



Three key steps for validating your transaction monitoring model

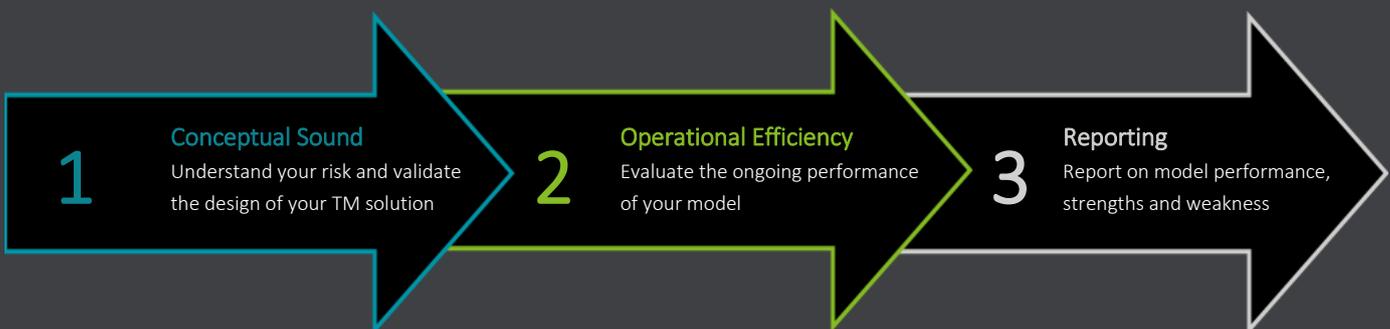
June 2020

Three key steps for validating your transaction monitoring model

Financial Institutions (“FIs”) are increasingly faced with pressure from regulatory authorities to prevent, detect and deter those who wish to use the global financial system for financial crime (“FC”). As criminal behaviour evolves, products become more complex and the regulatory environment develops, FIs look to use quantitative models that can help protect their organisation against these threats.

The challenge though, lies in being able to employ a robust qualitative and quantitative method when designing your Transaction Monitoring (“TM”) capability so that concepts of model validation can be applied to ensure your risk is identified and managed correctly.

There are three key steps that you should follow to validate your TM model



Step 1

Understand the risk and evaluate the conceptual soundness of the model

The focus when assessing the model’s conceptual soundness is on being able to evidence your model has been designed and implemented to meet your institutions FC prevention objectives. All aspects of the model should be assessed, including the steps that were taken to design the TM rules, the implementation of the model and the data that is required.

A thorough assessment of the conceptual soundness will include reviewing and understanding the following:



Model objective – The documents that should be reviewed will include an overview of the entire TM model that is comprehensive and detailed enough to allow independent reviewers a full understanding of the model. Key TM scenarios are then identified and selected for sample review. Start by confirming the scenario aligns to a known risk, as identified by a Risk Assessment. Review the data inputs to confirm it is complete and accurate. Validate that the selected scenario is producing the expected output.



Assumptions and limitations – Models are by definition a simplification of the reality, therefore it is important that any limitations and assumptions made when designing the model is evidenced. Start by identifying the model’s limitations and confirming these are in line with your risk-based-approach. Known assumptions and limitations should be fully documented and understood.



Data – The data (both internal and external) that is used to construct, implement and test the model should resemble the FI's customer and product base. All data inputs, including transformations, should be clearly evidenced. Key data points should be sample selected for review, start by selecting the ones that are more likely to influence a greater number of scenarios if incorrectly implemented. Validate the data mapping from source to the TM solution to confirm it is designed to be complete and accurate.



Implementation – All TM models that are purchased “off-the-shelf” require a number of customisations. The customisations and the quality of the user acceptance and testing should be reviewed to ensure it meets regulatory and industry standards. Consultation with your IT department is essential to ensure the security protocols are sufficient to keep the model and the data secure.

Step 2

Evaluate the ongoing performance of your model

Ongoing monitoring evaluates whether changes in products, customers, market conditions, FC risk typologies, redevelopment, or replacement of an existing TM model remain valid and up-to-date. Throughout the evaluation of ongoing performance, it provides the opportunity to identify issues and evaluate changes outside of the periodic review cycle as well as forming a view on how well the model is managed and the stability and reliability of its performance.

A thorough assessment of the ongoing performance will include the following steps.



Governance review – Key to ensuring the TM model is managed and updated on a regular basis. A structured model governance framework including definitions of roles and responsibilities for effective model risk management, reporting lines and any committees responsible for internal model governance and oversight.



Define a performance assessment framework – Performance assessment frameworks identify standards that are compared to the model performance. These should be split into five key areas:

- AML program management, indicates whether the overall programme is meeting its objectives.
- Monitoring effectiveness, indicates whether the model is producing alerts.
- Model accuracy, indicates whether the model is producing accurate alerts.
- Data accuracy and completeness, indicates that the data utilised by TM applications is complete and accurate.
- Emerging risks indicates that the model identified potential changes to the FC risk typologies that were previously assessed.



Ensure KPIs are appropriate – When designing KPIs, the aim should be to answer a very specific set of questions that will inform your decision if the model is operating as originally designed. The most important factor is that there is a process in place to review and react to the information, such as, the number of scenarios that have never triggered an alert can indicate that the thresholds are too low. These KPIs should be automated and monitored on a regular basis.



Tune and calibrate – This can be one of the most difficult and complex parts of managing a TM model as most rules typically involve multiple parameters such as a customer type, transaction type, time frame and a currency value or transaction volume. Review the outcome of previous calibration exercise and confirm that the rationale for threshold setting is clearly evidenced. Calibration should be conducted regularly and should be based on an ongoing monitoring of the scenarios effectiveness.



Review results against the expected outcome – The results from the ongoing monitoring will confirm how effective your model is in identifying suspicious activities in relation to the FC risk typologies previously documented. The outcome of the model should also be used as an input to the ongoing review of the scenarios and can be used as an indication that a risk assessment refresh is required.

Step 3

Report on model performance

The final step in model validation is to provide visibility of the overall model design and performance. At this point, the model strengths and weaknesses are well understood and documented, from both a design and operational efficiency perspective. All the findings, problems and weaknesses identified during model validation are clearly articulated, including the various types of analysis conducted when completing the assessment. Outcomes must be reported to appropriate internal bodies and any actions agreed, monitored to resolution and followed-up in a timely manner.

The application of TM models across the vast majority of FIs globally, truly reflects the extent to which an effective and well-designed TM model can improve business decisions, risk management and reduce costs. The need for a robust model validation process that provides effective challenge is a necessity that cannot be overlooked.



Andrew Oates

Partner, Forensic Technology

M: +44 (0) 7901 554 920

E: aoates@deloitte.co.uk



Paul Fenton

Director, Forensic

M: +44 (0) 7901 513 136

E: pafenton@deloitte.co.uk



Flavio De Castro Oliveira

Assistant Director, Forensic

M: +44 (0) 7721 967 510

E: fdecastrooliveira@deloitte.co.uk



Matthew Gementera

Assistant Manager, Forensic

M: +44 (0) 7827 954 641

E: mgementera@deloitte.co.uk



This document is confidential and it is not to be copied or made available to any other party. Deloitte LLP does not accept any liability for use of or reliance on the contents of this document by any person save by the intended recipient(s) to the extent agreed in a Deloitte LLP engagement contract.

If this document contains details of an arrangement that could result in a tax or National Insurance saving, no such conditions of confidentiality apply to the details of that arrangement (for example, for the purpose of discussion with tax authorities).

Deloitte LLP is a limited liability partnership registered in England and Wales with registered number OC303675 and its registered office at 1 New Street Square, London, EC4A 3HQ, United Kingdom.

Deloitte LLP is the United Kingdom affiliate of Deloitte NSE LLP, a member firm of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"). DTTL and each of its member firms are legally separate and independent entities. DTTL and Deloitte NSE LLP do not provide services to clients. Please see www.deloitte.com/about to learn more about our global network of member firms.

© 2020 Deloitte LLP. All rights reserved.