ACAMS NEW JERSEY Chapter

What You Need to Know About Model Validation and System Tuning

Andrea Rios Hernandez, Senior Manager, Financial Crimes Testing and Validation

Caroline Curley, Manager, Financial Crimes Testing and Validation

Elena Nezhivleva, Manager, Financial Services Analytics and Technology

Brian Caplice, Senior Consultant, Financial Services Analytics and Technology

Crowe

April 18, 2022

Moderator:
Todd Brungard, CAMS
ACAMS NJ Chapter Co-Chair
Financial Crimes Senior Manager, Crowe LLP

THE WEBINAR HAS BEGUN

- By default, all attendees are muted and cannot speak with other attendees or panelists. No one can see or hear you.
- Please submit questions through the Q&A button on your Zoom screen.
- If you encounter audio/video issues, please click the Q&A button and send a message to receive assistance.
- As a reminder, members of the Chapter will earn one CAMS credit for participation in today's virtual event. Please allow 10 business days for credits to appear in your ACAMS profile.

Please Note:

- ✓ We will be providing a copy of the presentation on the chapter website following the event.
- ✓ This event is being recorded - link will be posted to chapter website.

ACAMS

FINTECH & CRYPTO SUMMIT

JOIN US IN SAN FRANCISCO

May 3, 2022

#ACAMSFinTech

ACAMS

LAW ENFORCEMENT Seminar

The Next Generation of Financial Crime Investigation

JOIN US ONLINE

May 16-17, 2022

#ACAMSLawEnforcement

ACAMS

RISK MANAGEMENT & SECURITIES SUMMIT

JOIN US IN NEW YORK

June 29, 2022

#ACAMSNewYork
#ACAMSRisk

NJ Chapter Membership

Has your Chapter Membership lapsed?

Do you need ACAMS CPEs for your recertification?

Do you want priority access to future in-person events?

REMINDER:

Don’t forget to re-join the NJ Chapter annually. Unfortunately, ACAMS does not automatically renew/bill for Chapter Memberships. If your membership has lapsed, please log into your account and renew your Chapter Membership. These funds directly support your Chapter and help to bring you educational and networking events.

ACAMS NEW JERSEY Chapter

2022 Upcoming Events

Planning still in progress for May/June…….

May – TBD –

SWIFT Messaging and compliance with ISO 20022 – are your AML systems ready?

ACAMS NEW JERSEY Chapter

ACAMS NEW JERSEY Chapter

What You Need to Know About Model Validation and System Tuning

Andrea Rios Hernandez, Senior Manager, Financial Crimes Testing and Validation

Caroline Curley, Manager, Financial Crimes Testing and Validation

Elena Nezhivleva, Manager, Financial Services Analytics and Technology

Brian Caplice, Senior Consultant, Financial Services Analytics and Technology

Crowe

April 18, 2022

Moderator:
Todd Brungard, CAMS
ACAMS NJ Chapter Co-Chair
Financial Crimes Senior Manager, Crowe LLP

ACAMS NJ Presentation:

Model Validation & Optimization

April 2022

Agenda

- Panelist Introductions
- Model Validation Overview
- Model Optimization Overview
- Questions

Panelist Introductions

Andrea Rios
Validation SME

Andrea is a Senior Manager in Crowe's Financial Services Risk Consulting Practice with over ten years of experience managing AML & OFAC projects, system implementations and process improvement initiatives. Andrea has focused on enhancing the Financial Crime Model Validation program and currently serves as the Financial Crime Model Validation Solution lead. Andrea has worked with different financial institutions including global banks, US branches of foreign banks, Money Service Businesses (MSB), third party payment processors, prepaid card issuers, community banks and credit unions as well as FI software vendors.

Caroline Curley
Validation SME

Caroline is a Manager in Crowe's Financial Services Consulting practice and a member of the Financial Crime, Testing and Validation group. She has extensive experience working with clients in the banking and financial services industries, including banks, credit unions, payment processors, and FinTechs, on Bank Secrecy Act (BSA), anti-money laundering (AML) and sanctions compliance risk management. Caroline specializes in model validation and has worked with a variety of transaction monitoring, sanctions filtering, customer risk rating, and customer identification verification models.

Elena Nezhivleva
Optimization SME

Elena leads Crowe's Financial Crime Analytics offering within Crowe's Financial Services Analytics and Technology practice. She focuses on working with clients in the financial services industry to assess and mitigate regulatory risks. Elena's client experience includes a variety of institutions ranging from community banks to large global financial services providers. Elena specializes in Financial Crime system optimization, analytics, technology implementation, and project management. Elena serves as Financial Crime Innovation Lead to continuously transform client offerings, stimulate innovation collaboration, and support a culture of innovation.

Brian Caplice
Optimization SME

Brian leads Crowe's Financial Crime System Optimization offering within Crowe's FS Analytics & Technology practice. His professional experience has focused on leveraging technology and analytics to improve the overall effectiveness of his clients' AML monitoring programs (including TM, CRR, & OFAC). Brian's client experience has included large global financial institutions, mid-size banks, small community banks, and traditional financial intuitions (MSBs, FinTechs, payment processors, etc.). During his time at Crowe, Brian has assisted with optimization and implementation projects for Actimize, Verafin, FCRM, Patriot Officer, and JH's Yellow Hammer.

Model Validation

Andrea Rios and Caroline Curley

Smart decisions. Lasting value.™

Importance of Model Governance

Model Risk Management has been a hot regulatory item since the OCC/Fed/FDIC Supervisory Guidance on Model Risk Management (2011-12, SR 11-7 and FIL 22-2017).

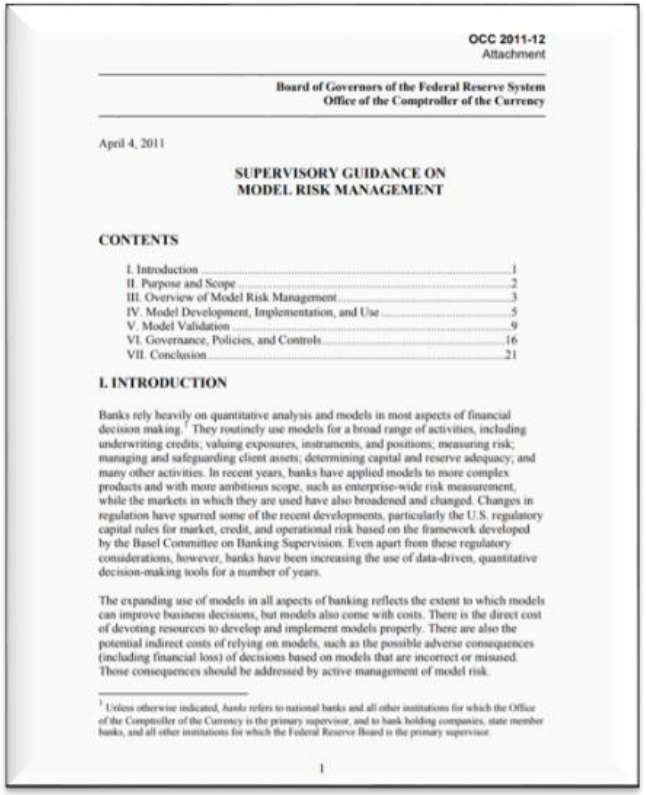
Model governance reviews should include key control design and operating effectiveness related to the following:

- Model Development, Implementation, and Use;
- Model Validation; and
- Model Governance, Policies, and Controls.

Metrics and reporting of ongoing model optimization/tuning should be critically challenged.

Recent enforcement actions include:

- USAA Federal Savings Bank, $60 million civil monetary penalty and consent order, issued in March 2022 for BSA/AML violations, including a “critically flawed customer risk score model.”
- M.Y. Safra Bank, consent order issued in January 2020 which required specific improvements to the Bank’s model risk management program.



OCC 2011-12
Attachment

Board of Governors of the Federal Reserve System
Office of the Comptroller of the Currency

April 4, 2011

SUPERVISORY GUIDANCE ON
MODEL RISK MANAGEMENT

CONTENTS

I. Introduction 1
II. Purpose and Scope 2
III. Overview of Model Risk Management 3
IV. Model Development, Implementation, and Use 5
V. Model Validation 9
VI. Governance, Policies, and Controls 16
VII. Conclusion 21

I. INTRODUCTION

Banks rely heavily on quantitative analysis and models in most aspects of financial decision making.[1] They routinely use models for a broad range of activities, including underwriting credits; valuing exposures, instruments, and positions; measuring risk; managing and safeguarding client assets; determining capital and reserve adequacy; and many other activities. In recent years, banks have applied models to more complex products and with more ambitious scope, such as enterprise-wide risk measurement, while the markets in which they are used have also broadened and changed. Changes in regulation have spurred some of the recent developments, particularly the U.S. regulatory capital rules for market, credit, and operational risk based on the framework developed by the Basel Committee on Banking Supervision. Even apart from these regulatory considerations, however, banks have been increasing the use of data-driven, quantitative decision-making tools for a number of years.

The expanding use of models in all aspects of banking reflects the extent to which models can improve business decisions, but models also come with costs. There is the direct cost of devoting resources to develop and implement models properly. There are also the potential indirect costs of relying on models, such as the possible adverse consequences (including financial loss) of decisions based on models that are incorrect or misused. Those consequences should be addressed by active management of model risk.

[1] Unless otherwise indicated, *banks* refers to national banks and all other institutions for which the Office of the Comptroller of the Currency is the primary supervisor, and to bank holding companies, state member banks, and all other institutions for which the Federal Reserve Board is the primary supervisor.

1

2021 Interagency Statement

April 9, 2021: Interagency Statement on Model Risk Management for Bank Systems Supporting Bank Secrecy Act/Anti-Money Laundering Compliance, released by the Fed, FDIC, and OCC.

This statement clarified that the risk management principles discussed in the 2011 MRM Guidance do indeed apply to models used for BSA/AML compliance. Three important points to keep in mind:

1. The determination by a bank of whether a BSA/AML system is considered a model is **bank-specific**, and a conclusion regarding the system's categorization should be based on a **consideration of all relevant information**.

2. Examples of what would **likely not be considered BSA/AML/OFAC models** are specified.

3. Testing and validation of BSA/AML/OFAC models should be **customized to fit the purpose of the model's use**.

NYDFS 504

January 1, 2017: The New York Department of Financial Services (NYDFS) adopted Part 504, a first of its kind set of regulations governing transaction monitoring and sanctions filtering programs for regulated institutions.

Two major requirements:

1. Install and maintain a risk-based BSA / AML Transaction Monitoring and OFAC Filtering Program.
2. Submit on an annual basis a “compliance finding” by the Board of Directors or Senior Officers to certify that the regulated institution is in compliance with Part 504.

Development announced by DOJ at the April 2022 ACAMS Conference

“Under a new policy announced at the conference, the U.S. Justice Department’s Criminal Division will ask federal prosecutors to consider requiring chief compliance officers and CEOs to certify that their companies’ compliance programs are effective at preventing violations of the law as a condition for resolving settlements with the department.”

Overview: What is a Model?

It is important to understand what a Model is and the different types there are.

Model Definition and Components:
As defined by the Office of the Comptroller of the Currency (OCC): The term model refers to a quantitative method, system, or approach that applies statistical, economic, financial, or mathematical theories, techniques, and assumptions to process input data into quantitative estimates. A model consists of three components:

Defined AML models should be validated on an ongoing basis to ensure the model is performing to expectations.

The Three Traditional Model Types:

Transaction Monitoring Model
Generates suspicious activity alerts/events based on transaction activity triggering pre-defined threshold limits. The alert/case/SAR case management system is often included as a component within the model.

Sanctions/Watch List Model
These models will scan the customer base, or specific transactions, against the OFAC SDN, 311, PEP, and other required government lists. Typically underlying “fuzzy” logic that defines system as model.

Customer Risk Rating Model
Uses both inherent risk (citizenship, occupation, etc.) and transactional activity to generate a customer risk score and rating in order to focus on highest risks. Customers rated “high” risk are typically subject to enhanced due diligence.

When to Validate?

Consider these critical factors to determine **the right validation timeframe for your institution.**

Regulatory Requirements

The 2011 MRM Guidance states that “It is generally good practice for banks to ensure that all models **undergo the full validation process… at some fixed interval**, including updated documentation of all activities.”

The 2021 Interagency Statement notes that “model reviews and validations are generally performed using a **risk-based approach**, and with a **frequency appropriate for a bank’s risk profile**.”

Changes to Risk Profile

- Validation should be considered when there are changes to the institution’s risk profile. This could include new or revised:
  - Products
  - Services
  - Customer types
  - Geographic locations
- Or if the institution expands through a merger or acquisition.

Material Changes to Models

- The 2011 MRM Guidance states that “material changes to models should be subject to validation.”
- **Conversion of a core banking system** or other source system of a model would be considered a material change and warrant observation.
- Validation should be performed following the **implementation of a new model**, once the model has been in use long enough to generate enough data to perform meaningful assessment.

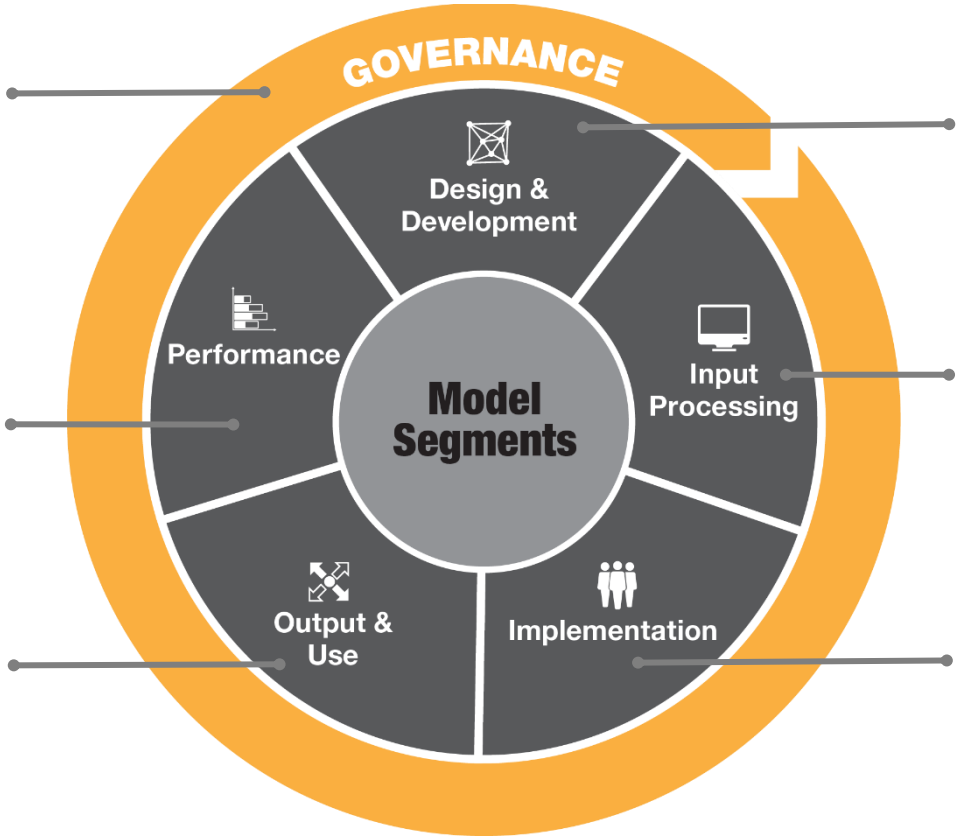
Model Validation Approach

The following sample model validation testing approach is focused on five key segments and the overall governance of the model, to address the validation pillars of the MRM guidance.

The governance surrounding the ongoing support of the model is evaluated throughout each of the five model segments.

Validates the procedures and processes used to prioritize and assess the model's outputs; evaluates the ability to calibrate and optimize the model performance over time.

Validates the policies, procedures, and processes in use to confirm that the model output is as designed and is being evaluated by the proper users without unexpected or unintended bias.



Validates the intended purpose of the model, the model logic and functionality, alignment of the model to the purpose, assumptions and limitations of the model, and methodology used to design and develop the model.

Validates the inputs relied upon by the model, including the accuracy and completeness of the model data as well as the ongoing maintenance of inputs.

Validates the integration of the model's design and functionality into the institution's business-as-usual processes and technology. Model versions and parameters tied to specific BUs, geographies, and products are assessed.

Common Findings

General

- Model documentation is incomplete, incorrect, or outdated.
- The institution is not performing ongoing monitoring or testing of the model (e.g., balance and reconciliation)
- Lack of a formal tuning methodology.

Customer Risk Rating

- Outdated dynamic lists (e.g., Occupation codes, NAICS codes, etc.)
- Unsupported thresholds and settings.
- Key risk areas are not covered by the model.

Transaction Monitoring

- Transaction code mapping is incorrect or not reviewed with frequency.
- Scenarios/Rules are setup with out of the box settings that may not be in line with Bank's risk exposure.
- Critical data elements are not mapped from source systems.

Sanctions Screening

- Model is not screening all relevant data fields.
- The model does not generate hits against countries, cities and ports related to comprehensive sanctions.
- False positive management controls (e.g., accept list, exclude list) are not periodically reviewed or tested.

Model Optimization

Elena Nezhivleva and Brian Caplice

Smart decisions. Lasting value.™

When to Tune?

The frequency of tuning is determined by the regulatory requirements and expectations, pain points your institution has, and mostly importantly your unique KPIs and KRIs.

Regulatory Requirements

The Federal Financial Institutions Examination Council ("FFIEC") BSA/AML Exam Manual states that the level of monitoring should be dictated by the **Bank's assessment of risk**, with emphasis on high-risk products, services, customers, and geographic locations. The FFIEC BSA/AML Exam Manual further states that "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."

Pain Points

- It is required that management review the coverage of its BSA/AML program and the effectiveness of parameters used within its financial crime applications.
- One of the primary pain points for institutions is increased expectations for AML Model Calibration.
- Increased expectations on calibration rigor, driving increased use of advanced statistical and analytical techniques.

Qualitative Triggers

Qualitative changes to an institution's risk profile could trigger a tuning exercise. These could include:

- Events, such as mergers/acquisitions, that result in changes to customer base
- Changes to institution's geographic footprint
- Changes to institutions product/service offerings
- Identification of new trends in money laundering schemes that could circumvent existing controls

Quantitative Triggers

Quantitative changes to an institution's transaction or customer data could trigger a tuning exercise. These changes are identified through KPIs and KRIs.

Key Risk Indicator (KRI)

- A metric used by the Bank to provide an early signal of risk exposures in various areas of the institution.

Key Performance Indicator (KRI)

- Quantifiable measures used to evaluate the effectiveness of the Bank's transaction monitoring program.

On-Going Monitoring

To maintain an effective and efficient transaction monitoring program, your institution must establish a process to continually monitor model performance using defined KRIs and KPIs.

KPIs & KRIs

These indicators help track an institution's risk appetite, identify emerging trends, and identify candidates for tuning. Common KPIs & KRIs include:

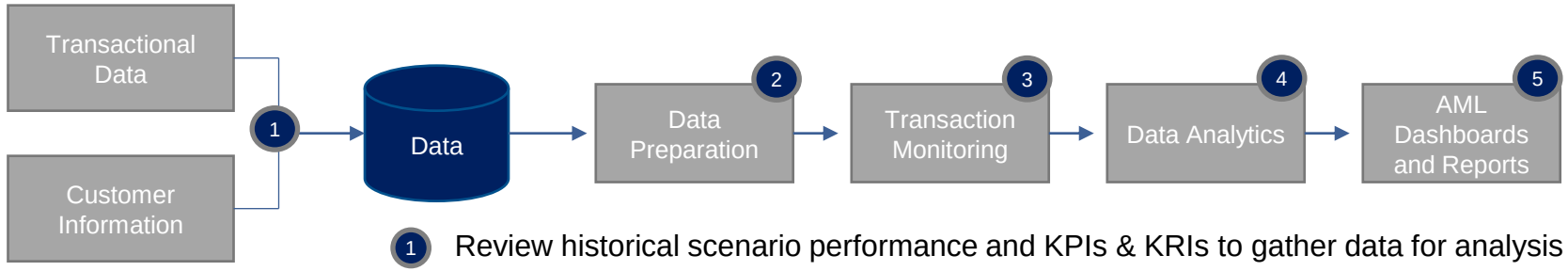
- **Case/SAR Yield:** Scenarios with low effectiveness could be candidates for ATL while scenarios with high effectiveness could be candidates for BTL
- **Alert Volume:** Changes to alert volume could signal a change to the institution's risk profile which may lead to a tuning exercise
- **High Risk Customer Distribution:** Increases to an institution's high risk customer population could signal a change to the institution's risk profile which may lead to a tuning exercise

Visual analytics

Effective governance and focused monitoring driven by periodic management reporting on key statistics. Culture of analytics must be embraced to develop and sustain model calibration program.

Reporting

Dashboards and reporting are becoming a necessary tool to take an assertive step toward changes to AML model performance to enhance the agility of the AML program and mitigate AML risks.



1. Review historical scenario performance and KPIs & KRIs to gather data for analysis
2. Prepare and validate data for accuracy
3. Evaluate tuning results for visualization
4. Massage the data and draw meaningful conclusion
5. Finalize the data for reporting

Current Trends

Based on our experience working with institutions of various sizes and feedback we have gathered from regulators, we have seen that the trends in model optimization are associated primarily with data quality, BTL tuning, model simulation, and customer segmentation.

Understand your data before conducting tuning:

It is critical to conduct a data quality assessment before executing a tuning exercise to produce better and more accurate results:

- When was the last time you have evaluated your data?
- Are there open or known data quality issues that might impact tuning results?
- Are there new product or transaction codes that have not been mapped to the current scenarios?
- Have you analyzed data integrity recently?
- Is your data accurate and reliable?

Conduct comprehensive below-the-line tuning:

BTL tuning is expected to be conducted as part of your tuning scope that should be comprehensive.

- Are you identifying scenarios for BTL in your tuning scope by evaluating all scenarios in production?
- Are you targeting scenarios that not only produce high alert/case and case/SAR but also produce zero alerts (are thresholds maybe set to high)?
- How are you defining the test threshold for BTL tuning? Are you lowering by X% or are you lowering to the de minimis values?

Consider model simulation when there are data limitations:

Model simulation or scenario replication can be used when you have a limitation with data availability.

- Is your data limited and not sufficient for tuning?
- Do you have a test environment to generate test alerts?

Customer segmentation:

Up-to-date customer segmentation is fundamental for more precise tuning results that are targeted to special customer populations and not scenario typology.

- Do you segment your customers based on their key attributes (risk level, customer type, product type, account type, transaction activity, etc.)?
- Do you use qualitative and quantitative methods to segment your customers?
- Is your customer segmentation up to date?

Model Optimization Methodology

A strong transaction monitoring tuning approach should be built on an institution's model risk management guidelines. The core MRM requirements of the supervisory guidance include:

Assess AML Model

Assess the model to understand performance and identify prioritization of enhancement opportunities:

1. Model coverage assessment
2. Data requirements: data quality assessment (DQA)
3. Model parameters and rules selection:
    - Tuning schedule and action plan

Conduct On-going Monitoring

Maintain a continuous cycle of review through performance-based metrics to identify future enhancement opportunities:

1. Risk and performance indicators (KPIs & KRIs)
    - Visual analytics
    - Reporting
2. On-going tuning schedule

Perform Testing & Analysis

Use the results of model assessment to conduct testing and analysis on model parameters and settings:

1. Scenario logic simulation (if required)
2. Tuning phase:
    A. Pre-production
    B. Production:
3. Model enhancement implementation: change control documentation and approvals

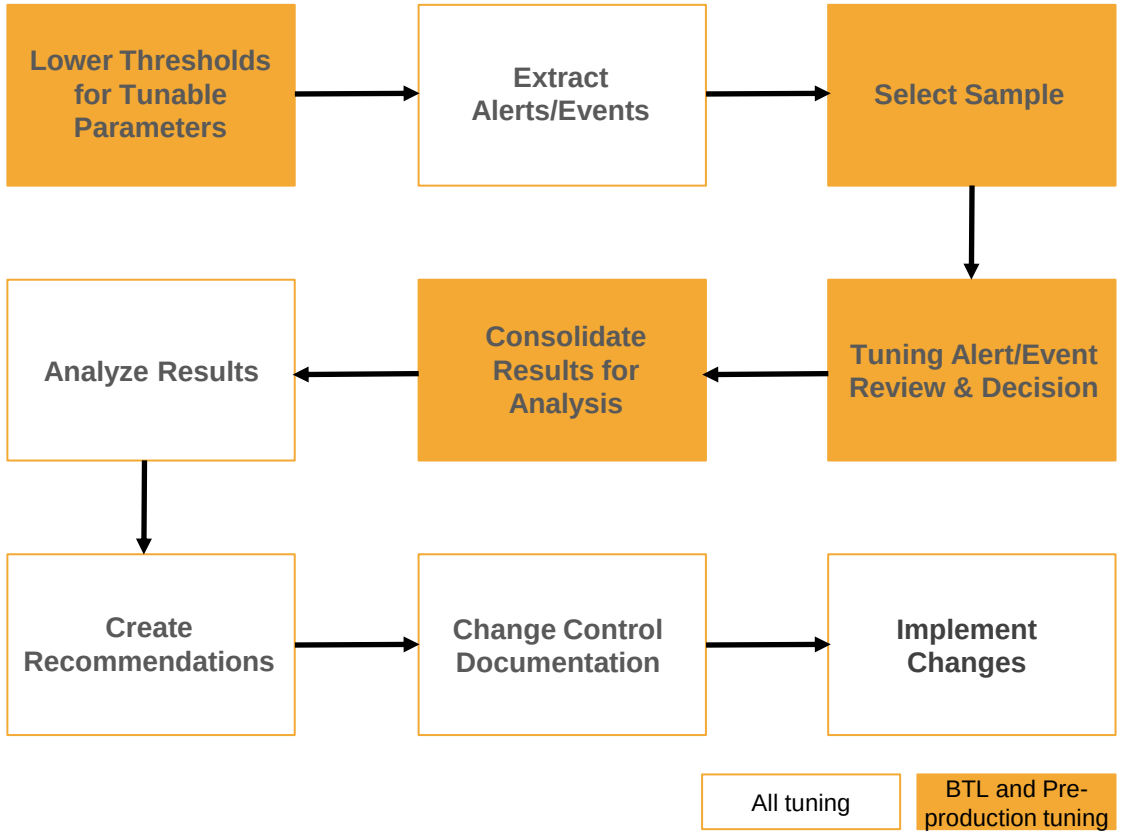
Model Optimization Methodology: Perform Testing & Analysis

A consistent and repeatable methodology enables appropriate justification.

Prescriptive Tuning Approach

- **Pre-production** tuning should be conducted for scenarios which are new to the institution and have not previously been included in the Production environment.
- **Production** tuning should be conducted for all other scenarios, as one of the following:
  - **Above-the-line** (ATL) – the goal is to review scenarios that have been previously established in production and to examine the quality of the alerts being produced for further improvement.
  - **Below-the-line** (BTL) – the goal is to ensure suspicious activity is not going undetected

- In pre-production tuning, lowest logical values ("LLVs") should be used as starting points for determining the baseline thresholds. The LLV threshold setting is determined through an analysis of the intended purpose of each individual scenario, the additional scenarios providing coverage for the transaction type, and knowledge of the typology.
- Alerts are extracted from a test environment for BTL and pre-production tuning and from the production environment for ATL.
- During the "Decision Alerts" step, each sampled alert is reviewed by a single investigator. The purpose of the review is to assess whether alerted transactions cannot be readily "cleared" as non-suspicious.



Thank you

Any questions?

Smart decisions. Lasting value.™