



BANGKO SENTRAL NG PILIPINAS

OFFICE OF THE DEPUTY GOVERNOR | FINANCIAL SUPERVISION SECTOR

MEMORANDUM NO. M-2023-013

To : **All BSP-Supervised Financial Institutions (BSFIs)**

Subject : **Guidance Paper for an Effective Anti-Money Laundering/Countering Terrorism and Proliferation Financing (AML/CTPF) Transaction Monitoring System**

In its Resolution No. 490 dated 13 April 2023, the Monetary Board approved the attached Guidance Paper on transaction monitoring system.

The Guidance Paper presents the key results of the thematic review on transaction monitoring system. It aims to provide sound practices and practical insights covering transaction monitoring system and other related facets, such as ongoing customer due diligence, alerts/case management, and suspicious transaction investigation and reporting, across different types of BSFIs.

BSFIs are expected to consider this Guidance Paper in the design and continuing reinforcement of their transaction monitoring and reporting systems as a key component of their overall AML/CTPF framework.

For information and guidance.

CHUCHI G. FONACIER
Deputy Governor

20 April 2023

Att: a/s



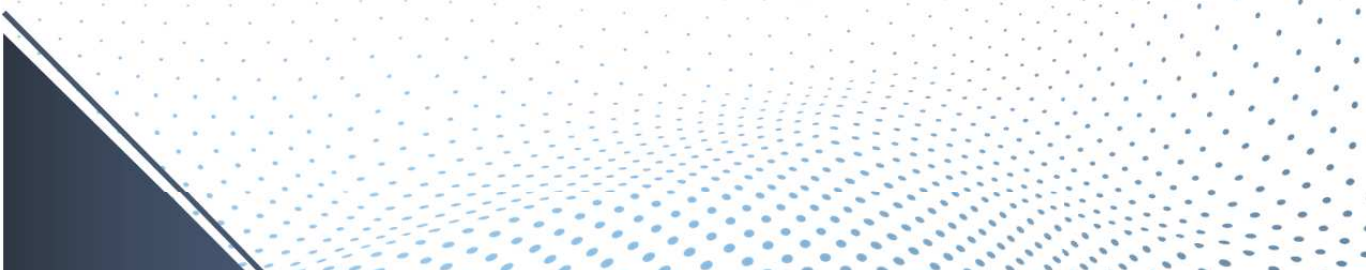
GUIDANCE PAPER
TRANSACTION
MONITORING
SYSTEM

March 2023



TABLE OF CONTENTS

1. Introduction	1
2. Executive Summary	1
3. Key Elements of a Transaction Monitoring System	2
3.1 Governance Structure.....	2
3.2 Planning, Development, and Pre-Implementation of TMS.....	4
3.3 Robust and Risk-Based TM Implementation	8
3.4 Suspicious Transaction Reporting and Post-STR Process	13
3.5 Self-Assessment - Audit and Compliance Testing	14
4. Conclusion and Way Forward.....	14



1. Introduction

- 1.1. Thematic review (TR) is an integral part of the supervisory framework of the Bangko Sentral ng Pilipinas (BSP). It is also known as horizontal or comparative assessment of a particular process or area that poses safety and soundness concern to the BSP-supervised financial institutions (BSFIs), in particular, or the financial system, in general. TR results serve as inputs to the BSP's policy development or reviews and supervisory engagement or actions to mitigate the identified risks.
- 1.2. This thematic review focuses on the transaction monitoring (TM) process and its related facets, such as ongoing customer due diligence and alerts/case management, as well as suspicious transaction investigation and reporting. The TR covered select BSFIs comprised of banks, money service business, electronic money issuers, virtual assets service providers, and a trust corporation.
- 1.3. Transaction monitoring (TM) is one of the pillars of an effective anti-money laundering (AML)/counter terrorism and proliferation financing (CTPF) framework. It is a key preventive measure to ensure that the customers' transactions are consistent with the BSFI's understanding of the customer and its business and risk profile, and to identify or detect possible suspicious activities or transactions. Considering the underlying variables, evolving factors and complex interdependencies with other aspects of the AML/CTPF process, it is regarded by BSFIs as among the most challenging. In the 3rd sectoral money laundering (ML)/terrorism and proliferation financing (TPF) risk assessment, effectiveness of suspicious activity monitoring and reporting was rated 'medium' for banks, non-bank EMIs, and VASPs, as well as trust entities and pawnshops. Identified areas for improvement include, among others, processes to facilitate risk and trigger-based updating of customer risk profile, conduct of transactional due diligence, as warranted, aggregation of activities at customer level, periodic calibration of the monitoring systems, including the suitability of parameters to generate meaningful alerts and suspicious transaction reports (STRs), and sufficiency of resources for alerts management.¹
- 1.4. Informed by the results of the TR, this guidance paper highlights good industry practices, in light of the governing global standards and regulatory expectations, as well as identifies areas where further work is needed. This document aims to inform, guide, and support the BSFIs in the design and continuing reinforcement of their TM and reporting systems as a key component of their overall AML/CTPF framework.

2. Executive Summary

- 2.1. In the AMLC's STR Quality Review for 2017-2020, STRs exponentially increased since 2013². Universal and commercial banks (UKBs) still account for majority of the STR filings for BSFIs. Nonetheless, it was observed, among others, that i) UKBs' share in total STRs decreased from 78% in 2017 to 51% in 2020; and ii) the share of non-bank financial institutions (NBFIs), particularly pawnshops and MSBs, constantly increased from 11% in 2017 to 29% in 2020³. The share of EMIs also significantly increased from 2% to 14% in the same period. These indicate that BSFIs are progressively learning to identify and detect the various threats in the financial system.
- 2.2. This TR provides a better understanding of the TM posture across the covered BSFIs and highlights good practices and practical insights that the industry can consider in calibrating their respective systems. Based on the TR, covered

¹<https://www.bsp.gov.ph/Regulations/Issuances/2021/M-2021-017.pdf>

² AMLC STR Quality Review 2017-2020 (Data Discovery) -

[http://www.amlc.gov.ph/images/PDFs/STR%20QUALITY%20REVIEW%20\(2017%20TO%202020\)%20DATA%20DISCOVERY2.pdf](http://www.amlc.gov.ph/images/PDFs/STR%20QUALITY%20REVIEW%20(2017%20TO%202020)%20DATA%20DISCOVERY2.pdf)

³ Ibid. In terms of ranking, PS and MSB at 2nd, EMIs at 3rd (increase from 2% to 14%)

BSFIs adopt risk and trigger-based, as well as tiered customer due diligence, while employing automated and/or manual Transaction Monitoring System (TMS), that is generally appropriate to their respective size, nature, and complexity of operations, to identify atypical activity in customers' transactions. Certain BSFIs also plan to complement the rule-based TM implementation with machine learning capabilities that will analyze customers' activities considering their historical or expected behavior and detect possible linkages between and among accounts.

Likewise, the review identifies certain areas for improvement, such as better cultivation of risk awareness across the BSFI, bespoke policies and procedures, resource allocation, and overall effective functioning of the TMS which is attuned to the evolving risks faced by the BSFIs. Accordingly, further work is necessary to achieve risk-driven implementation, such as conducting adequate investigation with audit trail within the alerts/case management process, sustaining the conduct of appropriate ongoing customer due diligence (CDD), including risk and trigger-based updating, and adoption of suitable TM infrastructure with machine learning capabilities, as warranted, that supports holistic review and effective analysis of customers' transactions. BSFIs should adopt risk mitigating measures for customers subject of STRs, commensurate to their risk profile.

- 2.3. A robust risk based TMS is key to a proactive and effective detection of suspicious patterns of account activities. This is achieved through, among others, continuous understanding of the nature and purpose of the customer relationship, dynamic risk profiling, and holistic review of a customer's transactions/activity behavior, on an aggregated and/or total relationship basis. This should be complemented by a TMS that is suitable to the BSFI's operations and risk profile. The design and complexity of the TMS to be adopted should be anchored on, among others, the results of the institutional risk assessment (IRA) and defined risk appetite. It is equally essential to foster awareness among all personnel of the risks and expectations relative to their roles and responsibilities in the TM process and inculcate risk awareness and compliance culture within the organization. The Board of Directors and Senior Management should uphold strong tone from the top and exercise active oversight on the TM process which can generate relevant information and reports to enable the Board of Directors or oversight committee to make strategic decisions. Finally, active stakeholder engagement is key to meaningful resolution and enhancement of the TM process of each BSFI to strengthen the industry's stance against ML/TF/PF risks.

3. Key Elements of a Transaction Monitoring System

3.1 Governance Structure

- a. **Board of Directors (BOD) and Senior Management (SM) Oversight⁴.** Active oversight by the BOD and SM is essential in setting the right tone from the top and to ensure that bespoke TM strategies and controls are adopted and aligned with the set risk appetite. TM manuals shall be maintained, communicated, and made accessible to concerned staff and officers, and kept up to date. The BOD and SM should be at the forefront of promoting continuous enhancements of the TMS.
- b. **Management Information System (MIS).** The BOD and SM should be provided with relevant information on the status and effectiveness of the TMS, alerts/case management systems and related processes, to enable them to make risk-informed decisions, including remedial actions, as needed. In this regard, BSFIs are expected to adopt suitable MIS process that is capable of generating complete, accurate and timely relevant AML/CTPF data and information to facilitate regular reporting to the BOD and SM.

⁴ Section 911 of Part 9 of Manual of Regulations for Banks (MORB).

- c. **Culture of Risk Awareness.** Effective implementation of policies and processes is anchored on adequate and informed personnel who possess the necessary skills and expertise to carry out their specific TM mandates and responsibilities. Management and employees should be aware of the risks and expectations relative to their roles and functions in preventing ML/TF/PF and other financial crimes. When practiced proactively and continuously, a culture of risk awareness and compliance within the BSFI is instilled.

To keep the BOD and SM abreast of their TMS posture, including the identified risks and challenges, BSFIs adopt a reporting system that considers the following, among others:

Table 1. TM Reporting System

<i>Elements</i>	<i>Best Practices</i>
Oversight Responsibility	BOD-level and/or SM AML oversight committee established.
Reporting Frequency	Monthly, quarterly or other regular intervals and as needed basis.
Audit Trail	Discussions are approved/noted by the Board and documented; controlled copies safekept by the Corporate Secretary, Compliance Office or others designated by the BOD or Local Management.
TM Reporting Standards/ Objectives	TM - Related Metrics/information monitored and reported
<ul style="list-style-type: none"> Effectiveness of the TM rules/scenarios and quality of alerts/cases generated 	<ul style="list-style-type: none"> System-generated and manually flagged alerts/cases to their respective STR ratio. False positive alerts/cases ratio. Results of periodic review to assess the effectiveness of manual and automated system, tools and processes used in identifying/detecting red flags/suspicious indicators.
<ul style="list-style-type: none"> Alerts/case handling and resolution 	<ul style="list-style-type: none"> Number or percentages of outstanding alerts (including aging) and resolved alerts/cases (with turnaround time) per risk category/prioritization level. Total alerts/cases per investigator ratio. Number, percentage of alerts requiring further investigation.
<ul style="list-style-type: none"> ST reporting measures 	<ul style="list-style-type: none"> Number, trend analysis for STRs per predicate crime/suspicious indicator. Statistics on delayed and timely STRs. Number of customers involved in STRs, with volume and value of transactions involved, SM decision, status of accounts/relationships involved and risk mitigating measures adopted.
<ul style="list-style-type: none"> Assurance based on independent reviews 	<ul style="list-style-type: none"> Results of self-assessment of TM controls, and TM-related independent reviews (e.g., Quality Assurance (QA), Compliance and/or Internal Audit).
Data Integrity and overall effectiveness of TMS	<ul style="list-style-type: none"> Data integrity issues (e.g., customers with lacking or incomplete information, inaccurate TM-related data generated by the system). Emerging risks and threats, including new ML/TPF typologies based on results of TMS or industry scanning, among others. Challenges, such as limitations on manpower and systems utilized in TMS or information technology incidents impacting TMS capability.

Case Study 1 - Reporting of key TM metrics to the AML oversight committee

The Compliance Officer (CO) of Bank A submits monthly report to the AML oversight committee on various AML/CTPF metrics, such as number of resolved and outstanding alerts/cases, number of customers subject of Freeze Order (FO) and STR filings, and TM-related issues noted by the Internal Audit and Compliance, among others. Meetings are adequately documented.

The report does not include data on efficiency of TM process and further analysis of the related ML/TF/PF risks and their impact (e.g., aging and root cause of outstanding alerts/cases, turn-around-time of resolved alerts/cases, predicate crime and/or typology involved in the FOs and STRs, risks associated with the outstanding audit and compliance testing issues) as well as status of actions taken or plans to mitigate risks. Bank A's latest update indicates that scope of reporting was enhanced to accommodate said metrics for proactive monitoring and management of ML/TF/PF risks.

<i>Good Practices</i>	<i>Area for Improvement</i>
<ul style="list-style-type: none"> <i>The CO regularly (i.e., monthly) reports key AML matters to the AML oversight committee.</i> <i>Discussions are documented and noted by the BOD.</i> 	<ul style="list-style-type: none"> <i>Expand metrics reported to enable informed decision-making (i.e., assess the adequacy and effectiveness of the entire TM process and devise action plans, as necessary).</i>

3.2 Planning, Development, and Pre-Implementation of TMS

- a. **General TMS Requirements⁵.** Considering the results of the IRA and the requirements of pertinent BSP regulations, the expected level of sophistication, automation, integration, and capabilities of the TMS should be commensurate with the size, nature, and complexity of operations of the BSFI. Accordingly, UKBs and other BSFIs considered complex⁶ should adopt an electronic AML system, while others may opt for less sophisticated mechanisms commensurate to their operations. Further, to mitigate the impact of cyber fraud, covered BSFIs should have automated and real-time fraud monitoring and detection systems (FMS) to aptly identify and block suspicious or fraudulent online transactions commensurate to their digital financial and payment platform risks⁷. The FMS should be linked or integrated with the AML systems for a cohesive financial crime prevention system.

Other factors to consider in designing the TMS include requirements from business units, audit, compliance, and information security (including data access, security matrices and audit trails), as well as vendor suitability, new system capacity, as applicable, and existing infrastructure integration, and compatibilities.

⁵ MORB Sections 911 (Monitoring and reporting Tools), 922 (Electronic monitoring systems for AML/CFT) and corresponding sections of the MORNBF1.

⁶ Pursuant to Sec. 131 (Definition of Terms) of the MORB

⁷ Circular No. 1140 (Series of 2022), Amendments on Information Technology Risk Management prescribes controls for electronic products and services.

Global Benchmarks - Data Integrity and Access Controls

To ensure integrity of data⁸, the following should be considered during the planning stage of adopting or designing a TMS:

- ✓ Data validation controls and similar measures to check process effectiveness, completeness and accuracy of data flowing from the sources (e.g., systems and files) to the TMS;
- ✓ Periodic reconciliation of transaction codes between the source systems and the TMS; and,
- ✓ Strict access controls on a need-to-know basis depending on user's function and responsibilities;

Dual control, including that embedded within the system, which requires two personnel (e.g., one maker, other checker) to complete a task, especially in ensuring that only authorized changes on TM rules, users, access rights, watchlist and sanctions database, as applicable, are effected, should be adopted to maintain integrity of the data processed and generated by the TMS.

Case Study 2 - Key controls at the planning stage of TMS acquisition, development, or enhancement

Certain modules (e.g., setting of scenarios, parameters or thresholds, defining users and their access rights, and maintenance of watchlist or relevant sanctions list database) of the automated TMS adopted by certain banks have no dual control embedded within the system. For example, changes or updates can be single-handedly effected without another layer of review or approval within the system. Changes or updates in the system undergo manual management workflow and approval prior to effecting the same in the production system by a single authorized user. However, said modules were not subjected to immediate independent review after the change or update has been effected, and regularly thereafter, to determine if no unauthorized changes are carried out. The BSFIs were i) directed to adopt risk-mitigating measures such as independent review of audit trail or logs of activities of the said user; and ii) advised to define and enforce segregation of duties (e.g., built-in maker-checker control within the system) during the planning stage of using a new or modified system.

Good Practice	Areas for Improvement
<ul style="list-style-type: none"> • <i>Changes/updates undergo the required management and approval process prior to implementing the same.</i> 	<ul style="list-style-type: none"> • <i>Consider and define minimum security control requirements (including maker-checker in this case) during the planning stage of using a new or modified system.</i> • <i>Adopt mitigating controls to ensure that no unauthorized changes are effected in the system.</i>

b. Vendor Selection. BSFIs are ultimately responsible for mitigating their ML/TF/PF risks and complying with AML/CTPF obligations⁹, including for processes covered by third-party arrangements. BSFIs should understand how embedded data integrations and functionalities (e.g., program logic) correlate with their requirements and ML/TF/PF risk exposures before system procurement. Accordingly, a service level agreement (SLA)¹⁰ with clearly defined key performance indicator (KPIs), among others, should be executed to achieve the intended performance or value of the TMS and ensure adequate support from the providers (e.g., IT department, vendor). The BSFI should establish systems to monitor the quality and quantity of delivered services. These should include a mechanism to identify root cause/s of deviations, ensure prompt resolution of issues and adoption of change management process for updates or modifications in the system.

⁸ Monetary Authority of Singapore (MAS) 2018 Guidance for Effective AML/CFT Transaction Monitoring Controls

⁹ Section 911 of the MORB and corresponding sections of the MORNBFIs state that it shall be the ultimate responsibility of the board of directors to fully comply with AML/CTPF laws and regulations and ensure that ML/TF/PF risks are effectively managed and that this forms part of the covered person's enterprise risk management system.

¹⁰ Section 148 Appendix 78 of the MORB and pertinent sections of the MORNBFIs require BSFIs to ensure all contract agreements outline all expected service levels and are properly executed to protect its interest.

c. Development of the TMS

- (1) **TMS Rules and Parameters.** Informed by the results of the IRA and other relevant customer, transactional and typology analysis/studies, BSFIs should develop relevant and bespoke red flags or indicators of possible suspicious activities. This will be useful in defining suitable TM scenarios, rules, and parameters and designing other alert triggers. Examples of red flags and alert triggers are included in Annex D of the 2021 AMLC Registration and Reporting Guidelines (ARRG) and/or its subsequent amendments. BSFIs may also refer to AML/CTPF guidance papers, typology studies and other reliable independent sources.

Global Benchmarks - TM Rules/Parameters Design

In designing TM scenarios/rules and other alert trigger controls, the following risk factors¹¹, among others, can be considered depending on the characteristic and profile of the BSFI's customers, products/services, delivery channels, and the jurisdictions it is exposed to:

- Size (e.g., amount, volume), frequency, velocity or other patterns of account activity indicating unusual or suspicious nature such as a suspected fraud or use of mule accounts, or with behavior akin to certain predicate offenses (e.g., Ponzi scheme, corruption, skimming, illegal gambling, online sexual exploitation of women and children [OSEC]);
- Transfer of funds involving different customers or accounts that may indicate undisclosed relationship;
- Out of ordinary transactions involving BSFI-issued cards (e.g., ATM, prepaid, credit cards) such as withdrawals from other countries involving many cardholders or online purchases spree of a cardholder within a very short period of time;
- Transactions where the sources of funding are unknown or cannot be identified;
- Transactions involving a person or entity included in the sanctions list;
- Activities that deviate from the customer's business or financial profile or transaction history, transfers are without economic justification;
- Heightened monitoring of customers that were previously suspected of or investigated for possible suspicious activity such as those that were subjected to STR filing, freeze order, or bank inquiry; and
- Other anomalous or unusual pattern of account activity involving the BSFI customer or facility which may indicate ML/TF/PF.

One or more of the foregoing factors can be used in the design of TM rules or parameters. This can be further enhanced, to the extent possible, by considering customer, product transaction type segmentations and/or other factors in calibrating their TM rules, parameters, or thresholds. Multi-factor detection scenarios are also useful to flag unusual account/transaction patterns or behaviors relative to known ML/TF/PF typologies. Examples of which include the following:

- Based on nature of work or source of fund, expected volume/value transactions (could be in range), frequency, and/or type of transactions (which can help detect individuals into OSEC, Ponzi scheme, or drug trafficking);
- Based on source of fund, geographic location of remitter or beneficiary, and/or profile of usual counterparties (to aid in determining possible receipt/disbursement of funds from illicit sources such as OSEC, mules, syndicates, terrorism financing);
- Relating total debits against total credits to deposit accounts to detect abnormal or unexplained offsetting of transactions in a short period of time (e.g., indicator of pass-through, mules); and,
- Relating results of TM parameters such as many to one, and vice versa, with geographic risk of usual counterparties e.g., OSEC, terrorism financing.

FATF emphasized the need to also employ Artificial Intelligence such as machine learning in this space, which provides greater speed, accuracy, and efficiency through monitoring of customers' business relationship and behavioral and transactional analysis in the following areas:¹²

¹¹ Most were taken from the respective corresponding guidelines set by the Australian Transaction Reports and Analysis Centre or AuSTRAC (source: <https://www.austrac.gov.au/business/how-comply-and-report-guidance-and-resources/amlctf-programs/transaction-monitoring>) and Monetary Authority of Singapore or MAS (source: https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Anti_Money-Laundering_Countering-the-Financing-of-Terrorism/Guidance-for-Effective-AML-CFT-Transaction-Monitoring-Controls.pdf)

¹² Opportunities and Challenges of New Technologies for AML/CFT by FATF - July 2021 (<https://www.fatf-gafi.org/en/publications/Digitaltransformation/Opportunities-challenges-new-technologies-for-aml-cft.html>)

- Unsupervised machine learning algorithms: To group customers into cohesive groupings based on their behavior, which will then create controls that can be set more adequately on a risk-based approach (ex: transaction threshold settings), allowing a tailored and efficient monitoring of the business relationship;
- Supervised machine learning algorithms: Allow for a quicker and real time analysis of data according to the relevant AML/CFT requirements in place; and
- Alert Scoring: Alert scoring helps to focus on patterns of activity and issue notifications or need for enhanced due diligence.

(2) Pre-Implementation Testing. A formal acceptance process¹³ should be established to ensure that systems promoted to production are adequately designed and reliably consistent with expected specifications. BSFIs should ascertain via pre-implementation testing¹⁴ if the defined stakeholder requirements will be met by the new or modified system. Material data mapping, transaction coding, and other data quality issues identified in the pre-implementation testing should be remedied and subjected to re-testing. Meanwhile, corresponding work-around or risk mitigating measures should be designed for key residual deviations or issues noted.

(3) Monitoring and Reporting. As part of an effective project management program¹⁵, mechanisms to monitor the development of TMS such as reasonable timelines and milestones for implementation, should be established. Key results should be regularly reported to the BOD, SM, or designated committees, as applicable.

Case Study 3 – Setting TM rules based on applicable red flags identified

Most BSFIs have red flags defined in their policies but have neither defined equivalent rules or scenarios in their TMS nor developed concrete guidelines or procedures for their identification or detection. Accordingly, they were not able to adequately detect and monitor customers' transactions with circumstances or pattern that exhibit said red flags. The BSFIs were directed to translate these red flags into meaningful rules or scenarios in their TMS or adopt concrete guidelines and procedures in identifying or detecting the same.

Case Study 4 – Customer information as basis in setting TM rules/parameters

In some BSFIs, the customer's financial profile is determined by obtaining, among others, the customer's expected financial activity upon onboarding. In certain cases, the financial data obtained are not considered in defining the corresponding rules or parameters in the TMS. The BSFIs were directed to utilize the customer data and information, as well as those gathered throughout the customer's relationship, in defining and calibrating the alert rules or parameters and in investigating the alerts and related transactions for disposition.

Case Study 5 – Testing TM system requirements, including rules/parameters,

Bank B adopted a new AML system for covered and suspicious transaction monitoring. Requirements set by the information security, audit and business were defined and ultimately tested via User Acceptance Testing (UAT). However, the TM rules (e.g., set of scenarios, parameters, and thresholds) under the new system were mere replications of the old system, and were not subjected to UAT and review, recalibration, and back-testing for effectiveness. As a result, previous system issues on voluminous irrelevant alerts linger even with the new AML system. The Bank was directed to review, recalibrate, and test the existing TM rules for effectiveness to generate meaningful alerts and to define additional relevant TM scenarios for red flags or suspicious indicators, as necessary.

Case Study 6 – Recalibrating TM rules/parameters

The TM rules set by Bank C in its TMS involved thresholds (such as P500,000 for high-risk accounts, material transactions of P1 million for individuals and P5 million for juridical entities), aggregation for structuring, and average daily balance. Various frequent and small value transactions which appear unusual or suspicious were not filtered by any of the defined TM rules. The Bank was directed to consider relevant typologies involving low value

¹³ Pursuant to MORB Appendix 76 (IT Risk Management Standards and Guidelines - System Testing).

¹⁴ Such as system integration Testing (SIT) to ensure compatibility of the TMS with source systems and other AML/CTPF compliance infrastructure, User Acceptance Testing (UAT) to ensure that the system performs as expected in the operating or live environment

¹⁵ MORB Appendix 76 (IT Risk Management Standards and Guidelines - Project Management Standards and Methodology / Change Management).

transactions¹⁶ such as drug trafficking, TF, OSEC, and money mules, in defining TM rules based on frequency, velocity or other pertinent patterns of account activity.

<i>Good Practices</i>	<i>Areas for Improvement</i>
<ul style="list-style-type: none"> • <i>Customer's financial profile is determined (by obtaining, among others, the expected financial activity from the customer) upon onboarding.</i> • <i>Information security, audit and business requirements were considered and defined during the planning stage of acquiring a new system and tested prior to implementation.</i> • <i>Customer risk, materiality of transactions and structuring scenario were considered in setting TM rules.</i> 	<ul style="list-style-type: none"> • <i>Develop concrete guidelines and procedures and define equivalent TM rules or scenarios to identify unusual or possible STs.</i> • <i>Consider customer financial data and information in defining and/or calibrating TM rules or parameters and in investigating alerts and related transactions for disposition.</i> • <i>Review, recalibrate and/or back test TM rules adopted in the new system, and subject them to UAT to ensure their effective functioning as intended.</i>

3.3 Robust and Risk-Based TM Implementation

- a. Ongoing CDD and Holistic Monitoring of Customer Activities/Transactions.** Appropriate customer onboarding, risk profiling, and trigger and risk-based updating of customer information and profile are fundamental to an effective TMS. Synthesizing all the customer data and information gathered will aid in understanding the normal and reasonable account or business activity of customers. In turn, these will enable the BSFI to detect unusual activity patterns or deviations from known circumstances.¹⁷ The TMS should be capable of holistic monitoring of customers¹⁸ with multiple accounts and/or related/associated accounts, especially those assessed as high risk. This can be done by adopting an aggregated view and assessment involving data and information collected from CDD, transaction monitoring, surveillance (including adverse news), fraud, complaints, and other risk or incident reports. These will feed into the risk-based updating of customer accounts and review of existing business relationship, as necessary.

Case Study 7 - Updating customer information and risk profile

Pertinent information gathered and analyzed by Bank D based on disposition of alerts (e.g., additional products or services availed subsequent to onboarding, sending and/or receiving counterparties, customer subject of STR filing) were not considered in updating the customer information and risk profile. The inadequate onboarding and customer updating process resulted in incomplete and unreliable CDD documentation. This impaired the analysis of the legitimacy of customer transactions. In which case, the appropriate due diligence and risk mitigating measures were not applied, notwithstanding the elevated ML/TF/PF risks noted based on transaction analysis. Bank D was directed to enhance the CDD process to ensure that customer information and risk profile are completed and updated accordingly (based on policy and defined triggers) with adequate audit trail.

¹⁶ Related AMLC Studies and References: (1) July 2020 COVID-19 Financial Crime Trend Analysis Typologies Brief; (2) 2021 Terrorism and Terrorism Financing Risk Assessment; (3) August 2020 Online Sexual Exploitation of Children: A Crime with a Global Impact and an Evolving Transnational Threat.

¹⁷ Section 921 of the MORB and pertinent sections of the MORNBF require covered persons to establish a system that will enable them to understand the normal and reasonable account or business activity of customers to ensure that the customers' accounts and transactions are consistent with their knowledge of the customers, and the latter's commercial activities, risk profile, and source of funds and detect unusual or suspicious patterns of account activity.

¹⁸ Section 922 of the MORB and pertinent sections of the MORNBF require covered persons to have appropriate system that is capable of aggregating activities of a customer with multiple accounts on a consolidated basis for monitoring and reporting purposes, among other functionalities.

Case Study 8 – Holistic review of customer transactions/profile

Bank E adopts a system where accounts and transactions are aggregated at a customer level, which can be accessed by an authorized user at any branch. Branch review and investigation are documented via the workflow within the automated TMS but this is limited only to the branch where the concerned account was maintained. It does not consider the other accounts or transactions of the same customer in other branches. Further, there are no concrete guidelines and procedures to determine the normal and reasonable customer account activity, to detect deviations. As a result, various alerts were unduly disposed as 'clean' despite the customers' total deposits or investments exceeding the expected cash inflows based on their financial or business profile. Bank E's aggregation capability is recognized, but it was directed to enhance the underlying system or process by adopting: (a) written guidelines and procedures in determining the normal or reasonable account activity of customer; and (b) holistic customer and relationship-level assessment of activities or transactions against its understanding of the customers' financial/business profile.

Good Practice: Generation of Consolidated Alerts and Review of Relationships

Bank F adopts an automated TMS that generates multiple-layer of consolidated alerts at account, customer, and enterprise-level, respectively (encompassing accounts and transactions globally), as well as alerts attributed to a customer's direct and indirect counterparties. Following the prescribed look-back period, Bank F performs holistic review and analysis of the customers' transactions relative to these alerts. If the required supporting documentation was not provided by the customer, subsequent transaction is suspended, while the existing relationship is re-assessed, as necessary.

Good Practices	Areas for Improvement
<ul style="list-style-type: none"> • Pertinent information (e.g., products or services availed, customer's counterparties, customers subject of STRs) are gathered and analyzed in disposing alerts. • Accounts and transactions are aggregated and can be viewed at a customer-level, and accessible at any branch by an authorized user. • Results of alerts review or investigation are documented. 	<ul style="list-style-type: none"> • Consider updated customer information in reassessing risk profile and updating CDD documentation to apply appropriate level of CDD. • Conduct holistic review of related transactions, activities or circumstances, including those conducted in other branches/units. • Develop adequate guidelines and procedures in determining the normal and reasonable customer account activity.

b. Manual or Less Automated TM Process. Where manual or less automated process is adopted commensurate to the BSFI's profile, it is still expected that the TMS is effective, including having the means of flagging and monitoring transactions that qualify as CT or ST.¹⁹ Adequate policies and procedures, especially in identifying or detecting activities or transactions that qualify as possible ST and in conducting and documenting the review or investigation should be adopted. Staff should be trained and guided, while the mechanism adopted should be able to detect complex risks by applying the same logic as what the TM rules or scenarios do.

c. Alerts/Case Management

(1) Alerts generated by the automated system and cases initiated/flagged manually such as those from complaints, fraud investigations, and crimes and losses, should be monitored and analyzed by investigators on a consolidated approach, where applicable, vis-à-vis the customers' history of activities, business, and financial profile. This is to holistically assess and determine whether an unusual pattern or behavior is manifested, which cannot be readily deciphered when alerts or cases are reviewed in silo.

¹⁹ Under Section 922 of the MORB and pertinent sections of the MORNBF, covered persons which are not required to have an electronic system of flagging and monitoring transactions shall ensure that they have the means of flagging and monitoring the transactions; and shall also maintain a register of all STs that have been brought to the attention of SM, whether or not the same was reported to the AMLC.

Disposition of alerts and cases should follow standard timelines aligned with the level of risk they pose and with due consideration of the prescribed timeline for submission of STRs. Risk scoring or prioritization methodology may be adopted especially for high volume alerts generated by the automated systems. Alerts with higher risk score or with shorter determination periods prescribed under the ARRG, as amended, should be prioritized for review and disposition. Compliance with set timelines should be monitored via KPIs (e.g., aging of outstanding alerts, turn-around-time of resolved alerts). Measures should be instituted to address the root causes of the noted deviations.

- (2)** In disposing alerts or cases, results of review and investigation, including ST filing decisions or non-filing thereof, should be adequately documented. It should be satisfactorily supported by relevant customer information, additional valid documents on a risk sensitive basis, and other data analytics collected during the investigation. Investigator, reviewer, and approver accountability should also be evident. The underlying escalation process should be diffused of any conflict of interest or lack of independence.
- (3)** BSFIs remain ultimately responsible in ensuring the effective disposal of alerts and cases including where a portion of the alert or case management is outsourced. Thus, the BOD and SM are expected to be fully apprised of risks arising from such arrangements and ensure these do not result in compromising the ML/TF/PF risk management and internal controls of the BSFI. Adequate oversight should be exercised through the following, at a minimum:
 - Periodic and risk-based monitoring and review of the outsourced functions, including compliance with SLA terms²⁰ stipulating appropriate KPIs, reporting structure, data confidentiality, right to audit clauses, including regulatory examination (e.g., BSP), and other requirements to comply with AML/CTPF obligations such as training and record-keeping;
 - Conduct of risk-based QA, compliance or other independent testing²¹ on closed alerts, to ensure propriety of disposition and documentation in accordance with BSFI standards;
 - Include the outsourced functions in the IRA²² to regularly assess its risks, and incorporate risk mitigation measures into the BSFI's risk management framework;
 - Obtain the customers' written consent before sharing their personal information (e.g., account, transaction) with subsidiaries, affiliates, or other third parties.²³ Said waiver is not absolute and should be limited only to the information necessary to fulfil the particular services outsourced by the BSFI.

²⁰ Consistent with Section 112 of the MORB and pertinent sections of the MORNBSFI on Management Contracts and Outsourcing, including the specific documentations required under the revised outsourcing framework are provided under Appendix 103 of the MORB.

²¹ Section 911 (Risk Management – Internal Audit / Compliance Office) also provided specific review coverages which include review of TMS and compliance to prescribed controls, among others.

²² Pursuant to Section 911 of Part 9 of the MORB and pertinent sections of the MORNBSFI, which require BSFIs to identify, understand and assess their ML/TF/PF risks, arising from customers, countries or geographic areas of operations and customers, products, services, transactions, or delivery channels

²³ Section 1002 of Part 10 of the MORB and pertinent sections of the MORNBSFI require BSFIs to protect client information by, among others, obtaining the consumers' written consent, unless in situations allowed as an exception by law or BSP-issued regulations on confidentiality of consumer's information, before sharing consumers' personal information with third parties.

Case Study 9 – Alert/Case Disposition

Bank G utilizes both an automated system to electronically generate and monitor alerts/cases and MS Excel to record and monitor manually flagged cases (e.g. from complaints, fraud, incidents). In disposing alerts/cases, no prioritization scheme is adopted, while turnaround time is set uniformly (e.g., up to 5 days) across all types of alerts/cases and regardless of the level of risk. For manually identified cases, only those reported as STRs are encoded in the automated system for customer-level monitoring, while information on those cases which were not translated to STRs are not considered in CDD updating and holistic review of customer's transactions. The existing procedures and guidelines do not provide adequate guidance on risk-based handling of alerts/cases, determining the reasonable account activity and documenting the results of investigation. Moreover, personnel responsible in disposing and reviewing alerts are not aware of some applicable standards and updated required timeline in filing STR. In this regard, the quality and completeness of investigation of alerts disposed as 'clean' are questionable. To effectively monitor transactions of customers, the BSFI was directed to:

- Enhance the TMS to facilitate holistic review of customer transactions by: (i) consolidating on a customer-level the alert/case monitoring process; (ii) defining concrete procedures and guidelines in disposing all types of alerts/cases, including risk-based prioritization, prescribed metrics/checklist (e.g., acceptable indicators) that will justify the decisions made, and the required documentation; and,
- Provide all responsible employees with role specific training.

Case Study 10 - Governance structure on outsourced arrangements

Bank H engaged the services of an affiliated foreign company to conduct the 1st level review of alerts generated by its automated TMS, while the 2nd level review and approval to close the same is performed by the Quality Assurance officer/s. A formal SLA with clearly-defined KPIs was executed, while the terms and conditions include a provision that the customer is giving his/her consent to share his/her personal and other account information to the said affiliate of Bank H. Disposed/closed alerts are subjected to compliance testing utilizing random sampling. Annual review of the performance of the said affiliate was not conducted.

Good Practices	Areas for Improvement
<ul style="list-style-type: none"> • Manually flagged cases are tracked and monitored. • Pre-defined metrics or checklist adopted in documenting the results of review/investigation of system-generated alerts and related transactions. • Appropriate escalation structure (i.e., no conflict of interest, and independence preserved). • Formal outsourcing SLA with clearly defined KPIs and customers provided written consent to share personal and other account information as necessary. • Disposed or closed alerts are subjected to independent control checks by the Compliance Office. 	<ul style="list-style-type: none"> • Include manually flagged cases that were not translated as STRs in the customer-level monitoring and consider in CDD updating and holistic review of customers' transactions. • Define procedures and guidelines in disposing alerts/cases, including risk-based prioritization scheme, standard metrics, or checklist for manually identified cases, and standard documentation requirements. • Inform responsible personnel of the risks and/or required procedures. • Conduct annual performance review of the outsourcing arrangement.

Best Practices: Pre-Transaction Review

As already practiced by most local banks, pre-transaction review for specific type of customers, products or services posing higher risks, (e.g., those with correspondent banking services, foreign remittance tie-up arrangement, cross-border remittances, trade), is being adopted, as added safeguard, on top of the post-transaction review conducted. The process is initiated when thresholds and/or other pre-defined rules are breached. Pertinent transaction and the customer are subjected to review and validation and requires SM approval prior to execution. Validation procedures usually include at a minimum, determining the purpose and nature of the transaction, obtaining supporting document(s) from the customer, and establishing the relationship between the customer and its counterparty, among others.

Case Study 11. Performing the prescribed due diligence during pre-transaction review

Bank I, which has an existing correspondent banking arrangement with a foreign bank, implements pre-transaction review for cross-border fund transfers/remittances that deviate from or breach the set rules and threshold values. These rules are based on historical data, while threshold values are not backed by risk or other related assessment. Based on sampling, breaches were not consistently accorded with prescribed due diligence (e.g., SM approval not secured, supporting documents and/or inadequate additional information not obtained). While the basis of the rule-based implementation is recognized, the values set as thresholds should be informed by an adequate risk assessment to justify propriety. This is to ensure that the Bank is not taking excessive risks by adopting thresholds higher than its risk appetite or utilizing excessive resources by implementing unnecessary controls/procedures beyond what is warranted.

<i>Good Practices</i>	<i>Areas for Improvement</i>
<ul style="list-style-type: none"> • <i>Pre-transaction review adopted for high-risk transactions such as cross-border fund transfers/remittances.</i> • <i>Rules defined in filtering transactions to be subjected to pre-transaction review were appropriately validated.</i> 	<ul style="list-style-type: none"> • <i>Set thresholds to trigger pre-transaction review based on results of risk/other related assessment.</i> • <i>Institute measures for consistent conduct of due diligence review for threshold breaches/rule deviations.</i>

d. Recalibration/Fine Tuning of TM Rules and Parameters²⁴. The TM rules, scenarios or thresholds initially designed should be periodically reviewed and recalibrated to ensure relevance and suitability. Reviews can also be initiated whenever material changes in the BSFI's risk profile and appetite, operating and regulatory environments, technical or operational issues, as well as emerging risks and typologies, are observed. Particularly, changes in customer activity behavior, new products/services and innovations, geographic reach expansion, and evolving threats should be carefully considered during ongoing reviews. KPIs and reports on the TMS are helpful references during reviews. Any significant changes/updates should undergo the appropriate change management process (i.e., documented, justified, approved and tested prior to implementation), and reported to the BOD and/or SM.

Recalibration of TM Rules/Parameters

A survey covering seven (7) banks showed that the average STR conversion from system-generated alerts/cases within a six (6) month period is at less than 1% as compared with the 92% conversion rate for manually flagged cases. This indicates the need to strengthen the automated TMS through periodic review and recalibration of TM rules or parameters, as well as complementing the same with machine learning capabilities to ensure generation of relevant alerts. By doing so, resources can be effectively allocated by focusing on meaningful alerts and other areas posing higher risk to the BSFI.

Since an effective TMS or mechanism aids in the interception or prompt detection of fraudulent/crime-related activities, it can ultimately minimize losses due to financial crimes, protect customers' welfare, and secure their continuing trust.

Good Practices: Periodic Review and Fine-Tuning of TM Rules/Parameters

Bank J had recently deployed a new automated TMS and instituted periodic review and fine-tuning of its existing alert rules or parameters for appropriateness and reasonability. These were then streamlined for more efficient administration and tested in the new automated TMS prior to its implementation. A year after implementation, the level of false positive alerts shall be determined and utilized to recalibrate the defined alert rules/parameters in the automated TMS.

²⁴ Sections 921 and 923 of the MORB and pertinent sections of the MORNBI provide for the risk-based approach in ongoing monitoring of clients/transactions such that BSFIs are expected to increase the number and timing of controls applied and select patterns of transactions for further scrutiny pursuant to enhanced monitoring measures. This is to ensure that transactions are consistent with the BSFI's knowledge of the customer, their business, and risk profile, including, where necessary, the source of funds.

3.4 Suspicious Transaction Reporting and Post-STR Process

- a. BSFIs should have effective ST reporting and record-keeping system to ensure complete, accurate and timely filing of STRs with the AMLC. When there is reasonable ground that accounts or transactions are deemed suspicious, BSFIs are required to file corresponding STR with AMLC, and keep adequate records thereof. Adequate records should likewise be maintained for alerts/cases escalated but with no corresponding²⁵ STR filed. These records should include documentation of the results of due diligence, review and assessment conducted, including the justification or rationale for not filing or filing STR. Where STRs are not filed, BSFIs should identify, document, and implement any risk mitigating measures, as warranted.
- b. Where STRs are filed, the risk posed by the subject customer or transactions should be (re)assessed. A review of corresponding transactions, which includes determining any materially linked or related accounts, as well as performing enhanced due diligence²⁶ for those posing high risk, should be conducted. Accordingly, the existing relationship with subject customer should be reviewed. If the BSFI retains the customer relationship, appropriate measures²⁷ to mitigate the risks posed by such customer should be adopted. These measures may take the form of increased monitoring and scrutiny of the customer or account, obtaining necessary approval(s) prior to transaction executions, and placing conditions on the account or on certain high-risk transactions. Where necessary, the AML Compliance Officer and/or SM should be proactively involved in the review process. BSFIs should also monitor new and existing accounts that could be related or associated to the subject account, even after its closure.

Case Study 12 - Post-STR monitoring process and independent reviews

Bank K established policies and guidelines that require SM review for customers with at least three (3) STR filings. There are no established mechanisms to monitor customers falling under the said indicator (i.e., 3 STR filing), hence, four (4) customers with three (3) STRs were retained without the required SM review and approval. These customers were subjected to EDD as the Bank reassessed their respective profiles. However, no corresponding enhanced measures were adopted while the customers remain active. Said process or activities were neither subjected to independent checks by the Compliance Office (CO) nor by Internal Audit (IA). To appropriately manage the risks, the Bank was directed to enhance controls in monitoring and handling customers subject of STRs and the AML CO and/or IA to review its effective implementation.

Good Practices	Areas for Improvement
<ul style="list-style-type: none"> • Policy is established for SM review of relationships of customers with STR filings. • Risk profile is re-assessed, and corresponding EDD is conducted for customers subject of STR filings. 	<ul style="list-style-type: none"> • Adopt procedures or mechanism to monitor the number of STR filings per customer to trigger review. • Implement enhanced measures to mitigate the risks posed by accounts subject of STR filings. • Cover in compliance testing and/or audit the post-STR monitoring process and/or related activities.

²⁵ Section 922 of the MORB and pertinent sections of the MORNBFBI require BSFIs to maintain records of all STs and supporting documents of alerts/flagged transactions investigated.

²⁶ Section 921 of the MORB and pertinent sections of the MORNBFBI provide that enhanced due diligence (EDD) shall be applied to customers/transactions that are: (i) assessed by the covered person or under its applicable rules as high risk for ML/TF/PF; (ii) if there are indications that any of the circumstances for the filing of a STR exists; and (iii) raises doubt as to the accuracy of any information or document provided or the ownership of the entity.

²⁷ Sections 921 and 923 of the MORB and pertinent sections of the MORNBFBI provide for the risk-based approach in ongoing monitoring of clients/transactions such that BSFIs are expected to increase the number and timing of controls applied and select patterns of transactions for further scrutiny pursuant to enhanced monitoring measures.

3.5 Self-Assessment – Audit and Compliance Testing

TMS, including its supporting processes such as ST reporting and post-STR, must be subjected to risk-based independent review and testing by internal auditors, and compliance officers to ensure it is operating as intended²⁸. Internal auditors and compliance officers should have the technical expertise and understanding of the BSFI's risks and context to determine its requirements, which shall be the basis in crafting recommendations. Review and testing must be guided by a risk-based assessment methodology and codified standards and procedures, and should consider, among others, the following:

- TM and supporting processes are based on reliable data and information and the TM rules remain appropriate and relevant;
- Measures adopted are effective and commensurate with the ML/TF/PF risk exposure of the BSFI;
- Concerned personnel perform their duties according to policy expectations and regulatory obligations; and
- The BOD and/or SM are well-informed of key ML/TF/PF risks (including trends, and control and performance issues, among others) and status of key AML/CTPF-related initiatives.

4. Conclusion and Way Forward

4.1 TM is one of the pillars of a sound AML/CTPF framework and is considered as one of the most challenging to implement. TMS needs to be dynamic given the diverse and evolving profile of customers, high volume and complexity of financial products, activities or transactions, wide accessibility of available channels, and cross-border nature of transactions in the financial system.

4.2 The TR discloses that BSFIs are progressively learning to identify and detect various indicators of abuses that are trying to exploit the Philippine financial system. BSFIs must sustain this and continuously strengthen their respective TMS, with due consideration of the observations cited in this guidance paper and the results of their respective IRAs, among others. Constant engagement among the industry players and with the regulators on best practices, including key emerging risks and trends, is also vital in raising the level of monitoring and detection capabilities of BSFIs and the industry, as a whole. Relevant and role specific AML/CTPF trainings within the BSFIs and the industry associations complemented by seminars provided local/international regulators and other reputable AML/CTPF practitioners should be sustained. BSFIs should also consider subscribing to the AMLC's Public-Private Partnership Program (PPPP)²⁹ to access critical information which could reinforce monitoring and suspicious transaction reporting.

4.3 Finally, the BOD and SM should recognize the intrinsic value of TMS as a critical risk management and mitigation tool against risks posed by ML/TF/PF and other financial crimes. The BOD and SM plays a pivotal role in the effective execution of TMS and related controls. This can be demonstrated by providing a robust oversight with clearly defined risk appetite, a TM framework instilling risk awareness and ownership, and sufficient and skilled manpower.

²⁸ Under Section 911 of the MORB and pertinent sections of the MORNBF, internal audit should comprehensively cover evaluation of the risk management, degree of adherence to internal control mechanisms related to the extent and standard of due diligence applied, CT and ST reporting and record keeping and retention, as well as the adequacy and effectiveness of other existing internal controls associated with ML and TF, and determination of the efficiency of the TMS functionalities, among others. Periodic compliance testing should cover evaluation of processes, policies, or procedures including ongoing monitoring, reporting channels, and effectiveness of the TMS, among others.

²⁹ Five of the Top 15 covered persons filing STRs re participants of the PPPP, p.6 AMLC STR Quality Review (2017-2020).