

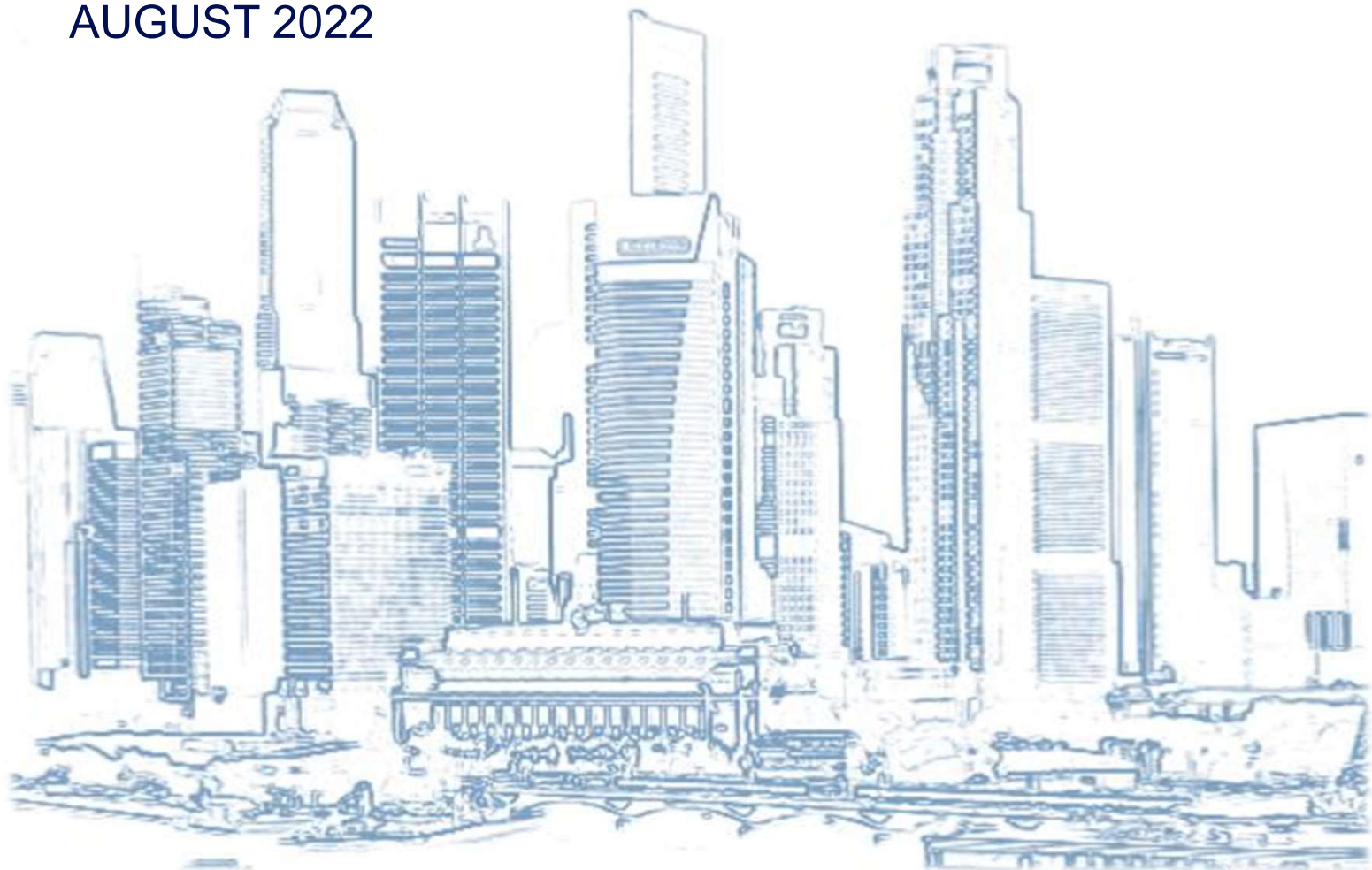


Monetary Authority of Singapore

STRENGTHENING AML/CFT PRACTICES FOR EXTERNAL ASSET MANAGERS

INFORMATION PAPER

AUGUST 2022



CONTENTS

A.	Introduction	3
B.	Governance	4
C.	Risk Assessment Frameworks	
	1. Enterprise-wide risk assessment	9
	2. Customer risk assessment	14
D.	Customer Due Diligence (CDD)	
	1. On-boarding of new customers	19
	2. Transaction monitoring	24
	3. Periodic reviews	28
E.	Enhanced CDD	31
F.	Suspicious Transactions Reporting	35
G.	Conclusion	37

A. Introduction

This information paper sets out MAS' supervisory expectations of effective anti-money laundering and countering the financing of terrorism (AML/CFT) frameworks and controls for external asset managers (EAMs)¹, also known as independent asset managers. The guidance is based on key findings from a series of thematic inspections and engagements conducted by MAS. EAMs should review their AML/CFT frameworks and controls against these expectations in a risk-based and proportionate manner. Where EAMs observe any gaps in their frameworks and controls, specific remediation/enhancement measures should be identified and implemented in a timely manner.

Format of information paper

Areas covered are as follows:



Governance



**Risk
Assessment
Frameworks**



**Customer
Due
Diligence
(CDD)**



**Enhanced
CDD**



**Suspicious
Transactions
Reporting**

Where relevant, case studies/specific examples have been included to describe the findings in greater detail.

Note: While the paper is premised on the inspections and engagements of EAMs, the takeaways are applicable to other fund management business models. All fund management companies (FMCs) should therefore incorporate the learning points from this information paper where relevant. The findings and examples highlighted in this paper are non-exhaustive, and FMCs should continuously enhance their AML/CFT frameworks and controls to ensure they are commensurate with the scale, nature and complexity of their business.

¹ EAMs in Singapore can have different business lines. Generally, they manage the assets of high net worth customers that are custodised with private banks on an advisory or discretionary basis, and/or manage funds that are sold to high net worth customers.

B. Governance

Board and senior management (BSM) play an important role to maintain good governance and sound AML/CFT risk management frameworks and controls at the EAMs. BSM should foster a strong AML/CFT culture within the EAMs and actively oversee the development and implementation of AML/CFT programs across the three lines of defence to effectively mitigate money laundering and terrorism financing (ML/TF) risks.

General practices that we observed

- BSM were aware that they were ultimately responsible and accountable for management of ML/TF risks and compliance with AML/CFT obligations.
- BSM also had a general understanding of the AML/CFT regulatory environment in which their businesses operate in.
- AML/CFT governance framework, established and formally approved by BSM of most EAMs, was based on the “three lines of defence” model.

Business Units



There were generally adequate policies and procedures in place to guide EAMs' relationship managers on how to assess customers' ML/TF risks, as well as detect and report suspicious transactions.

Compliance



Most EAMs, including those with smaller business operations (e.g. assets under management (AUM) of S\$50m and customer base of 40), had a dedicated Compliance function responsible for their AML/CFT program with direct reporting line to senior management.

Internal Audit



Regular internal audits (IA) on AML/CFT controls were done typically ranging from once a year to every 3 years for most EAMs.

B. Governance

- Senior management was involved in approving the onboarding of higher ML/TF risk customers and transactions. Potential ML/TF risk issues were also escalated to senior management.

Examples of better practices where senior management was more involved in the management of ML/TF risks



- In a few EAMs with smaller customer base, the Chief Executive Officer (CEO) of these EAMs personally approved the onboarding of all new customers and/or continuation of business relations with all existing customers after reviews conducted by Compliance and other front office staff.



- In addition to ad-hoc discussions, the CEO of another EAM had regular and frequent meetings with the Compliance team to ensure that he was kept updated on AML/CFT matters (e.g. AML/CFT regulatory developments, AML/CFT training for staff, summary of suspicious transaction reports (STRs) filed on customers) and that AML/CFT issues were monitored and resolved in a timely manner.


B. Governance



Areas of weaknesses that we observed

1. Poor risk awareness and failure to set the right tone from the top

Case examples

- Senior management of some EAMs approved the onboarding of higher ML/TF risk customers without taking into account the adequacy of enhanced due diligence measures that were performed. In some cases, information obtained and included in the EAMs' assessment was inaccurate or insufficient to support the customers' declared profiles. However, these lapses and shortcomings were not picked up by senior management, resulting in red flags not being identified or followed up appropriately. 
- For one EAM, multiple governance failures were observed which suggested that BSM did not take its AML/CFT obligations seriously :
 - There were no formal mechanisms (e.g. regular meetings/forums where discussions and decisions were properly recorded, and periodic reports on key ML/TF indicators) to ensure accountability and allow BSM to keep track and stay updated on key ML/TF issues.
 - There were no established key performance indicators, and key staff and representatives were also not held accountable for their poor execution of AML/CFT controls and non-adherence with regulatory requirements as well as internal policies and procedures (e.g. no disciplinary actions were taken against them).
 - There were repeat findings from a past MAS inspection, which indicated that remediation measures were ineffective.

B. Governance

1. Poor risk awareness and failure to set the right tone from the top

Case example

- An EAM had errors in its enterprise-wide risk assessment (EWRA) which affected the accuracy of its ML/TF risk assessment at the enterprise-wide level. These errors were not detected by the CEO and Chief Operating Officer who reviewed and approved the EWRA.



2. Inadequate compliance and/or IA arrangements

Case examples

- Despite substantial growth in its business and operations over a few years, the BSM of an EAM did not ensure its second line of defence kept pace with the growth and maintained proper oversight of the heightened ML/TF risks posed. Compliance resource was grossly insufficient and there was no AML/CFT audits by IA during this period.
- In another case, the BSM allowed the IA function to be performed by a non-independent person who had no relevant audit experience and knowledge of local AML/CFT requirements.
- A handful of EAMs also failed to conduct any internal audits to assess the effectiveness of their AML/CFT policies, procedures and controls.



B. Governance

Key takeaways

BSM should:

1

Be aware of the regulatory requirements and expectations, set the right ML/TF risk culture and maintain adequate oversight of ML/TF matters through proper monitoring and escalation mechanisms.

2

Take due care to review and query information presented to them for approval to ensure it accurately reflects the EAM's exposure to ML/TF risks.

3

Ensure that all three lines of defence are (i) aware of their AML/CFT responsibilities, (ii) held to account, and (iii) equipped with the relevant knowledge to detect ML/TF red flags.

4

Ensure that compliance resources, in terms of competence, experience and headcount, keep pace with business growth, and are commensurate with the EAM's ML/TF risk profile.

5

Ensure that IA function is independent and adequately resourced with relevant expertise and knowledge of local AML/CFT requirements.

IA scope and frequency should be commensurate with the scale, nature and complexity of the EAM's business.

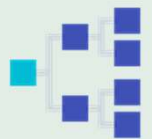


C. Risk Assessment Frameworks – Enterprise-wide Risk Assessment

EWRA enables EAMs to understand their overall vulnerability to ML/TF risks and develop a holistic approach to manage and mitigate the ML/TF risks that exist across all its business units, product lines and delivery channels.

General practices that we observed

- Most EAMs used a combination of quantitative and qualitative indicators in their EWRA, which were reviewed on a periodic basis.



Areas of weaknesses that we observed

1. Failure to consider relevant risk factors in the EWRA

Some EAMs did not have a holistic view of the ML/TF risks associated with their business model. This hampered their abilities to (i) manage their ML/TF risks effectively across all their business units and product lines and (ii) implement appropriate measures to mitigate the associated risks.

Case examples

a) Customer risk profile



- In conducting its risk assessment, an EAM did not take into account the ML/TF risk profile of its customers (e.g. number of higher ML/TF risk customers, including politically exposed persons (PEPs)). Another EAM who managed both segregated mandates and funds did not consider the ML/TF risk profile of its funds' customers. A number of EAMs did not factor in the ML/TF risks associated with their target customer markets and segments.

C. Risk Assessment Frameworks – Enterprise-wide Risk Assessment



Areas of weaknesses that we observed

1. Failure to consider relevant risk factors in the EWRA

Case examples

b) Customer transactions

- Some EAMs did not consider the aggregated volumes and sizes of their customers' transactions and fund transfers, when assessing their ML/TF risk profiles which could be indicative of heightened ML/TF risks if the transactions involved third parties and/or high-risk countries. This included customers for which the EAMs did not have full control over the management of the customers' assets (e.g. customers could direct payments to 3rd parties).
- One EAM allowed personal transactions (e.g. purchase of high value goods) to be undertaken in customers' investment management accounts but did not assess whether such transactions (e.g. frequency and quantum of transactions) could heighten its ML/TF risks at the enterprise-wide level.

c) Products/services and delivery channels

- Some EAMs did not consider the types of products/services that were offered (e.g. setting up fund vehicles to solely book customer's assets without active management, advising customers of investment options versus managing customers' monies on a discretionary basis, managing funds for multiple unrelated investors versus a single high net-worth family) and their associated ML/TF risks.
- Some EAMs also did not consider the ML/TF risks arising from the different delivery channels, such as the extent to which the EAM leveraged on technology or relied on third parties to perform CDD measures.

C. Risk Assessment Frameworks – Enterprise-wide Risk Assessment

2. Lack of clarity on EWRA methodology



- Some EAMs did not provide any guidance to staff on how the different EWRA risk and control factors should be rated which resulted in inappropriate and inconsistent assessments. For example, an EAM did not specify the thresholds for rating the quantitative risk factors as “Low”, “Medium” or “High”. There was also no guidance on the circumstances for assigning a “Strong”, “Average” or “Weak” rating to control factors. The methodology to determine the overall EWRA rating, based on the ratings of the individual risk and control factors, was also not specified.
- In a few instances, the EWRA was treated as a check-box exercise, with only ‘Yes/No’ inputs and no supporting justifications and assessments.

3. Inconsistent rating framework for individual customer risk assessment versus EWRA



- An EAM did not ensure consistency in the assessment of common risk factor (i.e. country risk) that is applied at the individual customer level and the enterprise-wide level.
- It adopted a less stringent country risk classification for its EWRA compared to its individual customer risk assessment. This resulted in the understatement of its ML/TF risks associated with its country exposure at the enterprise-wide level.

C. Risk Assessment Frameworks – Enterprise-wide Risk Assessment

4. Errors in EWRA



- An EAM had errors in its EWRA which affected the accuracy of its ML/TF risk assessment at the enterprise-wide level.
- It provided nil responses to certain risk factors, such as (i) number of customers domiciled in jurisdictions where terrorism or corruption was prevalent, and (ii) presence of audit findings. However, the EAM had exposure to such customers and its most recent internal audit report also contained several ML/TF findings.
- Another EAM's EWRA methodology was mathematically flawed. For instance, the sum of all the risk weights for the various risk factors did not add up to 100%. In addition, the EAM was unable to clearly explain how a 3-point rating scale ("High", "Medium", "Low") was used to score risk factors which had only two possible answers ("Yes" or "No").

5. No timely review and update of EWRA



- Some EAMs took more than two years to update their EWRAs. The longest time taken was four years.

C. Risk Assessment Frameworks – Enterprise-wide Risk Assessment

Key takeaways

EAMs should:

1

Consider all relevant risk factors, bearing in mind its business model, including target markets and delivery channels, when assessing ML/TF risks at the enterprise-wide level.

2

Ensure consistency in applying the risk assessment framework at the individual customer level and the enterprise-wide level.

3

Provide adequate guidance and conduct proper review of EWRA to ensure the inputs are accurate and the outcome of the assessments are reasonable.

4

Review and update their EWRA on a regular basis i.e. at least once every two years or when material trigger events/developments occur, whichever is earlier.



C. Risk Assessment Frameworks – Customer Risk Assessment

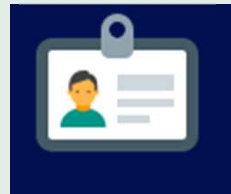
Customer risk assessment is important for EAMs to identify, assess and understand the ML/TF risks posed by their customers and apply the necessary level of customer due diligence and ongoing monitoring measures on them. Ultimately, the results of the assessment should enable the EAMs to make an informed decision on whether to establish, continue or terminate the business relations with a particular customer.

General practices that we observed

- In designing the risk assessment framework, all EAMs considered multiple risk factors to determine a customer's overall ML/TF risk level. A non-exhaustive list of examples considered is as follows:



Customer's / beneficial owner's (BO) place of domicile and nationality



Nature of employment / business



PEP exposure / adverse news / sanctions



Complexity of ownership structure for corporate customers



Product / service offered

- Most EAMs adopted the use of quantitative methodology with certain overrides. Customers were rated as posing higher ML/TF risks if the aggregate risk score assigned to them exceeds a certain threshold and/or if certain "High" risk factor(s) was met. Commensurate level of ML/TF controls were applied when the extent of ML/TF risks posed by each customer/BO(s) was accurately identified.

C. Risk Assessment Frameworks – Customer Risk Assessment



Areas of weaknesses that we observed

1. Failure to consider relevant risk factors in identifying higher ML/TF risk customers

Case examples

a) Higher risk countries or jurisdictions



- In determining higher ML/TF risk countries, some EAMs only considered countries that FATF had identified to have weak measures to combat ML/TF risks. They did not but could have reviewed other country-specific assessments by FATF (e.g. mutual evaluation reports) and/or include countries with corruption and tax evasion risk concerns identified by other credible bodies (e.g. Transparency International, the Organisation for Economic Co-operation and Development²) as posing higher ML/TF risks.

b) Higher tax risk



- Some risk factors used by EAMs to assess a customer's tax risk were not comprehensive or well defined. For example, some EAMs did not consider a customer's participation in tax amnesty programmes (TAP). In addition, an EAM considered the “existence of specific transactions” as one of the tax risk indicators without defining what these “specific transactions” were.

c) Frequent payments received from/sent to third parties



- Some EAMs did not consider customers with frequent or significant payments received from/sent to unknown or unassociated third parties as posing higher ML/TF risks.

² Jurisdictions highlighted as offering citizenship and residence by investment schemes which potentially pose a high risk to the integrity of the OECD/G20 Common Reporting Standard.

C. Risk Assessment Frameworks – Customer Risk Assessment

2. Poor execution of customer risk assessment framework

Case examples

a) Customers from countries that FATF called for countermeasures

Background of Customer



- Held dual citizenships of Country A and Country B.
- Born in Country A, a country that FATF called for countermeasures and re-located to Country B.
- Inherited his wealth from a family member who generated the wealth in Country A.



Assessment by EAM

- Only regarded customer as a citizen of Country B.
- Customer was risked-rated as medium risk and not subjected to enhanced CDD.

MAS' observations

- EAM should have considered the higher risk posed by the customer as (i) the customer's source of wealth could be traced back to Country A, and (ii) the customer was a citizen of Country A.

b) PEPs

- Some EAMs failed to consider some customers as having political exposure even though they were aware of the customers' association with PEPs (e.g. a customer was (i) the immediate family member of a senior political party member, or (ii) a connected party to a senior executive of a state-owned enterprise (SOE)).

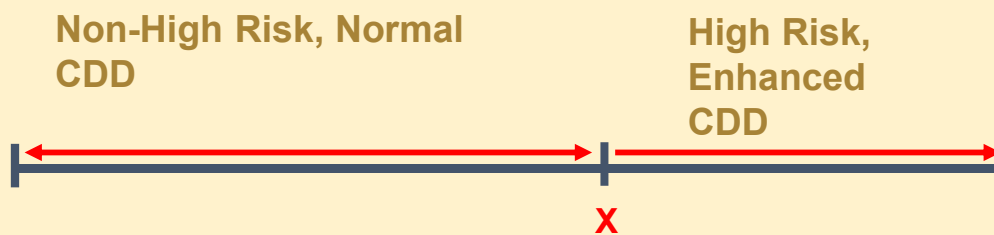
C. Risk Assessment Frameworks – Customer Risk Assessment

3. Inadequate CDD applied to PEPs

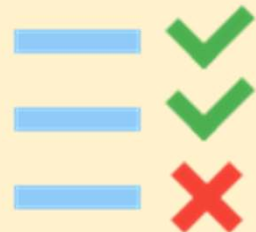
- An EAM had a few customers where the BOs should have been considered PEPs or close associates of PEPs. Notwithstanding, the EAM decided not to subject these customers to enhanced CDD without proper assessment of the roles and seniority of these individuals.



4. Limitation in the design of the customer risk assessment framework



- An EAM's risk rating methodology allowed a foreign PEP not to be classified as a "High" risk customer (where enhanced CDD would apply) when the cumulative score was less than "X", which was against the regulatory requirement for all foreign PEPs to be subjected to enhanced CDD.



C. Risk Assessment Frameworks – Customer Risk Assessment

Key takeaways

EAMs should:

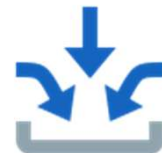
1

Be cognisant of regulatory guidance and ensure that all relevant risk factors are duly incorporated in the design of the customer risk assessment framework.



2

Consider pertinent and credible information to assess the ML/TF risks posed by customers/BOs, including PEPs, or family members or close associates of PEPs.



3



Execute the customer risk assessment framework judiciously on a regular basis to ensure all higher ML/TF risk customers are appropriately identified and subjected to enhanced CDD measures in a timely manner.



D. Customer Due Diligence – Onboarding of new customers

Adequate CDD measures should be performed when establishing business relations. Such CDD measures include the identification, verification and screening of a customer and its relevant parties (e.g. natural persons appointed to act on behalf of the customer, connected parties of the customer, and BOs of the customer).

General practices that we observed

- Most EAMs had a structured approach (e.g. use of customer onboarding forms and checklists) to ensure that they have adequately identified the customers and their relevant parties, performed the necessary verification and screening checks, and documented the profile of the customers/BO(s). These onboarding documents were signed off by relevant reviewing and approving parties.
- Most EAMs had face-to-face meetings with their customers/BO(s) prior to establishing business relations. 
- All EAMs subscribed to commercial screening databases to identify adverse information on their customers and the relevant parties. 

Example of better CDD practices

- Some EAMs completed all onboarding CDD measures, including screening, prior to signing an asset management mandate and/or a Limited Power of Attorney (LPoA).
- Some EAMs also performed internet searches to complement the screening performed using commercial databases.
- Ongoing screening was also automated for some EAMs, which allowed for daily checks to be conducted.

D. Customer Due Diligence – Onboarding of new customers



Areas of weaknesses that we observed

1. Inadequacies in the identification of customer and their relevant parties

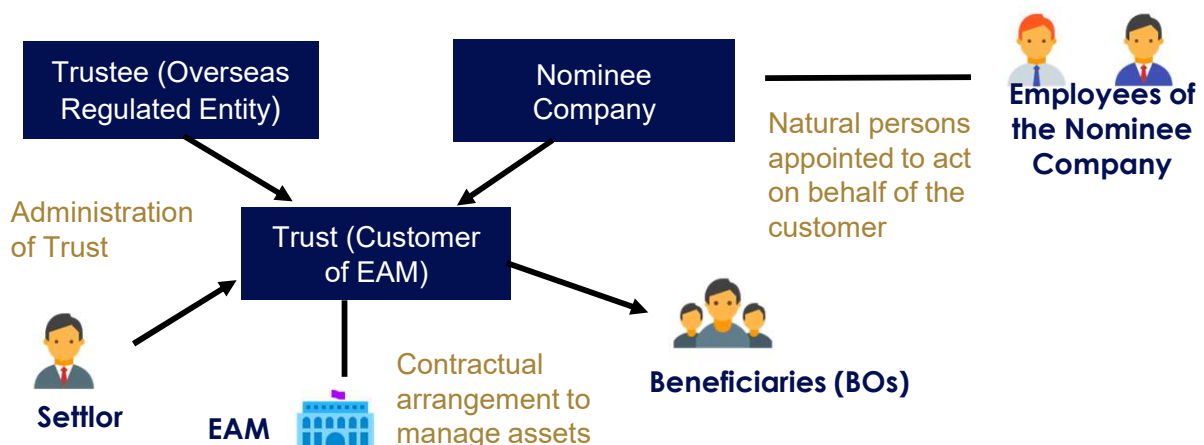
Case examples

a) Customers

- One EAM was appointed by certain trustees to be the investment manager for some investment-linked policies (ILPs) which were funded by trust assets managed by the trustees. The EAM erroneously identified the insurance company that issued the ILPs as the customer instead of the trustees, and did not accurately identify and/or verify the customer's relevant parties (e.g. the BO, natural person appointed to act on behalf of the customer).

b) BOs and natural persons appointed to act on behalf of the customer

- Some EAMs did not inquire on the BOs of customers with trust structures where the trustees were financial institutions set out in Appendix 1 or 2 of the SFA04-N02.

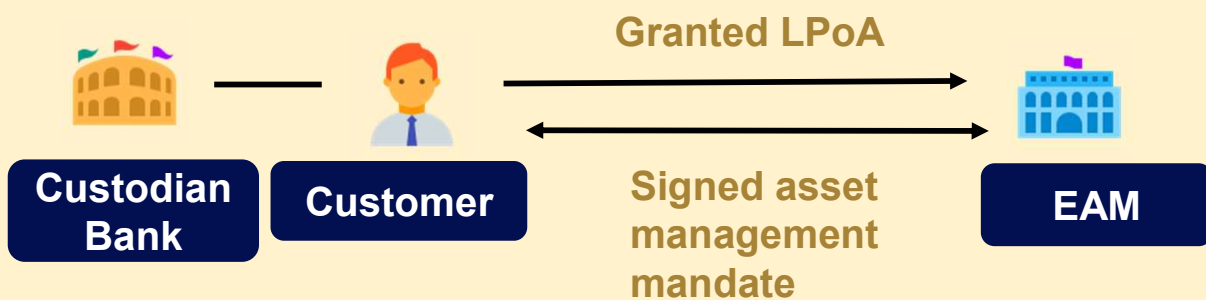


- In the above example, the EAM only obtained the names of the beneficiaries and did not verify their identities. It also did not identify, screen and verify the natural persons (including their due authority) who were appointed to act on behalf of the customer.

D. Customer Due Diligence – Onboarding of new customers

2. Lack of justification for deferring the completion of CDD measures

- EAMs would typically enter into an asset management mandate with a customer and be appointed by the customer via a LPoA to manage the assets of the customer placed with a custodian bank.



- The asset management mandate sets out the contractual agreement between the customer and the EAM for the latter to provide fund management services to the customer, regardless whether the assets are in existence yet.
- Business relations with the customer is established when the asset management mandate is signed between the EAM and the customer. The identity of the customer has to be verified before business relation is established.
- However, there were some EAMs which only verified the identification documents of a customer after they had signed the asset management mandate with the customer. They did not assess if the deferral of the completion of the verification was essential in order not to interrupt the normal conduct of business operations and whether ML/TF risks could be effectively managed (e.g. managing the customer's funds only after verifying the customer's identities).



D. Customer Due Diligence – Onboarding of new customers

3. Inadequacies in the screening process

a) Delay in screening

- Some EAMs were not familiar with the screening requirements for their customers and the relevant parties. As such, they did not screen them when, or as soon as reasonably practicable after, they had established business relations with the customers.



b) Lack of controls in the screening process

- There were also some EAMs who did not put in place adequate controls over the review of screening results.
- For example, a staff of an EAM, who was responsible for screening and reviewing the screening results during onboarding, was able to dismiss any screening hits singly without any justifications or independent review by another party. This increases the risk of erroneous dismissal of screening hits.



c) Lack of documentation on screening results

- Some EAMs did not ensure that their assessment of the screening results were properly documented for screening hits. Furthermore, the reasons for the EAMs' decision to onboard or continue business relation with the customer where there was a positive screening hit were also not properly documented.



D. Customer Due Diligence – Onboarding of new customers

Key takeaways

EAMs should:

1

Ensure that customers and all relevant parties of the customers are properly identified.

2

Ensure that the verification of the identities of the customers and their relevant parties is completed before establishing business relations with the customers.



In the event that an EAM allows for business relations to be established prior to completing the verification of the identities of the customers and their relevant parties, it should justify why the deferral is essential, and demonstrate it can effectively mitigate the resultant ML/TF risks. The completion of the outstanding verification should not exceed 30 business days after the establishment of business relations.

3

Ensure that screening is performed on all customers and their relevant parties when, or as soon as reasonably practicable after, they establish business relations with the customers.



In addition, the rationale for dismissing screening hits should be adequately documented, and the dismissal of screening hits should be subjected to effective independent checks and balances, such as maker-checker controls and regular independent quality assurance reviews. Guidance should be provided on what would be deemed as false or positive hit, to facilitate consistent implementation.

D. Customer Due Diligence – Transaction Monitoring

Effective transaction monitoring enables EAMs to detect and report suspicious, complex, unusually large, or unusual patterns of transactions or transactions that are inconsistent with the EAM's knowledge of the customer, its business and risk profile.

General practices that we observed

- Transaction monitoring was performed manually by the Compliance function and largely on an individual account basis for most EAMs.

Example of better CDD practices for transaction monitoring

- Some EAMs clearly informed their customers that the accounts under the EAMs' discretionary management should be used solely for investment purposes. All the investments in the accounts should be initiated by the EAMs and not the customers. The customers were also told specifically that they should not use the investment management accounts for other purposes (e.g. personal non-investment related transactions) and this was also monitored for adherence on an on-going basis by the EAMs.

D. Customer Due Diligence – Transaction Monitoring



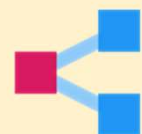
Areas of weaknesses that we observed

1. Inadequacies in the design of transaction monitoring framework



- Some EAMs' transaction monitoring was limited to reconciling its trading records against the custodian bank's records on a monthly basis.
- Some EAMs did not establish any parameters, thresholds and/or tailor the frequency of review to different customer risk profiles to identify suspicious, complex, unusually large or unusual patterns of transactions in their customers' accounts on an ongoing basis.
- Most EAMs did not monitor transactions across multiple managed accounts belonging to the same customer(s)/BO(s).
- Most EAMs also did not have any requirements to query their customers on the transfer of funds into and out of the managed accounts on an ongoing basis even if the amounts involved were significant and/or involved third parties.

2. Failure to pick up suspicious transactions across multiple managed accounts belonging to the same BOs



- An EAM failed to detect and/or properly review a series of third party transfers that were alternating between two separate managed accounts that belonged to the same BOs over 2 years. Although both accounts were for investment management purposes, there were no investments made in one of the accounts. This anomaly was also highlighted by the custodian bank. The source of the transfers were also not in line with the customers/BOs' declared source of wealth (SOW) and source of funds (SOF). However, the matter was not escalated to determine if suspicious transaction reports should be filed and whether the business relation with the customers should be maintained.

D. Customer Due Diligence – Transaction Monitoring

3. Failure to pick up suspicious transactions involving interconnected managed accounts



- There were multiple deposits and trades in a single stock within a period of a few months by a group of customers of an EAM. The EAM:
 - Did not investigate further and escalate internally even though the total amounts deposited were not in line with the EAM's knowledge of the customers' background, net worth and income level.
 - Failed to pick up anomalies in the trades executed despite (i) signs that the customers could be connected to the company whose stock they had traded in, and (ii) the custodian bank raising potential irregularities concerning the trades to the EAM.

4. Failure to follow up on anomalies concerning personal transactions in investment management accounts



- A customer of one EAM used the funds in an account that was to be independently managed by the EAM to purchase some antique books from brokers that were not in the business of dealing in antique books. However, the EAM did not enquire further or follow up on the anomalies noted and escalate internally.

D. Customer Due Diligence – Transaction Monitoring

Key takeaways

EAMs should:

1



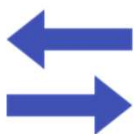
Put in place a proper transaction monitoring framework, including risk-based parameters and thresholds, to promptly detect and report suspicious, complex, unusually large, inconsistent or unusual patterns of transactions. Regular review of the parameters and thresholds should also be performed to ensure that they remain relevant and appropriate to the EAMs' operations and context.

2



Review transactions holistically across multiple managed accounts belonging to the same BOs or group of interconnected managed accounts, as the transactions could be structured to avoid detection.

3




Scrutinise all transactions i.e. inflows and outflows through the customers' managed accounts. Also pay special attention to those involving third parties, flagged by custodian banks for potential issues and/or are complex, large or exhibit unusual patterns to ensure that they are consistent with the EAM's knowledge of the customer/BO, its business, risk profile, SOW and SOF.

D. Customer Due Diligence – Periodic Review

Apart from having an effective CDD process at onboarding, periodic review of business relations is also important to ensure CDD data, documents and information are relevant and up-to-date. Such reviews will also help EAMs to identify changes to the customers' circumstances, both personally and professionally, which could affect their risk profiles.


General practices that we observed

- The risk rating of a customer would determine the review frequency. Customers with higher ML/TF risks were subjected to more frequent reviews, at least annually. Most of the EAMs kept to their stipulated review frequency. 
- Periodic reviews were documented and generally performed by Compliance, with inputs from relationship managers. In assessing if there was a change in the customer's ML/TF risk profile, EAMs usually considered whether there were any changes to the CDD data and information that was previously provided and the latest screening results of the customer and the relevant parties.
- Senior Management would approve the reviews of higher ML/TF risk customers and/or those whose risk ratings were notched up or down to/from a higher ML/TF risk category.



Areas of weaknesses that we observed




1. Lack of assessment in retaining customers suspected to be connected with ML/TF

- Arising from its on-going screening checks, an EAM noted that a customer was alleged to be involved in bribery payments. 
- The allegation raised reasonable grounds for suspicion that the customer could be connected with ML. However, the EAM did not substantiate and document the reasons for retaining the customer despite the adverse information.

D. Customer Due Diligence – Periodic Reviews

2. Ineffective execution of ongoing measures to detect and manage heightened ML/TF risks

An EAM had put in place measures to monitor its business relations with its customers on an ongoing basis. However, the measures were not rigorous nor implemented effectively.

<u>Measures put in place</u>	<u>Observations</u>
<p>Regular reviews with customers where the frequency is determined by their ML/TF risk profiles).</p> 	<p>Reviews focused on changes to the customers' investment portfolios (including performance) and objectives. Other developments, such as changes to the customers' circumstances (e.g. financial or professional status), adverse information flagged from screening checks, and changes in the nature, size and frequency of transactions noted in the customers' accounts, were generally not covered.</p>
<p>Annual validity checks on (i) identification documents / passports of individual customers, and (ii) register of members and directors of corporate customers.</p>	<p>Other existing CDD data, documents and information (e.g. residential address) used to identify customers and their relevant parties were not reviewed.</p> 
<p>Reviews for "High" risk customers required senior management's sign-off.</p> 	<p>There were instances where reviews of "High" risk customers were either omitted, submitted late without reasons or not signed off by senior management as required.</p>

D. Customer Due Diligence – Periodic Reviews

Key takeaways

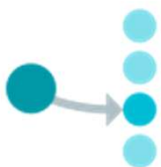
EAMs should:

1



Perform a robust assessment on the risk mitigation measures (e.g. exit the business relation, filing of STR) that should be taken, where there are reasonable grounds for suspicion that existing business relations with the customers are connected with ML/TF. Should the customer be retained, the reasons for doing so should be properly substantiated, documented and approved by board and senior management.

2



Ensure that the periodic reviews focus on and holistically consider all relevant ML/TF risk areas.

Examples of relevant ML/TF risk areas include; (i) changes in existing customers' CDD data, documents and information, (ii) outcomes of screening checks, and (iii) results of transaction monitoring.

Ascertain whether CDD measures imposed continue to be commensurate with the customers' updated risk profiles.

E. Enhanced CDD

EAMs should perform enhanced CDD measures on all customers who are identified to be of higher ML/TF risks. Such measures include (i) seeking approval from senior management to establish or continue business relations with the customer, (ii) establishing, by appropriate and reasonable means, the SOW and SOF of the customer and its BOs, and (iii) conducting enhanced monitoring of business relations during the course of business relations. These measures would facilitate informed decisions by senior management on whether to maintain or exit business relations with these customers.

General practice that we observed

- EAMs generally had a framework in place to subject customers with higher ML/TF risks, including PEPs, to enhanced CDD measures.



Areas of weaknesses that we observed

1. Failure to promptly identify and conduct enhanced monitoring on higher risk customers

- An EAM did not classify a customer as “High risk” when adverse information concerning the customer was first brought to the EAM’s attention.
- The same adverse information was subsequently made known to Compliance some time later. While the customer’s risk rating was elevated to “High” then, the customer was further omitted from enhanced monitoring due to Compliance’s oversight for a period of time.



E. Enhanced CDD

2. Lack of corroboration of customers' SOW and SOF

Some EAMs either relied on (i) customers' representations and did not obtain any documentation or information to independently corroborate their SOW and SOF; or (ii) obtained documents or information which failed to substantiate the customers' declared SOW and SOF.

Case examples

a) Lack of supporting documents and use of arbitrary assumptions



- A higher ML/TF risk customer had attributed his SOW and SOF to his employment income, investments and rental income.
 - Supporting documents were not obtained to substantiate the customer's representations. Information about the nature and composition of the customer's investments were also not requested.
 - Several assumptions concerning the customer's savings and the investments' annual rate of return were made without adequate basis.
- A customer's risk profile was raised to "High" risk due to several red flags noted as part of ongoing monitoring of its transactions and activities.
 - Supporting documents to substantiate the BOs' SOW and SOF, which were purported to be from their business, were not obtained. The EAM had instead made certain assumptions concerning the business' net profit margin.
 - Discrepancy between the declared duration of the BOs' business and the period reflected in public documents was not detected and followed up on.

E. Enhanced CDD

2. Lack of corroboration of customers' SOW and SOF

Case examples

b) Insufficient documentation to substantiate SOW and SOF



- A corporate customer was rated “High” risk. The BO’s SOW and SOF were from the BO’s deceased spouse.
 - While the EAM was informed that the wealth of the BO’s spouse was derived from the spouse’s business, it did not obtain any documentary evidence to corroborate the inheritance.
 - Subsequent documentation obtained by the EAM following MAS’ queries could only verify a fraction of the amount declared.
- A “High” risk customer, who was a senior executive of a foreign SOE, had other businesses which contributed significantly to his wealth.
 - While public searches were conducted to confirm the customer’s employment, his income was not corroborated against independent documentary evidence or public information sources.
 - An audit firm was appointed to perform agreed-upon procedures (AUP) to establish the customer’s SOW from his other businesses. However, the customer was on-boarded prior to the submission of the draft AUP report, and there were also quite a few anomalies concerning the information presented in the AUP report that were not questioned or followed up on.

E. Enhanced CDD

Key takeaways

EAMs should:

1

Ensure that customers/BOs posing higher ML/TF risks are promptly identified and subjected to enhanced CDD measures, including enhanced monitoring.



2

Perform adequate independent verification of customer/BO's SOW and SOF to assess the legitimacy of the funds/assets managed.



Assess whether the measures taken to obtain and corroborate the information represented by the customer/BO are sufficient and reasonable, and maintain proper documentation.

F. Suspicious Transactions Reporting

EAMs are required to file STRs with the Suspicious Transaction Reporting Office (STRO) in a timely manner (i.e. within 15 working days of the case being flagged as suspicious) whenever there are transactions suspected of being connected with ML/TF.

General practices that we observed

- In ascertaining whether the transactions were considered to be suspicious, EAMs generally considered and referred to Appendix B of the Guidelines to SFA04-N02, such as:
 - (i) Customers failing to reasonably justify the purpose of a transaction when queried;
 - (ii) Transactions noted were not consistent with the usual activities of the customer; and
 - (iii) Inability of the EAM to independently determine/verify the SOF of a customer/BO.



- Most EAMs had established escalation procedures, where suspicious transactions were brought to the attention of senior management, who would then decide on whether a STR should be filed or not.
- Once EAMs had a suspicion that a customer or a transaction was related to ML/TF, appropriate actions would be taken to mitigate the risk of the EAMs being used as conduits for ML/TF activities. Besides filing an STR, EAMs would review the business relations and risk classification of the customer, request for additional documents to independently verify the SOW/SOF and/or transaction to assess if the customer should be retained.

F. Suspicious Transactions Reporting



Areas of weaknesses that we observed

1. Lack of awareness to file STRs on customers with adverse information or conduct that suggested linkage to financial crime

Case examples

- STRs were not filed despite some EAMs having knowledge of the following:
 - Customers / BOs of corporate customers had participated in TAPs.
 - A customer was involved in ongoing legal proceedings for a money laundering case.
 - Multiple large deposits by a group of interconnected customers into their respective managed accounts, which were not consistent with the EAM's knowledge of their SOW and SOF.
 - The custodian bank involved in servicing the same customer had raised concerns about the legitimacy of the customer's funds to the EAM.



Key takeaways

EAMs should file an STR on a customer as long as they know or have reasonable grounds to suspect any property of the customer could be connected to ML/TF.

G. Conclusion

- EAMs are inherently vulnerable to ML/TF risks given the nature of their business model where they provide asset management services to high net worth customers. Hence, it is important that EAMs remain vigilant to ML/TF risks at every stage of the customer's lifecycle.
- Board and senior management play a key role in establishing an appropriate risk culture and putting in place necessary frameworks and controls to promote the right conduct among their staff.
- In addition, EAMs should ensure that their staff are equipped with the necessary knowledge, skills and resources to implement the AML/CFT frameworks and controls effectively to prevent the EAMs from being used by criminals for ML/TF purposes.
- MAS' thematic inspections and engagements of EAMs showed that there was room for EAMs to improve the design and effectiveness of their AML/CFT frameworks and controls to detect and mitigate ML/TF risks. Significant deficiencies were confined to a few EAMs.
- EAMs should continuously enhance their AML/CFT frameworks and controls to ensure they are commensurate with the scale, nature and complexity of their business.
- MAS will continue to provide guidance and share our supervisory expectations and observations from our inspections and engagements to improve industry practices³.



³ EAMs may also refer to past papers on AML/CFT related issues published by MAS for the list of observations noted in the inspections of other MAS regulated entities and MAS' supervisory expectation on these observations.

The relevant publications include the following (non-exhaustive):

- Use of MyInfo and Customer Due Diligence (CDD) Measures for Non Face-to-Face Business Relations published in January 2018;
- Guidance for Effective AML/CFT Transaction Monitoring Controls published in September 2018;
- Guidance to Capital Markets Intermediaries (CMIs) on Enhancing AML/CFT Frameworks and Controls published in January 2019;
- Strengthening CMIs' Oversight over AML/CFT Outsourcing Arrangement published in July 2020;
- Enhancing Robustness of EWRA on ML/TF published in August 2020;
- Effective AML/CFT Controls in Private Banking published in September 2020;
- Non Face-to-Face CDD Measures published in February 2022; and
- Strengthening AML/CFT Name Screening Practices published in April 2022