ANTI-MONEY LAUNDERING AND COUNTER FINANCING OF TERRORISM

Compliance Programme Structural Guidelines for Non-Regulated Service Providers (NRSPs)

Supervisory Department
Saint Vincent and the Grenadines Financial Intelligence Unit

6th October 2021
FIU REF:002/2021

Table of Contents

AML/CFT COMPLIANCE PROGRAMME STRUCTURAL GUIDELINES

These structural guidelines seek to provide the Non-Regulated Service Providers (NRSPs) with a template for the Anti-Money laundering and Counter Financing of Terrorism (AML/CFT) Compliance Programme that each institution is required to implement pursuant to **regulation 20(1)** of the **Anti-Money Laundering and Terrorist Financing Regulations 2014**, as amended by **SRO No.25 of 2017**.

This document is to be used in conjunction with:

a) National legislation (https://www.svgfiu.com/index.php/resources/law-regulations);

b) The existing Guidelines for Non-Regulated Service Providers Document (AML/CFT Guidelines) found on the Financial Intelligence Unit's (FIU) website under the "NRSP/DNFBP's" tab (https://www.svgfiu.com/index.php/nrsp-dnfbp/nrsp-guidance/guidelines);

c) The FIU's Training and Awareness Document (Training Document) that would have been e-mailed to your institutions between February 10th-17th, 2020; and

d) Any other referenced materials seen in the guidance boxes at the end of each chapter below.

Each manual created should **AT LEAST** have the following chapters. It is not a one size fits all template, nor is it exhaustive and as such some institutions may include other pertinent systems and procedures that are unique to their organisation.

COVER PAGE

Should include :

A. clearly depict the name of your institution;

B. Any desired graphic (not compulsory);

C. The date your manual was created or last updated; and

D. The author of your manual (not compulsory).

CHAPTER 1 - INTRODUCTION

This should be the first chapter in your manual and should include the following, in separate sub-headings:

1.1 Mission statement of your institution

1.2 The purpose of your manual

1.3 The areas your manual will address

1.4 List of relevant laws that govern your manual and the State. These can be found on the FIU's website under the "Resources" tab and the sub-tab labelled "Laws and Regulations". It should be noted that this list will increase once the NRSP specific Regulations are enacted.

1.5 Institution's structure – can be in chart form but should clearly depict the key roles in your institution, including the positions held by members of staff. An example would be Managers, Compliance Department, Board of Directors amongst other roles, these will vary depending on type and size of your institution.

GUIDANCE

1. https://www.svgfiu.com/index.php/resources/law-regulations
2. https://www.svgfiu.com/index.php/about-the-fiu/organizational-structure

CHAPTER 2 - DEFINITIONS & INTERPRETATIONS

This section should contain key definitions for common terms used, abbreviations and descriptions of key roles or functions. Examples of what should be included are as follows:

a) AML- Anti-Money Laundering

b) BO- Beneficial Ownership

c) CDD- Customer Due Diligence

d) SDD- Simplified Due Diligence

e) CFATF- Caribbean Financial Action Task Force

f) CFT- Countering the Financing of Terrorism

g) EDD- Enhanced Due Diligence

h) FATF- Financial Action Task Force

i) ML- Money Laundering

j) PEP- Politically Exposed Person

k) SAR- Suspicious Activity Report

l) TF- Terrorist Financing

2.1 Money laundering- definition, stages and examples

2.2 Terrorist Financing- definition, stages and examples

GUIDANCE

1. FATF AML/CFT Glossary- https://www.fatf-gafi.org/glossary/
2. AML/CFT Guidelines pages 4-8- https://www.svgfiu.com/images/pdf/NRSP/GUIDELINES_for_Non-Regulated_Service_Providers.pdf
3. Proceeds of Crime Act 2013, as amended by the Proceeds of Crime Amendment Act, No. 18 of 2017 (POCA) – section 2
4. The Anti-Money Laundering and Terrorist Financing Regulations 2014, as amended by SRO No.25 of 2017 (The Regulations)- section 3
5. Anti-Terrorist Financing and Proliferation Act No.14 of 2015 and No.17 of 2017 Amendment (ATFPA)- sections 2,3,6,10, 21-24

CHAPTER 3 - EMPLOYEE HIRING, TRAINING AND MONITORING

For this section it is pertinent to include the process for hiring staff, the methods used to ensure AML/CFT awareness and training and the process applied for on-going monitoring of staff. The following subheadings would prove useful:

3.1 General Hiring Process- detail what checks are put in place when considering new staff. Details such as interviews, background checks, reference checks, police records, copy of identification and personal details amongst any other pertinent details. The procedure highlighted should be the one applied to all staff. If there is an exception or varying procedures for different categories of staff this should also be detailed.

3.2 Compliance Officer/ Reporting Officer- as one of the key roles in your institution this section should include:

a) The relevant qualifications the Compliance Officer/ Reporting Officer should have as well as the duties the Compliance Officer / Reporting Officer will be responsible for;

b) The details of who fills the role of Compliance Officer in the event of the absence of the primary Compliance Officer/ Reporting Officer;

c) Clearly state that the compliance function is not to be outsourced. However, where appropriate, certain specific activities may be outsourced provided that your institution is satisfied that the person the activity is outsourced to will report any knowledge, suspicion or reasonable grounds for suspecting ML/TF activity to your institution's compliance officer/ reporting officer;

d) The timeframe in which notice should be given to the Supervisory Authority and other necessary parties when the Compliance Officer/ Reporting Officer is changed or removed;

3.3 Training- this should entail the areas of focus for the training, these may include but are not limited to the AML/CFT legislation of SVG, the AML/CFT policies, procedures, systems and the controls of your institution. It should also highlight the methods (workshops, seminars etc.) used to disseminate this training to all members of staff. It should also entail who conducts the training sessions and how often they are conducted. Should also indicate how the trainings and materials are documented.

3.4 Staff Awareness- this section should entail how employees' knowledge of their AML/CFT obligations that they would have been trained on is tested. It should entail the type of testing undertaken, the rating method that establishes what constitutes a pass or fail and the frequency of testing. It should also stipulate the sanctions applied by your institution where an employee does not meet the satisfactory requirements.

3.5 Employee Ongoing Monitoring- hiring does not absolve your institution of its duty to ensure staff are not abusing their positions. As such ongoing monitoring of the activities and behaviors of staff should be implemented. This section should set out the system of monitoring and updating employee details as well as indicators for changes in behavior and work patterns.

GUIDANCE:

1. Anti-Money Laundering and Terrorist Financing Code No. 24 of 2017 (the Code)- pages 149,155,160-166, 169-177,
2. Anti-Money Laundering and Terrorist Financing Regulations No.20 of 2014 and No.25 of 2017 Amendment (the Regulations)- Regulations 24-27

CHAPTER 4 - RISK BASED APPROACH

This chapter should detail the overall risk mitigation strategy that is implemented by your institution, thereby making it the key building block of your manual. Useful headings to ensure that pertinent information is covered will include but are not limited to:

4.1 Risk Assessment- While there are various types of assessments, the required type for NRSPs will be an internal risk assessment. This type of assessment is necessary as NRSPs must apply a risk- sensitive approach to their institutions to determine the extent and nature of CDD and ongoing monitoring measures to be applied. It will also inform the procedures, policies, controls and systems implemented. Therefore, it should clearly be stated in this subchapter who conducts the internal risk assessment and the aim of the assessment. The aim of the assessment can be pinpointed by highlighting the relevant stages of the assessment, these would include:

a) Identify Risks

b) Assess Risks

c) Develop Risk Reduction Measures

d) Implementation of measures

e) Review of ratings

4.2 Types of Risks - these are the areas which your institution would focus on to identify the risks. Your manual should clearly indicate each area and what is examined in each. They would include:

a) Customer Risk- state the categories your customers fall into (Companies, Trusts, Politically Exposed Persons etc.) and clearly identify the types of criteria used to assess them.

b) Product/ Service Risk- clearly identify the types of products (third party payments facilitated, cash payments and withdrawals, pooling of customers, anonymity of customers or accounts etc.) offered by your institution as well as the criteria necessary to assess them.

c) Delivery Risk- as seen with the other two categories, identify the types of delivery methods (direct, telephone transactions, non-face to face, use of intermediaries etc.) used by your institution and the criteria used to assess each.

d) Country Risk- this should clearly identify the criteria for assessing country risk. This type of risk considers the risks of the country or countries in which branches of your institutions are located as well as the countries your customers or business associates are in. This should be clearly stipulated to show that your institution considers all geographic risks.

4.3 Risk Ratings- here your institution should clearly identify the rating system used for classification during your assessment. Common ratings include Low, Medium and High, however, there can be variations such as Medium-High or other applicable variations. Regardless of the chosen system, it should be clearly stated and should also include the criteria to be satisfied for each rating.

4.4 Frequency- should clearly stipulate how often your risk assessment and ratings are reviewed and updated. This timeframe can vary for each institution depending on the growth and change of structural components that are assessed. For some institutions it may be required that this formal internal assessment be conducted annually, for others with an unchanging customer and product base it may be less frequent so long as policies remain up to date. Further guidance is provided in the sections below.

GUIDANCE

1. The Code- paragraphs 23, 25(3),26 and (xvii) at pages 145-148 and pages 151-152, 155, 100-106.
2. The Training Document- pages 14-16.
3. AML/CFT Guidelines- pages 10-11.

CHAPTER 5 - CUSTOMER DUE DILIGENCE

This chapter is pertinent as it shows how the findings of your internal risk assessment are applied to your customer base and how the risk-based approach is applied to the daily business of your institution. The sections should essentially show what actions are to be taken when establishing customer relationships and what exceptions if any exist as well as guidance on termination of business relationships. However, you should be mindful that customer due diligence (CDD) protocols will not be applicable to all NRSPs. Specifically, Casinos and Jewelers will only be required to apply such protocols if they fall within the financial threshold referenced below. Useful headings would include:

5.1 Categories of Customers- for each category of customer you must clearly stipulate who constitutes this category and the procedure applied to start a business relationship with your institution for each. Identify the type of identification and relationship information collected and the procedure or means used to collect this data. The type of relationship being referred to means the purpose and nature of the business relationship, type and volume of activity and beneficial ownership data, amongst other areas highlighted in the guidance sections below. The categories of customer may include but are not limited to:

a) Individuals/ Natural Persons
b) Legal Persons or Arrangements
c) Third Party Representatives
d) Non-Face to Face Clients
e) PEPs

5.2 Simplified Due Diligence (SDD)[1]- it should be clearly highlighted that SDD should only be applied to low risk customers. Possible measures to be applied in this instance would include but are not limited to:

a) Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship;

b) Reducing the frequency of customer identification updates;

c) Reducing the degree of on-going monitoring and scrutinising transactions, based on a reasonable monetary threshold;

d) Not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but rather, inferring the purpose and nature from the type of transactions or business relationship established.

[1] While these procedures are outlined in international best practices regarding AML/CFT procedures it should be noted that the national provisions regarding SDD as highlighted in Regulation 16 of the Regulations do not presently cover all necessary guidance and is presently being amended.

5.4 Customer Due Diligence (CDD)- it should be made clear that this is the standard procedure to be applied to customers once they do not satisfy the SDD and EDD requirements. The standard procedure to be applied will only require 2 pieces of documentation, one will be used for identification purposes and the other for verification purposes and this should be clearly stated.

5.3 Enhanced Due Diligence (EDD)- should clearly stipulate that EDD is to be applied to higher risk customers and should clearly identify the procedure for starting a business relationship with a customer who falls into the EDD bracket. The main difference is that with standard CDD there is only the need for **two (2) pieces** of documentation needed for identification and verification at the onboarding stage and then **one (1) piece** for transactions conducted afterward. Whereas with EDD it requires **three (3) pieces** of documentation at onboarding and **two (2) pieces** thereafter. This sub-paragraph should also identify common categories of customers that would fall into this category for EDD.

5.4 Acceptable Forms of Identification- should clearly identify an accurate list of acceptable types of documents that can be used for Verification and Identification. These can include but will not be limited to the Multipurpose Identification Card, National Identification Card, Passport, Police Identification Card. All primary or best forms of identification must be equipped with a photo and an expiry date. Independent sources otherwise known as secondary forms or those that can be paired with the primary forms for verification purposes can include utility bills, bank statements, birth certificate, letter from a justice of the peace, notary, landlord or pastor amongst other documents referenced in legislation. In specifying the types of acceptable documents should also clearly highlight the acceptable requirements for certified copies by stating who should certify the document and what details it should include.

5.5 Databases- If your institution uses any particular databases to cross-reference CDD information it should be stated which. These databases can be accessed locally through government institutions such as the Inland Revenue Department (IRD), National Insurance Services (NIS) or can be a purchased international service such as World Check and there are also free international databases such as the United Nations Sanctions and Designation listings, Interpol Red Notices and Interpol UNSC Special Notices and FIU listings. It is recommended that as many of these credible sources be used to assist with the verification of documents and information provided.

5.6 Intermediaries- if your institution relies on intermediaries to introduce customers to your business and to conduct CDD requirements this section must clearly state the procedure applied, the types of data collected, how confirmation of the intermediaries' compliance was determined, whether it was through a favourable rating from a Regulator or external auditor and the checklist of criteria any intermediary must meet prior to commencing this relationship.

5.7 Exceptions- should include any categories of persons or entities that may be exempt from CDD requirements. Specific guidance can be sought from **the Code** as referenced below in the guidance section.

5.8 On-going Monitoring- clearly state that the information held on customers should be monitored and updated accordingly. Should also indicate how often your institution does this as well as a list of reasons that may trigger immediate updating or change in status of a customer from Low to High risk thereby triggering EDD or vice-versa. This shows the effectiveness of your risk-based approach to customer handling.

5.9 Termination & Prohibitions- should clearly detail the procedure for termination of existing client relationships as well as the instances or grounds upon which this may become necessary. Should also clearly stipulate in what instances employees are not allowed to start a business relationship, carry out an occasional transaction or when to terminate the relationship. Three (3) common examples are where CDD information cannot be verified, where it appears to be fictious, or where there is suspected connection to money laundering or terrorist activity.

GUIDANCE

1. The Regulations- Regulations 11,12,13,17,18,19 and Schedule 1 (the upcoming threshold amendments will be applicable here therefore making these sections not applicable to NRSPs that do not fall within the threshold.)
2. The Code- paragraphs 4-21(pages 95-102, 105-146)
3. ATFPA- sections 52-55, 63-67
4. AML/CFT Guidelines- pages 13-18
5. Customer Due Diligence Guidelines

CHAPTER 6 - SUSPICIOUS ACTIVITY & REPORTING

This is one of the most pertinent obligations on institutions, consequently, this chapter must expand on the reporting procedure used by the institution and must sufficiently indicate the risks of not doing so. Useful headings would include:

6.1 Internal reporting- should detail the process applied for internal reporting. It should clearly identify the chain of command and which form should be used and who it should be submitted to for assessment. It should also entail actions to be taken by employees, whether approval is needed to continue transactions or any other existing procedure. It should also clearly indicate the timeframe in which the internal report should be filed. A chart may be used to emphasise the chain of reporting command.

6.2 External Reporting- this sub-chapter should clearly identify the reporting procedure used when filing a SAR with the FIU. It should clearly identify who is responsible for filing, timeframe for filing and any other pertinent information.

6.3 Indicators- as a means of identifying suspicious activity, users of the manual should be provided with a list of indicators that would guide their understanding and general identification skills. The list of indicators is not exhaustive but should include general indicators as well as those that may be specific to your institution. The indicators should cover instances of both money laundering (ML) and terrorist financing (TF).

6.5 Investigations & Cooperation – This sub-paragraph should inform staff of their continuing duty as it relates to assisting with investigations that may occur after the filing of a SAR. The type of assistance being referred to is responding to Director's letters for further information and court orders including production orders, search and seizure warrants, customer information orders, account monitoring orders, restraint and property freezing orders amongst other such injunctive actions. It is pertinent that staff be familiar with these requirements and as such should be a part of staff training.

6.4 Penalties- should clearly stipulate all relevant penalties for tipping off, failure to report, failure to cooperate with investigations and requests and any other actions that constitute prejudicing an investigation. These can be found below in the guidance section.

GUIDANCE:

1. Proceeds of Crime Act No.38 of 2013 and No.18 of 2017 Amendment (POCA)- Section 126,127,128,129,130,131, Part 5(V)
2. ATFPA- Sections 15, 17,18, 63-67,71,72,73,74
3. The Code- Paragraphs 29-32 pages 160-164 and 166-168
4. AML/CFT Guidelines- Pages 18-19 and 23-32

CHAPTER 7 - RECORD KEEPING

This chapter should aptly detail your institution's recording and storage procedure, useful subheadings would include:

7.1 Format- This section should duly set out how records are kept whether in hard copy or electronically.

7.2 Type- This should specify the different types or categories of records that will be kept by your institution. Basic examples are transaction logs, SARs, customer information, employee information, training information, data relating to security procedures amongst other things.

7.3 Location- it should be clearly set out where your storage will take place, whether at an off-site secured facility or within your institution. Particular safety procedures to ensure that these records are secure should be highlighted.

7.4 Timeframe- your institution should make clear how long documents are to be stored. By law, the period is seven (7) years, however, there is a caveat that requires that documents should be kept for a longer period if there is an on-going investigation or if an official request is made. Your institution can have a longer timeframe, but it cannot be shorter than seven (7) years. It may also be helpful to users of your manual to highlight the instances in which the time would be extended, this may prove useful for new staff.

GUIDANCE:

1. The Code- Paragraphs 35-42 at pages 177-181
2. The Regulations- Regulations 21-23

CHAPTER 8 – AUDIT FUNCTION

8.1 All institutions must conduct an internal audit to test the level of compliance with their AML/CFT policies, procedures, systems and controls. The details of such should be clearly specified in this section and should include who is responsible for such review and how often it is conducted.

8.2 An independent audit must also be conducted by an external entity, this audit seeks to test the effectiveness of the institution's AML/CFT policies, procedures and systems. The details of this audit must also be clearly specified in this section. Key areas to cover would be the entity or person responsible for the audit and how often the audit is conducted.

GUIDANCE

1. The Regulations- regulation 20(4)
2. The Code- paragraphs 24(2)(d), 25(3), (xvii) at pages 148 and 155.
3. AML/CFT Guidelines- page 21.

APPENDICES

This should be the final section of your institution's compliance manual and should include all standard forms used by your institution, any charts and/or diagrams. Common forms include but are not limited to:

Appendix 1- Employee Information Form
Appendix 2- Compliance Fit & Proper Form
Appendix 3- Customer Information Form
Appendix 4- Third Party Forms (if different from customer information form)
Appendix 5- Source of Funds Form
Appendix 6- Internal SAR Form
Appendix 7- External SAR Form
Appendix 8- Jurisdictional Designation Listing (countries on designation listings)

GUIDANCE:

1. ATFPA- Schedule 1 and 2
2. External SAR Forms- https://www.svgfiu.com/index.php/sars
3. Compliance Fit & Proper Form - https://www.svgfiu.com/images/pdf/NRSP/Compliance_Officers_Fit_and_Proper_Form_For_Non-Regulated_Service_Providers.pdf