for the risk level of the institution”
Program Efficiency Reviews

Are they using the software correctly?

—

Are they finding suspicious activity?

- Automation brings powerful tools, but are they turned on?
- Recognition of evolving crime trends?
Optimization/Tuning

**Meaningful investigations**

A “meaningful” investigation could result in a “no-SAR” decision

When is a Rule/Scenario Effective?

All alerts need not result in an investigation

Effectiveness & investigation differ based on intended purpose of scenario
Program Efficiency Review

Review & test

Focus on specific filters

Understanding how system works is critical
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.
Common Findings

- Default Settings
- No below/above the line testing
- Lack of documentation
- No evidence of validation
- Exclusion of customers, products, services
- Unsupported Sampling Methodology
- Validator really doesn’t understand tools
What is Data Integrity Validation?

Data Validation is a critical step in the use of software applications.
Data Validation

- You rely on data in systems to help you detect suspicious activity.
- Important to ensure you are not missing significant data.
- And that information is accurate.
- You never want your examiners to find suspicious activity that you missed!
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?
Periodic 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.
Common data Problems

- NAICS codes-Business Type
- Tin Codes
- Non Resident aliens
- Signer information
- Relationship codes
- Beneficiaries
- Employees
- Missing data
Critical Data Missing

Common Missing Data

- International wires
- Activity to Loans/Certificates
- Monetary instrument Sales
Timing.....Is Annual Enough

- Core System Changes
- Acquiring New Organizations
- Other Significant events

Certain Events May Require Re-Validation of Information
What To Validate?

**Codes and Tables**
- Validate information for:
  - Transactions
  - Products
  - 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
  - Open/Closed Date

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

Do the rules work as designed?
Working with your Data Companies

- In all aspects of risk management and compliance there is one central common denominator that is always present …

- It’s Data! But not just any type of Data

- It’s Data that is identifiable, reliable, easily sourced, normalized and can be aggregated

- Good Data governance and management establish the foundational elements to ensure the data an organization utilizes is accurate and complete
  - Staging Area / Data Warehouse
  - Data Quality Rules
  - Exception Reporting
  - Data Steward at 1st and 2nd line

- BSA/AML solutions rely on good, reliable data to produce actionable and informative information to help organizations to reduce BSA/AML related risks
Basic Elements

- A comprehensive data schema to identify the data flowing into the BSA/AML solution along with the outputs (i.e. Alerts, MIS, etc.)

- The schema needs to be updated consistently as the bank changes and evolves

- A test environment may be requested from the system provider as it takes the burden off using the production system and allows for the use of simulated data as part of the Model Validation
Working with System Provider to resolve issues / problems

• Establish a point of contact within the Bank and the vendor at the outset of the model validation

• Make them aware that a validation is taking place and that you will require their assistance

• They may say a validation is not necessary, but more and more they begin to understand the difference between system validation and model validation

• Involve the vendor on status update calls with the client, so they can hear the issue/bug first hand and begin working on solutions

• Keep following up with the vendor until the issue is resolved

• Once resolved, issues/bugs need to be retested as part of a 2\textsuperscript{nd} iteration Model Validation exercise
Responses & Remediation on Findings

- Comments and Recommendations
  - Their point of view
  - Recommendations may not be feasible to implement due to
    - Lack of data
    - System capabilities
    - Lack of resources
- Avoid redundancy
- Meaningful
- Sometimes you DO know your customer best
- Risk Based
Real Risk is doing Nothing.
THANK YOU QUESTIONS?

Copies of this presentation will be available on our ACAMS Chapter page
In addition to the ACAMS Chapter Webpage you can also find us on LinkedIn at
http://www.linkedin.com/groups?gid=2202988&trk=myg_ugrp_ovr
Follow us on Twitter @ACAMSOCAL
Feel free to send any suggestions or comments to:
  socalacams@yahoo.com