**FINANCIAL INTELLIGENCE UNIT**
**AUTORITI MONETARI BRUNEI DARUSSALAM**

# GUIDANCE PAPER TO FINANCIAL INSTITUTIONS ON ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM (AML/CFT) TRANSACTION MONITORING PROGRAMME

## INTRODUCTION

i. Financial institutions (FIs) are required under Section 12, Criminal Asset Recovery Order, 2012 (CARO) to conduct special monitoring on certain business relations and transactions. As such, FIs are required to have in place controls and processes to ensure that anti-money laundering and combating the financing of terrorism (AML/CFT) transaction monitoring is conducted effectively, as effective AML/CFT transaction monitoring is a crucial component of FI's AML/CFT Programme.

ii. Effective AML/CFT transaction monitoring enables FIs to detect and investigate money laundering and terrorism financing (ML/TF), and could help strengthen FIs' internal controls and risks mitigation measures for ML/TF. Failure to conduct effective AML/CFT transaction monitoring could expose FIs to increased risks and vulnerabilities deriving from ML/TF and the associate predicate offences.

iii. Part 4(h) of the General Guidance Paper to Financial Institutions and Designated Non-Financial Businesses and Professions on Anti-Money Laundering and Combating the Financing of Terrorism (General Guidance Paper) sets out the expectation for FIs to have in place an adequate transaction monitoring system (TMS) that:

1. Enables the detection and assessment of customers that may be or appear unusual or suspicious;

2. Facilitate FIs with a holistic view of customers' profiles, past transactions and behavioural patterns that are accurate and updated; and

3. Commensurate with the size, complexity and risk exposure of the FIs.

iv. FIs are expected to adopt an AML/CFT transaction monitoring programme that operates on a risk-based approach and is best suited to the business model, size, complexity and risk exposure of their respective institutions, as there is no one-size-fits-all AML/CFT transaction monitoring programme.

v. Risk assessments and justifications for the AML/CFT transaction monitoring programme adopted should be conducted and documented in writing, and provided to the Autoriti Monetari Brunei Darussalam (the Authority) when requested.

vi. This Guidance Paper is to provide clarification and guidance to FIs when developing and implementing their AML/CFT transaction monitoring programme, in line with the requirements of Part II of CARO.

vii. This Guidance Paper does not contain any new requirements.

viii. The key expectations of the Authority for an effective AML/CFT transaction monitoring programme are set out in Sections 1 to 5 of this Guidance Paper as follows:

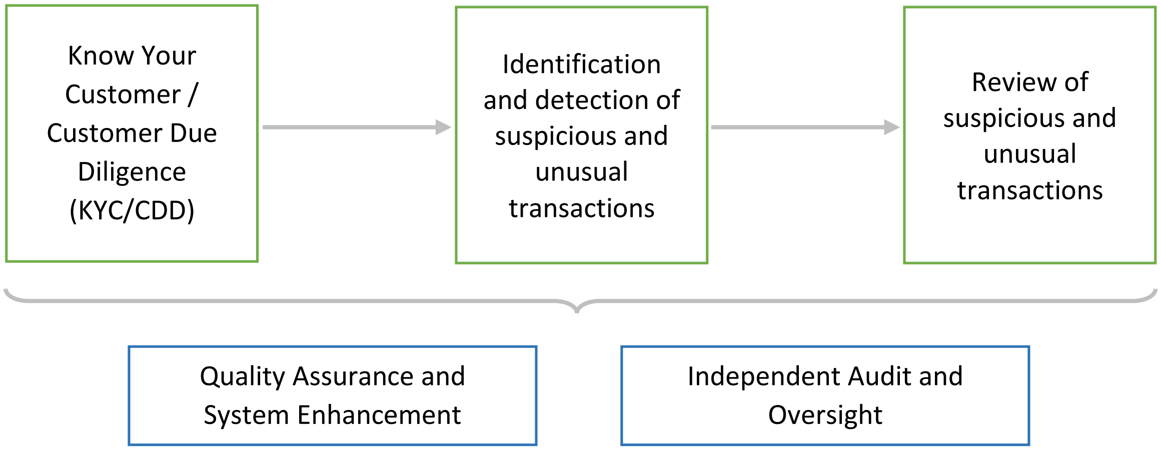
1. Sound understanding of customers and their risk profiles;

2. Effective detection of suspicious and unusual transactions;

3. Reviews and investigations of alerts generated by the TMS;

4. Quality assurance and system enhancement; and

5. Independent audit and effective oversight.


Know Your Customer / Customer Due Diligence (KYC/CDD)
Identification and detection of suspicious and unusual transactions
Review of suspicious and unusual transactions
Quality Assurance and System Enhancement
Independent Audit and Oversight

ix. This Guidance Paper should be read in conjunction with the following:

1. General Guidance Paper to Financial Institutions and Designated Non-Financial Businesses and Professions on Anti-Money Laundering and Combating the Financing of Terrorism;

2. Obligation to Submit a Suspicious Transaction Report (STR) under Section 15 of CARO and Section 47 of the Anti-Terrorism Order, 2011; and

3. Obligations under the Anti-Terrorism (Terrorist Financing) Regulations, 2013.

# Table of Contents

## 1. KNOW YOUR CUSTOMER / CUSTOMER DUE DILIGENCE (KYC/CDD)

1.1. The prerequisite for an effective AML/CFT transaction monitoring programme is FIs' sound understanding of their customers and the risks faced by the institutions, including risks derived from the products and services. Prior to the establishment of a business relationship, FIs are required under Sections 5 to 8, CARO to perform due diligence checks on their customers.

1.2. KYC/CDD procedures must be completed during on-boarding or any establishment of new business relationships. As part of establishing the basis of customers' known profiles or behaviours, FIs, at minimum, are expected to:

1.2.1. Understand the background and purpose of the customers' business relations with the FIs;

1.2.2. Establish customers' source of funds and source of wealth for customers and beneficial owners identified as politically exposed persons (PEPs); and

1.2.3. Establish the types and volumes of transactions expected.

1.3. FIs are responsible to ensure that the customer information obtained is complete, accurate and updated, particularly on high risk customers and PEPs.

1.4. FIs are expected to categorise customers according to ML/TF risks, as it would:

1.4.1. Increase FIs' ability to identify the discrepancies between known customer profiles and abnormalities in the transaction patterns; and

1.4.2. Enable AML/CFT transaction monitoring to be conducted on a risk-based approach, whereby resources are allocated efficiently and further scrutiny or enhanced monitoring is conducted on higher risk customers and transactions.

## 2. IDENTIFICATION AND DETECTION OF SUSPICIOUS AND UNUSUAL TRANSACTIONS

### A. BASIC CONTROLS OF AML/CFT TRANSACTION MONITORING

2.1. The purpose of AML/CFT transaction monitoring is to detect potentially suspicious and unusual transactions in a timely manner to ensure that suspicious transaction reports (STRs) are promptly submitted to the Financial Intelligence Unit, once suspicion of ML/TF is confirmed.

2.2. AML/CFT transaction monitoring, at minimum, must be able to:

2.2.1. Process and take into account the different customers, transactions, products and services offered;

2.2.2. Review customer information against past transaction patterns and red flag indicators;

2.2.3. Have access to the relevant customer and transaction information; and

2.2.4. Generate alerts for unusual and suspicious transactions.

2.3. More complex FIs with higher ML/TF risks and large volumes and variances of transactions, such as banks and remittance businesses, are expected to adopt automated TMS that is capable of automatically identifying, detecting and flagging up suspicious and unusual transactions.

2.4. Meanwhile, less complex FIs with lower ML/TF risks may rely on TMS that are less automated in the detection and flagging up of suspicious and unusual transactions, provided that:

2.4.1. The less automated TMS is able to fulfil items in Section 2.2.1 to 2.2.3 above;

2.4.2. Reviews of suspicious and unusual transactions are conducted on a regular basis; and

2.4.3. Adequate justifications and supporting documents are available in writing to support the adoption of a less automated TMS.

2.5. FIs have the option to adopt the TMS of their parent institutions. However, diligence must be taken to ensure that the TMS is able to take into account the different customer profiles, products and services offered by the subsidiaries.

## B. AUTOMATED TRANSACTION MONITORING

2.6. FIs utilising automated TMS are expected to:

2.6.1. Ensure that the automated TMS adopted takes into account the business model, size, complexity and risk exposure of the respective institutions, including the different customer segmentations and products and services offered;

2.6.2. Incorporate appropriate parameters and red flag indicators as part of the automated TMS; and

2.6.3. Conduct periodic assessments, reviews and fine tunings to ensure the effectiveness and relevance of these parameters and red flag indicators adopted, taking into account the current trends and typologies.

FIs may refer to a list of red flag indicators provided in Annex 1 of the Guidance Paper to Financial Institutions for The Obligation to Submit a Suspicious Transaction Report (STR) Under Section 15 Of Criminal Asset Recovery Order and Section 47 Of Anti-Terrorism Order.

2.7. The parameters adopted should be able to, at minimum:

2.7.1. Identify all complex, unusual large transactions and all unusual patterns of transactions which have no apparent economic or visible lawful purpose;

2.7.2. Identify transactions of persons, including legal persons and arrangements, from or in countries with weak AML/CFT regimes;

2.7.3. Identify potentially suspicious or unusual transactions, including transactions aggregated from frequent and/or smaller transactions (structuring) and transactions involving high risk individuals and entities and off-shore accounts;

2.7.4. Identify transactions that deviate from known customer profiles and transaction behaviours, as well as hidden relationships between customers or accounts through fund flows;

2.7.5. Compare customer profiles and transaction histories against ML/TF red flag indicators and typologies and activities or behaviours consistent with ML/TF predicate offences;

2.7.6. Monitor abnormal activities involving the use of products and services of the FIs, including trade financing and early termination of loans and life insurance; and

2.7.7. Other abnormal and unexplained patterns or behaviours.

## 3. REVIEW OF SUSPICIOUS AND UNUSUAL TRANSACTIONS

### A. ALERT HANDLING

3.1. Alerts generated during AML/CFT transaction monitoring must be reviewed and processed by FIs' compliance function. The handling of alerts should allow for a holistic assessment of the triggered transactions, taking into account the customer profiles and past transaction histories.

3.2. Such review, including the decision making processes and actions taken, should be documented in writing to demonstrate that diligence has been conducted in a timely manner on the alerts generated and justifications are provided before closing the alerts.

3.3. Findings from the review of alerts should be periodically used to update both the customer and institutional risk profiles to enhance the capabilities of the TMS, as well as used for staff training to enhance the investigation skills of the compliance function.

3.4. FIs should ensure that the staff tasked with reviewing the alerts generated have:

3.4.1. The appropriate skills, knowledge and expertise;

3.4.2. Undergone adequate AML/CFT trainings to perform their functions and responsibilities effectively; and

3.4.3. Ongoing training to ensure that they are well aware of current ML/TF risks and the associated predicated offences.

3.5. FIs are expected to have in place written policies and procedures for the AML/CFT transaction monitoring programme implemented. Such policies and procedures must be kept updated and should not delay the filing of STRs to the Financial Intelligence Unit.

### B. TIPPING OFF

3.6. Tipping off may occur when FIs collect further information from customers who have conducted suspicious transactions as part of their ongoing internal investigations. FIs are reminded to conduct such internal investigations discreetly.

3.7. FIs should ensure that internal policies and controls are put in place to prevent any staff from tipping off customers or any other persons subjected to ongoing investigations by law enforcement agencies or whom STRs have been filed on.

## C. DATA CONFIDENTIALITY

3.8. As part of protecting the data confidentiality of the TMS, FIs should ensure that:

3.8.1. The level of access to information in the TMS is commensurate with the roles and responsibilities of the staff;

3.8.2. Periodic reviews are conducted to manage the level of access to information granted to authorised persons and to disable or remove access to those who no longer require such access; and

3.8.3. Measures are in place to safeguard the confidentiality of TMS data, as they contain customers' personal information and transaction details.

## 4. QUALITY ASSURANCE AND SYSTEM ENHANCEMENT

### A. QUALITY ASSURANCE

4.1. FIs are expected to conduct quality assurance (QA) checks on a periodic basis on a sample of alerts to:

4.1.1. Test the robustness and effectiveness of the identification and detection of suspicious transactions, parameters adopted, review and investigation of suspicious and unusual transactions, and associated policies and procedures;

4.1.2. Detect and remediate any systemic weaknesses; and

4.1.3. Improve the quality of investigation of alerts generated and STRs filed.

4.2. The sample size selected for QA checks should be commensurate with the business model, size, complexity and risk exposure of the FIs, as well as the volume and variances of transactions.

4.3. More complex FIs with higher ML/TF risks are expected to conduct a larger sampling size to ensure that any gaps are effectively detected and remediated.

4.4. The gaps and weaknesses identified through the QA checks are expected to be promptly remediated and documented in writing.

4.5. The QA checks could either be conducted:

4.5.1. By a staff of the FI who is not involved in the review of the alerts generated; or

4.5.2. As part of the independent audit of the AML/CFT transaction monitoring programme.

### B. SYSTEM ENHANCEMENTS

4.6. Periodic updates, fine tunings and database maintenance should be conducted on the automated TMS and parameters adopted to ensure they remain current and effective in detecting ML/TF and other financial crimes. These reviews are to identify and remediate deficiencies, resolve abnormally functioning parameters, and ensure stability and efficiency of the overall TMS.

4.7. FIs with newly implemented TMS are recommended to conduct frequent reviews and assessments, at least once annually, to ensure the new TMS is robust and effective, and commensurate with the business model, size, complexity and risk exposure of the FIs.

## 5. INDEPENDENT AUDIT AND OVERSIGHT

### A. INDEPENDENT AUDIT

5.1. FIs are recommended to assess the effectiveness of the AML/CFT transaction monitoring programme to identify gaps and areas for improvements.

5.2. An independent audit at minimum would assist to examine the following:

5.2.1. Effectiveness of the controls to identify and detect suspicious and unusual transactions;

5.2.2. Effectiveness of the automated TMS and parameters adopted to identify suspicious and unusual transactions;

5.2.3. Accuracy and consistency of the reviews of alerts generated and filing of STRs; and

5.2.4. Effectiveness of policies and procedures for the AML/CFT transaction monitoring programme;

5.2.5. Effectiveness of the governance and control framework of the AML/CFT transaction monitoring programme.

5.3. The audit arrangements could either be conducted internally or by an external auditor, so as long as the audit conducted is independent from the direct oversight of management and the compliance function involved with the AML/CFT transaction monitoring programme.

### B. OVERSIGHT

5.4. As per the Part 2(a) of the General Guidance Paper, the Board of a FI, or any equivalent governing officer or body of a branch of a foreign branch (any and all of which are referred to herein as the "Board") is expected to conduct oversight over the effective implementation and operation of the AML/CFT Programme, while the senior management is responsible for the implementation of the AML/CFT Programme. This includes the oversight on the adoption and implementation of an effective AML/CFT transaction monitoring programme.

5.5. Findings from the QA tests, system enhancements, independent audit and any reviews conducted on the effectiveness of the AML/CFT transaction monitoring programme should be escalated to the Board, with the intention of endorsing and maintaining oversight over the implementation of the remedial actions prescribed.

Date: 16 January 2020