

GUIDANCE FOR EFFECTIVE AML/CFT TRANSACTION MONITORING CONTROLS

September 2018

Table of Contents

1	Introduction	2
	Use of this Guidance Paper.....	4
2	Execution of Transaction Monitoring	5
	Knowing the Customer	5
	Risk-based Calibration	5
	Robust Implementation.....	10
	Resolution and Enhancement	13
3	Risk Awareness.....	17
4	Governance	19
	Material Outsourcing of First Level Alert Reviews	21
5	Conclusion.....	23

1 Introduction

1.1 Transaction monitoring (“TM”) is a key control in financial institutions’ (“FIs”) anti-money laundering and countering the financing of terrorism (“AML/CFT”) policies and procedures:

- When on-boarding customers, FIs are required to perform risk assessments and due diligence checks to identify and mitigate any prospective money laundering and terrorism financing (“ML/TF”) risks, including proliferation financing (“PF”) risks, at the onset.
- However, risks can also manifest later, over the course of customers’ business relations with the FI.
- While these risk factors may be obscured at the on-boarding stage and during FIs’ performance of regular screening or periodic updates of customer information, they can often be detected through the robust conduct of TM.

1.2 An effective TM system enables FIs to detect and assess whether customers’ transactions pose suspicion when considered against their respective backgrounds and profiles. TM systems also facilitate the holistic reviews of customer transactions over periods of time, in order to monitor for any unusual or suspicious trends, patterns or activities that may take place.

1.3 An effective TM system is comprised of the following elements:

- **A well-calibrated framework:** The risks FIs face are dynamic and the transactions they carry out are varied and voluminous. FIs should therefore regularly review¹ and enhance TM frameworks, and also do so when trigger events occur. These reviews should be targeted at sustaining system effectiveness by imbibing the changing risk environment.
- **Robust risk awareness:** To ensure proper functioning and effectiveness of their TM systems, FIs must ensure that these are executed by competent and well-trained staff who exercise sound judgment in targeting unusual transactions, activities and behaviours.
- **Meaningful integration:** An FI’s AML/CFT regime is as strong as its weakest link. FIs should therefore ensure that their TM systems and frameworks reinforce, and are reinforced by, the broader AML/CFT controls that they employ. FIs should designate

¹ FIs with higher inherent risks or specific TM control deficiencies to address should perform more regular reviews in order to adequately mitigate their risks.

clear responsibilities for the effective conduct of TM across their three lines of defence, that comprise:

- FIs' frontline staff, who must be adequately equipped to establish good understandings of their customers' activities and behaviours, so as to alert their organisations to any unusual or suspicious activities in the first instance;
 - FIs' compliance and support functions, which perform systems-based TM and should be adequately equipped, managed, and resourced in order to promptly identify, assess and report unusual or suspicious transactions; and
 - Independent audit functions, which play an important role in testing and safeguarding the robustness of FIs' TM performance.
- **Active oversight:** Importantly, FIs' board and senior management must take an active role in overseeing the satisfactory performance of TM. FIs' board and senior management should drive the continual enhancement of their TM systems with a view to ensuring that their key risks are appropriately mitigated. When outputs or outcomes are compromised due to factors such as inappropriate calibration, process inefficiencies, staff issues or system failures, it is incumbent on the board and senior management to adequately resolve these matters in a prompt and timely manner. The board and senior management should communicate clear risk appetites within their organisations, and set a firm tone from the top that the detection, prevention and deterrence of ML, TF and PF are a priority.

1.4 When properly executed, TM allows FIs to gain deeper insights into their customers' profiles and behaviours, and strengthen their risk-based allocation of resources to tackling higher risk areas. Conversely, TM lapses expose FIs to the heightened risk of abuse as they allow illicit fund flows to be manoeuvred through Singapore's financial system, escaping detection. The consequences of such lapses can be severe, implicating these FIs and Singapore's financial system as a refuge or conduit for illicit funds.

Use of this Guidance Paper

1.5 Given the importance of robust TM, MAS conducted a series of AML/CFT banking inspections across Q4 2016 – Q2 2018 that scrutinised the effectiveness of banks' TM systems in the context of their broader AML/CFT regimes, using the following three pillar framework:



Diagram 1: Three Pillars of Effectiveness

1.6 This guidance paper reiterates the key recommendations by MAS to the inspected banks, setting out our supervisory expectations of sound practices for the effective conduct of TM. Additional context can be found in the box stories throughout the paper of case studies taken from MAS' onsite findings and our recommendations to FIs. The paper further highlights examples of best practices implemented by some of the inspected banks, which other FIs can consider emulating. Ultimately, while the paper does not impose any new regulatory obligations, FIs should nevertheless study and leverage on the guidance within to identify and address gaps in your execution of TM controls, to more effectively mitigate your ML/TF risks.

1.7 While this guidance paper is derived from MAS' banking inspection findings, the supervisory expectations and best practices therein are, with the appropriate modifications, equally relevant and applicable to other FIs. FIs should therefore incorporate the learning points from this guidance in a risk-based and proportionate manner, giving proper regard to the profile of their business activities and customers. In doing so, FIs should note that the takeaways in this paper are non-exhaustive, and they should continue to strengthen and refine their TM models according to their respective needs and context.

2 Execution of Transaction Monitoring

2.1 FIs should monitor and ensure the effective performance of TM at each stage of the TM process chain:

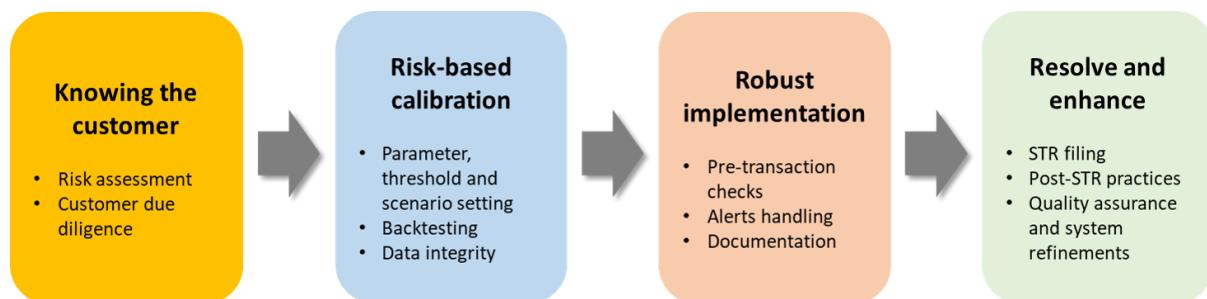


Diagram 2: TM Process Chain

Knowing the Customer

2.2 Effective TM is predicated on FIs' sound understanding of their customers, which provides the necessary context for FIs to identify unusual/anomalous transactions and assess whether customers' activity or behavioural patterns may pose reasonable suspicion. Before establishing business relations, FIs are required to perform customer due diligence ("CDD") checks and assess the level of ML/TF risks posed by their prospective customers. In this regard, FIs should ensure that (i) their risk assessment frameworks and methodologies and (ii) the scope and extent of CDD measures that they apply are aligned with the requirements in MAS' AML/CFT Notices, and more importantly enable them to detect and address risks posed by their customers.

2.3 After establishing a business relationship, FIs are required to maintain current and accurate knowledge of their customers through the performance of periodic reviews and/or reviews based on trigger events, and where appropriate enhance the frequency and intensity of customer engagement where the risks are assessed to be greater. Further guidance on the conduct of risk assessments and CDD will be set out in MAS' upcoming Guidance Paper on the findings and best practices from its AML/CFT inspections on capital markets intermediaries.

Risk-based Calibration

2.4 FIs are presently required to ensure that their TM systems are configured in view of their specific risks, contexts and needs. FIs with a larger scale of operations are expected to have in place automated systems capable of handling the risks from an increased volume and variance of transactions. While smaller FIs may rely on TM systems that are less automated,

they must still ensure that these are appropriately executed to satisfactorily address the risks from their day-to-day transaction activities.

i. *Parameter, Threshold and Scenario Setting*

2.5 When appropriately configured and implemented, TM parameters and thresholds enable FIs to flag unusual transactions with a reasonable degree of certainty of potential ML/TF characteristics warranting further inquiry. FIs should always ensure that their parameters and thresholds take into account their specific risks and context; and that they are appropriately back-tested for proper operation and effectiveness (see paragraph 2.11).

2.6 To this end, most banks perform risk-based customer segmentation in order to calibrate suitable parameters and thresholds for each segment, albeit there is room to improve how such segmentation is performed, and how the accompanying thresholds and parameters are derived. A good practice noted is that some banks have employed the use of certain statistical tools and methods such as above-the-line (“ATL”) and below-the-line (“BTL”) testing to better fine-tune their calibrations.²

2.7 In addition, banks have grouped TM parameters and thresholds into risk scenarios to enable them to more precisely target transaction patterns and behaviours consistent with known ML/TF typologies such as smurfing, pass-through payments, or circular flows involving opaque structures. Prior to implementing their HQs’ global TM parameters and scenarios, some banks performed assessments of the extent to which these parameters and scenarios complied with local requirements, and their effectiveness in addressing risks in the local context.

2.8 Aside from those mentioned above, other risk areas that banks have developed scenarios to detect include:

- Large or complex transactions with no visible/apparent economic or lawful purpose
- Aggregated frequent and small transactions
- Unusual patterns of physical cash deposits or withdrawals, which are large when aggregated over a period of time
- Significant deviations from past account activity (or inactivity)
- Transaction activities with nexus to higher risk countries or geographies
- Detection of activities or behaviours consistent with certain predicate offences (e.g. possible tax evasion or avoidance, corruption nexus, or terrorism financing)
- Hidden relationships between customers or accounts evident through funds flows

² ATL and BTL testing involves increasing and decreasing the pre-determined thresholds of TM rules in order to identify the best possible configuration, taking into account factors such as the efficiency of existing rules, the alert-to-case ratios obtained, and the extent of true hits and false positives/negatives generated by the tests performed.

- Anomalous activities involving the use of bank cards (e.g. ATM, credit or debit cards)
- Other anomalous and unexplained patterns or behaviours

2.9 The use of scenarios is not limited to banks or FIs with automated systems, as smaller FIs with less-automated systems should apply the same logic in training and guiding their staff to detect these more complex risks.

2.10 FIs should be mindful that there is no one-size-fits-all approach to configuring their TM rules, and that it is critical to ensure these are developed and calibrated in view of the risks they face, such as from their customer types, range of products, types of business activities, geographical exposures, cross-border nature and so forth. FIs should also bear in mind that the effectiveness of many of these rules hinges upon the proper conduct of holistic monitoring of customers with multiple accounts, and accounts of customers that are related/associated.³ FIs are reminded that the conduct of holistic monitoring is especially important for customers assessed to be politically-exposed persons (“PEPs”) or belonging to other higher risk categories.⁴ FIs should therefore ensure that TM is performed on a consolidated relationship basis and that their TM controls, whether at the system level or through processes, adequately cater for an aggregated view and assessment of multiple related accounts, including across business units.

ii. Back-testing

2.11 FIs should periodically test and refine their TM rules to ensure they remain current and effective in targeting riskier transactions and behaviours. Before effecting recalibrations, especially material recalibrations, FIs should assess whether to back-test the changes using sample data to ensure the proper functioning of new rules. FIs should also assess whether post-implementation testing should be performed to verify that the updates function according to expectations and do not inadvertently compromise the organisation’s conduct of TM. FIs should ensure that all testing outcomes and subsequent adjustments are properly justified and documented, and that senior management is appropriately apprised of key changes and outcomes. Where the back-testing results are deemed unsatisfactory, it is incumbent on FIs’ senior management to provide guidance and direction on remedying the issues.

2.12 From time to time, FIs may perform more comprehensive updates or sunset existing TM systems in order to migrate to newer platforms. In such cases, FIs should conduct user acceptance testing (“UAT”) and resolve outstanding issues before going live on new systems. In the interim, FIs should also assess the need for bridging measures to ensure the continued robustness of their TM and effective mitigation of transaction risks. Senior management

³ See Paragraphs 6.19-6.26 of MAS Notice 626, read in conjunction with paragraphs 6-10-10 and 6-10-11 of the Guidelines to MAS Notice 626.

⁴ See Paragraph 8 of MAS Notice 626.

should be updated on the implementation, monitoring, and outcomes of such interim bridging measures.

Best Practices

Some banks supplement their back-testing with ATL and BTL statistical analyses to corroborate the relevance and effectiveness of their new TM rules. Adjusting TM rules with the aid of such statistical analyses helps FIs to reduce the volume of false positives/negatives generated within a given risk appetite.

Box Story: Positive and negative practices by banks in setting and testing their TM rules

Case Study A

Bank A set inappropriately high thresholds for certain customer segments. This inhibited its effectiveness in detecting excessively large and potentially suspicious transactions by these customers. For example, the thresholds set by Bank A for its premium and private banking segments were at least double (and in one case, five times) the AUM that Bank A expected these customers to have. MAS directed Bank A to review and recalibrate its thresholds for excessively large transactions across all its customer segments, and for its internal audit function to validate the appropriateness of the revised thresholds, to ensure that the risks from such types of transactions were satisfactorily detected and addressed.

Case Study B

MAS found Bank B's scenario for detecting pass-through payments to be of limited effectiveness. The scenario triggered alerts based on cumulative credit and debit amounts over a pre-defined lookback period, which could have precipitated failures by Bank B in flagging potential 1:1 pass-through transactions within a predefined margin (e.g. +/- 10%). For example, MAS' examiners observed one account in which a US\$5 million inflow was transferred out three days later, for which no pass-through alert was generated. While Bank B's analyst manually detected and escalated the case despite the lack of an automated alert, MAS nevertheless required Bank B to tighten its scenario in order to adequately detect and safeguard against the risks posed by 1:1 pass-through transactions.

Case Study C

Bank C did not maximise the conduct of its semi-annual parameter and threshold reviews to identify and rectify problematic rulesets. The semi-annual reviews focused on rules that generated zero alerts, but overlooked the closer examination of those causing significant variances in its TM results, such as rules that led to 200-400% increases in the volume of alerts generated. Bank C's reviews also focused solely on comparing the number of alerts generated across periods while neglecting the use of quality-related metrics (e.g. alerts that led to information requests to front office and/or STRs filed, as well as feedback from the bank's financial intelligence unit), which could improve targeting of ML/TF risks from customers' transactions. MAS therefore directed Bank C to enhance the scope and conduct

of its semi-annual reviews, update relevant parts of its policies and procedures, and ensure that its enhancements were tabled and approved by the appropriate senior management forums.

Case Study D

Before performing any recalibration of TM parameters or thresholds, Bank D would subject these changes to UAT on sample datasets. Bank D would also conduct post-implementation reviews to verify that new parameters and thresholds were functioning properly. However, Bank D did not set out adequate guidelines on (i) the appropriate test environment for UATs, the size and quality of datasets to be used, and the acceptance criteria for new rules to be implemented; as well as (ii) the appropriate scope and depth for post-implementation reviews to be conducted.

Consequently, MAS' examination noted the following:

- *Some data inconsistencies and a sub-optimal test environment due to concurrent testing for other proposed system changes in Bank D's 2015 and 2016 UATs, which risked undermining the integrity of its pre-implementation test findings; and*
- *A lack of rigour in the post-implementation reviews for 2015 and 2016, as the bank did not assess and document whether the new rules had led to reasonable outcomes within the bank's expectations, or if the quality of the resultant alerts was deemed to be satisfactory.*

While acknowledging Bank D's pre- and post-implementation initiatives, the examiners recommended that Bank D further strengthen its UAT and post-implementation review guidelines and communicate these to the relevant staff. Bank D advised that it would provide in its procedures detailed guidance for the proper conduct of pre- and post-implementation reviews, and continue to explore the use of statistical tools and methods to enhance the performance of these reviews.

iii. Data integrity

2.13 Quality data is a prerequisite for the sound functioning of TM systems. FIs should periodically review the completeness and validity of data used in their TM systems – for instance, through the performance of data integrity checks to ensure that data is being completely and accurately captured in the source systems and transmitted to their TM systems; and performing periodic reconciliation of transaction codes in both the TM and core banking systems. FIs should put in place appropriate detection controls (e.g. conduct of trend analyses and generation of exception reports) to identify abnormally functioning TM rules or scenarios, and ensure that any such irregularities or malfunctions (e.g. significantly less or no alerts) caused by data integrity issues are properly assessed and explained. Where appropriate, root cause analyses should be performed, and the findings and remedial actions should be escalated to the appropriate senior management platforms to facilitate timely implementation decisions, progress reviews and learnings.

2.14 To safeguard the integrity of TM data, FIs should ensure that staff's access rights to their TM systems are commensurate with their roles and responsibilities. While sufficient access must be provided to key staff in the TM process chain (e.g. analysts, compliance staff and quality assurance teams) in order to perform their duties effectively, FIs should perform periodic checks on the levels of access being granted, and curb any excessive powers granted to unauthorised persons or those who no longer require such powers.

Robust Implementation

2.15 A fundamental challenge in operationalising any TM system is ensuring the quality, accuracy and consistency of staff's handling of TM alerts generated. MAS inspectors observed multiple instances in which the effectiveness of banks' TM was undermined by weaknesses in staff's risk awareness, ranging from one-off errors to more frequent or systemic ones that suggested wider risk awareness deficiencies within the organisation. These findings underscore the need for FIs to invest in adequate training and guidance for TM staff to carry out their duties satisfactorily, guided by sound understanding of the key risks their organisations face.

i. Pre-transaction Checks

2.16 Some FIs require their front office staff to conduct pre-transaction checks before executing transactions assessed to pose higher risks or involving higher risk customers. These checks include:

- Inquiring on the background and purpose of transactions that exceed predefined thresholds, to ensure alignment with customers' profiles and purpose of accounts;
- Engaging customers, filing call reports on the transaction date that detail relevant risk considerations (e.g. nature of the relationship between customer and beneficiary, identifying the origin and destination of funds), and attaching supporting documents supplied by the customer; and
- Obtaining approvals from line managers and/or compliance personnel before executing higher risk transactions.

2.17 Pre-transaction checks can strengthen FIs' TM by introducing an additional layer of safeguards. When executing pre-transaction checks, FIs should determine the appropriate type and extent of checks to be applied for different customer types, and ensure that frontline staff are adequately risk-sensitised to rigorously perform these checks. FIs' senior management have to devote adequate planning, guidance and monitoring for such pre-transaction initiatives to work as intended.

Box Story: Improving the execution of pre-transaction checks

Bank E sorted its customers into categories based on pre-defined sets of common characteristics, and applied the following types of pre-transaction checks to those customers classified as higher risk:

- *Requiring their front office staff to perform first level reviews of all transactions by these customers; and*
- *Conducting further inquiries with customers prior to executing substantially large transactions above a predefined threshold.*

By its own policies, Bank E required its relationship managers (“RMs”) to perform the pre-transaction checks and obtain line managers’ approval prior to executing these higher risk transactions. However, Bank E did not issue guidance to RMs and line managers on how to document the checks. As a result, MAS found that Bank E’s documentation of these checks comprised sign-offs by RMs’ line managers to approve the transactions, that provided minimal insights into whether the checks were properly conducted, the basis for approvals, and whether any risks had been detected and appropriately addressed. MAS therefore suggested that Bank E provide more guidance to RMs on appropriate documentation and approval justifications for these pre-transaction checks. MAS further suggested that Bank E consider subjecting these pre-transaction checks and approvals to some form of independent QA testing, to periodically validate the effectiveness of front office’s execution.

ii. Alerts Handling and Documentation

2.18 While most FIs have policies and procedures (“P&Ps”) in place for handling alerts and other ML/TF red flags, a consistent finding from MAS’ inspections is that FIs need to improve on the timeliness and quality of their staff’s alerts clearance and documentation.

2.19 FIs must ensure that clear and concise procedures exist for their TM staff to assess and escalate alerts generated by their systems, and that their P&Ps are supported by adequate training, guidance, and consultation channels (e.g. with compliance functions, or subject matter experts on country regulations) to enable analysts to make the right decisions.

2.20 TM analysts must exercise adequate due diligence and challenge before dismissing alerts, and FIs should task more complex cases to senior analysts such that higher risk transactions and accounts are viewed with a more experienced eye. TM analysts should understand the ML/TF risks they seek to mitigate. Where appropriate, analysts should look beyond individual alerts to review customers’ history of past transactions and alerts, in order to holistically assess whether broader ML/TF patterns or behaviours may have manifested beyond the scope of the immediate alert.

2.21 Where frontline functions are called upon to engage customers and obtain further information necessary for TM analysts to properly assess alerts, FIs should monitor and ensure that these requests for information are addressed by frontline staff in a timely and

satisfactory manner. Analysts should be prepared to challenge frontline's explanations and assertions, and should not accept these at face value without adequate due diligence (such as corroborating the explanations using available internal records and public information, or requesting for supporting documents where appropriate). Notably, FIs should monitor carefully for alert closures made on the basis of generic reasons (e.g. first party transactions, or transactions between accounts of a common beneficial owner) to assess whether these are being properly closed and the ML/TF risks are being adequately mitigated.

2.22 FIs should ensure the clearance of TM alerts in a timely manner, and establish internal timelines and procedures for monitoring and escalating overdue alerts to higher clearance functions and/or senior management's attention. Such timelines and procedures should be closely adhered to in order to pre-empt alert backlogs. Where backlogs do manifest, it is incumbent on FIs' senior management to ensure ageing reports are generated and escalated such that the backlogs are cleared promptly, and that the ML/TF risks are effectively mitigated. FIs should monitor for deviations between their planned and actual timelines for alert clearances, and take measures to address the reasons or root causes for these gaps.

2.23 FIs should foster an AML/CFT culture that supports the effective execution of TM, and should not allow business interests to override legitimate risk concerns surfaced from TM. In this regard, FIs should ensure that risk considerations are adequately deliberated and decisions regarding the alerts are well-documented, with any necessary risk mitigation steps duly executed. FIs should regularly review their resourcing for TM functions to ensure a satisfactory balance is struck, and that staff with TM roles are not overloaded and adequately equipped to perform their functions.

Box Story: Lapses in alerts clearance and documentation

Case Study F

MAS found that Bank F only focused on reviewing a narrow range of alerts without addressing the bulk of alerts generated. The review criteria were largely driven by human resource considerations rather than backed by strong risk-based justifications. Coupled with the absence of periodic BTL testing, this raised concerns that suspicious transactions flagged by the TM system which are true positives and of material nature would not be reviewed and duly followed up upon. MAS therefore required Bank F to conduct a thorough re-examination of its applied methodology for alert scoring and review, and table the results and recommendations to an appropriate local senior management forum for discussion and endorsement.

Case Study G

MAS observed instances where Bank G's TM analysts closed alerts without appropriate levels of inquiry and probing. The analysts deemed the unusual transactions to be aligned with customers' wealth and profile, and accepted the representations made by customers

and Bank G's RMs without further analysis and probing into the veracity of these claims, even when they ran contrary to past information obtained from the customers. In some cases, Bank G's analysts also inserted generic explanations (e.g. "customer and counterparty are in the same industry" and "the transactions are business-related") to dismiss cases without further inquiry. These practices were contrary to Bank G's P&Ps, which required analysts to perform independent verification checks and obtain supporting documentation before closing alerts. MAS examiners therefore directed Bank G to provide more detailed guidance and training on when and how to conduct independent corroboration, including the necessary inquiries to be performed for clearance of various types of alerts, as well as the triggers for obtaining supporting documents to corroborate clients' representations.

Resolution and Enhancement

i. *STR Filing*

2.24 Where transactions exhibit reasonable grounds for suspicion of ML/TF, FIs are required to file suspicious transaction reports ("STRs") with the Suspicious Transaction Reporting Office ("STRO") in a timely manner after these transactions come to their attention. FIs must ensure that their internal processes do not unduly delay the prompt filing of STRs. There should be appropriate justification for exceptional cases that require more time for checks and analysis before the STR filing. These cases, including the justification and progress of investigations, should be properly documented.

2.25 FIs should consider filing STRs on customers with adverse news or other indicators relating to financial crime. FIs should also consider performing CDD and transaction reviews for such customers assessed to pose higher risks. FIs must properly document these assessments and justifications, including when an STR is not filed. FIs should also familiarise themselves with the STRO Online Notices and Reporting platform ("SONAR") launched on 20 August 2018, and report suspicious transactions electronically via the new STR form, ensuring that all the structured fields within the form are properly populated to the extent possible.

2.26 FIs should maintain records and supporting documents for all suspicious transactions. This includes cases where alerts were internally escalated but decisions were taken to not report these to STRO (e.g. where the FI assessed there to be insufficient grounds to establish reasonable suspicion). To ensure proper accountability, where STRs were not filed, the basis and where necessary the risk mitigation measures taken should be properly substantiated and documented. FIs should note that while certain transactions or activities may not be deemed suspicious at the time, the situation may change over the course of subsequent transactions or developments, in which case FIs are obliged to revisit and re-assess the cases and file STRs as appropriate.

2.27 To ensure the quality and consistency of staff assessments, FIs should periodically update their ML/TF red flags and communicate the most current risk understandings, along with any new or emerging ML/TF typologies, to senior management and staff.

Box Story: Lapses in STR filing

Case Study H

Bank H filed an STR on a corporate account due to concerns over the beneficial owner's source of funds and potential pass-through transactions that had occurred. A transaction block was placed and the account was subsequently exited due to these concerns. However, Bank H's review neglected a second corporate account held by the same beneficial owner, as this had not been flagged by the bank's RM nor its TM systems. Consequently, no review was conducted on this second account to assess the risks posed and whether any risk mitigation measures were required. Furthermore, Bank H only listed the name of the corporate entity on its internal watchlist, and not the name of the beneficial owner to whom the account belonged. As a result, the beneficial owner was able to open a personal account with another Bank H RM two years later, without triggering any red flags due to his previous suspicious activities. Pursuant to MAS examiners' inquiries into this case, Bank H initiated an immediate review and detected multiple third party transactions involving the beneficial owner's personal and second corporate account that could not be reasonably corroborated and were misaligned with the customer's profile. Bank H therefore filed a second STR on the individual and exited both accounts.

Case Study I

Bank I held 13 accounts belonging to a PEP Mr A and his two close associates, Mr B and Mr C. In 2015, the bank observed transactions in one of the accounts indicative of possible insider trading behaviour. Bank I's investigation into the transaction activities led to it filing an STR on suspected insider trading involving several of Mr A, Mr B and Mr C's accounts. However, MAS observed that the scope of Bank I's inquiry focused on securities trading transactions but had not considered whether the non-securities fund flows could also pose ML/TF concerns. Prompted by MAS' inquiries, Bank I conducted further investigations and identified unexplained anomalies (e.g. circular flows) in the non-securities transactions taking place between Mr A, Mr B and Mr C's accounts. This led to Bank I filing 2 additional STRs in November and December 2016.

MAS assessed the root cause for this gap as arising from Bank I's segregation of review responsibilities for different types of transactions. In this case, the team tasked with performing the initial assessment was only mandated to look at trade-related transactions, resulting in the oversight. Bank I acknowledged MAS' finding and committed to enhancing its transactions review processes to enable holistic examinations of suspicious activities.

ii. Post-STR Practices

2.28 Where an FI identifies suspicious activities in relation to a customer's accounts or transactions, in addition to filing STRs, should the FI decide to retain the relationship, it should ensure that appropriate enhanced measures are taken to manage the risks of these accounts being abused for ML/TF activities. These enhanced measures include subjecting the accounts to increased scrutiny, obtaining compliance and/or senior management approvals prior to executing further transactions, and reviewing the risk classification and/or further business relations with the customer. The FI should also take into account any ongoing cooperation with law enforcement agencies in deriving the course of action, and should ensure that their actions do not tip-off the customer.

Box Story: Lapses in post-STR practices*Case Study J*

During MAS' inspection, examiners observed one instance in which Bank J's analyst erroneously closed an alert even though the bank's investigations were still ongoing. Furthermore, the analyst did not update the customer's records with details of the bank's investigations, including the fact that an STR was filed, and did not place the customer on the bank's internal watchlist. These lapses by the analyst impacted the treatment of subsequent alerts generated on the customer's ensuing transactions, as the assessment of these alerts by Bank J's other analysts did not detect and factor in the reasons for the initial STR that was filed. These oversights could have inhibited the bank from filing further STRs and imposing further risk mitigation measures on the account, including possibly exiting the customer relationship. MAS therefore directed Bank J to review and tighten its analyst procedures with regard to updating the bank's internal monitoring systems, such that all analysts have access to full, current and accurate information – including past suspicious activities – to perform their analysis of TM alerts.

iii. Quality Assurance

2.29 FIs should periodically sample the quality of their alerts handling in order to detect and rectify deficient cases as well as any weaknesses observed in their TM systems or processes. To this effect, many banks have put in place independent quality assurance ("QA") programmes to continually sample alerts handling and test the robustness of their TM processes.

2.30 FIs should ensure that the level of QA testing they perform is commensurate with the size of their business, volume of transactions, and nature and complexity of risks they face. MAS expects FIs with weaknesses in their TM processes, or that have recently completed remediation to address such weaknesses, to conduct QA testing on a larger sample of alerts to verify that the gaps have been effectively remediated.

Best Practices

Some banks focus their QA testing on thematic areas where they assess their TM performance to be weaker, or where enhancements were recently implemented.

Some FIs also leverage QA results when assessing staff performances in order to (i) embed good AML/CFT culture and practices throughout their organisations, and (ii) focus their efforts on weaker staff (e.g. by allocating more training, mentorship and maker-checker approvals) to ensure that the rigour of their TM is not compromised.

Box Story: Initiatives to enhance the quality of QA reviews***Case Study K***

Bank K's compliance team performed sample testing on TM alerts to assess the timeliness and quality of their handling, and whether Requests for Information ("RFIs") had been promptly and satisfactorily addressed by the front office with proper documentation. MAS observed the following good practices which helped enhance Bank K's handling of higher risk alerts and reduce the risks of inappropriate closures:

- Bank K consistently tasked higher risk (e.g. more complex) alerts to undergo additional reviews by senior analysts; and
- Bank K tracked and monitored the quality of RMs' responses to RFIs. RMs demonstrating poorer quality performance (e.g. unduly long RFI turnarounds or high rejection rates) were subjected to follow-up from their line management and/or compliance managers to assess the reasons and need for any further actions.

iv. *Post-mortem Fine-tuning*

2.31 FIs should implement processes for the risk-based conduct of post-mortem reviews. They should be conducted pursuant to STR filings or production orders involving a high degree of suspicion for ML/TF activities; as well as accounts associated with transaction reviews directed by MAS, including for nexus to TF/PF activities or sanctioned countries. Such reviews should aim to identify and remediate significant system deficiencies in FIs' TM systems and processes to identify possible areas for efficiency or effectiveness improvements.

Box Story: Enhancing the conduct and takeaways from post-mortem reviews***Case Study L***

Bank L would, on an ad hoc basis, select STRs that it had filed and subject these to post-mortem reviews. While the scope of the post-mortem reviews was not defined, they generally focused on re-examining the areas that the bank had investigated when formulating its assessment of whether to file an STR (e.g. TM, CDD, documentation aspects etc.) with a view to identifying possible enhancements to these controls. MAS recommended that Bank L formalise its process in order to enhance the conduct and takeaways from such

post-mortem reviews – e.g. by developing guidelines to identify what nature of STRs to subject to such post-mortems, the key focal areas to consider, and the scope and depth of review. Aside from STRs, MAS also suggested for Bank L to consider post-mortems on other types of risk events (such as the handling of customers with significant ML,TF or PF adverse news, tax information requests, or law enforcement production orders) with a view to identifying aspects of its AML/CFT regime that could be enhanced.

3 Risk Awareness

3.1 To ensure continued effectiveness in the execution of TM controls, FIs should foster a strong AML/CFT culture and risk awareness throughout their organisations. FIs' board and senior management should clearly communicate their risk appetite and an emphasis on AML/CFT as a priority throughout all three lines of defence, including support for the robust conduct of TM.

3.2 FIs must instil risk consciousness and embed good practices amongst staff, to facilitate vigilance in identifying TM red flags and to escalate and handle these appropriately. FIs should ensure that their lists of ML/TF/PF red flags⁵ are continually updated, not just to include new red flags but also to provide further guidance on existing ones, particularly when staff give feedback on a lack of clarity in interpreting these red flags (for example with regards to the treatment of complex transactions or patterns, classifying higher risk geographies and business activities, or determining whether certain transactions and patterns make economic sense).

3.3 Adequate TM training should be provided to strengthen staff's knowledge and expertise in this area. Banks should put in place a reasonable timeframe, as well as an effective escalation framework, to ensure the timely completion of mandatory training by senior management and staff. Mandatory training should also be extended to overseas-based staff whose responsibilities cover accounts booked in Singapore. Notably, training should be catered to the specific risks that staff will face in their respective tasks within the TM process chain, to enhance the effectiveness of their detection and handling. FIs should also incorporate tax crime related-red flags in the training sessions, so as to raise staff awareness of tax risks as well as updated tax evasion/avoidance typologies. Training attendance should be tracked and enforced at appropriate management platforms.

⁵ FIs should draw from multiple sources to ensure their ML/TF/PF red flags are regularly and comprehensively updated. These include MAS' AML/CFT Guidelines and guidance papers; STRO's red flag indicators on SONAR; guidance and best practice papers from the FATF, APG and other AML/CFT bodies; as well as information and intelligence obtained from relevant industry sources (e.g. ACIP and PBIG papers).

Box Story: Examples of inadequate risk awareness***Case Study M***

A customer of Bank M opened three accounts that, over the span of a few days, were used to route a series of large pass-through transactions that were ultimately transferred to an external third party. Bank M’s TM system generated multiple alerts in view of the suspicious pattern, but the bank’s analyst elected to close these alerts on account of these being “first party (inter-account) transfers” and therefore “not suspicious”, ignoring the point that the funds were ultimately transferred to a third party who was not a known counterparty of the customer. When queried, Bank M acknowledged that these alert closures were improper and attributed the root cause to the analyst’s lack of risk awareness, as the analyst should have queried the customer’s relationship with the third party and the purpose for these transfers, given that they appeared to be pass-through in nature. MAS examiners recommended Bank M to provide more specific guidance to its TM staff on identifying pass-through transactions and understanding their associated ML/TF risks, and the required actions to take when such activities are detected. In addition, Bank M committed to updating its training materials to tighten its stance on “first party transfers” in order to prevent inappropriate closure of alerts in future.

Case Study N

A Bank N account was opened for the purpose of holding Mr A’s bond and equity investments. Six alerts were subsequently triggered on account of five fund transfers made from Mr A’s account to an unknown third party. However, Bank N’s analyst dismissed these alerts after hearing the RM’s explanation that the external party was a company beneficially owned by Mr A’s sibling Mr B, and that the bond and equities investments in Mr A’s account were actually beneficially owned by Mr B. However, Bank N’s CDD records did not reflect Mr B as the beneficial owner (“BO”), connected party, or authorised signatory of Mr A’s account. While Bank N did verify that Mr B was indeed Mr A’s sibling, the use of Mr A’s account to hold securities belonging to Mr B was not aligned with Mr A’s stated purpose for opening his account, and raised concerns as to whether Bank N had properly identified and conducted the appropriate due diligence on the true BO of the account.

MAS directed Bank N to review how its TM analyst could have overlooked these clear BO lapses, and to implement appropriate measures to address the root causes. The bank acknowledged that the oversight stemmed from staff’s lack of awareness on the risks and red flags associated with front accounts, and committed to enhancing its training in order to equip analysts with the necessary skillsets to detect and escalate such risks, including where instances of possible assets commingling in customers’ accounts are detected.

3.4 FIs should embed AML/CFT-related performance indicators in staff appraisal frameworks and compensation practices in order to inculcate individual staff’s ownership of AML/CFT issues, and ensure appropriate staff accountability to escalate and/or mitigate ML/TF risks. In particular, FIs should consider instituting structured performance measurements that link AML/CFT compliance (including TM conduct) to appraisals for

persons in the TM process chain, covering all three lines of defences and notably including the frontline. Key performance indicators (“KPIs”) related to TM may include adequate scrutiny of anomalous transactions, quality of challenge by the second line, timeliness and adequacy of responses by the frontline, and the proper closure of alerts.

Best Practices

Some banks hold their material risk takers (e.g. senior management and voting members of specific committees) accountable for driving strong risk awareness and sound AML/CFT culture and practices within their organisations. As part of the performance appraisal process for these individuals, feedback is sought from the relevant heads of control functions (e.g. compliance, audit and risk) on their performance and effectiveness in this regard. Adverse feedback from these control function heads would negatively impact the variable compensation for material risk takers who prioritise business interests at the expense of proper AML/CFT risk mitigation.

For this procedure to be effective, FIs should ensure that timely feedback is obtained from all participants in the appraisal process, in order for a comprehensive picture to be generated that aids the material risk taker in understanding his strengths and areas for further improvement. Detailed responses are important to facilitate the appraisal process and enhance the usefulness of feedback. Nil responses should also be collected, e.g. where a control function head may have insufficient visibility on a specific individual to provide useful feedback.

4 Governance

4.1 Strong AML/CFT governance and management oversight are imperative to set the right tone for TM controls execution and effective risk management. FIs’ board and senior management should exercise active oversight of the key ML/TF risks and their mitigation, which includes continually assessing and enhancing the effectiveness of their organisations’ AML/CFT framework and controls.

4.2 To ensure proper oversight of the TM process, FIs’ board and senior management should ensure that clear, current and appropriate AML/CFT P&Ps are put in place, and that there are effective TM systems supported by adequate internal expertise and resources. TM functions should be given clear and distinct responsibilities for their respective tasks in the TM process chain (e.g. for alerts handling and filing of STRs).

4.3 FIs are expected to implement effective reporting systems to ensure that their board and senior management are updated on key ML/TF risks in a timely manner. Based on MAS’ inspections, there is scope for FIs to enhance their reporting and escalation of the following significant risk matters:

- System implementation delays;

- IT incidents or system limitations impacting the organisation's TM capabilities;
- Results and remediation of compliance or QA reviews; and
- Regular updates and follow-ups with regard to alert ageing statistics.

4.4 FIs should ensure the generation of TM statistics to provide their senior management with an adequate overview and context of the timeliness and quality of the organisation's TM alerts handling and resolution, as well as any remedial measures in train; and whether these effectively mitigate the organisation's ML/TF/PF risks.

4.5 In addition, any event or circumstance that could potentially negatively impact the organisation's TMs capabilities should be promptly highlighted to senior management, and to the board where warranted. The board and senior management should ensure the implementation of adequate interim risk mitigating measures where this is needed – for example, where system fixes require more time to complete and their risk impacts are material.

4.6 The findings from any reviews on the organisation's TM effectiveness (e.g. as performed by compliance, QA or audit functions) should likewise be surfaced to senior management, with assessments of whether the generation and management of TM alerts is commensurate with the FI's risk appetite, the root causes for any gaps, and the remedial actions proposed to address these. Senior management should be kept apprised of the progress of remedial actions so as to assess if additional interim measures are required to mitigate the risks.

Best Practices

To more systematically tune the effectiveness of its TM rules, one bank developed a tiered classification system to assess the usefulness of past alerts. These categories ranged from false positives to alerts culminating in an STR due to financial crime concerns, and included material cases of false negatives identified through other controls or information sources. When testing new TM thresholds, the bank would overlay the classification onto the test results in order to flag important alerts/material cases that were missed by the new thresholds, as well as the volume of less-useful alerts being surfaced. The bank's senior management would be apprised of the results and would need to decide on the bank's risk tolerance level to either:

- *Require further adjustments to the new thresholds to achieve more desirable outputs, or*
- *Approve the new thresholds as acceptable, if the findings from the back-test were within tolerance.*

Senior management's decisions were documented and used to guide subsequent TM tuning exercises. It is also important that the bank's senior management ensures that its risk appetite keeps pace with changes to the banks' business or customer profile and evolving ML/TF typologies.

4.7 FIs should strengthen their governance and oversight of tax crimes risk management. FIs should develop adequate tax risk assessment frameworks for their customers, and regularly review the effectiveness of their tax risk mitigation measures. Formalised procedures should be put in place to ensure the effective identification and review of tax crimes red flags that surface in the course of TM.⁶ Where there are grounds to suspect that transactions are related to tax crimes, FIs should conduct enhanced monitoring and where appropriate, discontinue the relationship. Should FIs be inclined to retain these customers, approvals must be obtained from senior management with the substantiating reasons properly documented. Suspected tax-illicit activities should be reported in STRs.

MAS' Expectations Regarding the Material Outsourcing of First Level Alert Reviews

4.8 MAS has observed that a number of banks outsource the performance of first level alert reviews to TM hubs within the same financial group. FIs should ensure that their outsourced functions are adequately staffed by personnel with the requisite ML/TF risk awareness and expertise to handle the alerts. The outsourced functions should also be provided with the proper training and resources (such as access to customer information) needed for them to properly assess the TM alerts. In their service level agreements with outsourced functions, FIs should incorporate appropriate KPIs, reporting, audit and inspection requirements, so as to properly monitor and control the quality and timeliness of outsourced services rendered. The measures should help FIs ensure that the outsourced service providers are effectively detecting and escalating unusual transactions to their financial intelligence units for further action. FIs are reminded that the outsourcing of first level alert reviews constitutes a material outsourcing arrangement under MAS' Outsourcing Guidelines⁷, which inter alia set out the following requirements:

- **Governance and Oversight:** FIs should ensure good governance and strong oversight of their material outsourcing arrangements. This means that FIs' board and senior management are expected to be fully apprised of any risks arising from their material outsourcing arrangements, and must ensure that these arrangements do not result in the compromise or weakening of their organisations' ML/TF risk management, internal controls and conduct of business. While FIs may delegate the responsibility for first level alert reviews to their outsourced service providers, ultimate responsibility for ensuring the effective clearance of TM alerts, as well as the adequate detection and mitigation of customers' ML/TF risks, continues to reside with the

⁶ FIs should also ensure that their red flags for detecting tax crimes are regularly updated; see paragraph 3.2.

⁷ MAS' Outsourcing Guidelines can be found at the following page: http://www.mas.gov.sg/~media/MAS/Regulations%20and%20Financial%20Stability/Regulatory%20and%20Supervisory%20Framework/Risk%20Management/Outsourcing%20Guidelines_Jul%202016.pdf

outsourcing FIs and notably their board and senior management.⁸ Where service standards of outsourced functions are deemed insufficient, it is incumbent on FIs' board and senior management to monitor and implement remedial measures to ensure that the rigour of their organisation's TM execution and risk mitigation is not compromised.

- **Risk Management Standards:** FIs should establish risk management frameworks to assess the adequacy and robustness of first level reviews performed by their outsourced functions, bearing in mind that risk management standards should not depart from the levels expected had the FIs not outsourced the activity. There should be regular and sufficient independent QA checks to ensure that alerts dismissed by the outsourced functions were properly executed, justified and documented.
- **Independent Audits:** FIs should ensure that independent audits and expert assessments of the outsourcing arrangements are conducted on a regular basis, and verify that policies, procedures and controls at the outsourced service providers are adequate to ensure data security and the proper mitigation of operational risks. FIs are expected to bring to the attention of their senior management any significant data security or operational risk issues and concerns highlighted in their audit reports or expert assessments, for timely resolution.
- **Access to Regulatory Oversight:** FIs should allow MAS, or any agent appointed by MAS, where necessary or expedient, to exercise the contractual rights of the FIs to access and inspect the outsourced service provider, and obtain records and documents stored at or processed by the outsourced service provider; as well as to access any report and finding made on the service provider, whether produced by the outsourced service provider's internal or external auditors, or by agents appointed by the outsourced service provider, in relation to the outsourcing arrangement.
- **Risk Assessment:** FIs should implement processes to regularly assess any risk exposures from their material outsourcing arrangements, and should ensure that the mitigation of such risks is incorporated into their own AML/CFT risk management frameworks. FIs should ensure that the MAS is promptly notified of any adverse developments on its (or its group's) material outsourcing arrangements that could impact its AML/CFT framework or controls, such as service failures or breaches of security or confidentiality..

⁸ For outsourcing arrangements with parties within an FI's group, the expectations may be addressed within a group-wide risk management P&P. For an FI incorporated outside of Singapore, the functions of senior management would lie with local management. Local management cannot abrogate its governance responsibilities to run the institution in a prudent and professional manner.

5 Conclusion

Robust TM is essential for FIs to detect and report suspicious transactions in a timely and effective manner, and take appropriate steps to mitigate the associated ML/TF risks. The conduct of TM is an organisation-wide responsibility and priority. FIs' board and senior management should set a strong tone from the top, and inculcate appropriate risk awareness, ownership of risks and their accompanying mitigation measures amongst all staff, to drive effective execution of controls in all three lines of defence.

FIs are further encouraged to consider the use of new technology and data analytics to improve their TM outcomes. Several banks are piloting work in this nascent area. To facilitate this development, a data analytics workgroup formed under the AML/CFT Industry Partnership (“ACIP”) is producing a report to share industry experiences of the use cases, key challenges and potential solutions to the adoption of such tools. This report is targeted for release in Q4 2018.