Garbage In, Garbage Out?
Don’t Let That Be Your AML Solution

Stephen R. King, JD, AMLP

CBA Regulatory Compliance Conference

October 7, 2015

Today's Agenda

- Model Risk Management
- BSA Risk Assessment
- BSA/AML Software Utilization and Validation
- BSA System Optimization
- FinCEN Advisory
- Enforcement Actions

What is a Model?

A quantitative method, system, or approach that applies statistical, economic, financial, or mathematical theories, techniques and assumptions.

- These features are used to process input data into quantitative estimates

Models consist of three components:

- Information input
- Processing
- Reporting

Model Risk

The use of models presents “Model Risk”

- Inaccurate data outputs
- Incorrect or misuse of model outputs and reports
- Potential for adverse consequences
  - Regulatory Risk
  - Reputation risk
  - Financial loss

Model Risk Management

Model Risk must be managed to eliminate downfalls:

- Develop the model accordingly
- Implementation and control
- Establish limits on model use
- Monitor performance
- Adjust or revise parameters over time
- Supplement model results with other analysis or information

Model Development & Implementation

- Purpose/Use/Data Flow of the Model
- Limitations
- Testing
  - Incorporate actual data
  - Incorporate low, moderate, and high areas of risk
- Document and summarize the results

Model Validation & Independence

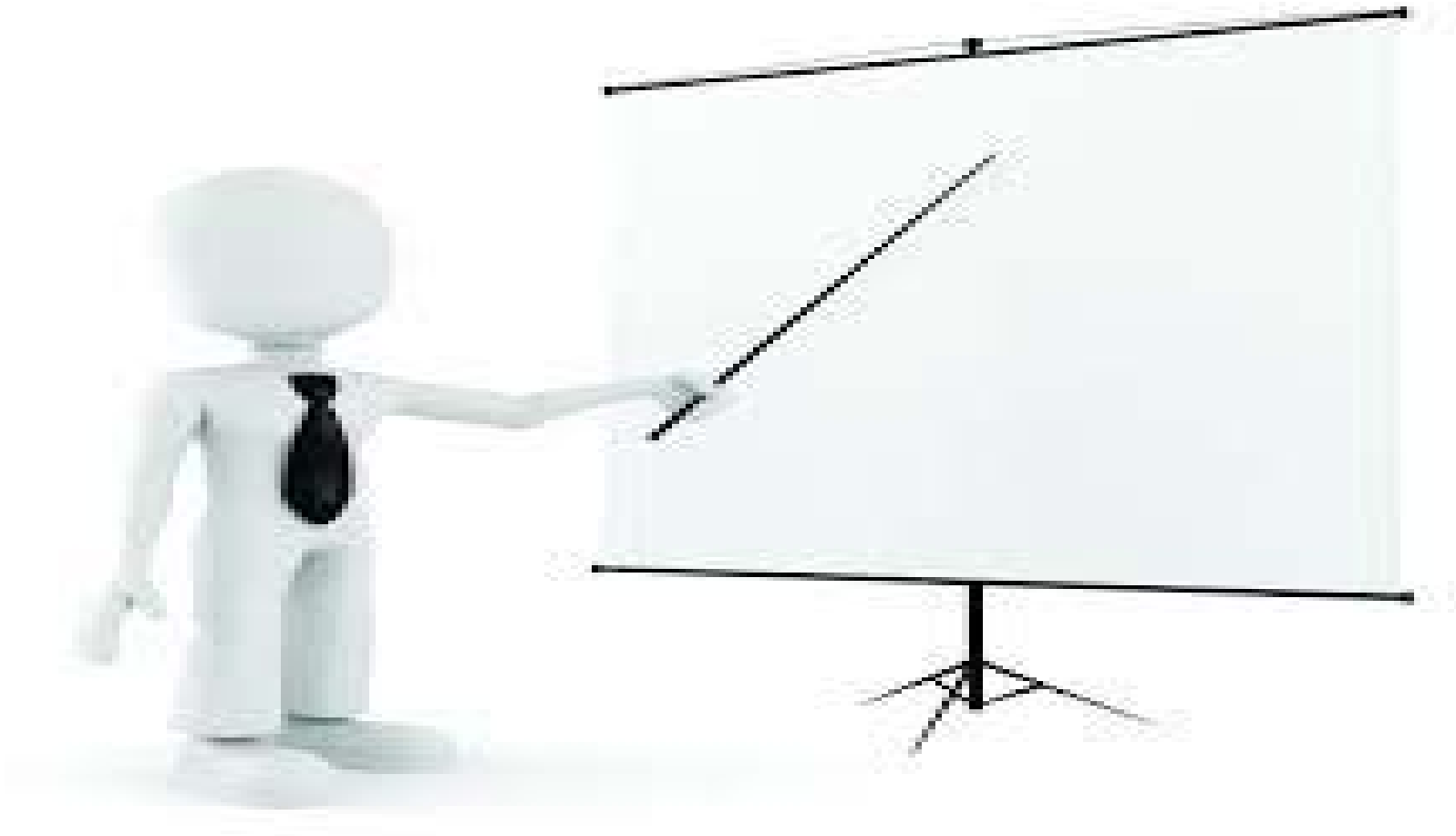
Set of processes and activities intended to verify that models are:

- Performing as expected
- Limitations have been identified & potential impact is known
- Model aligns with objectives and business use

Model data input, processing, and reporting should be subject to validation.

Actual validation must be performed by an independent party.

BSA Risk Assessment



BSA Risk Assessment

The FFIEC BSA Examination Manual requires institutions to create a Bank Secrecy Act/Anti-Money Laundering/OFAC risk assessment covering the institution's:

- Products and Services
- Customers and Entities
- Geographic Locations

BSA Risk Assessment

Structure:

1. Analysis of the Institution's products/services, customers/entities and geographic locations.
2. Identification of risks and the mitigating controls.
3. Statistical analysis culminating in risk ratings

The risk assessment should include appropriate documentation supporting the risk-based reasoning behind any dollar thresholds utilizes. Institutions should maintain back up documentation supporting their conclusions.

BSA Risk Assessment

Best Practices:

- The risk assessment should contain an overall rating for the BSA/AML and OFAC programs. Overall ratings for products/services, customers/entities and geography is also a good practice.
- The Risk Assessment should be presented to the Board for approval.

Areas where the Institution accepts the risk of not having certain controls in place should be included in the risk assessment so as to receive approval of accepting such risk from the Board.

BSA Risk Assessment

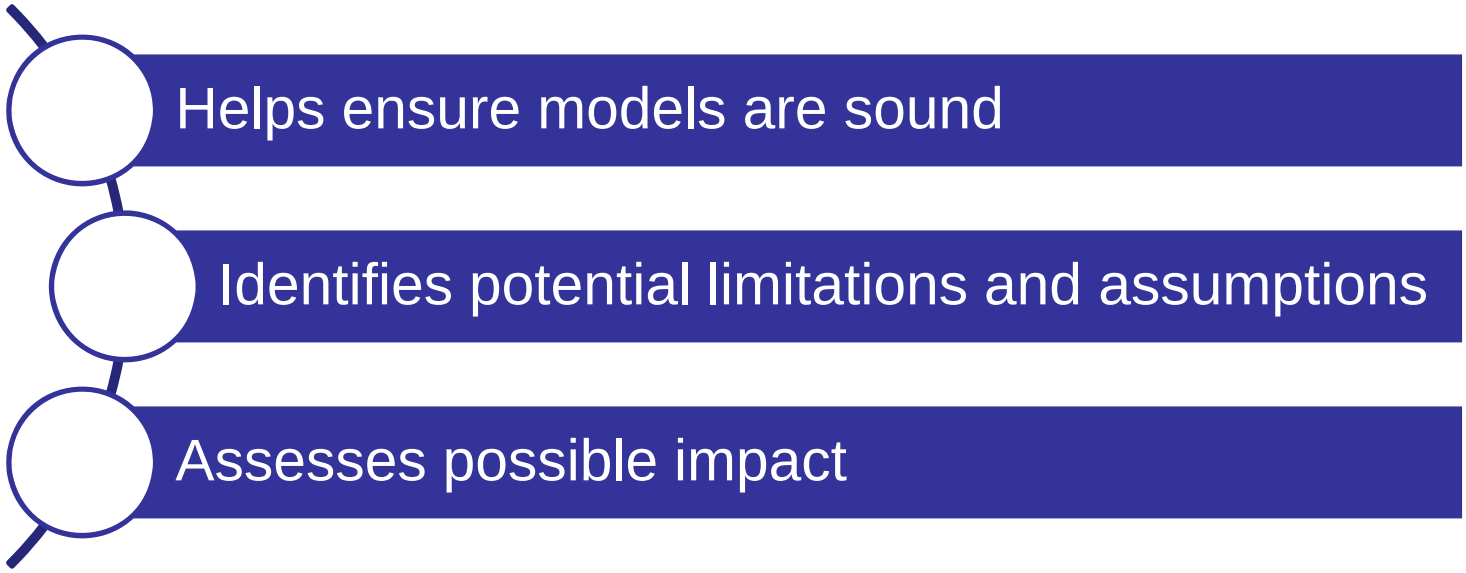
This risk assessment should be amended on at least an annual basis, or as major changes occur such as:

- New products and services
- Mergers or acquisitions
- New geographic areas
- New service providers
- New software
- Significant examination or audit findings

AML Software

Model Validation

Set of processes and activities intended to verify that models are performing as expected, in line with their design objectives and business uses.



Model Validation

Is model working efficiently?

User feedback and insight

Managers question methods and assumptions

Model functions well and reflects realities

Justifies assumptions and design

Model Validation

Validation requires degree of independence:

- Incentives aligned with goals of validation

- Staff must have:

System Validation - Responsibilities

- Initial Independent Validation
- Ongoing Change Monitoring
- Periodic Independent Validation

System Validation - Responsibilities

Where does the System Validation piece come from?

Appendix S: Key Suspicious Activity Monitoring Components

AML Software - Introduction

Many institutions have moved towards BSA Automated Software to assist in meeting their day to day BSA/AML/OFAC regulatory requirements.

There are various risks, expectations, controls and best practices that institutions should consider when implementing such software.

As with any other software or outsourcing utilized, the institution is still ultimately responsible for compliance.

AML Software - Introduction

Areas the Automated Software could impact include, but are not limited to:

- Suspicious Activity Monitoring
- Suspicious Activity Reports (“SARs”)
- Enhanced Due Diligence
- Currency Transaction Reporting (“CTRs”)
- CTR Exemptions
- 314(a) Request Lists
- OFAC
- Wire Transfers

AML Software - Structure

Automated Software often reviews customer activity by various means and identifies possible occurrences of suspicious activity, frequently referred to as “alerts”.

Similar to any suspicious activity that was manually identified, the institution has an obligation to review the activity to determine if a SAR filing is necessary.

How the Automated Software identifies these “alerts” is a key part of the software structure which should be understood by the institution.

AML Software - Structure

Automated Software is typically structured in one or both of these fashions:

Rules Based – Alerts are based on specific, often logic or activity based rules. When the criteria for that rule is met then an alert is generated.

Behavior Based – Alerts are based on specific customer behavior. Defined parameters exist for expected behavior (either overall or for specific customers) and alerts are generated when activity is outside such expected behavior.

AML Software - Structure

Rules Based System example:

- Customer is in business account type; **and**
- Customer is from HIDTA zip code (coded list in software); **and**
- More than 3 transactions between $8,000 - $10,000 take place in one month period

Alert is generated if all criteria are met

AML Software - Structure

Behavior Based System example:

- Expected activity for customer of specified type is $25,000 in currency per month; $50,000 is considered high
- Customer has $45,000 in activity during month, representing risk code of 95
- Bank's parameters are set to generate an alert for anything with a risk code of 50 or above

Alert is generated due to activity outside of expected behavior

AML Software - Structure

Based on the Automated Software, there may be times where the institution has to manually code risk ratings or figures that impact the risk rating. If this isn't done, the risk rating process can be adversely affected.

Examples:

- NAICS Codes
- Status as SAR suspect, 314(a) match, OFAC match (if there isn't integration between such reporting and the Automated Software)

AML Software - Structure

Many Automated Software solutions also provide for the establishment of risk ratings for customers and accounts.

Oftentimes this involves the calculation of a rating based on various factors such as products used, geographic location, business type, activity and other factors.

The risk rating may be used as part of the rules based or behavior based alert generation process, or may result in separate alerts or reporting on its own.

AML Software - Benefits

Benefits:

- Identify more suspicious activity
- Streamline risk rating and customer due diligence processes
- Facilitates electronic filing requirements
- Stronger integration

AML Software - Benefits

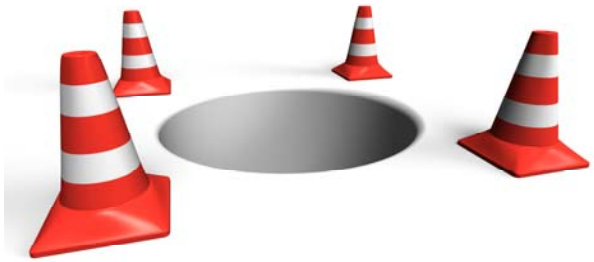
Benefits:

- Reduces reliance on manual processes
- Provides more detailed records and documentation
- Eliminates duplicative or contradicting information while avoiding version control

AML Software - Pitfalls

Pitfalls:

- Cost (direct and indirect)
- Examiners impose higher standard
- Increase time needed for monitoring suspicious activity if not properly managed
- Potential for superfluous false positives



AML Software - Pitfalls

Pitfalls:

- Quality Issues from data integrity
- Increased supporting documentation
- Increased vendor management oversight

AML System Validation - Challenges

- Limited regulatory guidance on scope and frequency of validation testing
- Identifying how the AML system operates and alerts
- Identifying data integrity issues
- Increased expectations to review more information

AML System Validation - Opportunities

- Assurance that the software is producing reliable results that support your AML program and records detailed trail of events

- Identifies opportunities to improve the quality of the output & usefulness of alerts

- Identifies any data integrity issues within the system

AML Software – Parameters

In establishing the parameters followed, it is critical that the institution utilize its risk assessment.

Parameters should be established based on internal, unique factors at the institution such as:

- Customer base
- Products and services offered
- Geographic location
- Volume of higher risk customers and regulatory reports
- Other historical information

AML Software – Parameters

Examples:

- Institution's customer base consists of many cash intensive businesses. Expected activity for cash is set at a higher level than initially recommended by vendor.
- Institution operates in rural area where international wires are occasional at best. Institution sets parameters for international wires to be more sensitive than those initially recommended by vendor.
- Customer usage of a particular product type is extremely rare (used 5 times in a year). Institution sets parameters such that any usage of such product is flagged.

AML Software – Parameters

All applicable transaction types should be considered when the software evaluates activity. This includes, but is not limited to:

- Cash
- Wire Transfers
- Monetary & Negotiable Instruments
- ATM/Debit Cards
- ACH
- Other Electronic Transfers
- Lending Transactions

AML Software – Parameters

Structuring

- Software settings have been done at a dollar threshold too high to capture activity appropriately (ex. $50,000 minimum)
- Date range for capturing activity is too brief, or too wide
- Parameters are not properly structured to apply to correct types of customers

End Result: Instances of activity are not properly identified, activity is never reviewed, and the institution fails to file SARs as required.

AML Software – Parameters

Wire Activity

- Institution has set dollar value of transactions at too low a level given typical customer activity
- Institution applies consumer dollar and transaction volume standards to both consumer and business customers
- Institution has failed to take into account that a large segment of its customer base are students receiving funds from abroad via parents

End Result: The software produces too many alerts, most of which are not relevant and the institution spends too much time reviewing non-suspicious activity.

AML Software – Parameters

Risk Ratings

- System has established that time deposit accounts earn higher numerical score than transaction accounts
- No specific business types in system have been identified as a high risk business type
- Institution fails to record in Automated Software what customers have had SARs filed on them
- Minimum score for a high risk account is set at a very high level such that only customers performing all types of high risk activities could possibly have such a score.

End Result: The software fails to appropriately identify high risk customers.

AML Software - Governance

Initial Set up/Periodic Maintenance

The individual at the institution primarily responsible for initial setup should have the sufficient knowledge of BSA/AML rules, as well as internal practices and risks at the institution.

Facts and reasoning utilized in establishing initial parameters should be documented and retained.

Appropriate input may be necessary from multiple areas (BSA/compliance, IT, Retail, etc…).

AML Software - Governance

Initial Set up/Periodic Maintenance

Any key decisions made to change parameters or functionality should be clearly documented.

Especially important in those instances where the institution is taking on more risk, such as by increasing thresholds to trigger alerts or reducing the frequency of review.

Appropriate dual control should be in place for changes.

AML Software - Governance

Timeliness of Review

The institution will want to ensure that alerts or reports produced by the software are reviewed in a timely manner so as to comply with regulatory requirements and also ensure volume does not become overwhelming.

Frequency of alerts may vary based on vendor and structure of reporting (daily, weekly, monthly, quarterly).

Dual controls should be established to allow for periodic secondary review of alerts or reports closed out as not suspicious.

AML Software - Governance

Board & Senior Management

- Establishment of policies & procedures designed to ensure compliance
- Clearly delineate roles and responsibilities as they relate to model risk management and controls
- Oversight of AML software development, implementation and validation
- Review internal audit findings and validation results
- Ensure prompt corrective action of deficiencies

AML Software - Governance

Policies and Procedures

Written policies and procedures concerning the usage of the software should be established.

Specifying internal practices in addition to simply relying on manuals provided by the vendor are recommended.

Also, any changes that have been made based on what is documented in any manuals should be documented as necessary.

AML Software - Governance

Training

Training concerning the software is critical. Examiners will criticize the institution if they believe employees do not have a proper understanding of the product.

Depth of training should be based on level of involvement.

- BSA Officer and staff should receive detailed training
- Other staff may only require training as warranted (ex. ensuring information is entered into correct fields to avoid subsequent data or timing issues).

AML Software - Governance

Resources

The institution should ensure that appropriate resources are in place concerning the usage of the software.

There should be sufficient staffing to cover alerts and other reports or obligations created via the software. There should also be sufficient staffing in place to ensure review mechanisms and dual controls.

Institutions should not adjust parameters to reduce the number of alerts solely due to resource issues. It should be risk-based in nature such that the institution is comfortable that alerts being excluded are not important.

AML Software - Governance

Reporting

Sufficient reporting to senior management should be done on the usage and effectiveness of the Automated Software, particularly at smaller institutions where costs can be a concern.

Major changes in the usage of the software should be communicated to the appropriate levels of management.

There are no specific guidelines for how such reporting should be done.

Fraud Software

Some Automated Software provide fraud alert reporting or are specifically establish to identify fraudulent behavior.

While this may assist in BSA monitoring efforts, this is not considered all encompassing. Fraud is not all inclusive of all suspicious activity, and the software should be structured to identify all types of suspicious activity.

Reporting

Automated software frequently assists with CTR and SAR reporting.

Oftentimes fields will directly flow from either core system or Automated Software into the applicable form fields.

The institution will want to ensure that such fields are being filled in properly and that manual edits are made when necessary.

Watch Lists

Automated Software can also provide means to review "Watch" lists such as OFAC and 314(a).

The institution will want to ensure that all applicable lists are being utilized and are properly flowing into the software (particularly when updates are made to lists or software).

Sensitivity of the software should be appropriate set so as to not leave out potential matches that can be of concern.

System Validation – Getting Started

What is the system doing in regards to your data?

- Identifying

- Evaluating

- Reporting

System Validation – Getting Started

Potential Breakdown Points:

1. Management should establish a clear and defined **escalation** process from the point of initial detection to disposition of the investigation.
2. Not having a system that captures the suspicious activity.

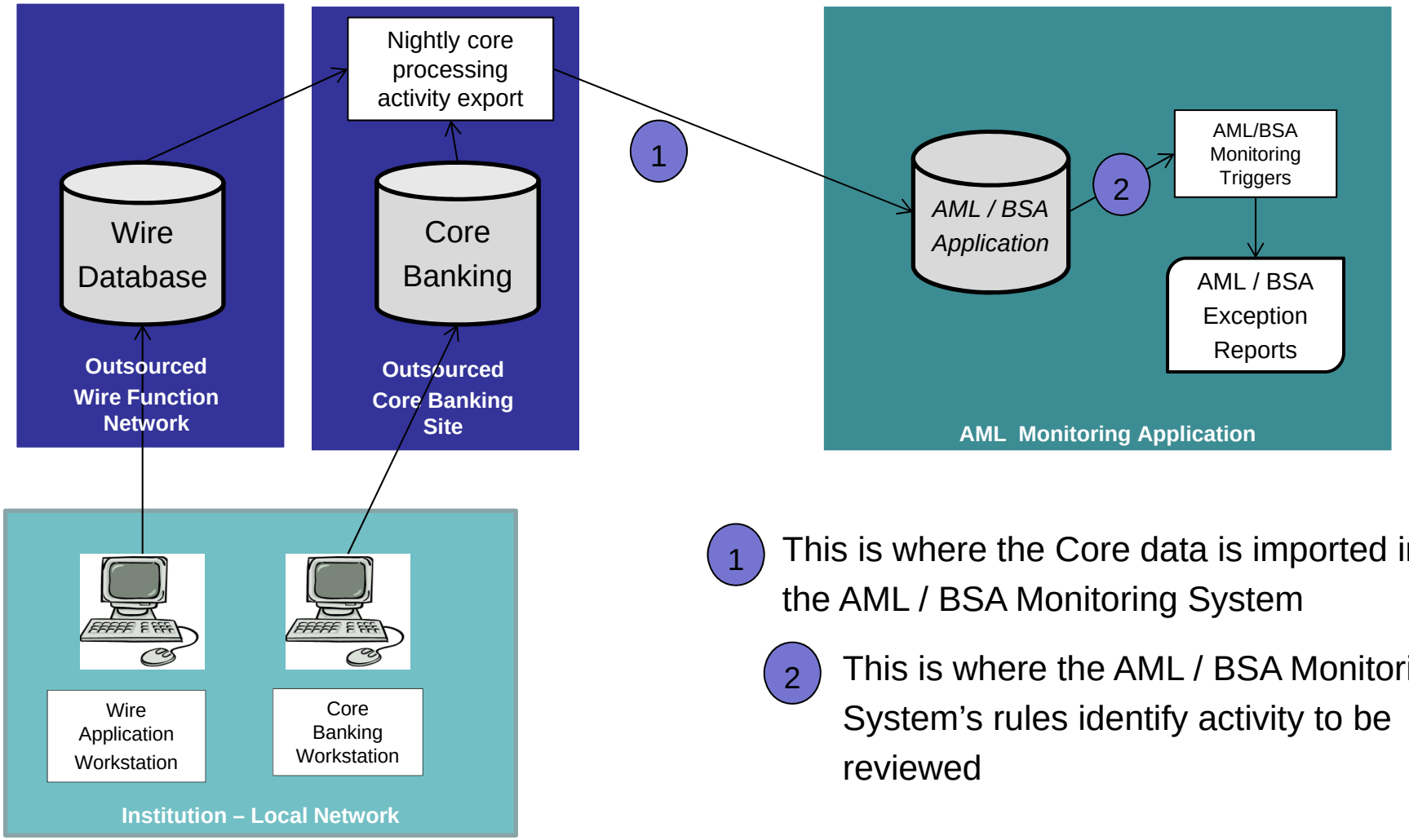
System Validation – Getting Started

Items Required for Testing:

- Core Reports showing all transactional data for the time period
- Wire activity reports
- BSA/AML system reports for rules and/or configurations
- Exception lists
- User Access List
- Employee Roster
- Change Management Policies and Procedures surrounding your BSA/AML system

System Validations – Data Flow

Where do we start? Identify the Data flow:



1. This is where the Core data is imported into the AML / BSA Monitoring System

2. This is where the AML / BSA Monitoring System's rules identify activity to be reviewed

System Validations - Testing

Testing the system involves validation of the following items:

- Import of information from the core (integrity / completeness)

- Results of the AML / BSA Monitoring system (integrity / accuracy)

System Validations - Testing

Core Data Integrity and Completeness Check:

- Capture and Aggregate activity reports from the Core Banking System and Wire System
- Select random samples from the core data and verify they are present in the BSA/AML system
- Data integrity check by ensuring data is appearing the same as it is within the core

System Validations - Testing

BSA/AML System results Integrity and Accuracy Check :

- Utilize rules configured within the AML / BSA System against the aggregated data
- Select samples that would be expected to “hit” rule criteria
- Compare the results of this testing against the AML / BSA exception reports

System Validations - Testing

General System Security Controls, including:

- User Accounts and Access Levels – Abilities to configure monitoring rules / abilities to configure report structures
- System security monitoring controls
- Change management policies and procedures along with periodic independent monitoring

System Validations - Known Issues

- Bad data inappropriately mapped to the BSA/AML system

- Entire Modules not flowing over to the BSA/AML system
- Random transactions not flowing over to the BSA/AML system
- Transactions not being appropriately risk rated in the BSA/AML system

AML Software – Exam Expectations

Examiners expect the Automated Software to be covered by independent testing as part of the BSA audit function.

The audit must be performed by an independent party that was not involved in the set up of the software and is not involved in the regular maintenance or usage of the software.

This can be done through an Internal Audit Department, third party auditors or other individuals in the institution as long as they are independent and have appropriate expertise.

AML Software – Exam Expectations

The audit coverage should ensure that the rules/parameters being utilized by the software are reasonable and appropriate. IT validation should cover any data entry/analysis concerns.

The audit should also cover the usage of the software, including:

- Ensuring that there is appropriate understanding by personnel;
- Timely addressing of alerts and reports
- Proper documentation for cases not resulting in SAR filings.

AML Software – Exam Expectations

- Has the institution performed an appropriate analysis when the product was implemented and not simply used "out of the box" parameters/rules?
- Does the institution periodically review its parameters to ensure that they are appropriate?
- Has the institution ensured that its parameters are appropriate in accordance with its risk assessment, policies and practices?

AML Software – Exam Expectations

- Is the institution performing its analysis of alerts in a timely manner?
- Is the institution reviewing alerts in a consistent manner, and properly documenting the results of its analysis?
- Do the appropriate individuals review these alerts, and is key information reported to the appropriate members of management?
- Is the usage of the software impacting BSA compliance or reporting in any negative fashion?

AML Software – Exam Expectations

- Controls to establish and changes parameters
- Appropriate user authorities and controls
- Testing of system changes
- Periodic validation of entire system

AML Software Optimization

Assess the adequacy of your Institutions AML software parameters. Whether your institution is using default parameters or customized parameters, consider the following:

- Are the parameters sufficient to identify areas that pose significant risk to your institution?
- Are the parameters adequate given your institutions risk model and risk assessment?
- Is the software generating quality alerts and are these alerts manageable?

Objectives of Optimization

Continued analysis and even adjustment of the parameters are crucial components of software validation.

Any changes made as a result of the analysis and adjustments must be documented and include an description of the changes, benefits, pitfalls/limitations, and anticipated results.

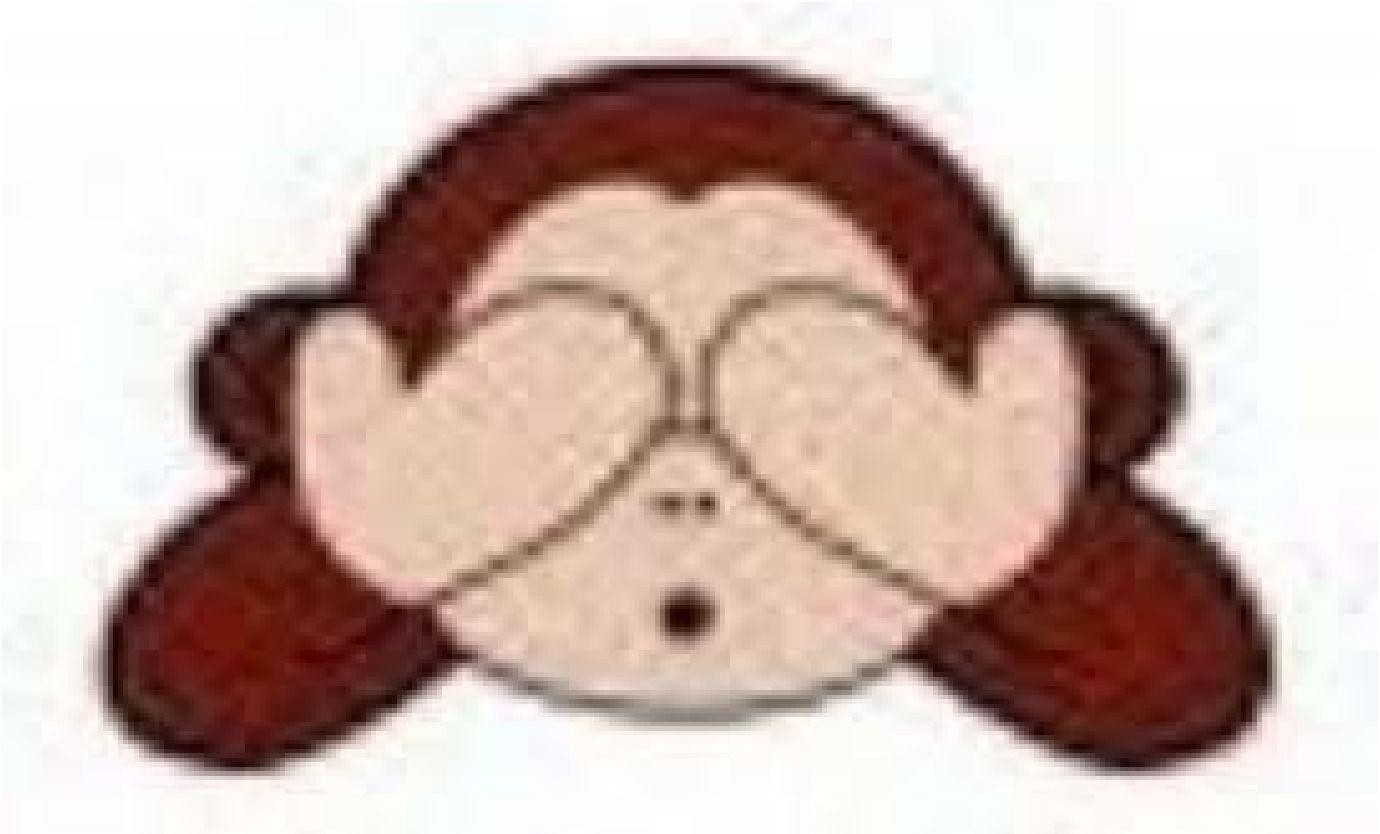
- Use of new data, new risks
- New model approaches
- New or improved reports

FinCEN Advisory

The strength of an Institution's compliance culture depends on:

- Support and understanding by leadership of compliance efforts;
- Efforts to manage and mitigate deficiencies/risks are not compromised by revenue interests
- Pertinent information from the business lines is communicated to the Bank Secrecy Act/Anti-Money Laundering Department
- Appropriate allocation or resources
- Effective compliance program – 4 pillars
- Understanding of the need for compliance and penalties for non compliance

Where do the shortcomings lead to?



Enforcement Actions

<u>April 2012: Citibank, N.A. OCC Cease & Desist</u>

Weak documentation of the validation and optimization process applied to automated transaction monitoring systems

– the independent BSA/AML audit function failed to identify systematic deficiencies

Enforcement Actions

September 2013: TD Bank $52.5 million

SEC and OCC fined Bank for its actions and non-actions regarding potential $1 billion ponzi scheme.

OCC = Failure to identify suspicious activities

= Failure to file SARs despite system alerts

Enforcement Actions

<u>September 2013: Saddle River Valley Bank $8.2 million</u>

FinCEN fined the Bank for failure to maintain an effective anti-money laundering program.

- Inadequate EDD over casas de cambio
- Failure to detect and report CDC suspicious activities
- ‘Insufficient experience” and inadequate training

Enforcement Actions

<u>January 2014: JPMorgan Chase Bank, N.A. $350 Million</u>

- Less than satisfactory Risk Assessment processes
- Systematic deficiencies in the Bank's transaction monitoring systems, due diligence processes, risk management, and quality assurance programs
- SAR decision-making deficiencies

Enforcement Actions

<u>January 2014: Old National Bank $500k</u>

OCC fine for BSA program failures

- Failure to conduct adequate Risk Assessment
- Inadequate suspicious activity monitoring program
- Lack of qualified BSA Officer and resources

Enforcement Actions

<u>June 2014: Associated Bank $500k</u>

OCC fine for BSA program deficiencies

- Failure to conduct adequate Risk Assessment
- Insufficient Customer Due Diligence
- Improper high-risk customer identification
- Inadequate suspicious activity monitoring program

Enforcement Actions

Nov 2014: North Dade FCU $300k

- 4 Pillars violation
- Failure to establish adequate AML Program
- Failure to establish adequate CIP
- Failure to Identify/Report CTRs and SARs
- Failure to review § 314(a) Request Lists

Enforcement Actions

FinCEN Dec. 2014: Thomas Haider $1 Million

- Willfully violated the requirement to implement and maintain an effective Anti-Money Laundering Program
- Willfully violated the requirement to report suspicious activity and file timely SARs
- Failure to termination known high risk agents
- Failure to conduct adequate due diligence of agents

Enforcement Actions

<u>Jan. 2015: Oppenheimer & Co. Inc. $20 Million</u>

SEC fine for BSA/AML program deficiencies:

- Failure to implement an adequate Anti-Money Laundering program
- Pattern of suspicious activity was identified based on the same two significant red flags
- Failure to implement an adequate due diligence program for a foreign correspondent account
- Failure to report a customers suspicious activity occurring through Oppenheimer accounts

Enforcement Actions

<u>Feb 2015: First Natl Community Bank $1.5m CMP</u>

$1m FinCEN fine and $500k OCC

- Failure to detect or report SARs timely
- Failure to comply with internal policies

Enforcement Actions

<u>April 2015: Lone Star National Bank $1 Million CMP</u>

OCC fine for BSA program deficiencies:

- Unsatisfactory EDD and CDD for high risk accounts
- Independent Audit
- Inadequate Suspicious activity monitoring & reporting
- Foreign Correspondent Relationship/Banking

Enforcement Actions

June 2015: Bank of Mango $5.7m (CMP/forfeiture)

- Failure to establish adequate AML Program
- Failure to establish adequate CIP
- Failure to Identify/Report CTRs and SARs

BSA Resources

FFIEC BSA Exam Manual – BSA/AML Risk Assessment

http://www.ffiec.gov/bsa_aml_infobase/pages_manual/olm_005.htm

FRB Supervisory Guidance on Model Risk Management

http://www.federalreserve.gov/bankinforeg/srletters/sr1107a1.pdf

FinCEN Advisory to U.S. Financial Institutions on Promoting a Culture of Compliance

http://www.fincen.gov/statutes_regs/guidance/pdf/FIN-2014-A007.pdf

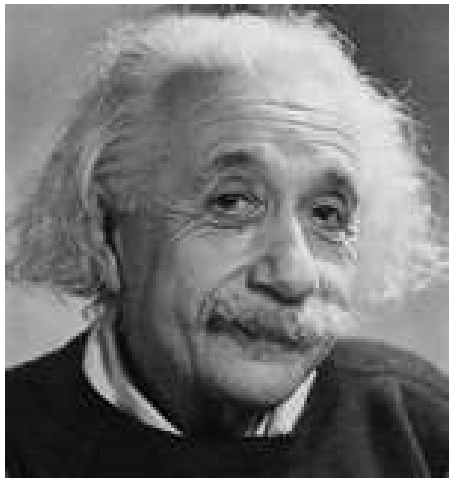
FinCEN Enforcement Actions

http://www.fincen.gov/news_room/ea/

Final Thought

"The level of thinking necessary to address today's problems must be greater then that which got us here."

Albert Einstein



Thank you

Stephen R. King, JD, AMLP
Director, Regulatory Compliance Services
617-428-5448
sking@wolfandco.com