

AML/CFT RISK BASED MANAGEMENT GUIDELINE

- **Establishment of risk-based management system of reporting organizations licensed by the Securities Exchange Law to combat money laundering and financing of terrorism**
- **Obligation to report suspicious transactions to SECM and FIU**
(AML Law Chapter 8, AML Rule Chapter 8, AML Order (45/2019), Instruction (3/2016), Instruction (1/2019))
- **This Guideline will be effective on 23rd December 2019.**

BASIC PRINCIPLES

- The government has implemented and published its National Risk Assessment (NRA) on money laundering and financing of terrorism. Based on the assessment, all reporting organizations are required to identify, assess and take effective action to mitigate their respective money laundering and terrorist financing risks, applying a risk-based approach.
- Reporting organization licensed under the Securities Exchange Law shall establish their risk-based management system taking into consideration the characteristics and situation of securities business and related services, following all the relevant laws and regulations.

CHECK POINT 1: RISK IDENTIFICATION

Risk identification is a process to identify ML/FT risks faced by a reporting organization through comprehensive and specific risk evaluation of the products and services offered, transaction types, the countries and geographic areas of transactions, customer attributes, and other relevant factors, and is the starting point of a risk-based approach. The SECM expects SECM-licensed institutions to properly conduct risk identification especially the followings:

- Identify the ML/FT risks it faces by evaluating risks of customer attributes, products and services offered, transactions types, the countries and geographic areas of transactions, and other relevant factors.
- When conducting a comprehensive and specific evaluation, consider the results of the national risk assessment, at the same time taking into account the reporting organization's specific features or business environment.
- When handling new products and services, or conducting transactions using new technologies or those with new characteristics, analyze and evaluate their ML/FT risks before offering such products and services.
- Coordinate and cooperate with all relevant divisions, under the proactive involvement of

management.

CHECK POINT 2: RISK ASSESSMENT

Risk assessment is the base for the risk-based management which assesses impacts of respective risks identified in the risk identification process and reflect respective business environment and strategy. The SECM expects SECM-licensed institutions to properly conduct risk assessment especially the followings:

- Establish firm-wide policies and specific approaches for risk assessment, and in line with such policies and approaches conduct the assessment based on the specific and objective grounds.
- Document the results of the risk assessment and utilize them for developing measures necessary for risk mitigation.
- Conduct the review of the risk assessment regularly at least once a year, as well as when an event such as the occurrence of new risks and the introduction of new regulation that may have a significant impact on AML/CFT measures occurs, and be readily available to the SECM.
- Involve management in the processes of risk assessment and obtain approval from management for the results of the risk assessment.

CHECK POINT 3: RISK MONITORING AND MITIGATION

Under a risk-based approach, reporting organizations required to collect and verify information about specific customers' profiles and activities, compare the information with the results of risk assessment conducted in accordance with aforementioned 1) and 2), determine and implement effective measures to mitigate those identified risk. The SECM expects SECM-licensed institutions to conduct appropriate customer due diligence measures based on their respective risk assessment as required by AML Law Chapter 8, AML Rule Chapter 8, AML Order (45/2019), Instruction (3/2016), Instruction (1/2019). Especially,

- Formulate a customer acceptance policy, based on the risk identification and assessment, to systematically and specifically identify and determine high-risk customers and transactions as well as timing and situation when due diligence measure and other actions are taken.

**Among other relevant considerations prescribed in related regulations, enhanced or simplified CDD shall be conducted before a transaction for a new customer if the transaction is equal to or above the threshold amount of USD 15000 or equivalent amount in any currency or as from time to time defined by the Central Body, whether conducted as a single transaction or several connected transactions. Other examples of suspicious indicators are provided below.*

- Conduct due diligence measures when the risk of money laundering and terrorist financing is identified as high risk of money laundering as a result of the risk assessment, conducting enhanced customer due diligence measures consistent with the identified risk, and determining whether or not the transactions or other activities are unusual or suspicious.
- Conduct simplified due diligence measures consistent with the level of risk, if the customer is identified as low risk according to the risk assessment of money laundering or terrorist financing.
- Terminate simplified due diligence measures on the customer if the customer is suspected of money laundering or terrorist financing, or identified as high risk.
- Conduct customer due diligence on beneficial owners, and domestic or foreign politically exposed person or international politically exposed person, and their family members and closed associates and take reasonable measures to verify the identity of such persons.
- Submit promptly suspicious transaction reports to the FIU and SECM if it suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing as a results of its CDD.
- Maintain the following records:
 - (a) Copies of all records obtained through the customer due diligence process;
 - (b) Including documents evidencing the identities of customers and beneficial owners, records and business correspondence, for at least five years after the business relationship has ended;
 - (c) copies of reports sent and related documents for at least five years after the date the reports were made.

CHECK POINT 4: AML/CFT PROGRAM

In order to ensure the effectiveness of AML/CFT measures, reporting organizations are required to establish an effective ML/FT risk management by adopting, developing and implementing internal programs, policies, procedures and controls for the implementation of the provisions in the relevant laws and regulation with the involvement of management. Furthermore, reporting organization are required to monitor the implementation of such policies and controls and enhance them, if necessary. The SECM expects SECM-licensed institutions to properly establish effective AML/CFT program following the relevant laws and regulation. Especially,

- Establish internal program, policies, procedures and controls which includes concrete and clear procedures for all employees to implement risk identification, assessment, monitoring and mitigation processes. These can be prepared and implemented individually or separately.
- Review the implementation of such policies and controls and enhance them, if necessary.

- Have an independent audit function to check in compliance with and effectiveness of the measures taken action in execution of the related laws and regulations.
- Establish procedures to ensure high standard of integrity of its employees and a system to evaluate the personal, employment and financial history of these employees. It needs to include proper remedial and administrative actions applicable for the employees who violate the internal policies as well as the relevant laws and regulations.
- Regular training programs for employees to assist with regard to know-your-customer, specific responsibilities of AML/CFT including reporting STRs.

CHECK POINT 5: MANAGEMENT INVOLVEMENT

The level of ML/FT risks faced by a reporting organization varies according to the way it operates based on its business strategy. Therefore, ML/FT risks must be assessed in the context of the organization's business strategy, as part of the processes of evaluating and reviewing risk appetite and resource allocation policy. Reporting organizations are required to establish effective risk-based management framework and keep it up-to-date. In order to establish such firm-wide risk management, a robust governance structure must be built, with the understanding and active involvement of management, including the appointment of an senior management with the responsibility and authority to implement AML/CFT measures, and clear definition of the roles and responsibilities of each division and employees. The SECM expects SECM-licensed institutions to properly establish sufficient management engagement on effective AML/CFT framework. Especially,

- Allocate adequate resources such as personnel with expertise and the sufficient budget to the division responsible for AML/CFT according to organizations' risk identification and assessment.
- Designate a compliance officer at the senior level, who has powers to access any documents, records, registers and accounts necessary for the performance of his tasks, and to request and access any information, notice, explanation or document from any employee of the reporting organization.
- Report the personal data including the name, qualifications, address, contact phone number and e-mail address of the compliance officer to the FIU and the SECM and immediately inform to the FIU and SECM if there is any changes of the compliance officer.
- Ensure that the compliance officer is asked for prior approval on important decisions regarding AML/CFT such as establishing or continuing a business relationship with politically exposed persons.
- The compliance officer shall submit regular reports to the board and SECM at least once a

year, including following facts:

- (a) identified suspicious transactions and participation thereto;
 - (b) performance of staff of compliance group and results of inspection of account independently in the system of money laundering and counter financing of terrorism in order to policies, procedures, system and controls of the anti-money laundering and counter financing of terrorism of their reporting organizations be strong;
 - (c) results of onsite inspection of the FIU and the SECM;
 - (d) performances to mitigate disadvantage in implementing by their reporting organizations.
- Ensure that management participates or is otherwise proactively involved in AML/CFT training for management and employees.

**Examples of suspicious indicators in relation to securities business,
which may trigger filing of STRs and/or require additional CDD measures**

- (1) Cash transaction or large transaction
 - Request to accept cash
 - 10 million kyats or above transaction
- (2) Suspicious Behaviour/Demeanour
 - Customer for whom verification of identity proves unusually difficult and who is reluctant to provide details
 - Same phone number or address with other accountholders
 - Fund transfer from unregistered bank accounts
 - Access from unusual or foreign IP address
- (3) Unusual large transaction
 - Transactions incompatible with customer's financial standing
 - Customer showing unusual concern of secrecy
- (4) Complex or unusual patterns of transaction
 - Sudden use of dormant accounts
 - Transaction which it is difficult to understand
- (5) Business relationship or transaction with foreign entities
 - Any relationship or transaction with a person or institution from or in a country which does not apply sufficient measures for AML/CFT

(Note1) This is not an exhaustive list; each element may not be relevant for all.

(Note2) Please refer to the "GUIDANCE FOR A RISK-BASED APPROACH: SECURITIES SECTOR" prepared by FATF, October 2018.

END