



GUIDE TO STRUCTURING AN AML/CFT COMPLIANCE PROGRAMME FOR FINANCIAL INSTITUTIONS AND LISTED BUSINESSES

PURPOSE

The purpose of this guide is to assist Financial Institutions and Listed Businesses in developing a written anti-money laundering/counter financing of terrorism (AML/CFT) Compliance Programme which is to be submitted to the Financial Intelligence Unit of Trinidad and Tobago (the “FIU”) in accordance with Regulation 31 of the FIU Regulations, 2011.

This guide strives to explain the basics of the written AML/CFT Compliance Programme which the FIU will consider in determining whether to will approval. The guide does not necessarily represent all the requirements under Law or the obligations imposed by the other Supervisory Authorities. A financial institution supervised by the Central Bank (CBTT) or the Trinidad and Tobago Securities and Exchange Commission (TTSEC) should also consult with the respective Supervisory Authority.

INTRODUCTION

A Financial Institution (“FI”) and Listed Business (“LB”) must develop an AML/CFT Compliance Programme that is designed for its individual business. In developing its programme the FI and LB should weigh factors including its size, location, complexity of business activities, the types of accounts it maintains, and the types of transactions in which its customers engage. It should incorporate risk assessment of relationships, cover all business lines, products and services. The policies should reflect what the risk assessment identifies as the higher risk areas.

The written AML/CFT Compliance Programme must bear the signature/stamp/seal of approval of the senior management officials (directors/partners/owner of the business) and the date of approval.

This AML/CFT Compliance Programme must be reviewed annually, ideally incorporating benchmarking and best practice reviews in its approach to AML/CFT, and resubmitted to the FIU every two years.

THE WRITTEN COMPLIANCE PROGRAMME

The written AML/CFT Compliance Programme should have four key components: a system of internal compliance controls; a designated AML/CFT compliance officer; ongoing employee training; and an independent audit to test the system. It should be well structured so that the policies will be easy to apply in practice.

A well-structured AML/CFT Compliance Programme includes:

1. TABLE OF CONTENTS

- 2. A POLICY STATEMENT** which should include the purpose of the AML/CFT Compliance Programme and the FI's or LB's commitment to the Government of Trinidad and Tobago's initiatives in combating Money Laundering and the Financing of Terrorism. It should be explained that its purpose is to help its employees detect and prevent money laundering and terrorist financing as well as to ensure that suspicious activities and transactions can be identified and reported thereby protecting the business from being used for illegal purposes.

It should state which regulatory requirements the policies and procedures developed are designed to meet e.g. CBTT, TTSEC, Financial Obligations Regulations, 2010. The obligation that all employees are required to abide by them **must** be made explicit.

3. OVERVIEW OF MONEY LAUNDERING AND FINANCING OF TERRORISM CRIMES

Explain the crimes of Money Laundering and the Financing of Terrorism. Money Laundering is the attempt to conceal or disguise the nature, location, source, ownership, or control of illegally obtained money. The Financing of Terrorism is providing funds directly or indirectly intending or knowing that the funds are to be used to fund terrorist acts or organizations.

Explain that the laws namely the Proceeds of Crime Act (the "POCA"), the Anti-Terrorism Act (the "ATA"), the Financial Obligations Regulations, 2010, the FIU Act and the FIU Regulations, 2011 require certain businesses to file specific reports, maintain records on certain transactions to help prevent the Laundering of Money and the Financing of Terrorism and to obtain documentation that may be used to prosecute money launderers and those who commit terrorist acts or facilitate the commission of terrorist acts.

Clearly state that the FIU Regulations, 2011 require that the FI/LB (whichever is applicable) must register with the FIU and adopt a written AML/CFT Compliance Programme which is reasonably designed to ensure proper recordkeeping and reporting of certain transactions, and to prevent the FI/LB from being used to launder money or to finance terrorism. *This written AML/CFT Compliance Programme must be approved by the FIU and will bear its seal of approval.*

4. INTERNAL POLICIES, PROCEDURES AND CONTROLS WHICH DESCRIBES THE WHO, WHAT, WHY, WHEN AND HOW OF THE PROGRAMME.

This section communicates the policies, procedures and controls that employees are expected to follow to ensure that the FI or LB complies with its AML/ CFT obligations under the law.

The Internal Policies should:

Indicate in a clear statement the persons to whom the manual applies – i.e. all staff, all directors, and whether persons are required to sign a form that they understand their obligations and duties as contained therein. A sample form should be attached as an Appendix.

Identify the FI's or LB's responsibilities under the Law including the POCA and Anti-Terrorism Act and Regulations –the offences may be summarised in an Appendix.

Identify the types of risk and where the high risk activities lie in the Organisation.

Identify the Customer Due Diligence ("CDD") measures. Include customer identification documentation required, and how verification of customer information is to be carried out e.g. current utility bill, third party verification, etc.

Identify Due Diligence measures for Individuals, for companies, and Enhanced Due Diligence ("EDD") measures for non face to face customers, for Politically Exposed Persons ("PEPs") in case of foreigners, for non- residents and when business is obtained through introducers. Indicate whether copies of documentation are acceptable and whether they need to be certified and by whom. Include CDD details in accordance with Regulations 15-17 of the Financial Obligations Regulations, 2010. **Sample Identification forms listing the Identification data to be collected could be attached as an Appendix.**

Include the Monitoring of the business relationship measures which will identify unusual business transactions of the client.

Include Procedures to govern cash transactions. Is there a threshold? Include the compulsory requirements of due diligence on large transactions of \$TT90, 000 and over, wire transfers of \$TT 6,000 and over, and occasional transactions (structured/linked transactions). Is there a threshold for particular kind of payment method? State when a customer would be required to complete a Source of Funds Declaration (“SOFD”). The S O F D form could be attached as an Appendix.

Include the measures to be adopted for Due Diligence for cross border business.

Include the EDD measures to be adopted in respect of business transactions with persons and FIs from other countries which do not sufficiently comply with the recommendations of the Financial Action Task Force.

Clearly state the internal reporting procedures. The law requires the filing of a suspicious transaction/activity report (STR/SAR) with the FIU for any transaction or pattern of transactions that is attempted or conducted for ANY amount that you know or suspect or have reason to suspect:

- a. Involves funds derived from a specified offence or is intended to hide funds derived from a specified offence ;
- b. Is structured to avoid recordkeeping or reporting requirements;
- c. Has no business or apparent lawful purpose; or
- d. Facilitates criminal activity.

Indicate When and How a suspicious transaction or activity will be reported to the Compliance Officer (the “CO”). A sample form for Employees to make the suspicious report to the CO may be attached as an Appendix.

Include a notification to all Employees that it is illegal to tell a customer that they are filing a STR/SAR. (Avoid “tipping-off “). ‘Tipping-Off’ should be clearly explained and behaviour that would constitute Tipping –Off should be illustrated.

Include a caution that Employees must not reveal the identity of the CO; his/her identity must be held in strict confidence.

An Appendix illustrating examples of suspicious activities or transactions that are industry specific may also be included.

5. DESIGNATION OF A COMPLIANCE OFFICER

Identify the level at which the designated CO (and if necessary the substitute CO) is in the Organization, (the CO should be at a responsible level, preferably at management level). It is not necessary to state CO's name in the written AML/CFT Compliance Programme. The CO's and the substitute CO's identities and contact details **must** be provided to the FIU under separate cover.

State the responsibilities of the CO. The CO is responsible for the day-to-day compliance with the AML/CFT's Laws and Regulations such as the Submission of STRs/SARs to the FIU.

Include the CO's reporting obligations and specifically the following:

- that the STR/SAR should be in the form as prescribed in the Third Schedule of POCA (You may include a copy of the form as an Appendix);
- the time within which the form must be sent to the FIU (s. 55(3B) of POCA);
- the reporting provisions of the ATA (both sections 33(1) and 22C reporting requirements);
- the duty to cooperate with FIU;
- the duty to report BOTH **Complete and Incomplete or Declined Business**;
- the Submission of Quarterly reports on Terrorist property; and
- the submission of a SAR if there is reasonable belief that that property is being used for terrorist activities.

Include the CO's duty:

- to monitor FATF's lists of Non-Cooperative Jurisdictions and High Risk Jurisdictions and listed entities issued by the FIU; and
- to keep a Register of enquiries of made by Law Enforcement Authorities and a register of STRs/SARs submitted to the FIU.

6. RECORD KEEPING PROVISIONS

Records of transactions and identification data must be kept for at least 6 years and for at least 6 years after relationship ends. State how they will be kept – electronic or written form.

7. ONGOING EMPLOYEE TRAINING

Include measures to ensure all employees are made aware of the relevant laws governing anti-money laundering and counter terrorist financing. Include training provisions for new staff and additional/refresher training for existing staff. (Such Training will usually be given by the CO). One good training tool will be this AML/CFT Compliance manual.

The CO and substitute will need more in depth training.

8. REVIEW OF PROGRAM

The FI and LB must periodically assess the risk of criminal conduct and take appropriate steps to design, implement, or modify its compliance program to reduce the risk of criminal conduct identified through this process.

How often? The CP must be reviewed annually to ensure its adequacy and a revised CP to be submitted to FIU every 2 years (unless otherwise directed by the FIU).

External Audit – Indicate how often and how it will be done, whether a written report will be prepared and to whom it will be sent.

Independent Internal Audit – Indicate how often it will be conducted and whether a written report will be prepared and to whom it will be sent. By ‘independent audit’ is meant review, (by persons who are not part of the AML/CFT compliance team of the FI’s or LB’s AML/CFT policies and procedures), for their appropriateness, compliance and effectiveness.

Caution: Financial Institutions and Listed Businesses are required to follow all of the requirements of AML/CFT laws and regulations. This guide may NOT contain all those requirements and does not create a safe harbour from regulatory responsibility. The obligation to develop an AML/CFT Compliance Programme is not a “one-size-fits-all” requirement, and you must tailor your plan to fit your particular financial institutions or listed business’s legal obligations.

Dated this 21st day of March 2011

End