Transaction monitoring model validation

An approach to self-attestation

The bar for transaction monitoring by financial institutions has been raised during the past decade. Recently, several banks have been confronted with high fines relating to insufficient and ineffective transaction monitoring. There is an increasing number of regulators that expect (mainly) banks to perform self-attestations with respect to their transaction monitoring models. This is, however, a complex exercise with many challenges and pitfalls. This article aims to provide some guidance regarding the approach and methods.

Jori van Schijndel MSc
is a manager at KPMG Advisory N.V.
vanschijndel.jori@kpmg.nl

Chrit van Beusecom MSc
is a manager at KPMG Advisory N.V.
vanbeusecom.chrit@kpmg.nl

INTRODUCTION

Many people consider financial crime like money laundering as a crime without real victims. Perhaps a large company loses money, or the government gets fewer taxes, but nobody really suffers true harm. Sadly, this is far from the truth. From human trafficking, to drug wars and child labor, the human cost of financial crime is very real and substantial. Financial crime is therefore considered to be a major problem by governments around the world. As a consequence, increasingly strict regulations regarding transaction monitoring where imposed on the financial industry since the beginning of the financial crisis as they are the gatekeepers to the financial system. These regulations have predominantly, although not exclusively, an effect on banks. Financial institutions are increasingly confronted with complex compliance-related challenges and struggle to keep up with the development of regulatory requirements. This especially applies for financial institutions that operate on a global level and that are using legacy systems. The penalties of non-compliance are severe as demonstrated by amongst others UBS with a fine of 5,1 billion (USD) and a case in The Netherlands where ING Bank settled for €775 million with the public prosecutor. As time progresses, the bar for financial institutions is being raised even higher.

In 2017, the New York State Department of Financial Services (NYDFS) part 504 rule became effective. The NYDFS part 504 requires – starting in 2018 – that the board of directors or senior officers annually sign off on the effectiveness of the transaction monitoring and filtering processes, and a remediation program for deficiencies regarding internal controls. The nature of the NYDFS part 504 rule is similar to that of the SOx act. This seems to be a next step in transaction monitoring regulatory compliance requirements.

For example, the Monetary Authority of Singapore has increased its focus both on anti-money laundering compliance as well as independent validation of models. In the Netherlands, De Nederlandsche Bank (DNB) as supervisory authority has issued a guideline in December 2019 ([DNB19]) regarding, for now, voluntarily model validation with respect to transaction monitoring.

Given the increased attention for transaction monitoring and model validation (self-attestation), this article zooms in on the way model validations for transaction monitoring can be approached. The next section contains an overview of the compliance framework for transaction monitoring after which the common pitfalls and challenges for model validations are discussed. The five-pillar approach of KPMG enables financial institutions to cope with these pitfalls and challenges and is also explained as an outlook to the near future regarding transaction monitoring and technologies for model validation. Finally, a conclusion is provided.

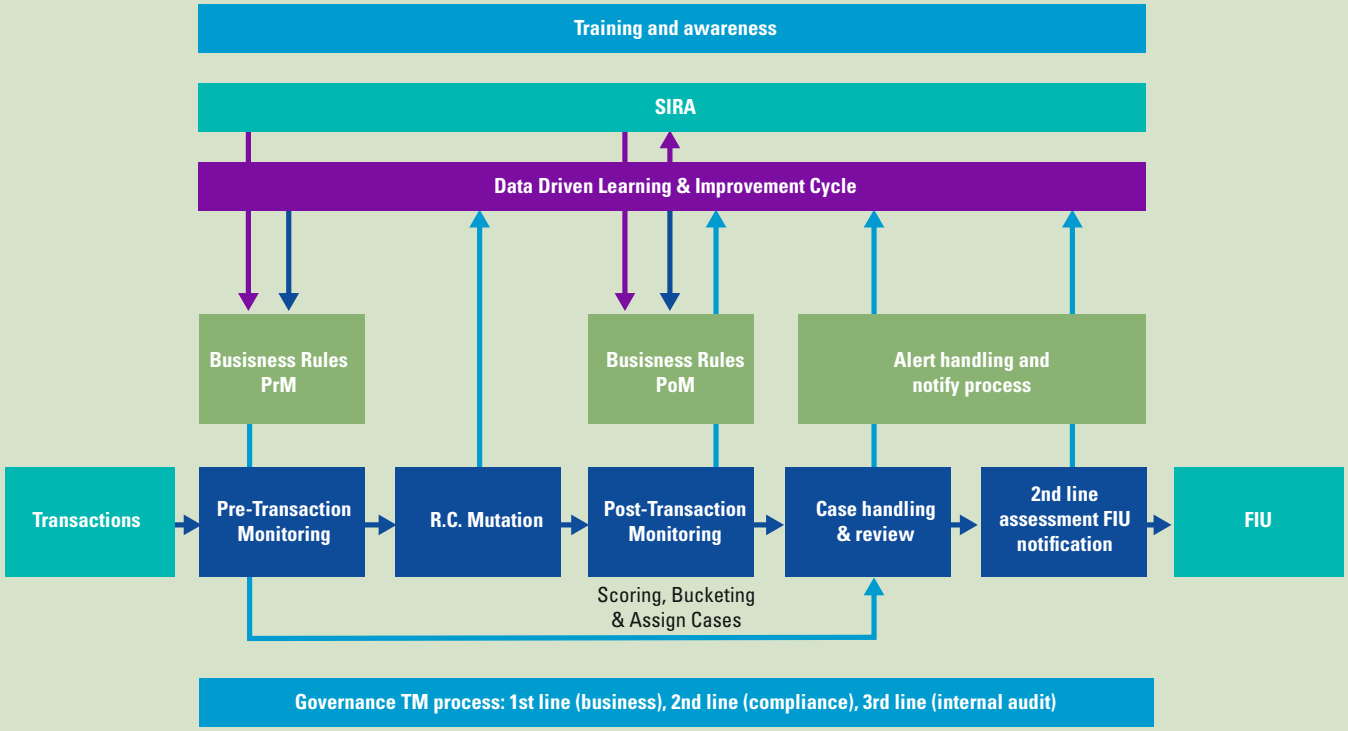
High-level transaction monitoring process

Before discussing model validation in more detail, it might be helpful to provide a high-level overview of the transaction monitoring process, as an example of a compliance model. Figure 1 contains a graphical high-level overview. The SIRA (Systematic Integrity Risk Analyses) and the transaction monitoring governance are at the basis of the process. When transactions are initiated, pre-transaction monitoring activities are triggered (e.g. with respect to physical contact with the client, relating to trade finance or Sanctions) based on business rules. This might result in alerts which are followed up in accordance with the governance and escalation procedures.

Inbound and outbound transactions ("R.C. Mutations") are processed after which post-transaction monitoring activities are triggered based on business rules, again resulting in potential alerts which are followed up and reported to the FIU if required (Financial Intelligence Unit, a supervisory authority regarding money laundering and terrorism financing).

Parallel to daily activities a data-driven learning and improvement cycle is in place in order to decrease false positive and false negatives alerts and to increase efficiency.

Figure 1. High-level overview of the transaction monitoring process ([DNB17]).



COMPLIANCE FRAMEWORK

Banks and other financial institutions use a multitude of models to perform quantitative analyses like credit risk modeling. As a response to the increased reliance on such models, different regulators as well as other (inter)national organizations have issued regulations and guidance in relation to sound model governance and model validation.

Within the compliance domain we see an increasing reliance on compliance models, like transaction monitoring systems, client risk scoring models or sanction screening solutions. These models are used to ensure compliance with laws and regulations related to, among other, money laundering, terrorism financing and sanctions. Where these models are intended to mitigate specific integrity related risks like the facilitation of payments related to terrorism, the usage of such models introduce model risk. And if not handled well, can result in an unjustified reliance on the model. Therefore, the model-related guidance, either specifically related to the compliance domain or more general, is equally relevant for compliance models. Examples include Bulletin OCC 11-12 from the Federal Reserve and Office of the Controller of the Currency or the Guidance for effective AML/CFT Transaction Monitoring Controls by the Monetary Authority of Singapore. The DNB has presented guidance on the post-event transaction monitoring process for banks on how to set up an adequate transaction monitoring model and related processes, including a solid Three Lines of Defense.

Internationally, different regulators have not only issued guidance in relation to model risk and sound model governance. They have additionally introduced or are requesting reviews, examinations and even mandatory periodical attestations by the board of directors or senior officers to ensure that compliance models are working as intended and that financial institutions are in control of these models. For example, the New York Department of Financial Services (NYDFS) requires senior officers to file an annual certification attesting to compliance with the NYDFS regulations that describe the minimal requirements for transaction monitoring and filtering programs. The DNB for instance has stated, in the updated guidance on the Wwft and SW, that both the quality and effectiveness of e.g. a transaction monitoring system must be demonstrated and that by carrying out a model validation or (internal) audit, an institute can adequately demonstrate the quality and effectiveness of such a model.

In our experience, banks are increasingly considering compliance models to be in scope of the regular internal model validations processes that already being performed for more financially related models, requiring sign-off by internal model validation departments prior to implementation and/or as part of ongoing validation of e.g. transaction monitoring systems. Additionally, compliance departments as well as internal audit departments are paying more attention to the internal mechanics of compliance models rather than looking at merely the output of the model (e.g. generated alerts and the subsequent handling). Especially due to recent regulatory enforcements within the EU and specifically the Netherlands, we have seen the topic of compliance model validation being more and more part of the agenda of senior management and the board, and banks that are allocating more resources to compliance models.

Given the increased awareness by both external parties such as regulators, as well as internal parties at financial institutions, these models introduce new risk management challenges. Simply put; how do we know and show that these compliance models are functioning as intended?

ISSUES, PITFALLS AND CHALLENGES

Effectively managing model risk comes with several issues, pitfalls and challenges. Some of these are part of the overall model risk management (MRM) process and other relate more specifically to compliance models. We have also seen recurring observations, findings or deficiencies in models that can impact both the efficiency and effectiveness of the models. This section describes some of these challenges and deficiencies so that when designing, implementing and operating compliance models or when validating or reviewing such models, these can be considered upfront.

KPMG has conducted a study to identify key issues facing model developers and model risk managers. This study, which is not specifically focused on compliance models, shows that key issues include that the definition of a model is subjective or even obscure and that the dividing line between a model and a more simpler computational tool – like an extensive spreadsheet – keeps shifting towards including more and more tools as a model. In addition, creating a consistent risk rating to apply to both models as well as model-related findings, is considered difficult, making it difficult, if not impossible, to quantify individual model risk as well as the organization's aggregate model risk. Other key issues include not having a consistent IT platform, inefficient processes and the difficulty in fostering an MRM culture.

More specifically, compliance models may have certain challenges that can be extra time-consuming or painful. For many financial institutes, the current validation of e.g. a transaction monitoring system is a first-time exercise. This means that the setup and overhead costs are high when organizations recognize that certain crucial elements are not adequately documented or dispersed across the organization, making the start of a full-scale validation difficult.

Perhaps there isn't even sufficient insight into all the relevant source systems and data flows that impact the models.

From an ownership perspective more and more activities related to compliance models, which historically have been more managed by compliance departments, are being introduced to the first line of defense. This means that e.g. certain historical choices have been made and are unknown by the current system owners when such choices have not been historically documented.

For financial institutes that have activities in multiple countries, the lack of a uniform regulatory framework means that incorporating all relevant global and local requirements can be challenging. Even within the EU, although minimal requirements are similar, certain requirements, like what constitutes sufficient verification or what are mandatory sanctions lists, may differ per country. Outside the EU, even more distinct requirements might be relevant. What is sufficient in one jurisdiction might be insufficient or even unacceptable in another.

Because compliance models, due to regulatory pressure, are getting more resources to improve and upscale current activities, models are less static than before and become a moving target with frequent changes to data feeds, scenario logic, system functionality or even complete migrations or overhauls of current models. In addition, increased staffing in relation to compliance models, means many new employees don't have the historical knowledge of the models and we also see difficulties in the market when recruiting and retaining sufficient and skilled people.

An inherent element of such compliance models, similar to e.g. fraud-related models, is the lack of an extrinsic performance metric to determine the success or sufficient working of the model. Transaction monitoring systems or sanction screening solutions currently have a high "false positive" rate of alerts of sometimes as high a 99%. When banks report unusual or suspicious transactions they generally lack the feedback from regulatory organizations to determine if what they are reporting is indeed valuable (i.e. being a true positive). Furthermore, for all transactions that are not reported, banks do not know if these are indeed true negatives or that these perhaps still relate to money laundering. This uncertainty makes it very difficult to objectively score model performance compared to more quantitative models that are used to e.g. estimate the risk of defaulting on a loan.

All these elements make the validation of these compliance models a major challenge, something financial institutes are confronted with.

When financial institutions actually conduct a model validation or when internal or external reviews or examinations are conducted, this can result in findings like model deficiencies. Based on public sources and supplemented with KPMG's experience, certain recurring of common compliance model deficiencies resulting from validations or examinations are ([Al-Ra15], [OM18]):

- Monitoring not being applied at the correct level of granularity. E.g. monitoring individual accounts instead of the aggregate behavior of customers, entities or ultimate beneficial owners or monitoring being done across various separated systems;
- Application of different character encodings which are not completely compatible or inadvertently applying case-sensitive matching of terms and names;
- Applying capacity-based tuning and system configurations instead of a setup commensurate with the risk appetite of the organization;
- Programming errors or fundamental logic errors resulting in unintended results[1];
- A lack of detailed documentation, appropriate resources and expertise and/or unclear roles and responsibilities to effectively manage and support model risk management activities;
- A conceptual design that is inconsistent with the unique integrity risks of an organization and minimal regulatory expectations;
- Insufficient risk-based model controls to ensure consistent workings of the system;
- Issues related to data quality like the incomplete, inaccurate or untimely transfer of transactional or client data between systems that feed into the compliance model.

Model risk management is a process wherein institutes should be able to demonstrate to, among other, regulators that their compliance models work as expected and that the model risk aligns to the risk appetite of the bank. Therefore, both the challenges and common model deficiencies mentioned in this section are relevant to consider when commencing a model validation.

FIVE-PILLAR APPROACH: AN APPROACH FOR TRANSACTION MONITORING MODEL VALIDATION

When discussing model validation, it is helpful to elaborate on the foundations first. For more statistical mod-

1 An example of a logical error, or undocumented limitation, can be that a system is configured to detect specific behavior or transactional activity within a week period instead of a 7-day period. I.e. when a certain combination of transactions occurs on a Monday till Wednesday, this generates an alert, whereas when the exact same behavior occurs on a Saturday till Monday nothing is detected due to the system setup instead of due to a deliberate design of the logic.

els, the task of model validation is to confirm whether the output of a model is within an acceptable range of real-world values to fit the intended purpose. Looking at compliance models, model validation is intended to verify that models are performing as expected, to validate whether the model is in line with the intended purpose and design objectives, and business uses. The validation is also used to identify potential limitations and test assumptions and assesses their potential impact.

During the validation it is substantiated that the model, within its domain of applicability, processes a satisfactory range of accuracy consistent with the intended application of the model and the validness of the assumptions underlying it.

To validate models, an approach is required. Whereas for certain statistical or predictive models there are a lot of well-established techniques, for compliance models this is less the case; the validation approach is highly dependent on the model, type of model and system being used and the validation of compliance models is a relatively new domain. KPMG has developed an approach consisting of five interrelated pillars. The approach has been successfully used globally for both international banks as well as smaller institutions and has evolved based on global and local practice experience.

KPMG's global model validation approach

The KPMG approach for transaction monitoring model validation consists of five pillars:

1. Governance
2. Conceptual Soundness
3. Data, System & Process Validation
4. Ongoing & Effective Challenge
5. Outcomes Analysis & Reporting

Governance
For an effective model, not only the technical model but also its governance, is a prerequisite to success. The governance framework related to the model needs to be reviewed. This review should include policies and procedures, roles and responsibilities, resources and training for comparison against existing authoritative standards for compliance and controls programs as well as industry leading practices and experiences with comparative institutions. This is predominantly done by conducting interviews with stakeholders based on structured questionnaires and documentation review.

Conceptual Soundness
The foundation of any compliance model is its conceptual design. Therefore, an assessment is required regarding the quality of the model design and development in order to ensure that the design criteria used in model design follow sound regulatory requirements and industry practice. In addition, key actions include a review of the risk evaluation, rules/settings assessment and the assessment of developmental evidence and supporting analysis.

Data, System & Process Validation
A (conceptual) design of a model generally gets implemented into an information system which requires (input) data to function and has processes that govern aspects of the system regarding, for example, change management. This pillar of the validation approach has three main types of activities that differ depending on the exact model and system being used:

- The first type of activity involves performing a number of tests to assess whether data feeds and information from ancillary systems are appropriately integrated into the models. Preferably this is done from and end-to-end perspective (from data creation to processing to retention).
- The second activity involves testing the system to assess its core functionality is working as intended. For example, for a Transaction Monitoring system, rules may be (independently) replicated based on documentation to determine if they are implemented and working as designed. Additional or alternative tests, depending on the model, can be considered, such as control structure testing or code review.
- The third and final component involves reviewing the processes that govern the use of the system.

Ongoing & Effective Challenge
A model's effectiveness needs to be assessed on an ongoing basis to ensure that changes in products, customers, risks, data inputs/outputs, and regulatory environment do (not) necessitate adjustment, redevelopment, or replacement of the model or whether model limitations and assumptions are still appropriate. Key activities of this pillar include ongoing verification, sensitivity testing (safeguarding the balance between the number of alerts and missing false negatives), performance tuning, and quantitative and qualitative benchmarking with peer organizations.

Outcomes Analysis & Reporting
Outcomes analysis compares and evaluates prospective scenario or rule changes, scoring, or alerting process changes to historical outcomes. This way, opportunities for efficiency improvements or to substantial parameter changes that may exist are identified. The key activities of this component include outcomes analysis and reporting.

As the validation of compliance models is a relatively new domain, model validations are struggling with the required level of depth needed to do an adequate validation without going beyond what is required. The use of a global methodology allows for a consistent and structured approach and way-of-working with both the benefit

of consistency throughout time, locations and different institutions as well as having an approach that maps back to regulatory guidance. This methodology needs to be able to cope with regulatory compliance differences per jurisdiction.

TRANSACTION MONITORING OUTLOOK

Enhanced compliance frameworks, digitalization and globalization causes transaction monitoring to become more and more intricate. In addition, due to growing polarization between certain countries, also the sanctions regimes are increasingly complex. How can organizations tackle these issues?

As a consequence of the digitalization, the availability of unstructured data has also increased significantly over the last years. It is therefore no surprise that applying artificial intelligence (AI) and machine learning (ML) for models is advancing rapidly. Also financial institutions are having their initial experiences in using AI/ML in reducing both false positives to increase efficiency as well as trying to detect the, previously unknown, false negatives to increase effectiveness. This is happening while they are also trying to reduce, or at least control, the costs of monitoring.

When looking from a validation perspective, however, there are some attention points when using AI and ML for compliance models. The first attention point is the knowledge and experience of the model developers with AI and ML. Due to the complexity, it is hard to master AI and ML and as a consequence reach conceptual soundness if these techniques are used. In addition, there is the risk that the model becomes a black box which is only understood by a few staff members. That way key man risk regarding the model potentially becomes an issue as well. This makes the model less transparent. The complexity of applying AI and ML to large volumes of data for modelling makes it hard to ensure the integrity and unbiasedness of data. By using integrity validation rules to collect data, the model can become biased as a consequence of decision making by the developers.

In the author's opinion challenges as mentioned above should not withhold financial institutions to selectively apply AI and ML. But they do require extra attention for regular model validation, develop AI and ML capabilities within the organization and enhancing the risk culture. For financial institutions that are still in the beginning of their AI and ML journey, it might be interesting to start applying it for the challenger model in the validation process of the current transaction monitoring model.

Another interesting development in the field of transaction monitoring is that on 19 September 2019, the Dutch Bank Association announced that five Dutch Banks (ABN AMRO, ING, Rabobank, Triodos and Volksbank) will join forces and set up an entity for transaction monitoring: Transaction Monitoring Netherlands (TMNL). Other banks can join at a later stage. This does however require a change to existing legislation (competition related). It will be interesting to follow this development and to see whether new entrants may also join this initiative. In addition, it is the question whether the business case can be realized, since this TMNL only monitors domestic traffic. It will be interesting to see whether similar initiatives will be launched elsewhere in the EU.

CONCLUSION

Regulatory requirements regarding financial crime are making it increasingly complex for financial institutions to become and stay compliant with respect to transaction monitoring. Having a model for transaction monitoring is not sufficient anymore. Regulators are increasingly expecting financial institutions to be able to demonstrate effectiveness of transaction monitoring and in the process of doing so, to validate their models. Certainly for financial institutions that operate internationally, this has proven to be quite a (costly) challenge. The best way to validate a model is to start with a broad perspective and include processes and activities that surround the model as well. The five pillars cover the required areas for model validation. However, there is no one single way of validating a model. The focus regarding the five pillars depends on the nature of the model. AI and ML can be utilized for both the model and to serve as a challenger model. However, in practice the application of AI and ML also creates challenges and potential issues. Collaborating with FinTechs or join forces as financial institutions might be a key with respect to ensuring compliance and keeping the cost base at an acceptable level.

References

[Al-Ra15] Al-Rabea, R. (2015, September). *The Challenge of AML Models Validation.* Retrieved from: http://files.acams.org/pdfs/2016/The_Challenge_of_AML_Model_Validations_R_Al_Rabea_Updated.pdf

[DNB17] De Nederlandsche Bank (2017). *Post-event transaction monitoring process for banks.*

[DNB19] De Nederlandsche Bank (2019, December). *Leidraad Wwft en SW.*

[OM18] Openbaar Ministerie (2018). *Onderzoek Houston: het strafrechtelijk onderzoek naar ING Bank N.V. Feitenrelaas en Beoordeling Openbaar Ministerie.* Retrieved from: https://www.fiod.nl/wp-content/uploads/2018/09/feitenrelaas_houston.pdf

About the authors

Jori van Schijndel MSc is a manager at KPMG Advisory N.V. He is part of the Forensic Technology team and is focused on the combination of technology and financial economic crime.

Chrit van Beusecom MSc is a manager at KPMG Advisory N.V. He is part of the Innovation Advisory team and is focused on risk and governance in combination with payments, FinTech and banking.