Model Validation for Community Bankers

What a Model Validation is and How to Take a Risk Based Approach

A Banker's Toolbox White Paper
December 2014

What Will We Cover?

A Table of Contents

- Parts of a Model Validation **|** pg. 3-4
- Program Evaluations **|** pg. 5-7
- Types of Data Validation **|** pg. 8-9
- Risk Based Validation **|** pg. 10-14
- Components of Model Validation **|** pg. 15-16
- Examiner Opinions **|** pg. 17-18

Parts of a Model Validation

There are two parts to a Model Validation: Program Efficiency Review and Data Validation.

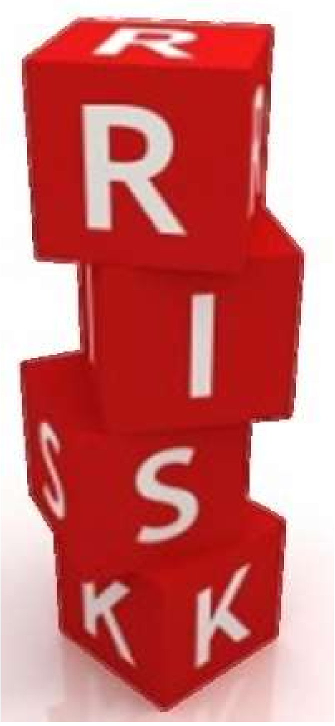
The first part of a Model Validation is a Model Program Efficiency Review, also referred to as Program Tuning, Model Evaluation, or Program Evaluation. During this process, you will:

- Evaluate your rules, thresholds, filtering criteria, and parameters used to generate reports (manually or through alerts) to ensure they are reflective of your institutions risks.

- Review your parameters and reports to eliminate redundancies and increase synergies between the different reports.

- Determine whether you have documented and are able to explain rationale behind your existing rules and thresholds, and that filtering criteria and parameters are reflective of your institutions risk.

- Evaluate all management reports designed to measure the effectiveness of specific rules.



Parts of a Model Validation

The second part of a Model Validation is the Data Validation.

During this process, you will:

- Overview your core banking system and transaction activity to understand your institution’s business and systems feeding into software.
- Cross check your transaction code lists in your software to your financial institution’s list.
- Transaction testing comparison between data importing into software and original data sources.
- Review existing data integrity tests performed by your institution that would validate that relevant customer, transaction, other data elements are being captured by software. Evaluate the scope and frequency of existing reconciliation tests to ensure accuracy and completeness.
- Determine controls are in place to ensure appropriate access to software.

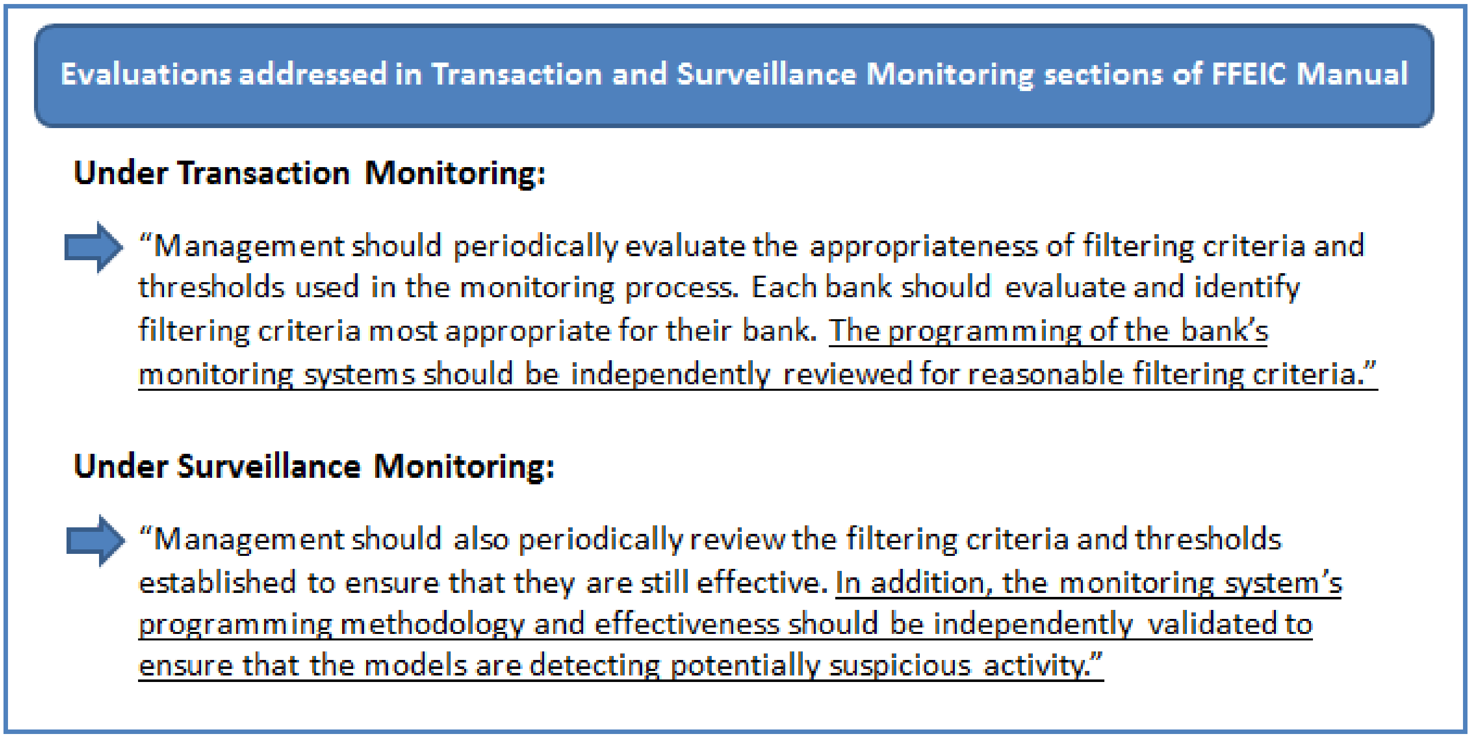
While this might seem overwhelming, the real risk is not doing anything. Though you will find that you are not being expected to have a data validation completed regularly, many institutions are doing these proactively. There could be critical flaws in your model that might go undetected until the examiners arrive.

Program Evaluation

Program Evaluations are addressed in both the transaction and surveillance monitoring sections of the FFIEC Exam manual. Both sections state that the management of your institution should periodically evaluate the filtering criteria and thresholds of your program to determine whether or not they are still appropriate. The manual also states that these should also be independently reviewed.

If you have an internal audit department that is autonomous from your BSA department, this could be considered independent. Make sure they receive training on your system so they understand the capabilities. If you do not have an independent internal auditor, you will have to look outside of your institution for someone who also has knowledge of the mechanisms and capabilities of your software and your system.

Automation brings you powerful tools, but must be used properly to be most helpful to you. Then again, even if you are using it efficiently, ask yourself: have the rules of your system been kept up-to-date in recognition of evolving money-laundering patterns? Not only has your institution changed, but money laundering patterns and tools have also evolved over the last couple of years. Think about digital currency and marijuana businesses; these types of changes give money launderers the ability to expand their practices to new territories.



Evaluations addressed in Transaction and Surveillance Monitoring sections of FFEIC Manual

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

The ultimate goal is to determine if you are choosing the filtering criteria for both manual transactions and surveillance monitoring that is most appropriate for the risk at your institution. You are expected to review and test your system capabilities and thresholds on a periodic basis.

We recommend you do this on an annual basis to coincide with your risk assessment updates, but you might need to do it more frequently if you've had an acquisition, merger, conversion or any other major event at your institution, like opening a new branch. You need to focus on if the specific parameters or filters in place will actually be able to capture suspicious or unusual activity.

It is also vital that you regularly perform updates or enhancements your automation provider offers, and update your employee's system training regularly.

When you're evaluating filters, you need to consider your institutions higher risk products and services, customers, entities, and geographies; not only the geography where your institution is located, but also your customer's locations. Examiners are now putting emphasis on not only the geography of your customers, but also where your customer's customers are located.

The filters you use need to be based on what is reasonable and expected activity for each account type. Consider business versus consumer checking, or loans versus CDs. They are not all going to have the same expected activity, so the filters you use to monitor these accounts needs to take this into consideration.

Banker's Toolbox™

Program Evaluations

The OCC Model Guidance was originally drafted to evaluate the systems that banks use to model their credit risk, especially to articulate the elements of a sound program for effective management of risks that arise when using quantitative models in bank decision making.

Banks routinely use these models for many activities, including underwriting credit, valuing exposures, measuring risk, and determining capital and reserve adequacy. In recent years, banks have applied models to more complex products and with more ambitious scope, such as enterprise-wide risk measurement. Changes in regulation, particularly the new regulatory capital rules based on framework from the Basel Committee on Banking Supervision, have also spurred some of these developments. Practical application of this guidance should be based on the bank's risk exposures and business activities.

Now for BSA/AML, banks and credit unions should still continue to follow the guidance that is listed in the FFEIC exam manual. With that in mind, there is still good advice that we can apply and learn from the OCC guidance that can be carried over into how we view and analyze our particular BSA/AML programs, especially if we rely solely on surveillance systems to identify our suspicious activity.

> "Understanding the filters in your system and how your system works is critical to assessing the effectiveness of your monitoring program."

Types of Data Validation

Daily data validation is one of the two types of data validation you can choose to perform. Using this method, it is important to go into your system and look at your non-posts to ensure there are no failures to guarantee a high quality of imports. If you choose to perform a daily data validation, consider the following:

- What will you validate?
- What dollar amounts?
- Make sure it is a risk-based decision.
- Document your procedures and methodologies.

On at least an annual basis, you need to perform a more comprehensive data validation that includes trancodes, verifying mapping of critical information and transaction testing.

During an annual data validation, it is important that you review and verify that CIS and Account Level codes are being imported accurately, and that you validate your host system software for all product types available, including: Checking (DDA), Savings (SAV), Loans (LAS), and Certificates of Deposit (COD). It is recommended that this process be performed for five of each account types available in your database.

However, an annual data validation may not be enough. If your institution has a core system change, acquires a new organization, or experiences any other significant event, you might need to revalidate your information.

What do I 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:

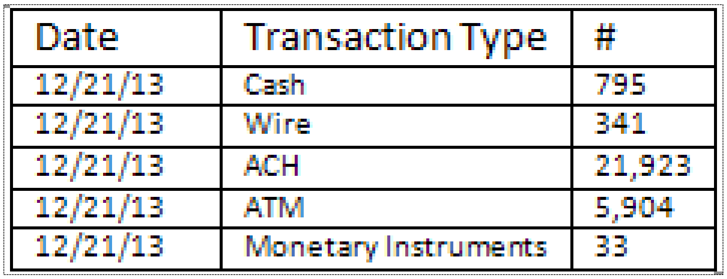
- **Tran Dates**
- **Tran Amounts**
- **Descriptions**
- **Matching**

Types of Data Validation

When you are looking at customer information, it is important to look at a broad spectrum of accounts. Make sure the accounts you choose to look at have a variety of transaction types, like ACH, ATM, MI, wire activity, etc.

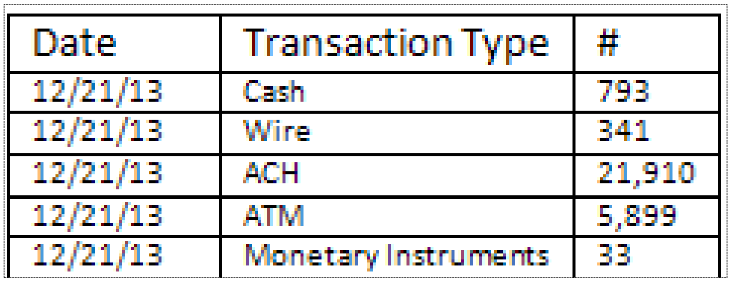
Do some overall number testing. If you have not been concerned with validating small items, you are not going to get a perfect match all the time between your source data and your software data. Perform a two or three day comparison. Look at the source and see how many came into the software. Ask yourself: is the variance acceptable for the risk at your institution?

Source Data



Date	Transaction Type	#
12/21/13	Cash	795
12/21/13	Wire	341
12/21/13	ACH	21,923
12/21/13	ATM	5,904
12/21/13	Monetary Instruments	33

Software Data



Date	Transaction Type	#
12/21/13	Cash	793
12/21/13	Wire	341
12/21/13	ACH	21,910
12/21/13	ATM	5,899
12/21/13	Monetary Instruments	33

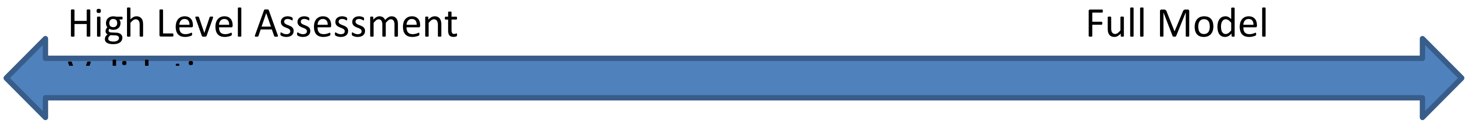
“Perform a two or three day comparison. Look at the source and see how many came into the software. Ask yourself: is the variance acceptable for the risk at your institution?”

Risk Based Validation

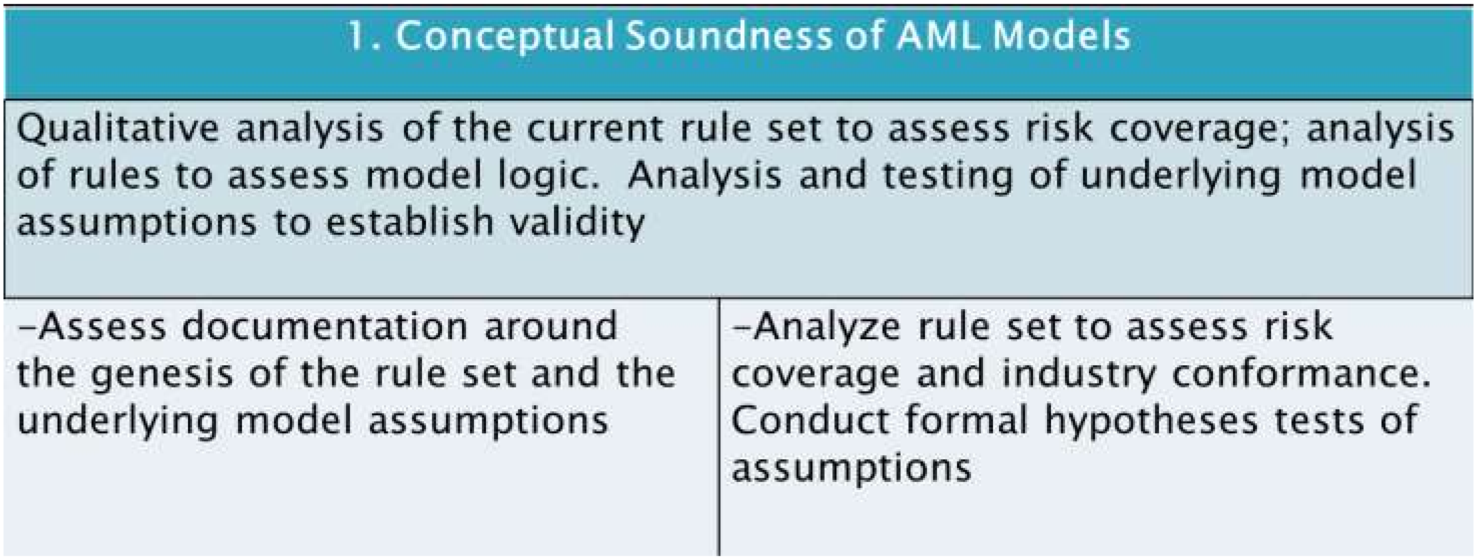
Just like your BSA program, your BSA program validation should also be risk-based. It's really unrealistic to expect to catch everything.

Take the different components of a model validation. Depending on your size, risk and complexities, instead of a full model validation, you might just need more of a high level assessment.

This would include looking at the soundness of your model. Instead of analyzing your rule set to assess risk coverage, industry conformance, and conduct formal hypotheses tests of assumptions, you may only need to assess documentation around the genesis of the rule set and determine whether or not that rule makes sense for your program. Take this approach throughout all of the different components of your model; think of your institution and think of what makes sense in all of the different areas.


High Level Assessment

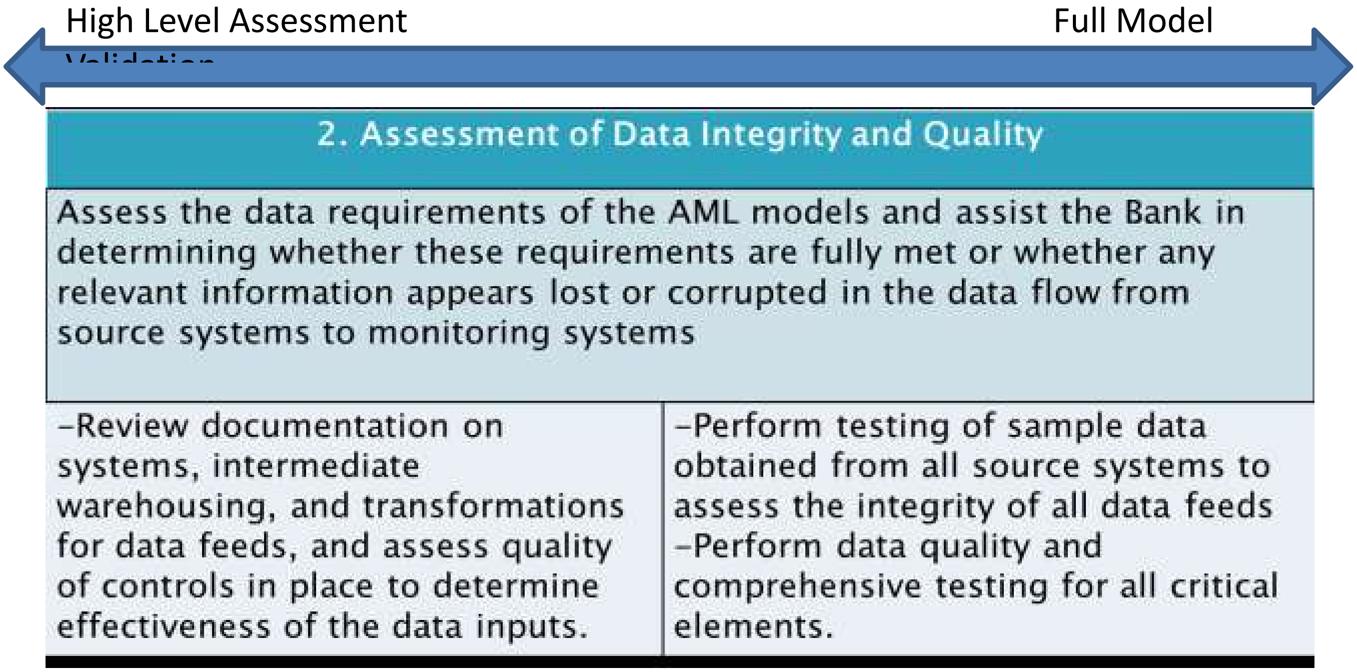
Full Model



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

Risk Based Validation

The second area where you need to assess is your data integrity and quality. Once again, you might have to do a full model validation depending on the risk and complexity of your institution, or you might want to consider doing a high level assessment. You do need to do something, whatever is appropriate for your institution.



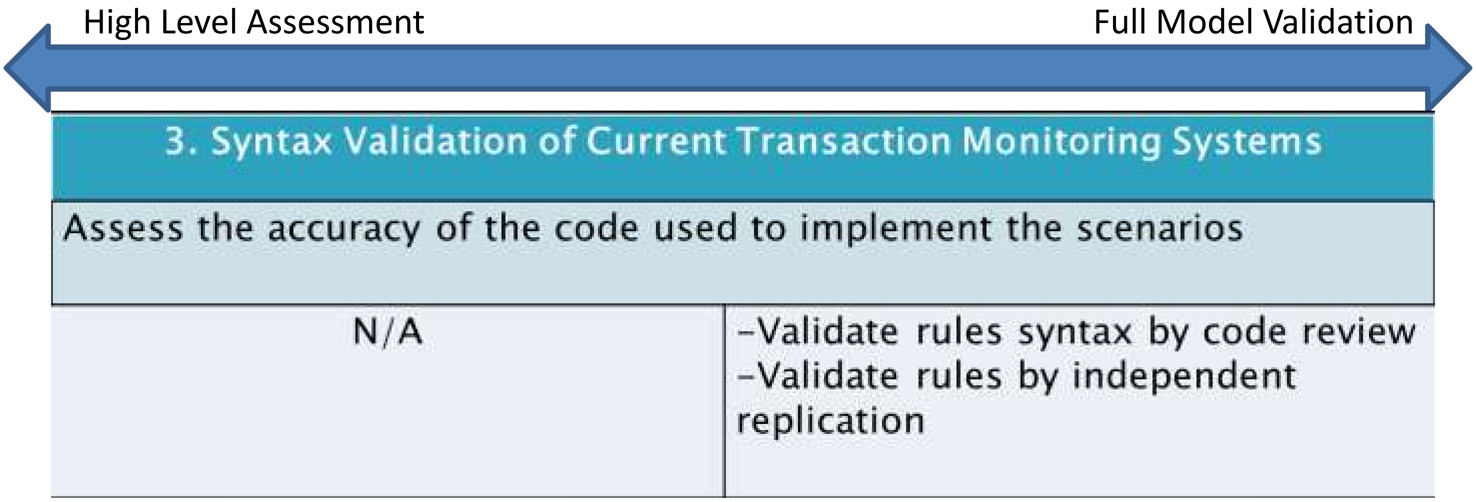
High Level Assessment

Full Model

Validation

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.

When you're reviewing the syntax of the code that was used to implement the scenarios and you write your own code, you need to validate rules syntax by code review. You would also need to validate rules by independent replication to make sure they work the way they were intended to work.



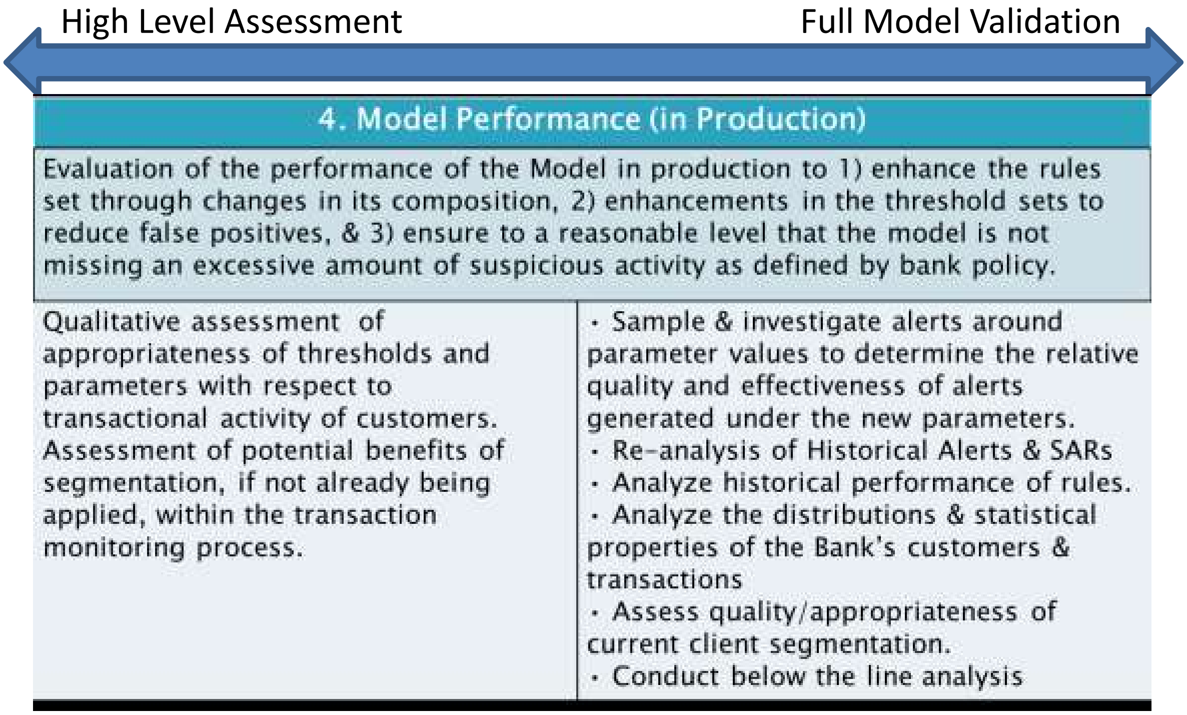
High Level Assessment

Full Model Validation

3. Syntax Validation of Current Transaction Monitoring Systems	
Assess the accuracy of the code used to implement the scenarios	
N/A	-Validate rules syntax by code review -Validate rules by independent replication

Risk Based Validation

When looking at the actual performance of the model, take the risk based approach and determine your approach based on the size and complexity of your institution.

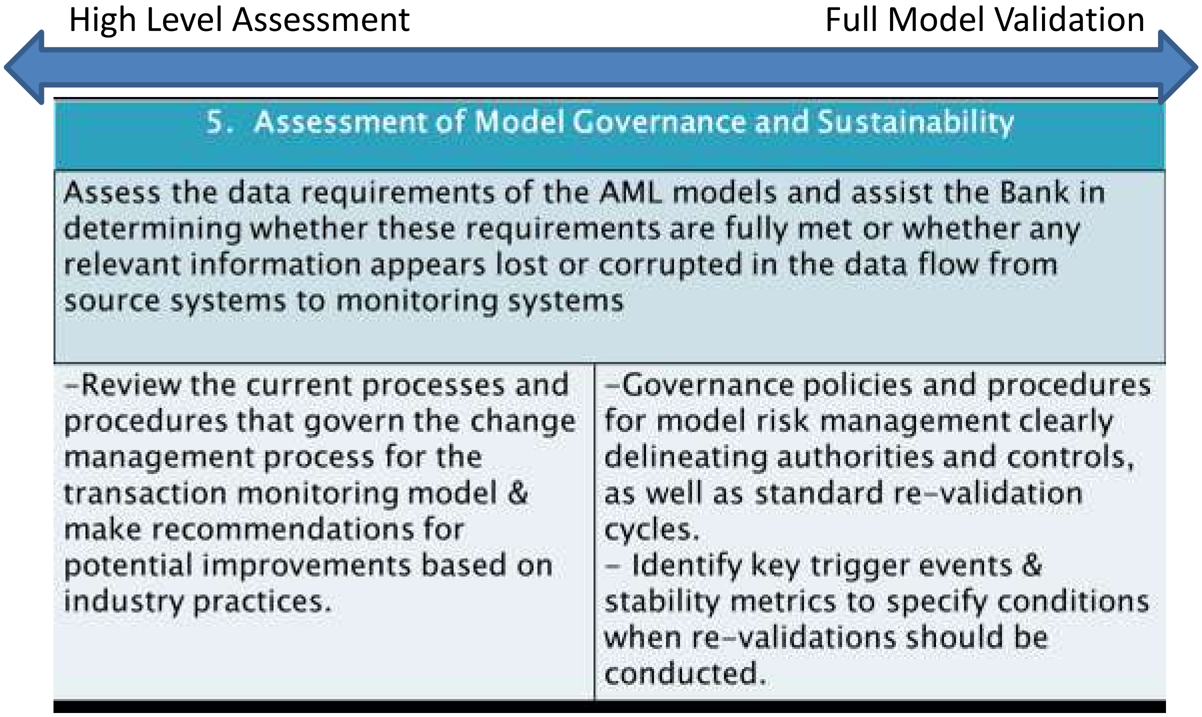


High Level Assessment

Full Model Validation

4. Model Performance (in Production)	
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, & 3) ensure to a reasonable level that the model is not missing an excessive amount of suspicious activity as defined by bank policy.	
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.	• Sample & investigate alerts around parameter values to determine the relative quality and effectiveness of alerts generated under the new parameters. • Re-analysis of Historical Alerts & SARs • Analyze historical performance of rules. • Analyze the distributions & statistical properties of the Bank's customers & transactions • Assess quality/appropriateness of current client segmentation. • Conduct below the line analysis

When looking at the management and governance of the entire program, think about how much fits the complexity of your institution. All of these areas can either be validated more deeply or they can be scaled back.



High Level Assessment

Full Model Validation

5. Assessment of Model Governance and Sustainability	
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 the current processes and procedures that govern the change management process for the transaction monitoring model & make recommendations for potential improvements based on industry practices.	–Governance policies and procedures for model risk management clearly delineating authorities and controls, as well as standard re-validation cycles. – Identify key trigger events & stability metrics to specify conditions when re-validations should be conducted.

Risk Based Validation

During the evaluation process, do not forget: examiners will also be look at your case management.

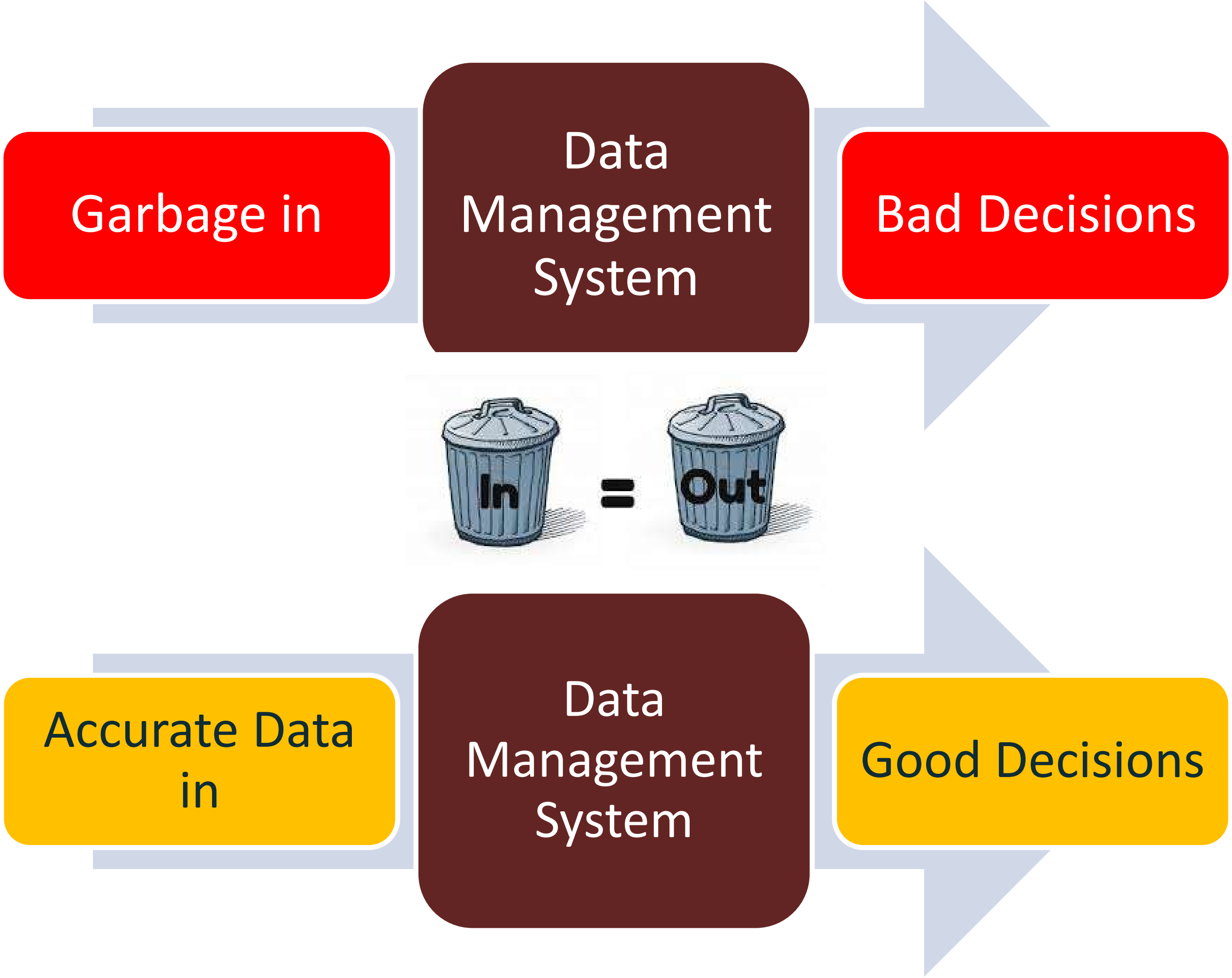
What are you processes for your case investigation, escalation, and alert triage? Are there any possible biases in the resolution of cases? Is anyone doing a random review, either monthly or quarterly, on some of your analysts' no-SAR decisions? Is there a reasonable process for alert triage or some way to prioritize your alerts to your cases, depending on the severity?

Statistical tests and evaluations of potential biases in the resolution of cases may be necessary and can be used to show your decision making process when resolving cases. Analysis and validation of alert triage and scoring models used for base prioritization or case closure may also be necessary.

"During the evaluation process, do not forget: examiners will also look at your case management."

Risk Based Validation

Your program models need to make sense in order to give you a better handle on your risk and make better decisions. It’s very important to remember: garbage in, garbage out. If you are getting garbage, you are going to make bad decisions. In order to make good, strong decisions, you need good data coming in.



Garbage in

Data Management System

Bad Decisions

Accurate Data in

Data Management System

Good Decisions

The important thing to remember is you rely on the data in your reports to help you detect suspicious activity. You want to make sure you are not missing significant data in your monitoring reports. You never want an examiner to find something significant that you’ve missed, so you need to ensure your information is accurate.

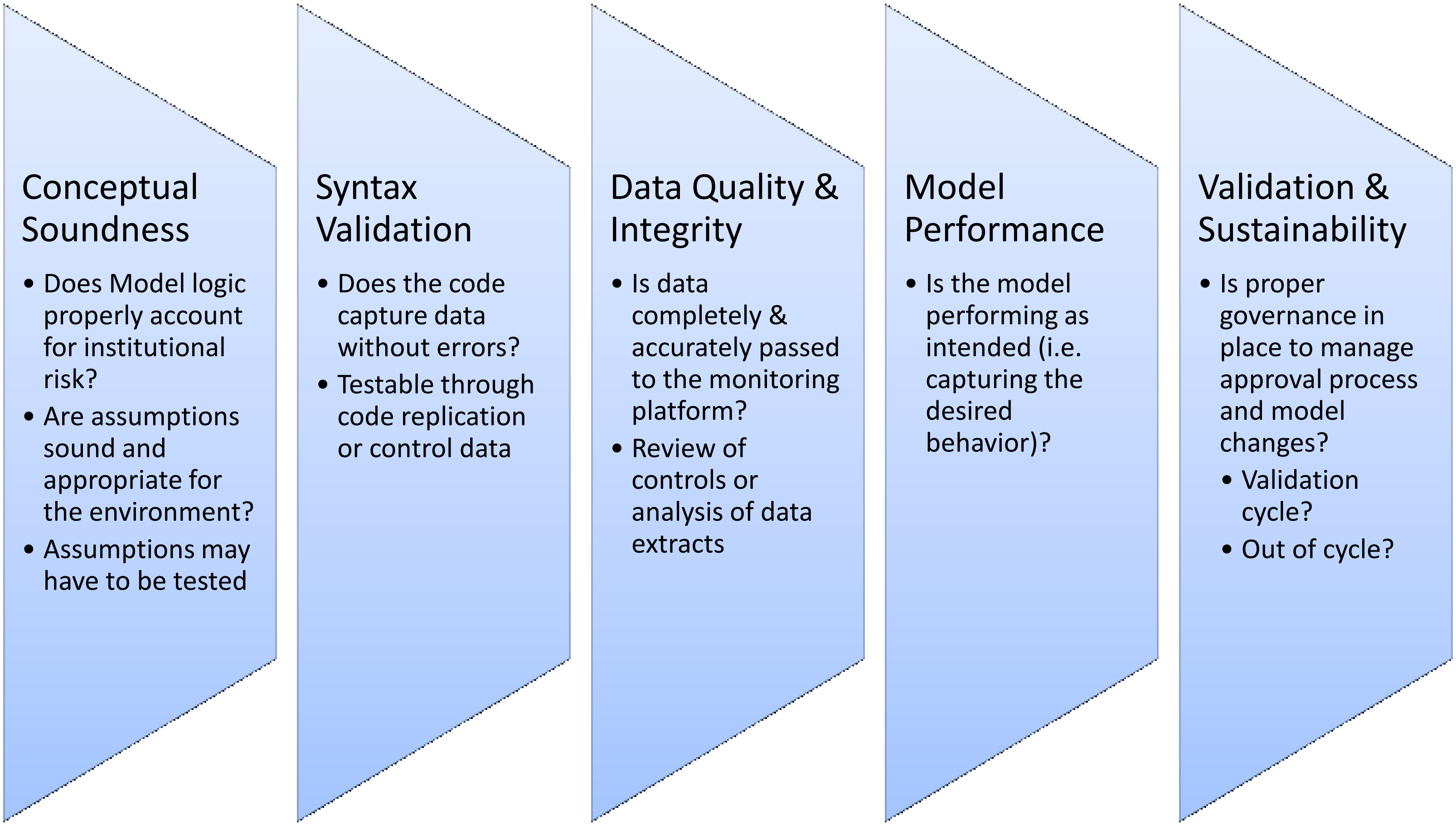
Components of Model Validation

A model is defined as a quantitative method, system or approach that applies statistical, economic, financial, mathematical theories, techniques and assumptions to process input data into quantitative estimates. This could actually apply to our BSA AML automated system.

The OCC Model Guidance points out that a model will have three components: information and input, the processing of that information, and the reporting that we use to analyze and look for suspicious activity.

It also discusses Model Governance. Model Governance includes the development of the BSA program, the implementation of the program, the actual use of the program, and finally the validation or audit of the processes.

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 the 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?

Components of Model Validation

When the OCC Model Guidance is talking about optimization and tuning, it is really asking, “Is the rule/scenario effective?” The effectiveness of the rule is measured by the production of a “meaningful” investigation. A meaningful investigation could result in a “no-SAR” decision, but the effectiveness will differ based on the purpose or intention of the rule.

Do not delete a rule just because you get fewer hits triggered by that rule than expected. It might be a rule that is particular to activity that is rare at your institution, but you need to keep it in place because, if it does happen, you want to make sure that particular activity is caught.

Define in your policy and procedures the person or persons who will have the authority to establish or change filters. Those changes need to require the approval of the BSA Officer or senior management at your institution. You must also document and be able to explain your filtering criteria, and how they are appropriate for the risk at your institution. It is important that you keep this documentation for your auditors, examiners, and for the evaluator of your program. They want to see this and rate this process to determine if it is working appropriately for your institution.

When the examiners come out, they are going to look closely at your system’s capabilities. What can it do and how are you using it? What rules or scenarios do you have available to use? If you are not using them all, why do you not use them? What type of activity do you have feeding into your system?

When developing your models, decide, “What is the risk?” Pull out your risk assessment and determine what type of criminal typologies are you susceptible to at your institution. Only then can you determine the rules and scenarios to put into place to help you identify those particular patterns.

Examiner Opinions

How well equipped are your processes, procedures and systems?

How are those tools working?

Are they being used correctly?

Are they making an impact?

Examiners are putting an emphasis on efficiency, which means they want to know how well equipped your program is to identify risk. What processes, procedures and systems are you using to locate suspicious activity? Are those tools working? Are you using them correctly? Are you using them to their full capacity? Are they even making an impact on finding and identifying suspicious activity?

The attention paid in the area of BSA/AML data validation is steadily increasing. Examiners are suggesting, and in many cases mandating, audits on BSA/AML activity monitoring systems to ensure the data feeding into your system is complete and accurately able to produce reliable alerts and reports of potential criminal activity. Data integrity from end-to-end is one concern, but there's more to the validation process.

Consider conducting an efficiency review and evaluation before an examiner visit to proactively catch issues beforehand. If your system isn't validated, it is harder to prove your program is justified, and you will likely receive criticisms from examiners. They want to see what you are doing with your system and how you are using it – because remember: no two financial institutions are exactly alike. They want to see what *you* have done with the system you have purchased.

Examiner Opinions

Model validation continues to be a challenging topic in the BSA world. In today's current environment, many financial institutions walk into their exams feeling confident, but walk out of their examine feeling bombarded. Examines are becoming more vigorous, and the expectations from the examiners conducting these exams are also intensifying.

While criticisms coming from examiners and auditors may vary, here are some we see often:

- **Use of Default Settings:** Examiners generally do not appreciate the use of default settings. Even if these settings seem appropriate for your institution, you still need to investigate further and determine if they are and document why or why not.
- **No Below/Above the Line Testing:** Examiners want to see if you are line testing. This is when you run "what if" type reports and scenarios to see what would happen if you raised or lowered your parameters. This can be the fine balance between missing suspicious activity and having so many hits you can't see the forest through the trees.
- **Lack of Insufficient Documentation Supporting Scenario Thresholds:** Examiners want to see documentation of the reasons for your changes and the methodology behind any statistical samples that you pull for setting your thresholds.
- **Exclusion of Customers, Products and Services:** Examiners do not want to find that you have excluded certain customers or products from monitoring without a reasonable explanation.
- **Scarce Evidence of Threshold Validation**
- **Unsupported Sampling Methodology**

At Banker’s Toolbox, we want to help those working at all financial institutions to create better BSA programs. We hope this paper shed light on how to conduct a successful Model Validation and will help you protect your financial institution and customers. If you have questions please do not hesitate to reach out to us at Experts@BankersToolbox.com.

Want to learn more?

Please visit http://www.bankerstoolbox.com/ConsultingServices to read a case study about Banker’s Toolbox consulting services helping a financial institution meet BSA/AML compliance standards. At Banker’s Toolbox, we retain a team of certified independent consultants who can perform an array of consulting services, including risk assessments, program evaluations and model validations. We are working to help you stop fraudsters, crooks, gangsters, human traffickers, drug dealers, terrorists and all those who would do us harm with the help of our independent consultants and through our industry leading fraud and AML detection solution, BAM+.

About Banker’s Toolbox

Austin, TX-based Banker's Toolbox, Inc. helps community financial institutions manage risk and streamline compliance examinations. The company's product suite consists of proven solutions for money laundering detection and reporting, risk management through fraud and kite prevention, secure wire processing automation, and commercial real estate loan portfolio risk assessment. The Banker's Toolbox team is a unique combination of seasoned bankers, former regulators, and information technology consultants who specialize in designing, developing, and implementing risk management solutions while providing unparalleled customer service. For more information, visit the company's website at www.bankerstoolbox.com.

Banker’s Toolbox™