Monetary Authority of Singapore

GUIDANCE TO CAPITAL MARKETS INTERMEDIARIES ON ENHANCING AML/CFT FRAMEWORKS AND CONTROLS

January 2019

Table of Contents

1 Introduction

1.1 Globally, money laundering and terrorism financing ("ML/TF") schemes and typologies are becoming increasingly sophisticated. As a trusted financial centre, Singapore is constantly vigilant to these evolving ML/TF risks. The Monetary Authority of Singapore ("MAS") requires financial institutions ("FIs"), including capital markets intermediaries ("CMIs")[1], to have adequate anti-money laundering and countering the financing of terrorism ("AML/CFT") controls. As important participants in the financial system, CMIs have pertinent roles to play in detecting, disrupting and deterring attempts to abuse the financial system for illicit purposes. It is against this backdrop that MAS recently conducted a series of AML/CFT inspections on CMIs.

1.2 MAS applies a three-pillar framework comprising Governance, Risk Awareness and Execution in our AML/CFT inspections.

(a) **Governance:** The Board and Senior Management (BSM) plays an important role to maintain sound governance frameworks for active management of ML/TF risks. Setting a firm tone from the top with adequate oversight for effective AML/CFT controls should be a priority.

(b) **Risk Awareness**: Strong risk awareness across the FI is needed to enhance the assessment of the nature and level of ML/TF risks faced by the firm, and strengthen the FI's ability to properly identify and escalate risk issues as well as determine appropriate risk mitigation measures.

(c) **Execution:** Effective execution of controls within the organisation is necessary to achieve desired outcomes of detecting, preventing and deterring ML/TF risks.

1.3 The key aspects of the three-pillar framework are illustrated in the diagram below.

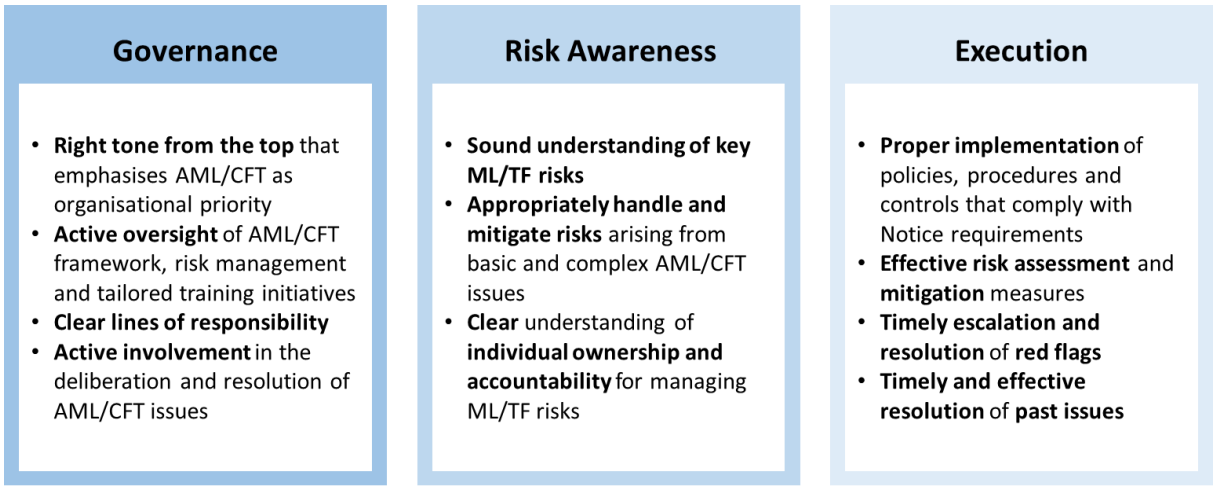

***Diagram 1**: Key aspects of three pillars of effectiveness*

[1] For avoidance of doubt, the term "capital markets intermediaries" used in this guidance paper includes capital markets services licensees and licensed trust companies.

1.4 This guidance paper does not impose any additional legal requirements on FIs, but seeks to clarify MAS' supervisory expectations of existing AML/CFT requirements through the sharing of key observations on aspects of the three pillars from our recent CMI inspections. CMIs should study and leverage this guidance paper to identify and address effectiveness gaps so as to enhance their AML/CFT frameworks and controls in a risk-appropriate manner. For better illustration of our findings, we have included case studies taken from MAS' inspections.

1.5 While this paper is premised on the inspections of CMIs, the takeaways are applicable and relevant to other types of FIs, with the appropriate calibrations, and they should therefore incorporate learning points from this guidance paper. FIs should also note that the findings and case examples highlighted in this paper are non-exhaustive, and FIs should continue to implement appropriate AML/CFT controls that are commensurate with the nature and complexity of the FI's business.

2 Governance

2.1 The Board and Senior Management (BSM) is ultimately responsible for instilling strong ML/TF risk awareness, fostering a sound risk management culture, and ensuring the effectiveness of AML/CFT controls. In this regard, members of the BSM are accountable for deficiencies in the CMI's AML/CFT controls.

2.2 The BSM should be cognisant of the ML/TF risks that the CMI is exposed to, and exercise active oversight of the development and implementation of a robust AML/CFT risk management framework that effectively mitigates those risks. The BSM should ensure, *inter alia*, that:

- AML/CFT policies and procedures, that are up-to-date with regulatory requirements and calibrated to address ML/TF risks arising from the nature and complexity of the CMI's business, are implemented;
- The three lines of defence[2] are suitably qualified and adequately resourced, and assigned clear AML/CFT responsibilities that are reinforced through AML/CFT performance indicators; and
- Reporting and escalation mechanisms are implemented to ensure that BSM is promptly updated on key ML/TF risks and concerns.

Key Findings and Recommendations

i. Insufficient appreciation of AML/CFT by BSM

2.3 The Authority is concerned that the BSM of certain CMIs did not appreciate the extent of the organisations' ML/TF risks, and therefore did not devote sufficient attention to AML/CFT matters. In a few instances, BSM had prioritised business considerations over ML/TF risk mitigation, and exhibited a dismissive attitude in dealing with ML/TF concerns that were escalated by staff. Such behaviours by BSM are unacceptable.

> Box Story: Inappropriate tone from the top
>
> Case Study A
> The compliance staff in CMI A highlighted ML/TF red flags regarding the onboarding of a number of customers. Despite the concerns raised, CMI A's senior management failed to address the attendant ML/TF risks and instead directed staff to complete the onboarding processes to meet the deadline stipulated by the customers.

[2] The **first line of defence** refers to the CMI's business units (e.g. front office, customer-facing functions) in charge of identifying, assessing and controlling the ML/TF risks of their business; **second line of defence** refers to the CMI's AML/CFT compliance function, as well as other support functions such as operations, human resource or technology, which work together with the AML/CFT compliance function to identify ML/TF risks when they process transactions or applications or deploy systems or technology; **third line of defence** refers to the CMI's internal audit function.

Learning point: Where there are reasonable grounds to suspect the legitimacy of the customer's monies, CMIs should not onboard the customer and should file STRs. BSM needs to send a clear message that adequate ML/TF risk mitigation is critical to safeguarding the interests of the firm and should not be unduly compromised by commercial considerations.

Case Study B

CMI B (a licensed trust company) onboarded a customer who was rated higher risk. However, CMI B did not have access to nor the authority to operate the bank accounts of the customer's underlying investment companies, even though this access/authority was required by the CMI's own policy. As such, the CMI was unable to, over a prolonged period of more than 7 years, obtain the bank statements to conduct transaction monitoring. The CMI's staff escalated this lapse to the BSM, highlighting that the customer was rated higher risk. The staff's concerns were dismissed with no follow-up actions taken by CMI B.

Learning point: Where there are impediments to proper execution of AML/CFT controls, BSM needs to instruct staff to address those impediments, and closely monitor the progress. CMIs also need to assess and implement appropriate risk mitigation measures, which may include discontinuing the business relationship with the affected customer.

2.4 Given the inherent ML/TF risks in CMIs' businesses, the BSM should put in place a robust AML/CFT risk management framework as an organisational priority, and emphasise the importance of detecting, disrupting and deterring ML/TF attempts. BSM needs to ensure that the ML/TF risks arising from a CMI's business are properly assessed and mitigated in line with the organisational risk appetite. BSM should also take steps to foster strong AML/CFT practices and behaviours that permeate the firm. These steps may include, for instance, factoring effectiveness of AML/CFT compliance in staff performance appraisal at all levels and taking stern action against individuals who perpetuate improper AML/CFT conduct.

ii. Failure by BSM to ensure the adequacy of AML/CFT frameworks, processes and controls

2.5 To aid in the fulfilment of its AML/CFT responsibilities, BSM should put in place robust risk assessment frameworks and implement effective processes to control risks. In this regard, MAS observed that CMIs' proficiency in enterprise-wide risk assessment ("EwRA") need to be enhanced. A properly conducted EwRA[3] is imperative for the CMI to understand its vulnerabilities to ML/TF risks, and forms the basis for the development of relevant AML/CFT processes and controls in order to adequately address the ML/TF risks it faces. BSM's oversight of the implementation of AML/CFT controls also require improvement in many cases.

[3] The scale and scope of the CMI's EwRA should be proportionate to the nature and complexity of the CMI's business and encompass the broad ML/TF risk factors of (i) customers, (ii) countries, and (iii) products, services, transactions and delivery channels. For further guidance on the sub-considerations under each factor, please refer to the various Guidelines to the MAS AML/CFT Notices.

a. Room for improvement in EwRA

Design of EwRA framework

2.6 A CMI is required to identify, assess and understand its ML/TF risks in relation to:

(a) its customers;
(b) the countries or jurisdictions its customers are from/in;
(c) the countries or jurisdictions the CMI has operations in; and
(d) the products, services, transactions and delivery channels of the CMI.

2.7 MAS observed instances where CMIs' EwRA failed to sufficiently take into account the aforementioned risk factors. There were also CMIs that adopted the use of EwRA templates provided by external parties, without assessing the applicability or relevance of the risk factors/sub-risk factors to their business models and context. Consequently, the CMIs failed to properly evaluate their ML/TF risks.

2.8 MAS also noted inadequacies in the way CMIs have assessed the ML/TF risks arising from countries or jurisdictions that their customers are from/in. A few CMIs relied solely on the Financial Action Task Force's ("FATF") Public Statement and Improving Global AML/CFT Compliance lists, without factoring in other considerations such as corruption and tax evasion risk concerns. There was also a lack of proper guidance for staff conducting risk assessments. In many cases, the assessment was left up to staff's interpretation of what constitutes higher country risk. To illustrate, one of the CMIs used a webpage that showed the different tax rates of various jurisdictions in the world as the CMI's country risk list, but did not provide clarity to staff on how the tax rates should be used to determine if a customer from any specific country on that list poses higher tax risk.

2.9 Internal inconsistencies were also noted in the way CMIs have operationalised their EwRA frameworks. For example, a CMI did not align its EwRA template to its AML/CFT policy. Although its AML/CFT policy stipulates that all PEPs should be rated as 'High' risk, the CMI's EwRA did not associate foreign PEPs as presenting higher ML/TF risks.

Box Story: Poor design of EwRA frameworks

Case Study C

In assessing the ML/TF risks arising from the countries/jurisdictions that its customers are from/in ("country risk assessment"), CMI C considered only FATF-listed jurisdictions that had serious deficiencies in their AML/CFT systems ("FATF list") as posing higher ML/TF risk. This was despite its EwRA policy indicating that other factors including *"higher levels of corruption" or "organised crime"* are required to be taken into account in arriving at the overall country risk score. As a result, all of CMI C's customers were considered to have low country risk, even though it had customers from countries where there are high levels of corruption or organised crime, which were not included in the FATF list.

CMI C also omitted to consider how the following could impact its ML/TF risks:

- Products, services, and distribution channels, which are dependent on factors such as complexity and range of product complexity, extent of direct dealing with customers, reliance on third parties etc; and
- Volume and size of transactions and fund transfers.

Learning point: CMIs need to take into consideration factors that contribute to country risks, such as those arising from corruption levels and tax regimes, in addition to referring to the FATF list of jurisdictions with serious AML/CFT deficiencies. CMIs also need to ensure that they do not omit assessments of ML/TF risks arising from their customers, products, geographies, transactions, services and delivery channels.

Case Study D

CMI D1 had customers that were foreign PEPs, but its EwRA did not take into consideration the corresponding (higher) risk score for customer risk. CMI D1's explanation was that the foreign PEPs it served were not political office holders, and hence did not pose heightened ML/TF risk to the firm. This is inconsistent with the MAS AML/CFT Notice, as well as the CMI's own policies and procedures, which consider all foreign PEPs as higher risk. This points to the CMI's lack of understanding about the ML/TF risks posed by such customers.

In CMI D2's assessment of the ML/TF risks posed by its service and delivery channels, CMI D2 represented that the ML/TF risks are low when it used non-face-to-face ("NF2F") means to establish business relations with the customers; and further allowed third party payments to parties unrelated to its customers.

CMI D2's assessment that they pose low ML/TF risks contradicts with (i) Paragraph 8-2(c) of the Guidelines to MAS Notice TCA-N03[4], which highlights that trust companies allowing payments to and from third parties, and in particular to unidentified and/or un-associated third parties, would heighten exposure to ML/TF risks from such transactions as the sources of funds are unknown and could potentially stem from illicit activities; and (ii) Paragraph 6-10-3 of the Guidelines[5], which states that trust companies, when establishing NF2F business relations, should impose additional checks and controls (including enhanced CDD measures), to mitigate potential impersonation risks.

Learning point: CMIs need to analyse and get a proper understanding of the risk factors that they have included in their EwRA methodologies, and ensure that the calibration of the risk scores are aligned with the degree of ML/TF risks.

Frequency of EwRA

2.10 In spite of the EwRA requirement having been implemented since April 2015, a few CMIs did not conduct any EwRA until they were inspected by MAS. A number of CMIs conducted their EwRA in

[4] The equivalent paragraph in the Guidelines to MAS Notice SFA04-N02 is paragraph 8-2(c).
[5] The equivalent paragraph in the Guidelines to MAS Notice SFA04-N02 is paragraph 6-11-3.

2015, but failed to update their assessment on a regular basis i.e. at least once every two years or when material trigger events occur, whichever is earlier.

b. Inadequate BSM oversight of effectiveness of AML/CFT controls

2.11 Having frameworks and processes in place is necessary but not sufficient on its own. There must be adequate BSM oversight that AML/CFT controls are effectively implemented. MAS has observed instances where BSM failed to monitor whether the CMIs' AML/CFT controls were functioning effectively. In a few of those cases, there were systemic breakdowns of AML/CFT controls over a sustained period. This underscores the importance of implementing effective reporting and escalation mechanisms that would enable BSM to be promptly apprised of AML/CFT issues. At the same time, the BSM has to devote sufficient management bandwidth to oversee the implementation of AML/CFT systems and controls, including the adequacy of training and progress of remediation efforts. Where there are implementation issues, BSM is expected to make timely interventions to address those issues, and to ensure the continuing effectiveness of the CMI's AML/CFT frameworks and controls.

Box Story: Lack of active BSM oversight over effectiveness of AML/CFT processes and controls

Case Study E

The BSM of CMI E1 and CMI E2 were aware of the large number of overdue periodic reviews (a majority of which were higher risk accounts), but did not take adequate remediation steps to reduce the outstanding reviews. For CMI E1, more than 50% of the accounts were overdue by more than six months, and 81% of these overdue accounts were higher risk accounts. The longest outstanding review period for six accounts was 10 years. For CMI E2, more than 18% of the accounts were overdue by more than three months, and 33% of these overdue accounts were higher risk accounts. Some periodic reviews of higher risk accounts even had outstanding action points from more than four years ago.

Learning point: BSM needs to set the right tone from the top and ensure effective AML/CFT controls. BSM needs to institute escalation frameworks and processes that enable them to closely monitor the effectiveness of implementation of AML/CFT control measures. Even if escalation frameworks and processes have been set up, serious AML/CFT deficiencies could still occur if BSM does not actively oversee execution and intervene promptly to rectify ML/TF issues where needed.

Case Study F

CMI F's BSM repeatedly failed to ensure appropriate alignment of its policy and procedures with the MAS AML/CFT Notice requirements. The policy and procedures were initially drafted based on MAS Notice 626 for Banks rather than the applicable MAS AML/CFT Notice for CMIs, and were not updated for protracted periods despite revisions of the MAS AML/CFT Notice.

Learning point: BSM needs to put in place processes to ensure that it stays up-to-date on regulatory developments, and ensure that the CMI's frameworks, policies and procedures are aligned with the relevant regulatory standards.

iii. Failure to ensure appropriate compliance management and resourcing arrangements

2.12 A common observation by MAS was the lack of well-trained and adequately resourced AML/CFT compliance functions that are empowered to provide robust inputs to management risk deliberations. In CMIs with smaller operations, the focus of the sole compliance officer was observed to be diluted by areas of responsibilities outside of the compliance scope. In a few CMIs where the compliance function was outsourced, the BSM failed to adequately monitor the effectiveness of those outsourced functions, which resulted in multiple deficiencies in the CMIs' AML/CFT controls.

2.13 In one CMI with a group reporting structure for compliance, there was a lack of clarity over the delineation of AML/CFT roles and responsibilities, and the reporting lines of the local compliance function vis-à-vis group compliance. Consequently, the local compliance function was ineffective in performing its role as the second line of defence, and numerous gaps in AML/CFT frameworks, control lapses and red flag indicators went undetected.

Box Story: BSM's failure to put in place an effective compliance function

Case Study G

CMI G only had one local compliance headcount, who is supported by an administrative officer, to manage all compliance affairs (including AML/CFT) of CMI G's group of Singapore-based entities, which comprised multiple lines of businesses. Additionally, MAS' inspection found that local compliance focused more on complying with the group's compliance procedures without giving due consideration to CMI G's local compliance requirements. As such, he did not manage to adequately perform his AML/CFT responsibilities in overseeing CMI G's AML/CFT processes and controls on a daily basis, and failed to identify and address AML/CFT issues faced by CMI G.

For example, the compliance manager prioritised the timely completion of periodic reviews for customer accounts that were flagged by group compliance but failed to resolve the backlog of late periodic reviews based on local risk rating methodology, which was more stringent than the group's methodology.

Learning point: BSM needs to ensure that there is an effective local compliance function. Even where there is group oversight, local BSM is ultimately responsible for compliance with local regulations. Hence, there is a need to clarify the mandate/key performance indicators of the local compliance function, and adequately assess the performance of the local compliance.

Case Study H

CMI H outsourced its compliance function to a law firm. However, the outsourced compliance arrangement did not function well – the law firm was not involved in the handling of day-to-day AML/CFT matters and did not ensure that AML/CFT systems and controls were effectively implemented. These duties, including periodic reviews and transaction monitoring, were instead carried out by the operations manager of CMI H, who was not adequately qualified. As a result, several ML/TF risk issues were unsatisfactorily resolved and the required mitigation measures were not taken.

Learning point: CMIs need to determine an appropriate compliance model that is suitable for their context, and business/risk profile. Where AML/CFT compliance functions are outsourced, either in whole or in part, mechanisms need to be put in place to regularly and adequately monitor the performance of the outsourced functions. Where necessary, the firm should reassess the appropriateness of the compliance model.

2.14 As the core of the second line of defence, the AML/CFT compliance function is responsible for monitoring the quality of execution of the relevant business and control functions. Compliance also needs to provide risk management input and be engaged in risk deliberations, particularly for higher risk accounts. In this regard, BSM needs to ensure that AML/CFT compliance functions are adequately resourced and effective by:

(a) empowering compliance functions to drive the monitoring and review of risks and controls;
(b) providing sufficient clarity on compliance function's AML/CFT mandate in the policies and procedures (particularly for compliance functions which have multiple responsibilities and reporting lines); and
(c) equipping compliance functions with adequate AML/CFT resources as well as capabilities through appropriate training.

iv. BSM did not establish appropriate independent audit arrangements; or monitor remediation of audit findings

2.15 CMIs are required to maintain an independent and adequately resourced audit function that is able to regularly assess the effectiveness of their internal policies, procedures and controls, and compliance with regulatory requirements. Such an audit function would assist the BSM in its efforts to monitor the effectiveness of the CMI's AML/CFT controls.

2.16 MAS noted that a few CMIs had failed to establish an independent audit arrangement. This is not in line with the MAS regulatory requirement.

Box Story: Inappropriate independent audit arrangements

Case Study I

CMI I did not maintain an audit function that regularly assessed its internal policies, procedures and controls, and its compliance with regulatory requirements. While CMI I did undergo annual financial audits, these audits were designed mainly to ascertain the reliability of the firm's financials, and not to assess the effectiveness of the CMI's AML/CFT internal policies, procedures and controls, and its compliance with regulatory requirements, as required by the MAS AML/CFT Notice.

Case Study J

CMI J's compliance function doubled up as its independent audit function. As such, there was no independent assessment of CMI J's compliance function as well as effectiveness of AML/CFT systems and controls, and gaps in its AML/CFT framework were not rectified.

Learning point: The independent audit function – as the third line of defence – plays an important role in supporting BSM's oversight of the effectiveness of the compliance function and AML/CFT controls. BSM needs to establish an effective independent audit function, and set up proper reporting arrangements so that BSM can be promptly updated on audit issues and concerns.

2.17 Other CMIs had an independent audit function, but in a few cases, BSM failed to actively oversee the remediation of audit findings. In a couple of instances, audit findings remained unresolved despite being repeatedly raised by auditors over a sustained period of more than 3 years.

Box Story: Lax monitoring of audit remediation

Case Study K

CMI K's BSM did not actively monitor the progress of remediation arising from an AML/CFT external audit, which led to persistence of bad AML/CFT practices within the firm and repeated findings in a subsequent internal audit and MAS' inspection.

Learning point: Delays in rectification of audit issues, if left unaddressed, can expose the firm to heightened ML/TF, legal, reputational and regulatory risks. BSM needs to follow up on audit issues and send a strong message to staff that tardy attitudes in remediating audit findings will not be tolerated.

2.18 Policies and procedures for periodic AML/CFT audits, reporting of strengths and gaps, as well as monitoring and closure of follow-up actions should also be established and implemented. The BSM needs to institute appropriate reporting structures, so that they are kept updated regularly on audit issues and are able to assess whether the control gaps and recommended enhancements raised by auditors have been appropriately addressed in accordance with agreed timelines.

3 Risk Awareness

3.1 Strong risk awareness among BSM and staff is a necessary precondition for effective AML/CFT risk mitigation. Without adequate risk awareness, it would be difficult for BSM and staff of CMIs to properly identify and address ML/TF risks even if they were equipped with comprehensive checklists. To cultivate the appropriate level of risk awareness, BSM and staff need to be provided with sufficient training and guidance, and assigned clear AML/CFT responsibilities. It is important that each employee of the CMI understands the nature and extent of ML/TF risks arising from the company's business, as well as his/her individual ownership and accountability for managing ML/TF risks.

3.2 CMIs are expected to inculcate strong ML/TF risk awareness across the three lines of defence, so that staff apply sound judgment to:

- Adequately identify key ML/TF risks, understand and assess the consequences of these risks, and take the appropriate risk mitigation measures; and
- Effectively escalate and communicate pertinent ML/TF risk concerns to BSM for them to (i) assess the adequacy of risk mitigation measures, and (ii) where necessary, deliberate on the continuation or termination of customer relationships.

Key Findings and Recommendations

3.3 In a few of the inspected CMIs, the MAS examiners observed poor ML/TF risk awareness across all three lines of defence that undermined the effectiveness of the CMIs' AML/CFT controls. There was a lack of awareness, particularly in respect of STR reporting obligations and the identification of ML/TF red flag indicators, including indicators of tax-related ML risk.

i. Inability of first line of defence to detect ML/TF red flags

3.4 MAS noted that in a number of instances, the CMI's front office staff, the first line of defence in charge of identifying, assessing and controlling its ML/TF risks, focused on rote fulfilment of compliance requirements, and were not attuned to identifying ML/TF risks. ML/TF red flags may arise from customer representations or anomalies in supporting documents provided, and could be early indications that a customer's monies were from illicit activities. Hence, there is a need for CMIs to be alert to such red flags and promptly take mitigation measures, including enhanced monitoring of customer, filing of STRs where warranted, or even exiting the customer relationship.

3.5 There were several instances where CMIs' staff displayed a lackadaisical attitude in fulfilling their AML/CFT responsibilities. In a few cases, staff were apathetic when faced with apparent red flags (e.g. transactions that did not make sense economically, evasive behaviour) and did not probe further to determine if mitigation measures need to be applied.

Box Story: Failure to identify and follow up appropriately on ML/TF red flags

Case Study L – Intentional layering to mask the actual source of funds of the assets settled into the account

CMI L's customer, Mr X, had always specified the need for heightened confidentiality. At onboarding, Mr X set up a Singapore-incorporated investment holding company to pump monies into the underlying company of the structure managed by CMI L. Mr X mentioned that the rationale for injecting funds via the newly created Singapore-incorporated company was to avoid possible queries from tax authorities in Country A, where the monies were generated. The customer claimed to have taken extra care to make himself a non-tax resident in Country A, although his source of wealth was evidently from his business in Country A. CMI L failed to follow up on the tax-related red flags at onboarding as well as on an ongoing basis, and failed to file an STR.

Case Study M – Behavioural red flags

CMI M's (a licensed trust company) customer structured the trust such that CMI M did not have control over the bank accounts of the immediate asset holding companies. Moreover, the customer was highly uncooperative in furnishing the bank statements and financial statements of the immediate asset holding companies on a regular basis, with some of these statements provided only three years later. This impeded CMI M's ability to monitor the business relations of the customer on an ongoing basis. Notwithstanding, staff of CMI M did not take appropriate risk mitigation measures or escalate the case to senior management.

Learning point: CMIs need to imbue in staff a sense of responsibility for detecting ML/TF red flags. While ML/TF typologies may be complex, tell-tale signs are often present and staff who are adequately trained and have individual ownership over ML/TF risks would be able to detect unusual transactions or suspicious patterns of behaviour so that appropriate risk mitigation measures, including enhanced monitoring and filing of STRs, can be taken.

3.6 MAS observed that the poor risk awareness arose primarily due to the lack of (i) emphasis from top management on the importance of AML/CFT; (ii) staff performance evaluation and incentive structures that support clear accountability of AML/CFT issues; and (iii) guidance and training that are tailored to the specific business model and risk profile of the CMI.

3.7 It is essential for CMIs to develop guidance on ML/TF red flags specific to their business operations[6] so that employees can identify and assess ML/TF red flag indicators effectively. To ensure that staff are able to fulfil their respective AML/CFT responsibilities, tailored training should be provided for staff performing different AML/CFT functions. CMIs should also consider expounding learning points from specific real-life case studies, e.g. sharing with front office and other relevant staff suspicious transactions and customer behaviours which could lead or led to filing of STRs, that have been encountered by other staff of the CMI.

[6] CMIs can refer to Appendix B of the various Guidelines to the MAS AML/CFT Notices for examples of suspicious transactions. CMIs are to refer to STRO's website for the latest list of red flags. In this regard, the website address as at 20 August 2018 can be found at this link.

ii. Lack of awareness concerning STR reporting obligations

3.8 MAS noted that several CMIs lacked awareness of their legal obligations pursuant to the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act ("CDSA") to report any knowledge or reasonable suspicion of property potentially linked to criminal conduct ("STR reporting requirements"). A few CMIs had the wrong notion that it has to be proven beyond doubt that a customer was involved in criminal activity before an STR is filed. There were also CMIs that thought erroneously that they need not file STRs because other FIs (e.g. custodian banks) were involved in servicing the same customer, and they could leave it to the other FIs to file the STRs. These misconceptions led to the failure of a few CMIs to promptly file STRs where required.

3.9 CMIs are reminded that they have an obligation to lodge an STR with STRO and extend a copy to MAS whenever there are *reasonable* grounds for suspicion that funds are/were connected to criminal conduct or terrorism financing. For example, CMIs should file an STR when they become aware of their customers' participation in tax amnesty programmes ("TAP"). While participation in TAP, in and of itself, does not mean that the customer has committed a tax crime, it is nonetheless an indication that funds in the customer's accounts managed by the CMI could be proceeds of tax crimes. A follow-up STR may subsequently be filed upon the CMI's review of the customer's account if there is additional pertinent information leading to ML suspicion in the customer's transactions and account conduct.

iii. Inadequate awareness of tax-related ML risk

3.10 From our interactions with the CMIs, MAS observed the following common misperceptions:

- The advent of the Foreign Account Tax Compliance Act ("FATCA") and the Common Reporting Standard ("CRS") equate to the elimination of tax-related ML risk for customers; and
- A customer's participation in TAP eradicates tax risk concerns and implies that the customer's tax situation is fully regularised.

3.11 CMIs should exercise vigilance and avoid having a complacent mind-set in assessing tax-related ML risks of their customers. In this regard, a CMI could consider in its assessment of tax-related ML risks, factors such as the relevant countries'[7] compliance with the Exchange of Information on Request standard as well as commitment to adopt CRS/Automatic Exchange of Information[8], level of AML/CFT compliance in relation to customer due diligence ("CDD"), and the customer's participation in a TAP.

3.12 Tax arbitrage opportunities remain despite FATCA and CRS implementation, as not all countries have signed agreements to automatically exchange information with one another. For instance, a customer may choose to change his tax residency to a country without an arrangement with Singapore to exchange information. Although he/she may have good reasons for the change in

[7] These could include the customers' countries of incorporation/origin as well as countries where the customers' sources of funds originate from.
[8] Please refer to http://www.oecd.org/tax/transparency/

tax residency, the CMI should enquire further into this change and request for corroborative evidence of the tax legitimacy of his/her funds, where relevant. CMIs should be alert to the possibility that the customer may be trying to circumvent CRS reporting requirements to countries where he is a tax resident.

3.13 Likewise, tax-related ML risk remains a relevant AML/CFT consideration for customers in spite of their participation in TAPs. CMIs should not assume that the tax affairs of these customers are fully regularised and should continue to monitor for tax-related red flags.

Box Story: Failure to detect tax-related ML red flags

Case Study N

CMI N (a licensed trust company) was engaged as a trustee to a group of customer accounts which hold equal shares in a Singapore-incorporated investment holding company. The customer is resident in Country X where his business is also based; and had no business links to Singapore. The customer had insisted on a high level of secrecy and all communication with CMI N was through the customer's lawyer. CMI N had not had a face-to-face meeting with the customer since onboarding.

The customer had refused to sign a tax compliance declaration since 2013, and had not provided CMI N with his FATCA declaration and CRS self-certification forms. In recent years, the customer's lawyer was also unwilling to provide CMI N with documents to corroborate the legitimacy or economic purpose of the transactions of the Singapore investment holding company. CMI N was also not kept informed of the transactions and activities of the underlying companies held by the Singapore investment holding company.

Moreover, as CMI N did not have control over the underlying companies' bank accounts, it was unable to carry out transaction monitoring since the corporate director of the underlying companies did not provide CMI N with the bank statements.

Despite the apparent red flags and the customer being designated as higher risk by CMI N, CMI N failed to conduct enhanced monitoring of its business relationship and transactions, or file an STR on the customer.

Learning point: Serious tax crimes are ML predicate offences. CMIs must be alert to tax-related ML risks. Where there are red flags and customers are not forthcoming in providing information and supporting documents that would help address any suspicions, appropriate risk-mitigation measures should be taken. These include enhanced monitoring of customer, filing of STRs (where warranted), and discontinuing the customer relationship, where ML risks are unacceptable to the CMI.

4 Execution

4.1 The effectiveness of a CMI's AML/CFT controls is dependent on the quality of staff's execution. A CMI's ML/TF risks should be adequately addressed and mitigated through proper implementation of systems, processes and controls that are carried out by staff with good risk awareness and understanding.

Key Findings and Recommendations

4.2 MAS noted a number of execution lapses in the CMIs inspected that stemmed from the "check-box" approach taken by CMIs. BSM and staff did not fully understand the risk considerations and purposes underpinning certain AML/CFT controls. Given the increasing complexity of ML/TF typologies and the need for CMIs to be vigilant in detecting suspicious customer behavioural patterns, such a "check-box" approach is clearly inadequate, and has resulted in CMIs missing out significant ML/TF red flags.

i. Knowing your customer – reliance on third parties to conduct CDD

4.3 The inspected CMIs generally had policies and procedures in place for the identification and verification of customers and beneficial owners. For customers that were not natural persons, the CMIs also sought to understand the ownership and control structure of the corporate entity.

4.4 Where new customers were referred to the CMIs by third parties, some CMIs relied on the third parties to obtain the necessary CDD information for onboarding. While CMIs are allowed to rely on third parties to perform CDD measures on prospective customers, CMIs should satisfy themselves that the third party's CDD standards meet regulatory requirements as well as their own internal policies. Additionally, CMIs should assess that the third parties used are licensed and supervised for compliance with AML/CFT requirements that are consistent with FATF standards, and have adequate measures to comply with those requirements (i) before placing reliance on third parties for CDD and (ii) on a periodic basis. Where there is reliance on third parties, CMIs are required to immediately obtain the CDD information which is obtained by the third parties.

Box Story: Reliance on a third party to conduct CDD

Case Study O

CMI O onboarded a new customer without face-to-face contact, via an overseas third party which was assessed by CMI O to have met the requirements for reliance on a third party as set out in the MAS AML/CFT Notice.

During the inspection, the MAS examiners found out through internet searches that the beneficial owner in this case was a family member of a PEP; and there was adverse news on the beneficial owner's brother e.g. misusing company funds, insider trading and money laundering and violation of banking and stock transaction laws. However, CMI O was unaware of these potential red flags and thus failed to perform enhanced CDD measures on the account. In addition, CMI O had

executed several transactions by taking instructions from the third party without making enquiries on the unusually large transactions.

Learning point: Where there is reliance on third parties in the CDD process, CMIs remain responsible for their AML/CFT obligations in the MAS Notice. CMIs are required to conduct ongoing monitoring of business relations with customers and cannot rely on third parties to do so. CMIs must secure the necessary information and documentation to adequately manage the customer's risk on an ongoing basis. In addition, for customers who present higher risks, CMIs should endeavour to meet such customers to better assess and mitigate the ML/TF risks posed.

4.5 CMIs should have policies and procedures in place to independently monitor and review business relationships with third parties periodically. In reviewing the reliance on third parties, the CMIs' assessment should include the quality of CDD measures performed by the third party through sample checks, and ensure that the CMI's ability to manage ML/TF risks is not undermined.

4.6 CMIs are reminded that they remain responsible for their AML/CFT obligations in the applicable MAS Notice, and there should not be any reliance on third parties for ongoing monitoring of their customers.

ii. Inadequacies in source of wealth ("SOW") and source of funds ("SOF")

4.7 MAS found that some CMIs failed to perform sufficient enhanced CDD measures for higher risk customers. In a number of cases, there was a lack of corroboration of the SOW and SOF of higher risk customers.

4.8 While the background information of customers and beneficial owners (e.g. business and investment activities, professional careers, family background) were generally obtained and documented by CMIs, a number of CMIs had purely relied on self-declarations and curriculum vitae provided by customers and beneficial owners, and did not seek to independently corroborate the SOW and SOF of higher risk customers as required by the MAS AML/CFT Notices and Guidelines. CMIs should assess and validate the plausibility and reasonableness of the customer's net worth against their understanding of the customer's background by obtaining supporting documentation and/or using public sources of information as reference points. Examples of independent corroboration measures include citing reliable publicly available information sources such as corporate registration websites, company websites and news, as well as obtaining documentary evidence such as companies' financial statements or management accounts, bank statements, independent third party professionals' (e.g. tax advisors) confirmations. CMIs are also reminded to ascertain the legitimacy and credibility of the documents furnished by the customers in this regard.

Box Story: Inadequate corroboration of SOW and SOF

Case Study P

CMI P1 did not implement processes to corroborate either the SOW or SOF of higher risk customers. At onboarding, CMI P1 focused solely on establishing customers' SOF and was

unfamiliar with the concept of SOW. In this regard, CMI P1 performed internet searches on the background of customers, but failed to establish and corroborate the customers' SOW. In some instances, the Company did not even obtain an indication of the size of the customers' wealth.

CMI P2 consistently conflates SOF and SOW, treating these terms interchangeably, and failed to provide adequate guidance on how to distinguish, assess and corroborate SOW and SOF separately. For example, CMI P2's policies and procedures advise that the corroboration of SOF and SOW should be done on an "as appropriate" basis, without elaborating on what "as appropriate" means. Notwithstanding that SOF and SOW may sometimes overlap in practice, such conflation risks glossing over (i) the different ML/TF risks that SOW and SOF pose, and consequently (ii) the different approaches that staff should take to assess and corroborate SOW and SOF. Moreover, some of CMI P2's staff solely relied on the customers' self-representations (e.g. Curriculum Vitae) to corroborate SOW. This resulted in unsatisfactory risk assessment of its higher risk customers.

Despite CMI P3 being aware of a large third party injection for the funding of a higher risk customer account, it relied solely on the beneficial owner's representation that the third party had the same beneficial owners of the customer. CMI P3 failed to seek clarification nor obtain supporting documentation (e.g. constitutional documents) to explain the relationship between the third party account and the customer, and independently corroborate the source of third party's funds.

Learning point: CMIs should obtain a proper understanding of the separate requirements related to SOF and SOW, which are elaborated in the various Guidelines to the MAS AML/CFT Notices. Corroboration of customers' representations using independent sources of information is important for higher risk accounts, in order to detect customers whose monies may be of illicit origin.

4.9 CMIs should obtain a good understanding of the customer's intended purpose and nature of the business relationship with them. For higher risk customers, CMIs should take reasonable means to establish and corroborate their SOW and SOF. Where it is not possible to obtain reliable supporting documents from the customer (e.g. audited financial statements, salary slips, documentary evidence of sale of property), CMIs should, at minimum, validate customers' representations against independent sources of information (e.g. salary benchmarking reports from Human Resource consultancy firms, publicly available financial performance data for businesses of similar scale and nature), and document its assessment of the plausibility of its customers' wealth. Where necessary, CMIs should consider obtaining more stringent independent verification options such as obtaining customers' tax returns filed with the relevant tax authorities or commissioning external intelligence reports.

iii. Deficiencies in ongoing monitoring framework

a. Improvements required in respect of ongoing monitoring

4.10 There is room for improvement in the CMIs' ongoing monitoring framework. In determining which transactions are to be reviewed, a few CMIs applied a single quantum threshold that did not take into consideration differences in customers' risk profiles. A few CMIs also took a 'silo' approach of reviewing each transaction and/or account on a standalone basis. As a result, these CMIs failed to detect a few cases where unusual patterns of transactions, which were individually below the CMIs' monitoring threshold but collectively amounted to a significant quantum, were inconsistent with customers' profiles and warranted additional scrutiny.

4.11 CMIs should apply a risk-based framework that allows them to adjust the extent and depth of their monitoring of customers according to the customers' ML/TF risk profile. Additionally, CMIs need to ensure that their ongoing monitoring is conducted meaningfully based on patterns of transactions and aggregated positions (e.g. for customers with multiple accounts, and accounts of related customers) to (i) better understand the risks associated with their customers; (ii) identify potential ML/TF risks; and (iii) report suspicious transactions. For further guidance on transaction monitoring, please refer to the applicable Guidelines to the MAS AML/CFT Notices, and the guidance to banks for effective AML/CFT Transaction Monitoring Controls[9] published in September 2018.

Box Story: Lapses in ongoing monitoring

Case Study Q

CMI Q1 applied a relatively high single threshold quantum to monitor its customers' transactions. As a result, CMI Q1 failed to scrutinise a series of customer transactions that were not consistent with the purpose of the account stated at set-up as the transactions were individually lower than its transaction monitoring threshold, although the transactions cumulatively amounted to a significant amount. CMI Q1 did not pick up several unusual elements and inconsistencies in the sale and purchase agreements that were used to substantiate the transactions until prompted by the MAS examiners. For instance, there were errors in the sale and purchase agreements, particularly in regard to the customer's bank details such as the wrong bank name, address and SWIFT code. In addition, prices stated did not appear to entirely match the products sold, and from a quick internet search, the nature of business of some sellers appeared to be different from the product being sold.

CMI Q2's policies and procedures did not require its staff to holistically monitor multiple customer accounts with common beneficial owners. This has led to gaps in its ability to monitor suspicious activities arising from more complex transactions involving multiple related accounts. MAS noted that there were transactions and patterns of fund flows between a few related account structures, as well as a separate PEP (whom CMI Q2 had assessed to pose significant ML/TF risk) that ought to be flagged for closer scrutiny. As such, CMI Q2's failure to implement the necessary

[9] The guidance for effective AML/CFT Transaction Monitoring Controls can be found at this link.

holistic monitoring measures led to lapses in the detection, review and conduct of the necessary follow-up for several transactions that did not make economic sense.

CMI Q3 did not implement an adequate transaction monitoring framework to detect suspicious transactions on a timely basis. Its transaction monitoring practice was to peruse the bank statements of its customers' accounts as well as the customers' underlying companies on a monthly basis. According to CMI Q3, it would also obtain and review the financial statements of the customers' underlying companies. However, CMI Q3 did not track and periodically follow up on the status of these transaction reviews, or keep a record of transaction details (e.g. date, size, purpose, counterparties). Further, there was no documentary evidence that the financial statements/ bank statements obtained had been reviewed. Without a proper overall transaction monitoring tracking and documentation system and process, CMI Q3 may inevitably fail to identify any potentially suspicious transactions that warrant further mitigation measures in a timely fashion.

Learning point: CMIs need to strengthen the design and implementation of their ongoing monitoring frameworks. Among other considerations, CMIs may need to segment their customer groups and establish appropriate parameters and scenarios to better detect deviations of customers' activities from their stated purpose of the accounts and expected transactions/behaviours. In this regard, unless a CMI's customer pool is homogeneous in business/risk characteristics, a single monetary threshold for transaction monitoring is unlikely to be meaningful.

b. Enhancements needed in risk assessment and risk mitigation measures for complex structures

4.12 A number of CMIs appropriately viewed the complexity of a customer's ownership or control structure, as well as those of their downstream asset/investment holding structures as one of the key indicators in their ML/TF risk assessment. However, some of them did not provide clarity on how a 'complex structure' should be determined and assessed in their risk assessments or policies and procedures. Examples of considerations that CMIs can use for assessing the risks posed by the complexity of a customer's structure include:

- the number of layers involved within the structure;
- the extent to which the layers increase the structure's opacity and impede the CMI's ability to effectively monitor for suspicious behaviours and transactions;
- whether the CMI is able to satisfactorily understand and explain the rationale for the layers; and the structure is consistent with the nature of the customer's profile and his/her intended purpose for setting up the account;
- whether the CMI is impeded in understanding the corporate entities due to the control structure and nature of business of the corporate entities, e.g. operating companies held as trust assets controlled by settlors and the licensed trust company does not have adequate sight over the operating companies, through for example, obtaining their annual financial statements.

4.13 While there may be legitimate reasons for the use of complex structures, such structures are more vulnerable to being abused for ML/TF as they can be used to cloak or carry out illicit activities. In dealing with complex structures, CMIs are expected to understand the rationale, purpose and intended activities of the structures in order to ascertain their legitimacy. In this regard, CMIs need to also identify the natural persons having ultimate beneficial ownership and control of these structures. Additional due diligence measures that CMIs can consider adopting to mitigate the risk(s) include, *inter alia*:

- reviewing the financial statements and/or management accounts of all entities within the structure on a regular basis;
- reviewing the entities' transaction activities regularly to detect unusual or suspicious patterns and behaviours;
- obtaining independent legal or other expert advice (e.g. tax advice) to help the CMI make informed risk assessments of such structures;
- performing the following due diligence measures before accepting operating companies ("OpCo") as injections into their customers' accounts e.g. trust accounts, bespoke investment funds:
    - Understand the profile and operations of the OpCo via meetings with customers and publicly available sources of information;
    - Obtain the OpCo's constitutional documents and audited financial statements to ascertain the legitimacy of the OpCo's business;
    - Perform site visits to the OpCo's business premises to detect shell operations;
    - Conduct screenings and/or internet searches for adverse ML/TF news on directors and shareholders of OpCos.
- reviewing periodically (at least annually) activities of the corporate entities/OpCos using financial statements and bank statements to ascertain whether the transactions are in line with the CMI's knowledge of the customer's profile and business, or whenever there is any change in the customer's structure or OpCo's business, whichever is earlier.

Box Story: Insufficient downstream due diligence conducted in respect of OpCos

Case Study R

CMI R1 acknowledged that the presence of OpCos within a structure pose a heightened challenge to CMI R1's effective monitoring of these accounts for suspicious activities, as CMI R1 may not have access to or understand the OpCo's business and its transactions enough to assess whether any suspicious activities may have taken place. In spite of this, CMI R1's risk assessment framework did not consider the presence of OpCos as a risk indicator requiring consideration.

CMI R2 represented that it would obtain and review financial statements and bank statements for structures which involve OpCos. However, there was no guidance to staff on the i) review and analysis of these documents, ii) frequency of reviews, and iii) escalation process to management upon identification of red flag indicators.

In the absence of a proper transaction monitoring framework for structures involving OpCos, coupled with the lack of an overall tracking and documentation system, CMI R2 consequently failed to detect potentially suspicious transactions that were flagged by the MAS examiners.

Learning point: Most of the inspected CMIs share the view that OpCos within customer structures create challenges for AML/CFT ongoing monitoring. CMIs need to assess whether they are able to address any consequential impediments to effective AML/CFT controls, the extent of residual risks, and whether those residual risks are within the risk appetite of the firm.

5 Summary of Supervisory Expectations

Through the inspections of CMIs, MAS has noted areas where the industry could benefit from additional guidance. Key areas of concern and corresponding recommendations for sound practices have been discussed in the earlier sections. To aid in the prioritisation of CMIs' efforts to continually enhance their controls, this section sets out MAS' key supervisory expectations covered in this guidance paper.

Governance

5.1 To build a robust AML/CFT governance framework, BSM should have adequate oversight of the effectiveness of AML/CFT systems, processes and controls, and put in place competent and adequately resourced compliance and independent audit arrangements. There should also be adequate and timely reporting to BSM on key ML/TF risk issues and concerns. CMIs should also:

- G.1 Put in place a review process to periodically assess the adequacy and effectiveness of the firm's AML/CFT compliance frameworks, systems and processes. The EwRA framework should be one of the key areas prioritised for the initial review.
- G.2 Clearly define the roles and responsibilities of compliance and independent audit functions, and periodically review their effectiveness in acting as the second and third lines of defence respectively.
- G.3 Review and enhance AML/CFT reporting processes to ensure that (i) the BSM receives sufficient and timely updates on key ML/TF risks and challenges so that ML/TF concerns are actively monitored, decisions on mitigation measures are taken and guidance for effective execution are provided where necessary; and (ii) the remediation of audit findings is timely, effective and sustainable.

Risk awareness

5.2 To strengthen risk awareness of BSM and staff, CMIs should:

- R.1 Formalise individual ownership and accountability over AML/CFT controls, so that BSM and staff are aware of, and understand their respective AML/CFT responsibilities.
- R.2 Develop and communicate clear guidance tailored for the various AML/CFT functions. Guidance should include the nature of ML/TF risks that arises from the firm's business, red flags based on customer behaviours and account activities, and appropriate escalation and risk mitigation measures.
- R.3 Review periodically, and enhance training programmes and curriculum (e.g. by including new relevant typologies as and when they arise) to ensure that specialised training is provided for the various AML/CFT functions and a framework for continuous learning is developed within the CMI. To help staff obtain a better understanding of the AML/CFT issues they might encounter in their daily work, case studies and/or role plays should be incorporated, where appropriate, in AML/CFT trainings.

Execution

5.3 To support effective execution of AML/CFT frameworks, systems and controls, CMIs should:

E.1 Periodically review and enhance policies and procedures to ensure that they are aligned with regulatory requirements and supervisory expectations, as well as any audit recommendations. In this regard, the corroboration of SOW and SOF of higher risk customers and timeliness of periodic review assessments should be amongst the key focus areas.

E.2 Implement an ongoing risk-based monitoring framework which ensures that enhanced CDD measures are adequately applied on customers that pose higher ML/TF risks.

E.3 Put in place systems and processes for the identification, assessment and escalation of ML/TF red flags, as well as the implementation of risk mitigation measures, including filing of STRs, where required.

6 Conclusion

6.1 It is important that CMIs maintain effective AML/CFT controls so as to prevent the abuse of their products and services for illicit purposes. Adequate focus has to be accorded to AML/CFT. CMIs' BSM need to set the proper tone from the top, imbue strong ML/TF risk awareness and drive the effective execution of controls across the three lines of defence.

6.2 In the face of changing business environments and evolving ML/TF typologies, CMIs need to continually review, adapt and enhance their AML/CFT controls in order to remain effective. CMIs should also conduct a gap analysis, in light of this guidance paper, and take appropriate measures to remedy control gaps or deficiencies identified within a reasonable timeframe. MAS will continue to provide guidance and share sound practices gleaned from our inspections to improve industry practices.