HONG KONG MONETARY AUTHORITY
香港金融管理局

Insights for Design, Implementation and Optimisation of Transaction Monitoring Systems

April 2024

Introduction

Since the AML/CFT Regtech Forum in 2019, the HKMA has been supporting the digital transformation of the AML eco-system, identifying opportunities for Authorized Institutions (AIs) to adopt Regtech in AML work, including through the AML Regtech Lab (AMLab) series.

Machine learning[1], a specific type of Artificial Intelligence with potential to help address excessive false positive alerts in transaction monitoring and screening was a topic discussed extensively in the 2019 Forum. Optimisation of systems and operations, including data and infrastructure, as well as developments in people and capabilities were identified as foundational elements in supporting progress.

To help enable these changes, we have targeted our supervisory engagement in two ways. First, in some of our publications we shared specific practical user experiences from AIs[2]. Second, recognising that rule-based TM systems[3] remain an essential element of AML/CFT controls, we targeted knowledge gaps through a thematic review.

AIs which have been successful in significantly reducing system inefficiencies using machine learning and other Regtech tools have done so by setting clear outcomes and good design principles, recognising that there are no simple plug-and-play shortcuts. They have recognised the importance of leveraging institution-specific knowledge, integrating subject matter experts into the innovation process.

[1] Machine learning is subset of artificial intelligence techniques that can train and improve algorithms based on large datasets without human intervention, which then makes predictions or decisions.

[2] "AML/CFT Regtech: Case Studies and Insights" Volume 1 published in January 2021 (https://www.hkma.gov.hk/eng/news-and-media/press-releases/2021/01/20210121-3/) and "AML/CFT Regtech: Case Studies and Insights" Volume 2 published in September 2023 (https://www.hkma.gov.hk/eng/news-and-media/press-releases/2023/09/20230925-3/).

[3] The term, *TM system* in this document refers to an automated system producing alerts to help identify unusual transactions or abnormal pattern.

Background

AIs are required to establish and maintain adequate systems and processes to monitor customer transactions. The design, degree of automation and sophistication of these systems and processes should be commensurate with the nature and size of AIs' businesses and level of ML/TF risks.

A deep-dive thematic review was conducted, focusing on the end-to-end processes of design, implementation and optimisation of TM systems. The review utilised technology solutions to review the data integrity, scenario logic and parameter and threshold settings of AIs' TM systems.

This report summarises the key observations from the thematic review, including a number of case studies, and provides insights for AIs to strengthen the design, implementation and optimisation of TM systems to make them more effective and efficient, including by adopting more advanced technologies. This report also shares relevant Regtech adoption cases that have demonstrated improved outcomes in respect of TM systems, and which supplement use cases provided in recent HKMA technology publications.

This report should be read in conjunction with the AML/CFT Guideline[4], guidance papers[5] and circulars issued by the HKMA which provide guidance in other areas relevant to TM systems.

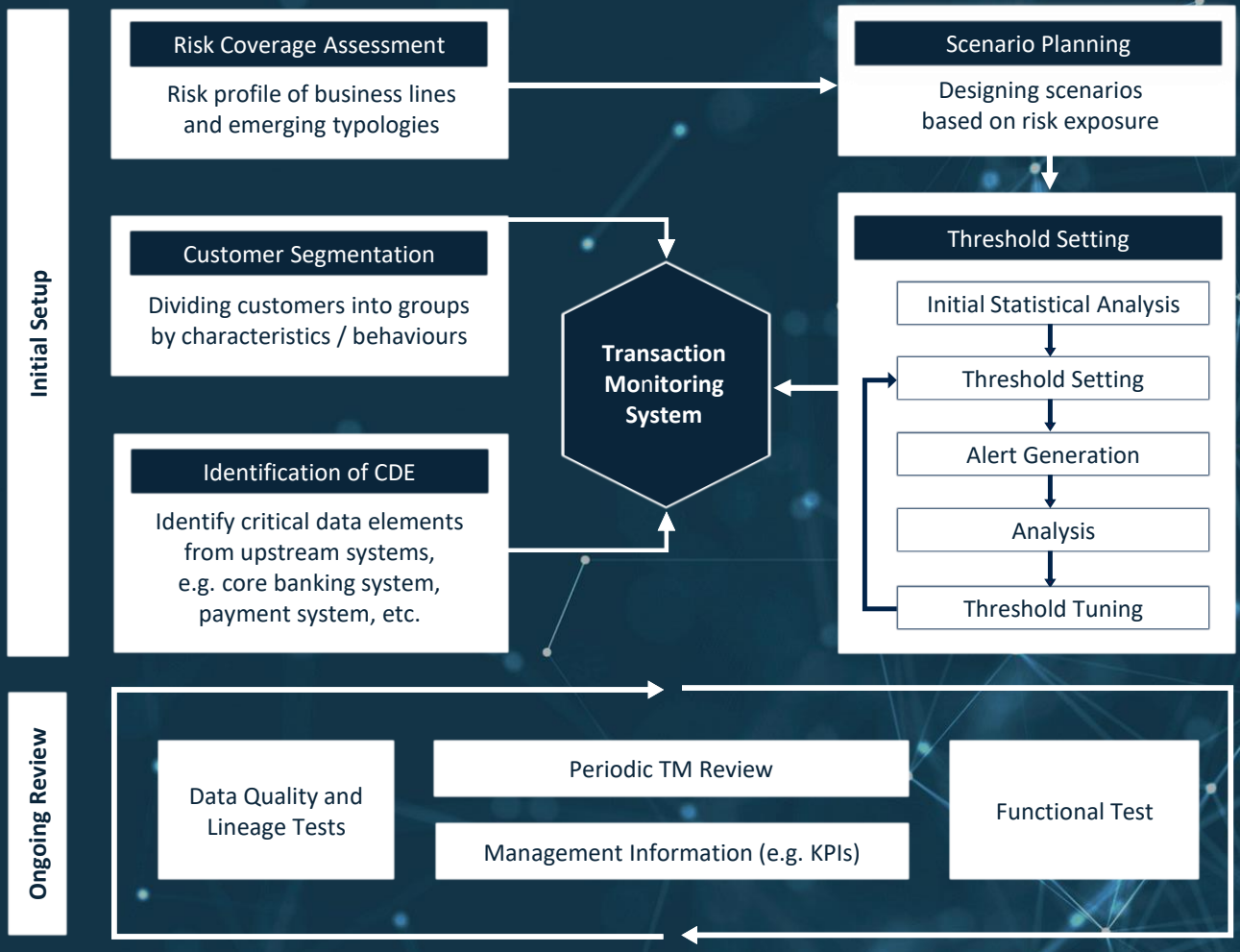
[4] See especially Chapter 5 of the Guideline on Anti-Money Laundering and Counter-Financing of Terrorism (For Authorized Institutions) on TM systems.

[5] For example, HKMA Guidance Paper for Transaction Monitoring, Screening and Suspicious Transaction Reporting issued in February 2023.

Key processes of design, implementation and optimisation of transaction monitoring systems

The thematic review covered AIs' processes for design, implementation and optimisation of TM systems. In general, these included:

- Management oversight and governance
- Assessment of the risk coverage of the TM system and selection of detection scenarios
- Identification of Critical Data Elements (CDE)
- Data quality and lineage testing
- Customer segmentation
- Threshold setting and tuning
- Functional testing
- Periodic review
- Optimisation using Regtech, including Artificial Intelligence

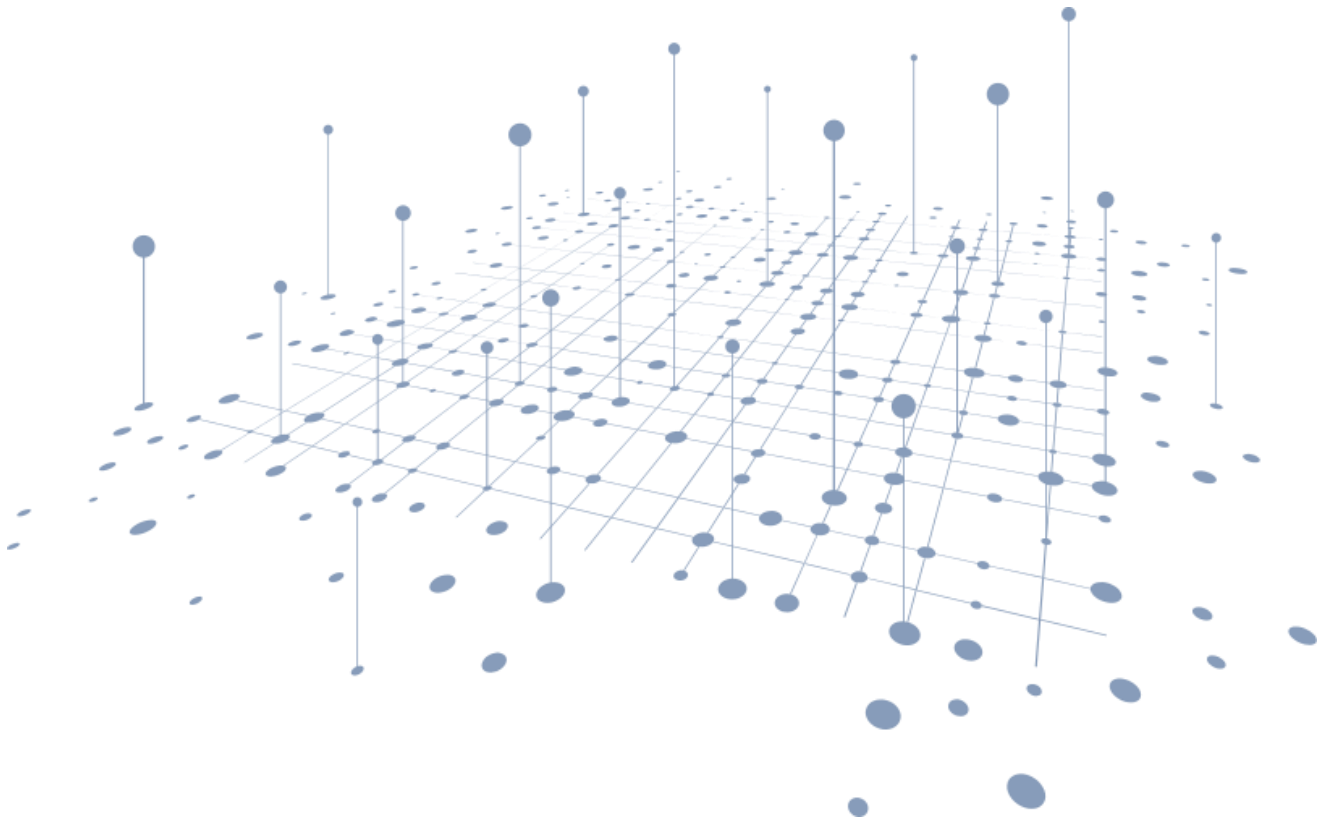


01 Management oversight and governance

Management oversight and governance are crucial to ensuring that an AI's TM system is adequately designed and implemented, and functions effectively to detect ML/TF risks which may arise from the AI’s product and service offerings and customer base[6].

Most AIs reviewed had established committees to oversee the cycle of development, implementation and ongoing enhancements of TM systems, as well as assessment of risk coverage, tuning and optimisation of system settings, and system effectiveness indicators.

[6] See paragraph 2.12 of the HKMA Guidance Paper for Transaction Monitoring, Screening and Suspicious Transaction Reporting issued in February 2023.



Case Study

One AI demonstrated strong management oversight and governance over the design and implementation of its TM system:

Oversight committee

The AI's AML committee provided appropriate and effective oversight of its TM system, by including stakeholders from the AML, technology, operations and business units. System implementation was promptly and appropriately addressed in the AML committee and escalated to senior management when necessary. A strong audit trail was maintained, including adequate records of discussions and justifications for decisions taken.

Ongoing monitoring of system performance

A tuning report driven by Key Performance Indicators (KPI) was compiled annually to identify possible enhancements to detection scenarios, thresholds and segments. The KPIs are calculated based on factors such as numbers of active customers, alerts and productive cases and the STR conversion rate. Proposed changes triggered by the tuning report are reviewed and approved by the AML committee.

02 Assessment of risk coverage of TM system and selection of detection scenarios

AIs are expected to be able to demonstrate that the design of a TM system is commensurate with the size and complexity of their business, nature of products and services and associated ML/TF risks.

Most AIs reviewed were able to do this, at differing levels of detail. A number of AIs undertook regular assessments of the risk coverage of their TM systems, including the transactional risks associated with the products and services offered. Such assessments provided justifications for the TM detection scenarios selected and any supplemental manual controls used (e.g. MIS reports).

Case Study

Risk coverage assessment for TM system

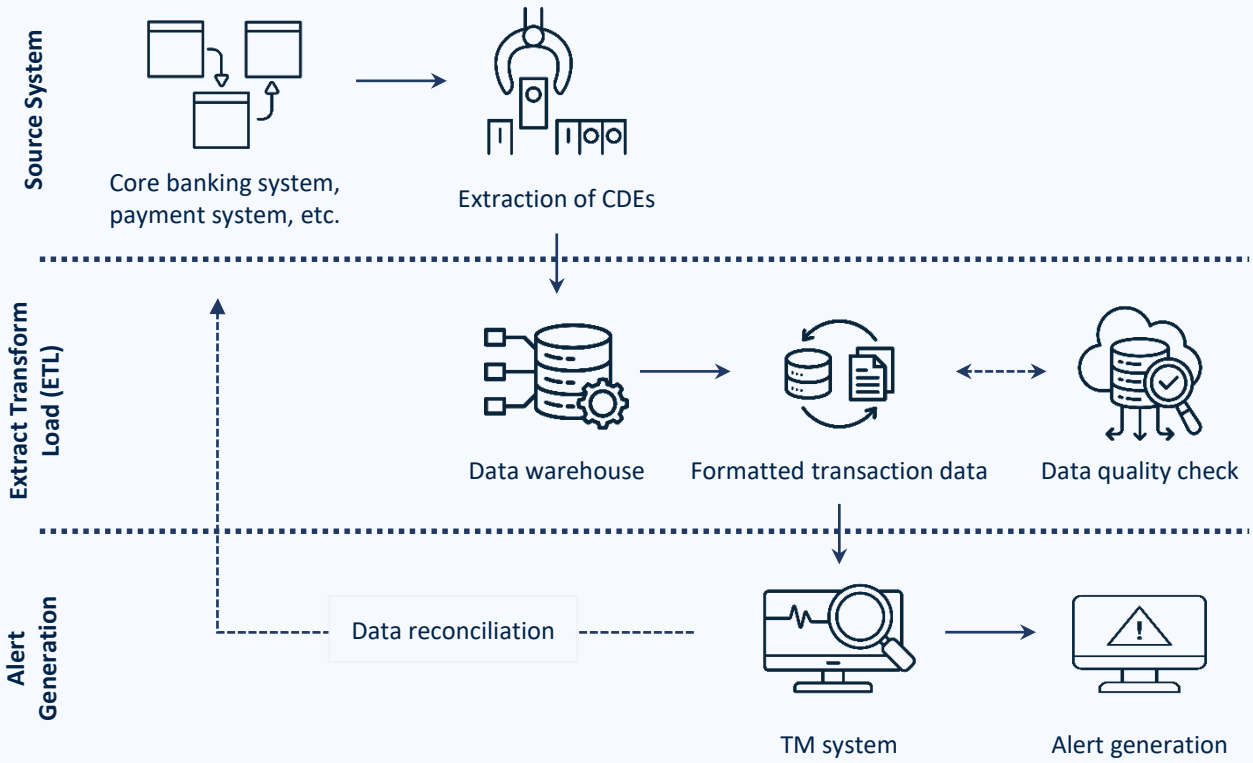
One AI included a risk coverage assessment in its annual review of its TM system, taking into account the risk profile of its different business lines / segments and typologies of existing and emerging threats, to assess whether the system adequately covered relevant ML/TF risks, and whether any enhancement was required.

Another AI covered new products and services to be launched during the year in its annual assessment to identify and assess any implications for its TM system, including whether new detection scenarios should be deployed to cover ML/TF risks associated with the new products. This practice also provides the AI's senior management with a better understanding of relevant ML/TF risks and helps facilitate allocation of resources, where required, to enhance the TM system.

03 Identification of Critical Data Elements

Critical Data Element (CDE) identification is one of the fundamental processes in establishing an effective TM system. It identifies all data points, which need to be fed into the TM system from different systems in the AI (e.g. core banking system and payment system) to ensure its proper functioning.

In particular, data explicitly used within detection scenarios are critical because of their direct impact on the accuracy and reliability of the TM system. All AIs reviewed were able to document key data fields related to their TM systems. Common CDEs include customer attributes (e.g. name and account number), transaction details (e.g. amount, date and type) and counterparty information (e.g. originator and beneficiary names and jurisdictions).



> ***There is a direct correlation between maturity and quality of data and the ability to leverage the opportunities presented by advanced technologies, such as machine learning.***

04 Data quality and lineage testing

The review included data quality tests to assess the completeness and validity of CDEs used in AIs' TM systems. Data lineage tests were also conducted to assess whether data had flowed correctly from the source systems to the TM systems. Most of the AIs had established mechanisms for regular data quality and lineage testing.

The review noted that most of the AIs had performed data reconciliation testing regularly (e.g. daily) or as part of periodic TM system reviews. Where no control processes for data quality and lineage testing were in place, the AIs were unable to ensure the accuracy and completeness of the data used in the TM systems.

In previous supervisory engagements, a few AIs showed weaknesses in accounting for certain critical data during changes made to core banking systems. This could lead to prolonged and significant gaps in monitoring, resulting in legal and regulatory risks. AIs are reminded to exercise care on data quality during system changes, and allow for sufficient testing and review.

Using Regtech to enhance data quality checks

AIs can use artificial intelligence to conduct data quality checks and improve the accuracy of TM system performance[7]. For example, artificial intelligence is able to identify and correct errors in large datasets quickly and accurately. It uses machine learning algorithms to identify patterns and inconsistencies in the data, and then applies automated cleansing techniques to correct errors, remove duplicates, and standardise data formats .

05 Customer segmentation[8]

Customer segmentation is used in TM systems to divide customers into groups based on shared characteristics or behaviours. This allows AIs to set appropriate thresholds for more targeted monitoring. In some cases, inappropriate segmentation led to less effective threshold setting and tuning with higher volumes of false-positive alerts. In addition to making the TM system less efficient, certain higher ML/TF risks may also be left un-monitored.

[7] For more examples of Regtech adoption, please refer to "AML/CFT Regtech: Case Studies and Insights" published in January 2021 (https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2021/20210121e2a1.pdf) and "AML/CFT Regtech: Case Studies and Insights Volume 2" published in September 2023 (https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/aml-cft/AMLCFT_Regtech-Case_Studies_and_Insights_Volume_2.pdf).

[8] Please refer to paragraph 2.8 of the HKMA Guidance Paper for Transaction Monitoring, Screening and Suspicious Transaction Reporting issued in February 2023.

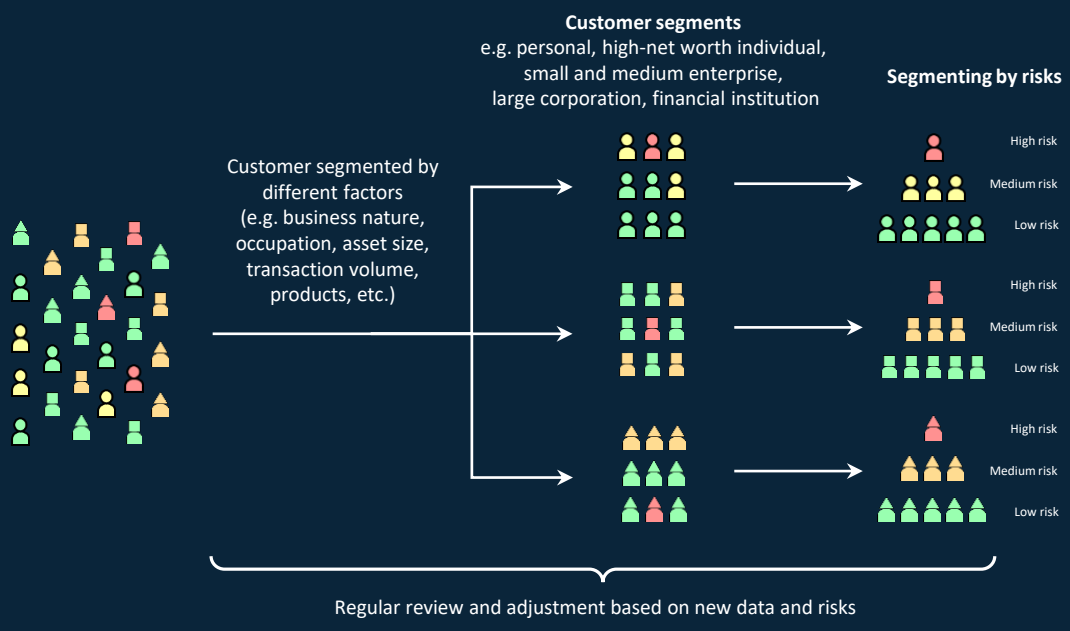
> *Appropriate customer segmentation reduces noise and improves the quality of alerts.*

Case Study

Key steps of customer segmentation

All the reviewed AIs applied customer segmentation to varying degrees in their TM systems. Common steps in the decision-making process included:

- Defining segmentation criteria: the factors used to group customers, such as transaction frequency, size and type, geographical location, occupation and business nature.
- Collecting transactional data and other relevant information, such as customer profile and transaction history.
- Analysing data using statistical methods (e.g. clustering and regression analysis) to group customers based on their characteristics or defined criteria.
- Further segmenting customers by risk: the initial segments can be further broken down by customer risk ratings to allow risk-based monitoring. High-risk customers' transactions are subject to more stringent thresholds for enhanced monitoring.
- Reviewing and refining customer segments: regularly review and adjust segmentation criteria based on new data or changing risk factors.



06 Threshold setting and tuning

Appropriate detection scenario thresholds are critical for the TM system to identify unusual or suspicious activities effectively and efficiently. Since institutions' risk exposures and appetites differ, AIs should tune threshold settings to align with their individual needs and circumstances.

Reviewed AIs generally adopted a risk-based approach to threshold setting and adjustment, which is supported by regular statistical analysis, e.g. reviewing value and volume of historical transactions, identifying any patterns requiring threshold adjustments, and reviewing alerts leading to STR filings.

Case Study

Statistical tools and methods for threshold setting and tuning

While there is no standardised method for threshold setting and tuning, reviewed AIs commonly used statistical methods to calibrate and tune parameters and thresholds. Examples include:

- Setting thresholds based on a certain number of standard deviations away from the mean of historical transaction data; or percentile rank among historical transaction amounts.
- Clustering analysis: grouping transactions based on criteria such as transaction amount or location, and setting thresholds to identify clusters that are more likely to be unusual.
- Above-the-line and below-the-line testing which involves adjusting current thresholds and parameters to arrive at an optimal configuration.
- Sensitivity analysis of how changes in input parameters, or configurations, such as scenario thresholds, rule configurations, or risk scoring models affect the TM model's performance.

While statistical methods can assist in threshold setting, AIs should be aware of the strengths and limitations of different approaches. It is important that AIs understand their risk profiles in order to determine the appropriate thresholds to detect unusual transactions for investigation. Some reviewed AIs were able to provide and document analysis supporting threshold setting and explaining how scenarios are configured to address risk exposure.

07 Functional testing

Functional testing is a critical aspect of TM system validation that ensures functional specifications are leading to intended outcomes. It is an effective way to identify technical issues such as data-mapping logic, incorrectly configured scenario thresholds, and transaction codes issues which can be difficult to identify through management dashboards or other monitoring approaches.

The thematic review used a technology solution to conduct functional testing, which replicated AIs' detection scenarios according to their TM system functional specifications, and then compared the outputs (e.g. alerts generated) between simulated and deployed scenarios. The majority of TM detection scenarios deployed by AIs were found to be functioning as intended. A few AIs conduct functional testing as part of regular TM system reviews to ensure accurate alerts are being generated for each scenario.

08 Periodic review

Reviewed AIs generally conducted periodic reviews and regularly configured TM systems to reflect changes to their risk profiles. Most had established tuning and optimisation policies that clearly articulated the methodology, protocols and frequency of TM system reviews.

Depending on the size and complexity of the AIs' business models, the frequency of periodic reviews ranged from 12 to 24 months. Some AIs' policies and procedures also stipulated ad-hoc TM system reviews following trigger events (e.g. surge of alert volumes, changes in AIs' products and services, emerging ML/TF typologies). Trigger event reviews allow timely and proactive optimisation to ensure the system is configured appropriately to address emerging risks and changes to AIs' business profiles. This also helps to reduce false positives/negatives.

Case Study

Key Performance Indicators (KPI) for TM systems

AIs had generally established KPIs, such as numbers of alerts generated or cases warranting further investigation, false positive rates and STR rates, to monitor and assess the effectiveness of their detection scenarios, customer segments, thresholds, and case-scoring models. These metrics were reported to the oversight committee quarterly and used to identify potential enhancements to increase efficiency while maintaining appropriate risk coverage. Using KPIs allows AIs to target transactions presenting higher ML/TF risks while minimizing false positives.

Engagement of subject matter experts for TM system review

A few AIs undertook TM system reviews with assistance from external subject matter experts. Using teams independent of the TM model developers or users to conduct model validation provides a fresh perspective and minimizes bias. Independent teams often have sector-wide experience and can bring new ideas, approaches and insights, which can help identify potential issues or weaknesses in the model that the development or user teams may overlook. Having independent experts review and validate the model can also increase confidence in the model's accuracy and reliability. In some AIs, the capability to undertake such testing was provided at Group level.

Trigger event review of TM system

One reviewed AI conducted ad-hoc threshold tuning analysis (including statistical, sensitivity and below-the-line and above-the-line analysis) to ensure thresholds were appropriate and able to generate productive alerts and remained responsive to the changing risk landscape.

09 Optimisation using Regtech, including Artificial Intelligence

Artificial Intelligence in AML/CFT

In response to the increasing volume of data generated by AML/CFT systems and increasingly sophisticated evolving threats, a number of AIs had explored or implemented innovative technologies, such as machine learning. The most common uses were in name screening and transaction monitoring, which involve high volumes of false positive alerts, and where appropriate improvements may free up resources for higher value work. This section sets out the HKMA's views on the use of artificial intelligence and advanced technologies for AML/CFT, and provides some use cases from different AIs.

Regtech for TM system optimisation

Machine learning for handling transaction monitoring alerts

An AI developed a machine learning model to assign an additional risk score to each TM alert. High-risk cases were prioritised and reviewed manually, while low-risk cases were auto-discounted and subject to sample checking. This enabled the AI to prioritise resources for high-risk cases using a more consistent approach.

Auditability was apparent throughout the development life cycle of the model, which was subject to regular reviews and calibration to ensure that it was performing as expected and continued to effectively identify unusual transactions, taking into account the AI's risk exposure. The model can also be adapted when required, based on emerging risks.

The model used is designed to ensure the performance of the algorithm improves over time, which is monitored through KPIs, including the percentage of alerts incorrectly discounted by the system.

Network analytics

A number of AIs have adopted network analytics to facilitate investigation of unusual transactions arising from TM alerts, allowing them to identify hidden relationships demonstrating suspicious behaviour for further investigation.

The HKMA's regulatory expectations

Given that artificial intelligence presents both opportunities and some new risk management challenges for AIs, the HKMA issued guidance in 2019[9] in the form of high-level principles on the use of artificial intelligence applications, covering governance, application design and development and ongoing monitoring and maintenance. These principles reflect sound industry practices and similar principles formulated by leading overseas authorities, and remain relevant to AIs considering adopting advanced technologies[10]. While AIs are expected to take these high-level principles into account when designing and adopting artificial intelligence applications, they are not intended to inhibit responsible innovation and development, including in AML/CFT work.

AIs considering the use of artificial intelligence in AML/CFT may clarify critical areas of controls and regulatory expectations in the HKMA's Fintech Supervisory Chatroom or through the Fintech Supervisory Sandbox. During such engagements and this thematic review, we have observed a number of good practices that underpin successful deployment:

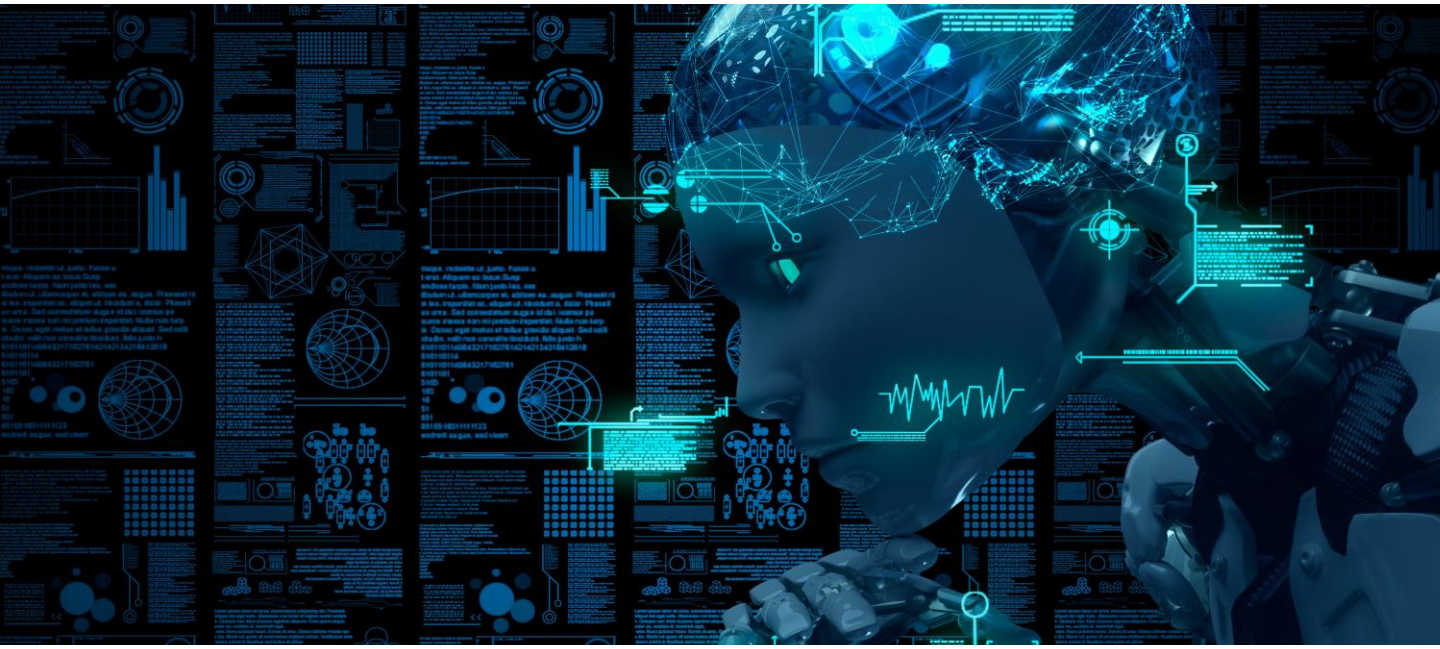
- Planning
- Readiness, talent and other considerations
- Change management
- Data governance and data quality
- Model testing, validation and periodic review
- Awareness of limitations

Planning

Certain applications (e.g. artificial intelligence, including machine learning in transaction monitoring alerts handling) are more complex and require higher levels of expertise than other applications, such as robotic process automation for repetitive tasks, that may be easier to integrate into an AI's existing processes.

[9] Please refer to the HKMA Circular 'High-level principles on Artificial Intelligence' published on 1 November 2019 (https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2019/20191101e1.pdf).

[10] In 2021, the Financial Action Task Force (FATF) addressed AML/CFT artificial intelligence related compliance and adoption issues in a report, which identified machine learning as having significant potential in AML/CFT by helping financial institutions to better identify risks and monitor suspicious activities (https://www.fatf-gafi.org/en/publications/Digitaltransformation/Opportunities-challenges-new-technologies-for-aml-cft.html).



The HKMA publications[11] provide guidance on the planning process, and steps to be taken before embarking on artificial intelligence adoption in the AML/CFT space. These include establishing a problem statement to identify pain points to be addressed and conducting a rigorous assessment to prioritise opportunities for adopting Regtech, including artificial intelligence. This process helps to identify opportunities in the areas of greatest interest (which may differ between AIs) and to ensure the solution is fit-for-purpose, while avoiding the pitfall of being overly focused on a particular technology.

It is also important to start discussions with stakeholders early and maintain close communication, to ensure the proposed approach aligns with management expectations.

Readiness, talent and other considerations

Whether or not the solution is developed in-house or sourced externally, it is critical for end-users to work closely with the technical experts and/or service providers so that requirements are clearly communicated. End-users should take an active role in relevant testing and provide feedback. In successful use cases, this collaboration continued throughout the application's deployment to mitigate the risk that the model could "drift" or its deviating from an expected outcome. Controls should be in place to review and ensure the application remains fit for purpose. Successful artificial intelligence deployments were supported by careful consideration of the AIs' readiness, not only in respect of the design and deployment but also the ongoing management.

Some AIs have co-creation partnerships with vendors to develop solution fit for their specific needs. For example, some AIs partnered with tech firms to participate in the HKMA's Fintech Supervisory Sandbox 3.0 (FSS 3.0) to explore AML Regtech use cases.

Change management

Most AIs had adequate oversight over change management. Some had established a taskforce to oversee the project and facilitate coordination, which often included subject matter experts in various areas, such as financial crime, data, technology, products and business operations.

Given that applications involving artificial intelligence and machine learning are able to automate the taking of certain decisions, a proper governance framework and supporting risk management are essential for helping the senior management to remain fully accountable for the outcomes and decisions made by advanced technologies.

[11] "AML/CFT Regtech: Case Studies and Insights" Volume 1 published in January 2021 (https://www.hkma.gov.hk/eng/news-and-media/press-releases/2021/01/20210121-3/), "AML/CFT Regtech: Case Studies and Insights" Volume 2 published in September 2023 (https://www.hkma.gov.hk/eng/news-and-media/press-releases/2023/09/20230925-3/), and "AML Regtech: Network Analytics" published in May 2023 (https://www.hkma.gov.hk/eng/news-and-media/press-releases/2023/05/20230509-3/).

Data governance and data quality

Since using artificial intelligence in AML/CFT controls, such as review of level 1 screening alerts, may give rise to legal and regulatory risks, some AIs have expressed concerns about adoption. In some cases, these concerns have been addressed through the HKMA's Fintech Supervisory Chatroom. For example, the quality and sufficiency of data are often cited as grounds for reluctance to adopt, given that accuracy and performance are heavily dependent on the data used to train the models. While these are legitimate concerns, they can be addressed by establishing effective data governance frameworks and sufficient data to support development and training of artificial intelligence models.

Model testing, validation and periodic review

AIs in general performed rigorous validation and testing of models before deployment of applications and as part of a process of periodic review, often involving an independent party.

Some AIs conducted a parallel run of the application in the early stages of deployment to ensure the model's appropriateness, by comparing against existing controls to assess whether the model is working as intended.

Awareness of limitations

AIs demonstrated a healthy level of caution regarding over-reliance on artificial intelligence for decision-making, and that such applications should be built on their understanding of their institutions' risks and risk appetite.

AIs also generally appreciated that money laundering is not a constant, and that typologies and techniques change and evolve. Models developed based on past data may not always be well-equipped to deal with emerging threats, and therefore should be subject to periodic review and evaluation.

Hong Kong Monetary Authority

55/F Two International Finance Centre,
8 Finance Street, Central, Hong Kong

Telephone: (852) 2878 8196
Fax: (852) 2878 8197
E-mail: hkma@hkma.gov.hk

www.hkma.gov.hk

For more information, please contact us at aml@hkma.iclnet.hk.