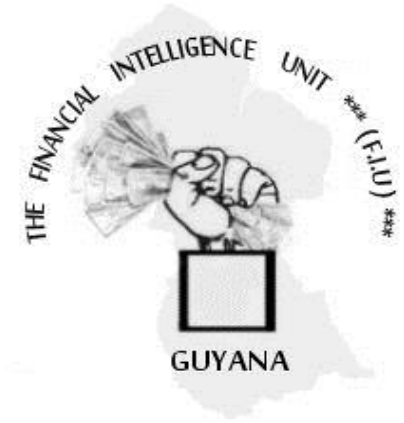


DESIGNATED NON-FINANCIAL BUSINESS OR PROFESSION (DNFBPs)

AML/CFT- Compliance Regime

(UPDATED JUNE 2021)

Issued in accordance with Section 9(4)(e)(iv) of the AML/CFT Act Cap 10:11

Date of issue: June 1, 2021

Contents

Table of Acronyms

AML	Anti-Money Laundering
AML/CFT	Anti-Money Laundering & Countering the Financing of Terrorism
CDD	Customer Due Diligence
CFATF	Caribbean Financial Action Task Force
CFT	Countering the Financing of Terrorism
CO	Compliance Officer
DNFBP	Designated Non-Financial Businesses or Professions
EDD	Enhanced Due Diligence
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
FSRB	FAFT Styled Regional Body
FT	Financing of Terrorism
ML	Money Laundering
NPO	Non-Profit Organisation
PEP	Political Exposed Person
RBA	Risk Based Approach
RE	Reporting Entity
SA	Supervisory Authority
STR	Suspicious Transaction Report
TCSPs	Trust Company or Service Providers
TPR	Terrorist Property Report
TTR	Threshold Transaction Report

Definition of Key terms

Beneficial ownership	‘‘Beneficial ownership” means ownership by a natural person or persons who ultimately exercise individually or jointly voting rights representing at least twenty-five per cent of the total shares, or otherwise have ownership rights of a legal entity; or ownership by a natural person or persons who ultimately owns or controls a customer or the person on whose behalf a transaction is being conducted and includes those persons who exercise ultimate effective control over a legal person or arrangement.
Customer	A 'Customer', for the purpose of this guideline, is a person (natural or legal) who seeks to establish a business relationship; or to carry out a "one off transaction" with any of the businesses or professions described in the First Schedule of the AMLCFT Act Cap. 10:11 under the definition for Designated Non-Financial Businesses or professions (DNFBPs). The term customer includes a client of a DNFBP, where in that context the term client applies.
DNFBP	'Designated non-financial business or profession (DNFBP)' refers to a business or profession, which carries on any of the businesses/professions/activities, as listed in the First Schedule of AML/CFT Act Cap. 10:11 under definition for ‘reporting entity’ under the ACT.
Terrorist Financing	'Terrorist Financing' means wilfully providing or collecting funds, by any means, directly or indirectly, with the unlawful intention that they should be used or in the knowledge that they are to be used in full or in part- (a) to carry out terrorist acts; (b) by a terrorist organisation; or (c) by an individual terrorist.
Money Laundering	'Money Laundering' means conduct which constitutes an offence as described under Section 3 of the AML/CFT Act Cap. 10:11 “A person commits the offence of money laundering if he knowingly or having reasonable grounds to believe that any property in whole or in part directly or indirectly represents any person’s proceeds of crime: - (a)converts or transfers property knowing or having reason to believe that property is the proceeds of crime, with the aim of concealing or disguising the illicit origin of that property; (b) conceals or disguises the true nature, origin, location, disposition, movement or ownership of that property knowing or having reason to believe that the property is the proceeds of crime; (c) acquires, possesses or uses that property, knowing or having reasonable grounds to believe that it is derived directly or indirectly from proceeds of crime; (cA) assist any person who is involved in the commission of an offence in paragraphs (a), (b) or (c) or (d) participates in, associates with or conspires to commit, attempts to commit or aids and abets, counsels or procures or facilitates the commission of any of the above acts.
Politically Exposed Person	A 'Politically Exposed Person' is described in the AML/CFT Cap. 10:11 as:- ‘any individual who is or has been entrusted with prominent public functions on behalf of a state, including a Head of State or of government, Senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials, including family members or close associates of the politically exposed person whether that person is resident in Guyana or not.

Proliferation Financing	Proliferation Financing includes the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual use goods used for non-legitimate purposes), in contravention of the provisions of any law or, where applicable international obligations.
Reporting Entity	A 'Reporting Entity' refers to any person whose profession or business involves the carrying out of any activity listed in the First Schedule of the AML/CFT Act Cap. 10:11 or any other activity as may be described by the Minister responsible for Finance.
Risk Based Approach	A 'Risk Based Approach' to AML/CFT means that the DNFBPs are expected to identify, assess and understand the ML/TF risks to which they are exposed and take AML/CFT measures commensurate to those risks in order to mitigate them effectively.
Supervisory Authority	'Supervisory Authority' means the authority set out in column 2 of the Fourth Schedule of the AMLCFT Act Cap. 10:11, who has compliance oversight over the reporting entity set out in column 1 of the Schedule or as may be appointment by the Minister of Finance.
Suspicious Transaction	A 'Suspicious Transaction' is one for which there are reasonable grounds to suspect that the transaction is related to a money laundering offence or a terrorist activity financing offence.
Suspicious Transaction Report	A 'Suspicious Transaction Report' is a report required to be submitted to the FIU pursuant to Section 18(4) of the AMLCFT Act Cap. 10:11, whenever a reporting entity suspects or has reasonable grounds to suspect that funds, a transaction or attempted transaction are connected to the proceeds of criminal activity, money laundering of terrorist financing offences or funds suspected of being linked, or related to or to be used for terrorist acts or by terrorist organisations.
Terrorist Property Report	A 'Terrorist Property Report' is a report required to be submitted to the FIU pursuant to Section 68 of the AMLCFT Act Cap. 10:11, when a Reporting Entity knows or believes that it has in its possession, funds or other assets (property) of a person or entity designated pursuant to the United Nations Security Council resolution (UNSCR) 1267(1999) and its successor resolutions or specified by the Minister responsible for Finance under section 2(2) of the AMLCFT Act Cap. 10:11 pursuant to UNSCR 1373(2001).

Introduction

This guideline is a revision to the Financial Intelligence Unit's Guideline No 1 of 2016 which was issued as a guide to Designation Non-financial Business or Professions (DNFBPs) to assist them in implementing measures to ensure their businesses are not used to launder monies into the formal financial systems. Following the issuance of that Guideline (No. 1 of 2016), several amendments were made to the Anti-Money Laundering and Countering the Financing of Terrorism (AMLCFT) Act Cap. 10:11, many of which touched and concerned the AMLCFT obligations of reporting entities, hence the need for this revised version.

The main objectives of this guideline are to assist reporting entities with the design, implementation and/or enhancement of their AMLCFT compliance framework and to ensure the AMLCFT Act Cap. 10:11, achieves its primary objective of preventing money laundering, terrorist financing or other criminal activities. This requires the commitment of and implementation of appropriate measures by Reporting Entities, to identify and report suspicious transactions to the Financial Intelligence Unit in a timely manner.

DNFBPs are obligated to comply with specific obligations under the AMLCFT Act Cap. 10:11, which include, but are not limited to the following:

a) the implementation of customer/client due diligence measures;
b) identification and verification of identity of all classes of customers/clients;
c) maintenance of customers/Clients' records;
d) Assess, manage and mitigate the ML/TF risks associated with products and services, and clients/customers;
e) the submission of reports to Financial Intelligence Unit (FIU).

The guideline provides broad measures, some of which may or may not be applicable or appropriate for some of the DNFBPs. The DNFBPs are required to apply a **risk-based approach** and based on the assessment of risks associated with the particular DNFBP, it would be required to apply measures that best suit its size, nature and complexity

The implementation of AMLCFT measures by DNFBPs is not a "one size fits all endeavour, as the ML/TF risks posed varies among the sectors. The nature, size and complexity of each entity will determine how the reporting entity manages its relationship with its customers/ clients and its designated supervisory authority.

This guideline is not intended to override the provisions of the AML/CFT Act Cap. 10:11 or its regulations, and is required to be read in conjunction with AML/CFT Act Cap.10:11, its Regulations, subsidiary legislation, directives and other applicable guidelines currently in force or as are amended or updated from time to time.

The DNFBPs referred to in this guideline include the following categories of entities as outlined under the First Schedule of the AMLCFT Act of Cap. 10:11.

- **Gaming Sector**
  - I. Casinos (including internet casino)
  - II. Betting Shops
  - III. Lotteries

- **Dealings in Real Estate**
  - I. Real Estate Agents
  - II. Real Estate Brokers
  - III. Real Estate Developers

- **Mining/Extractive Sector**
  - I. Dealers in Precious Metals (Gold Exporters)
  - II. Dealers in Precious & Semi Precious Stones
  - III. Dealers in Precious Minerals/Traders

- **Professions**
  - I. Attorneys-at-Law
  - II. Notaries
  - III. Commissioners of Oaths to Affidavits
  - IV. Accountants
  - V. Auditors

When, on behalf of or for a client, they engage in a transaction in relation to the following activities-

1. ***buying and selling of real estate;***
2. ***managing of client money, securities or other assets;***
3. ***management of bank, savings or securities accounts;***
4. ***organisation of contributions for the creation, operation or management of companies; or***
5. ***creation, operation or management of legal persons or arrangements, and buying and selling of business entities***

- **Professions cont'd**
  - VI. Trusts or Company Service Providers

When, by way of business, they provide services or prepare for and carry out transactions for a third party in relation to the following activities:

1. ***formation or management of legal persons;***
2. ***acting as or arranging for another person to act as a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;***
3. ***providing a registered office, business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement;***
4. ***acting as or arranging for another person to act as a trustee of an express trusts; or***
5. ***acting as or arranging for another person to act as a nominee shareholder/Director for another person.***

Legal and Regulatory Framework

The AML/CFT Act Cap. 10:11, Regulations made thereunder, other relevant Legislation, Guidelines, international standards and best practices govern and guide, the legal, regulatory and institutional frameworks for detecting and preventing money laundering, terrorist and proliferation financing in Guyana.

Sections 15, 16, 18, 19 and in some instances 20 of the AML/CFT Act Cap. 10:11 provide the specific obligations with respect to the DNFBPs. As mentioned above, these obligations relate to the identification and verification of customers; record keeping; appointment or designation of a compliance officer; reporting; training and awareness for employees and engagement and monitoring of customers/ clients of the DNFBP.

Pursuant to Sections 22 and 23 of the AML/CFT Act Cap. 10:11, Supervisory Authorities are required to be appointed to, inter alia, examine, supervise, issue instructions and guidelines, provide training to entities under their supervision, and enforce the requirements via sanctions that can be implemented against the entity for not compliance with their AMLCFT requirements.

In addition to the compliance obligations under the AMLCFT legislation, the DNFBPs are required to comply with other legislation governing, among other things, the requirements to obtain license(s) and/or registration, and other regulatory measures provided for under those laws.

Establishment of an AMLCFT Regime

The overall responsibility for establishing the AMLCFT Compliance Regime lies with the owner(s), directors where applicable and/ or senior management of a reporting entity. This is to ensure that an effective AMLCFT system is always in place. This responsibility includes, but are not limited to, the implementation of the following measures:

a) Register with The Financial Intelligence Unit (FIU);
b) Appoint a Compliance Officer (CO) to implement the AML/CFT Act Cap. 10:11 preventative measures;
c) Establish and maintain (***where applicable at all branches***) policies, procedures, controls and systems which must to be documented in an AMLCFT Manual.

The AMLCFT Manual[1] is required to include, but are not limited to, the following measures or procedures –

- Registration with FIU
- ML/TF/PF Risk Management and Risk Mitigation
- Customer Identification & Verification (Know Your Customers);
- Reporting requirements;
- Record Keeping
- Ongoing Monitoring (of customers);
- Employees' Awareness & Training;
- Employee Screening (as applicable)
- Independent Audit/Tests of AMLCFT systems;
- Preparation for AMLCFT Supervisory Examination.

Registration Procedure[2]

Section 19(4) of the AML/CFT Act Cap. 10:11 requires all reporting entities, including, the DNFBPs to register with the FIU. The Registration Process include the following steps:

(a) Uplift a FIU Reporting Entity Registration Form from the FIU's Office located at 49 Main & Urquhart Streets, C/O Ministry of Finance Compound; **Or** the form may be downloaded from the FIU's website at www://fiu.gov.gy.

(b) Complete the Registration Form and attach copies of the following documents (as may be applicable to the DNFBP):

[1] Refer to FIU Guidance Notes No 1 of 2017 – Policy Manual. http://fiu.gov.gy
[2] Refer FIU – Reporting Entity Registration Policy. http://fiu.gov.gy

(i) Identification for Owners/ Senior Executives;
(ii) Reporting Entity's Registration Document/e.g. Certificate of Registration /Incorporation documents (as applicable);
(iii) Reporting Entity's Operating License/Practice Certificate (as applicable);
(iv) By laws/Constitution/Rules/or similar governing document
(v) Entity's most recent Financial Statement and/or Annual Returns.

(c) The completed registration form must be signed by a senior officer (Chairman/Head/President/Compliance Officer) or Beneficial Owner of the reporting entity.

(d) The Completed form should be stamped with the seal or official stamp of the reporting entity, where applicable.

(e) The reporting entity must thereafter submit (by hand or post) the completed Registration Form along with copies of relevant document(s) to the Director, FIU with a cover letter. The cover letter is required to be done in duplicate. *A Sample of the cover letter can be found on FIU's Website: www://fiu.gov.gy or as may be distributed to the entity at a training session hosted by the FIU, independently, or in collaboration with the Supervisory Authority.*

(f) Upon submission of the completed registration form by the reporting entity, the form will then be stamped by the FIU's employee and the duplicate cover letter will be returned to the Entity for its record.

(g) The submitted Registration Form and the copies of attached documents will be reviewed and verified for accuracy.

(h) The FIU employee who checks/verifies attachments/documents will sign off as verifying the authenticity of the completed Form and attached documents.

(i) Once the Registration Form is accurately completed and all relevant documents are attached and in order, the FIU will prepare a "*Reporting Entity Registration Confirmation*" letter which will be issued to the Reporting Entity and copied to the Supervisory Authority.

(j) If the Registration Form is not accurately completed, or the relevant documents are not submitted or found to be out of order, the FIU will prepare a "Reporting Entity Incomplete Registration letter notifying the reporting entity of such status and requiring the entity to make the necessary correction(s).

(k) This letter will indicate the inaccuracies, missing information or 'out of order documents' and will clearly state that the Registration was incomplete. The Registration Status of the reporting entity will remain incomplete until or unless the Form is accurately completed, and all relevant documents are properly submitted.

(l) The FIU's 'Reporting Entity' Register will then be updated accordingly; and

(m) The FIU will contact the RE on the next steps to be taken to commence the implementation of its Compliance Obligations in general and to the FIU in particular.

Risk Management System /Applying a Risk-Based Approach

A 'risk' can be defined as the ability of a threat to exploit a vulnerability. For there to be a risk, both a threat and a vulnerability must be present.

The Reporting entity is required to implement a risk management system to enable it to identify, assess and understand the ML/TF/PF risks associated with its activities. Where the reporting entity considers that a person or entity with whom it establishes a business relationship or carry out a 'one off' transaction is high risk, then that entity must apply enhanced due diligence measures. The risk management system requires the reporting entity to, based on the level of risk assessed, implement mitigating measures commensurate with the ML/TF/PF risk identified (if any).

A Risk assessment is required for all business relationships established by the entity, including with its partners or other persons or entities with which it engages.

Where the risks associated with a business relationship or transaction are considered as "high", then enhanced due diligence measures are required. Such business relationships or transactions may include those involving large amounts of cash, complex legal arrangement (such as express trusts), dealings with non-nationals, those involving Politically Exposed Persons (PEPs), sectors that are inherently higher risk (dealers in semi-precious and precious and stones/ minerals), etc.

Some risk mitigation measures may include, in the case of partnership arrangements, the application of clear policies and procedures when establishing a business relationship with customers who claims to be doing business as a 'Partnership'.

The policies should seek to ensure that information to be obtained include full details of the ownership and control structure of the partnership arrangements, where the business involves foreign partner or beneficial owners operating in a foreign jurisdiction.

Appointment of a Compliance Officer[3]

The reporting entity is required under Section 19 of the AMLCFT Act to appoint a Compliance Officer (CO) to assist the entity with implementing the AMLCFT policies and procedures. The legal requirements for the CO's appointment and functions include, but are not limited to, the following:

(i) The CO must be a person who possesses the necessary competence to function at management level or possesses adequate skill to carry the functions of a CO;

(ii) The CO must have full access to the Board/ Committee of Management (as applicable) and be able to operate in a manner free from undue influence or any situation which give rise to a 'conflict of interest'. This is particularly important where there is involvement of a beneficial owner, board member or senior management in a suspicious activity;

(iii) The CO must be able to submit suspicious transaction reports ***independently*** and must be in a position of neutrality (free from bias);

(iv) The CO must be able to communicate/liaise independently with the FIU in relation to ML and TF or related matters on behalf of the reporting entity;

(v) Be able to implement the policies, procedures, systems and controls following their formulation and approval by the owner(s), Board or Committee of Management of the reporting entity.

The following lists provide guidance and best practices on the type of information and/or documentation a reporting entity may seek to ascertain and/or obtain when carrying out a 'one-off transaction' or establishing a business relationship with a customer/client:

[3] Section 19 AMLCFT Act Cap. 10:11; Regulation 14 of Regulation No. 4 of 2010

Identification and verification

- ### Natural Person

a) Customer's (client's) full name (including maiden name -where applicable)
b) Identification document - National Identification or Passport
c) Permanent and mailing address (including PO Box numbers-if necessary)
d) Telephone Numbers, email etc.
e) Date and place of birth
f) Nationality
g) Occupation/or nature of business (where self-employed)
h) Name and address of employer (if applicable)
i) Signature

- ### Legal Entity[4]

a) The Name and legal form of the organisation/legal entity/business
b) The Registered Address of the entity
c) Country of Incorporation/Registration
d) Information on the purpose and intended nature of the Business relationship e.g. a signed Director's statement/or similar document)
e) Identify and verify the identity of the beneficial owners within the entity using reliable source documents
f) Identity of Principal owners/shareholders
g) Identity of Senior Management, Directors, Secretary or Partners
h) Copies of identification documents for the directors, Secretary or partners
i) Evidence of the authority given to enter into a business relationship (for e.g. A copy of the Board Resolution)
j) Share Certificate issued by the entity
k) Articles of Incorporation or continuance
l) Certificate of Incorporation or continuance (for a company)
m) Certificate of Registration or similar evidence of establishment or existence
n) By-Laws of the entity
o) Partnership Deed - If business is a partnership
(p) Business operation licenses - if applicable

[4] A legal entity may include, a company established on the Companies Act Chapter 89:01, a person trading with a Business Name registered under Business Name Registration Act Cap. 90:05, a Partnership under the Partnership Act Cap. 89:02, an Organisation, Association or a similar body under the relevant law establishing such body.

- **Legal Arrangement**

Where the transaction involves dealing with an express trusts or other similar legal arrangement, the following procedures may apply:

a) Identification of person action on behalf of and the principal/settler/donor
b) Obtain copies of Power of Attorneys
c) Letter of Authorisation
d) Trust Instruments e.g. Trust Deeds, statement or authorisation from the Trustees
e) Identify beneficial owner-natural person that owns and controls the legal arrangement

Where it appears that the person on whose behalf the person/representative acts is located in another country, the reporting entity should seek to establish 'whether the country is a ML/TF high risk jurisdiction' and/or if it is subject to oversight or regulatory mechanism by the FATF or a FATF Styled Regional Body (FSRB).

- **Political Exposed Person[5] (PEP)**

A 'Politically Exposed Person' (PEP) is any individual entrusted with prominent public functions on behalf of a State: for examples:

(i) A Head of State or of government
(ii) Senior Politicians
(iii) Senior government, judicial or military Officials
(iv) Senior executives of state-owned corporations
(v) Important political party officials
(vi) Family members or close associates of a PEP
(vii) whether the PEP is resident in Guyana or not.

The reporting entity, using a 'Risk-Based Approach', must develop policies and procedures to enable it to apply (where necessary) Enhanced Due Diligence (EDD). Such measures may include controls to enable it to -

a) Identify PEPs - at establishment of a business relationship or later if a customer becomes a PEP after the relationship has been established;
b) Maintain a PEP register (***this is a best practice***);

[5]Refer to FIU PEP Guideline No 3 of 2017

c) Assign risk ratings for PEPs/developing risk profiles of PEPs, examples of factors to consider-

(i) PEPs from international organizations or foreign countries;
(ii) PEPs from countries with higher rates of corruption/or inadequate AMLCFT Regulation;
(iii) PEPs who have been the subject of adverse media coverage.

d) Obtain and verify customer identification data on the PEPs;
e) Gather information on the source of wealth or funds (if necessary);
f) Ensure that approval of senior management is granted before establishing a business relationship or if the customer becomes a PEP during the business relationship;
g) Ensure regular monitoring of the business relationship with the PEP.

- **Non-Face-to-Face transaction**

Reporting entities must establish and implement policies, procedures, systems and controls to manage specific risks associated with conducting transactions where the customer is not physically present. This includes but is not limited to procedures relating to the identification and verification of activities for the transaction and the relationship.

The reporting entity, at a minimum, must require one form of official identification which has been authenticated (certified appropriately) and one form of documentation that will verify the physical address of the customer.

- **Non-Resident (foreign customers)**

(i) The reporting entity must pay particular attention to non-resident or non-national customers, whether it be a natural person or legal person.

(ii) The identification requirements for natural persons resident in Guyana also apply to natural persons that reside outside of Guyana. Given the higher level of risk posed by non-residents, additional enhanced due diligence procedures may be required when doing business with such individuals.

(iii) Where certified copies of documents are being used to conduct transactions, the reporting entity must be satisfied that the documents are authentic. The purpose of the transaction by the non-resident customer must also be obtained and documented.

(iv) Where the customer is a Foreign Legal Entity, (for example a Company), the documents required for registering in Guyana must be requested and retained. Attempts must also be made to have the documents properly authenticated. Such documents may include, but are not limited to, a registered 'Power of Attorney' document and a certified copy of the corporate instruments of the Company.

Record Keeping and Maintenance[6]

The AMLCFT Act Cap. 10:11 and Regulations made thereunder, require reporting entities to keep sufficient records for all unusual, large cash or complex transactions or established business relationships with its customers (clients). This is to enable it to submit accurate 'suspicious transaction reports', terrorist property reports or other relevant information, as may be requested by the FIU. It also facilitates the availability of an audit trail to support any investigation that may be initiated by Law Enforcement.

- **Records required to be kept**

a) Evidence of the customer's identity;

b) Account files and business correspondence in relation to the transactions and identities of persons involved in the transactions;

c) The name, date of birth, address and occupation of the customer (client) and where appropriate/possible, the business or principal activity of each person conducting the transaction or if known, on whose behalf the transaction is being conducted, as well as the method used to verify the identity of each person;

d) The nature and date of the transaction;

e) The type and amount of currency involved in the transaction (that is which jurisdiction/country the currency originates) and include, whether it is coin, paper money, bank notes or other negotiable instruments), disposition of the funds (e.g. was the cash deposited, converted to another currency, or used to buy money orders, traveller's cheques, etc.) and whether any other individuals or entities were involved in the transaction.

[6] Section 16 AMLCFT Act Cap. 10:11

- **Record Maintenance**

a) The records/documents obtained for all transactions should be safely stored to facilitate their protection. That is to prevent records from becoming, blurred, defaced, illegible, mutilated or in any other way deteriorated.

b) Records being stored digitally or electronically must be easily retrievable or capable of reproduction in a printable and legible (readable) form.

c) Records must be retrieved promptly or without undue delay by the organization when requested by the Financial Intelligence Unit (FIU).

d) Records are required to be kept and maintained for a period of at least seven years from the date when the relevant transaction was completed or termination of business relationship, whichever is later or for such period as may be determined by law or administrative proceedings.

- **Other Record keeping functions**

a) The reporting entity must ensure that a special register for AMLCFT queries is kept;

b) Records of customer's risk profiles, risk mitigation measures applied or imposed;
c) Records kept must be relevant, up to date and reviewed on an ongoing basis;

d) There should also be back up system for all records, whether such storage is offsite, onsite or digital.

Reporting Procedures[7]

The reporting entity must ensure it has systems in place to facilitate timely and accurate reporting of suspicious transactions, threshold and terrorist property reports.

Mechanisms should also be established for the implementation of the 'UNSCRs' Targeted Financial Sanctioning Regimes. This requires the development of effective detection measures, and internal and external communication and reporting systems.

[7] Section 18 AMLCFT Act, Regulation No 4 of 2010; Guidelines No 1, 2013; No 2 of 2015; No 3 of 2015; No 2 of 2016; & No 1 of 2018

- **Suspicious Transaction Report**

A suspicious transaction is any attempted or completed transaction or activity which raises in the mind of a person involved, any concerns or indicators that such a transaction or activity may be related to money laundering or terrorist financing or other unlawful activity. It causes the person or compliance officer to have a feeling of apprehension or mistrust about the transaction or activity.

A Suspicious Transaction Report is required to be submitted to the FIU by the reporting entity, through its Compliance Officer, once it suspects or has reasonable grounds to suspect that **fund**s, a **transaction** or **attempted transaction** are the proceeds of a criminal activity, money laundering or terrorist financing offences or is suspected of being linked, related to or to be used for terrorist acts or by a terrorist organisation. Where any such suspicion is raised, the following steps apply:

a) The STR must be submitted as soon as possible but not later than three (3) days after forming the suspicion;

e) Some factors that should be considered when assessing whether or not a transaction is suspicious include, complex and/ or unusually large business transactions; unusual patterns of transactions, whether completed or not, that have no apparent economic or lawful purpose and are inconsistent with the profiles of the persons carrying out such transactions;

f) The completed STR must be delivered to the Director, Financial Intelligence Unit (FIU), Ministry of Finance Compound, 49 Main & Urquhart Streets, Georgetown, Guyana;

h) The STR must be kept confidential as it is an offence for a person who knows or suspects that a report is being prepared or has been sent to the FIU, to disclose that information to another person, other than a court, or other person authorized by law.

In evaluating a potential suspicious activity, the reporting entity should seek to ascertain whether the customer (legal or natural person) poses a terrorist financing risk or appears to be linked to terrorist activities or a terrorist organisations and determine whether the customer's name appears on the United Nations Security Council (UNSC) Consolidated List of terrorists. If the customer is so identified, then a Terrorist Property Report must be filed pursuant to UNSRs 1267, 1373, 1718 or 2231.

However, where the customer's name does appear on the UNSC Consolidated listed, but there are reasonable grounds to suspect that the funds are linked, related or to be used for terrorist acts or by a terrorist organisation, then the reporting entity must consider filing a suspicious transaction report to the FIU.

For further details on submitting suspicious transaction reports, please refer to the FIU's STR Updated Guideline No 1 of 2021.

- **Threshold Transaction Report**

A 'Threshold Transaction Report'[8] (TTR) is a report required to be submitted to the FIU pursuant to the AMLCFT Act and Regulations No. 4 of 2010, for transaction(s) conducted by a reporting entity with a client or customer, that meets a predetermined limit or threshold.

The established threshold or limits for sectors within the DNFBPs are as follows:

(i) Casinos, large betting shops and lotteries, any cash transaction equal to or above five hundred thousand dollars ($500,000);
(ii) Small betting shops, sixty thousand dollars ($60,000); and
(iii) Dealers in Precious Stones and Metals/Minerals, Real Estate Agents and Used Car Dealers, any cash transaction equal to or above two million dollars ($2,000,000).

TTRs are required to be submitted by the 7th of each month following the month in which the transaction(s) occurred and should be reported in such manner or format as prescribed by the FIU.

For further information on 'threshold transaction reports', please refer to the FIU's AMLCFT Handbook for Reporting Entity, published February 18, 2021, accessible from the FIU's website at: fiu.gov.gy.

- **Terrorist Property Report**

A 'Terrorist Property Report' (TPR) is a report required to be submitted to the FIU pursuant to AMLCFT Act & the Regulations made thereunder, where the reporting entity discovers it is holding assets or funds or dealing with a person or entity listed on the United Nations Security Council Resolutions list of Terrorist and include persons or entities listed on United Nations Security Council Resolution (UNSCR) 1267(1999) and its successor resolutions; or

[8] Regulation 12(3) of the AMLCFT Regulation No 4. of 2010; First Schedule of the AMLCFT Act Cap. 10:11.

specified by the Minister responsible for Finance under section 2(2) of the AMLCFT Act Cap. 10:11 pursuant to UNSCR 1373(2001); or UNSCR 1718 (2006) or 2231(2015).

A Terrorist Property Report (TPR) must be made to the FIU, ***immediately,*** when a Reporting Entity knows or believes that it has in its possession, funds or other assets (property) of a person or entity designated pursuant to the above UNSCR resolutions. If a Reporting Entity is not sure that it is dealing with funds or other assets of a designated or specified person or entity, but suspect that it might be, then a Suspicious Transaction Report is required, whether or not a transaction was completed.
A Terrorist Property Report may be sent to the FIU by registered or regular mail or hand delivered to the Director, Financial Intelligence Unit, Ministry of Finance Compound, Main & Urquhart Streets, Georgetown.

The TPR must contain information that describes the funds or other assets (property). The report must also provide information about the designated or specified person or entity and anyone who owns or controls the property on their behalf. In addition, if there were any completed or attempted transactions related to the funds or other assets (property), the report must contain information about such transactions.

***For further information on TPR reporting and other relevant legal obligations, please refer to TPR Guidelines No. 2 & 3 of 2015 and No 2. of 2016*.**

Monitoring Function[9]

Reporting entities are required to have a system in place to monitor transactions with its customers/clients. The monitoring function may also be extended to situations where the business relationship is considered vulnerable to ML, TF or PF. In applying a risk-based approach, the reporting entity may (on an ongoing basis) pay special attention to and monitor its relationships with donors, partners or associates, members, and develop risk profiles for those relationships that it considers as posing a risk for ML/TF/PF. Some high-risk situations may include, 'one off' transactions that appear unusual, involve large amounts of cash, are complex and do not match the profile of the customer.

The reporting entity must ensure records relating to, the monitoring process, its findings, the enhanced due diligence measures applied to determine the source and the ultimate destination of such funds, including the background and purpose of the transaction, must be retained and maintained for easy and timely access.

[9] Section 19 AMLCFT (as amended)

This is to enable an evidence trail is available and accessible in the event of an investigation being undertaken by the FIU or a law enforcement agency.

AMLCFT Training[10]

- ### Employee

The reporting entity must also have a system in place for staff training (where the organization employs individuals) particularly those employees who are required to deal with identifying customers.

Where a member is employed to carry out specific AMLCFT functions, training must be provided to enable that employee to have a clear understanding and adequate awareness of the AMLCFT preventative measures. Where the employee is directly responsible for recognizing unusual, complex transaction and reporting suspicious transactions or other reports to the FIU, specialised training on the reporting requirements, including the enhanced due diligence measures must be provided to such employee.

Training must be ongoing and/or refreshers' training on the AMLCFT obligation and relevant procedures must be provided throughout the tenure of employment to the employee who is dealing with the AMLCFT compliance functions.

The reporting entity must ensure it keeps abreast with all updated AMLCFT laws, new developments, relevant technology, current trends and methods for dealing with or addressing issues relating money laundering, the financing of terrorism and proliferation (which has a history in some jurisdictions of being linked to many charitable organizations). The AMLCFT policies and procedures developed by the organization should be documented (in a manual) which should be accessible to all employees.

- ### AMLCFT - General Awareness

The reporting entity should have a system to provide general knowledge to management and other staff of updates on all relevant AMLCFT laws, regulations, policies and procedures, guidelines and other information related to Money Laundering, Terrorist and Proliferation Financing. An effective communication system would ensure relevant AMLCFT information is disseminated to the relevant employees.

[10] Section 19 AMLCFT Act

Employee Screening

The reporting entity must ensure procedures are in place for screening of all employees prior to employment or engaging in voluntary services for or on behalf of the entity. This may include the requirement for appropriate qualification and experience of staff to fill job vacancies, which must be appropriately verified. This may include a risk-based policy requiring police clearance, background checks and character references to be included for recruiting some or all categories of employees or volunteers (as the case may be).

Independent AMLCFT Audit

A system of ongoing independent reviews of the compliance measures implemented, would provide relevant insight and feedback on the effectiveness of the reporting entity's AMLCFT Compliance Regime, and recommendations on how same can be made more effective. These reviews may involve examining whether the AMLCFT activities planned were effectively carried out and whether necessary solutions are provided for challenges that arise from time to time. The mitigation measures or corrective actions undertaken should be documented.

Additionally, all business relations with customers must be reviewed to ensure information received are consistent with the reporting entity's knowledge of the customer, its business and risk profile and where appropriate, the source of wealth or funds.

The audit or review process is established to test the effectiveness of the AML systems. The system is expected to utilise established auditing standards and include procedures for sample testing. This is essentially an internal control measure used to assist with the management of the ML/TF/PF risk faced by the reporting entity. The independence of the audit function is important to ensure findings and conclusions of the audit and unbiased. The requirement of an independent audit should be clearly specified in the reporting entity's AMLCFT manual.

The importance of the audit function, include but are not limited to, the following:

1. To test the overall integrity and effectiveness of the AML/CFT systems and controls;
2. Test the money laundering and terrorist financing risks management system and determine level of exposures based on the size, type of business, customers/clients and geographic locations;
3. Assess the adequacy of internal policies and procedures;
4. Test compliance with the relevant laws and regulations;

5. Test transactions in all areas with emphasis on high-risk customers/clients, products and services;
6. Assess employees' knowledge of the laws, regulations, guidance, and policies & procedures;
7. Assess the adequacy, accuracy and completeness of training programmes; and
8. Assess the adequacy of the process of identifying suspicious activity.

Role of Supervisory Authority[11]

The role and functions of the Supervisory Authority (SA) are provided for in the AML/CFT Act (Sections 22 and 23). The functions of the SA include, but are not limited to, the following:

a) Assess the ML/TF/PF risks associated with the Sector;
b) Examine, regulate, supervise and train the reporting entities on their obligations;
c) Issue instructions, guidelines or recommendations to the reporting entity;
d) Cooperate and share information with competent authorities;
e) Submit STRs to FIU if upon examination of a reporting entity, it finds reasonable grounds for suspicion of ML/TF/PR other crimes is found;
f) Submit examination reports findings and information on sanction imposed on reporting entities to the FIU;
g) Maintain statistics of onsite/offsite or desk-based examinations;
h) Enter the premises of the reporting entity and, among other functions, observe the way in which certain functions are undertaken; and
i) Impose sanctions for non-compliance with the AMLCFT obligations.

- **Supervisory Authority: Sanctions**

The SA is vested with the power to impose sanctions under Section 23 of the AMLCFT Act where the reporting entity has been found to be non-compliance with the provisions under Sections: 15, 16, 18, 19 and 20. The possible sanctions include the following:

a) Written warnings;
b) Order to comply with specific instructions;
c) Instruct the organization on measures it is taking;
d) Prohibit convicted persons from employment within the sector;
e) Recommend to the appropriate licensing authority/Registration authority to suspended, restricted or withdrawn; and

[11] Sections 22 & 23 AMLCFT Act Cap. 10:11 (as amended) provide further details on the role and powers of the Supervisory Authority.

f) In the case of default attributable to directors and senior management of a reporting entity, direct the reporting entity to remove them from the Board or relieve them from their functions to which the default is related; additionally, supervisory authorities shall impose a monetary fine of not less than five million dollars nor more than fifteen million dollars.

Section 23(2) AMLCFT Act also has a general provision, which creates an offence for a reporting entity, where any of its directors, managers, officers or employees who breaches its obligation under this Act, and where no penalty is provided, shall be liable on summary conviction to a fine of not less than five million dollars nor more than fifteen million dollars and to imprisonment for a term not exceeding three years, and in the case of a body corporate to a fine of not less than fifteen million dollars nor more than forty million dollars.

- **Expectations of the reporting entity - SA Examination**

The reporting entity is expected to be aware of any scheduled AMLCFT Examination to be conducted by the SA. Training for staff/relevant member (as the case may be) is therefore important to prepare them for such examinations.

The reporting entity must also ensure it keeps and maintains records of those AMLCFT examinations. All reports of findings, recommendations and/or follow-up actions taken or to be undertaken by the reporting entity following the SA's examination should be accurately and safely maintained.

AML/CFT Provisions relating to certain Professions & ML/TF Risks associated therewith

The Money Laundering and the Terrorism Financing (ML/TF) risks associated with independent professions lie basically in the potential misuse of these professions, to conceal the identities of the beneficial owners of the transactions done through or with them.

Countries are therefore required to impose certain obligations on these categories of reporting entities to mitigate ML/TF risks posed when they carry out the activities specifically identified within the FATF 40 Recommendations.

ML/TF activities are possible through the financial sector and DNFBPs. This makes it necessary for AMLCFT preventative measures to be applicable to both categories of Reporting Entities.

This includes professions such as Attorneys-at-Law, Notaries, Commissioners of Oaths to Affidavits, Accountants and Auditors, Trusts and Company Service Providers, when they carry out specified activities for or on behalf of their client (as expressed in the AMLCFT Act).

The AMLCFT provisions do not apply where the professional is employed within the public service, public authority or in-house counsel, and where the nature of work of these professionals do not involve the specified activities outlined in the Act.

The AMLCFT Act at Section 18(11) Cap. 10:11 provides that subsections (4), (9) and (10) are applicable to Attorneys-at-law, Notaries, Commissioners of Oaths to Affidavits, Accountants and Auditors, when they provide the specified services as outlined above.

In summary, subsection 4 provides, inter alia, that these professionals must take reasonable measures to-

- ascertain the purpose of the transaction,
- the origin and destination of the funds,
- identify and obtain the address of the beneficiary of the fund
- and submit reports to the FIU - if based on reasonable grounds, a transaction is suspicious and the funds associated with the transaction(s) are connected to criminal activity, money laundering or proceeds of crime; and

Subsections 9 and 10 require, among other things, these professionals to provide further information, if requested by the FIU, on the suspicious transactions submitted. The FIU may direct the professional (based on the FIU's assessment of the transaction) to cease with carrying out the transaction with the client for a period that may be determined by the FIU.

▪ Legal Professional Privilege

According to Section 18(12), nothing in the Act requires any **attorney-at-law** to disclose any privileged communication. Pursuant to Section 18(13), for the purposes of this section, a communication is a privileged communication **only if**-

a) it is to a person who is a professional legal adviser and the disclosure falls within paragraph (b);
b) a disclosure falls within this subsection if it is a disclosure-

(i) to a professional legal adviser (or a representative of the professional legal adviser) of the client in connection with the giving of legal advice to the client by the Legal Adviser; or

(ii) to any person in connection with legal proceedings or contemplated legal proceedings;

(iii) A disclosure does not fall within this subsection if it is made with the intention of furthering a criminal purpose.

Legal professional privilege should be construed in accordance with the AML/CFT Act, the Legal Practitioners Act Chapter 4:01, the amendments made under those Acts, including the ethical obligations outlined in the Code of Conduct/Rules (in the Fourth Schedule of the Legal Practitioners (Amendment) Act No. 26 of 2010).

If, as an Attorney-at-Law, a suspicion is formed of money laundering or terrorist financing, there is need to carefully consider: how to handle the situation to avoid disclosing any information, which is likely to prejudice an investigation; and whether or not to make a report in light of the legal privilege exception.

Money Laundering and Terrorist Financing - Red Flags

Professions [12]

Client is secretive or evasive about -

- its identity or that of its beneficial owner;
- the source of funds or money; or
- why the client is doing the transaction in a specific manner:
- the client is known to have convictions, or to be currently under investigation for, acquisitive crime or has known connections with criminals;
- related to or is a known associate of a person listed or suspected as being involved with terrorists or terrorist financing operations;
- involved in a transaction that involves a highly technical regulatory regime that imposes criminal sanctions for breaches (increasing the risk of a predicate offence being committed); or is unusually familiar with the ordinary standards provided for by the law in satisfying customer identification, data entries and STRs, or asks repeated questions on related procedures.

[12] "A Lawyer's Guide to Detecting and Preventing Money Laundering"- A collaborative publication of the International Bar Association, the American Bar Association and the Council of Bars and Law Societies of Europe, October 2014);
Professionals include Attorneys-at-law, Notaries, Accountants, Auditors, commissioners of Oaths to Affidavits and Trust and company Service Providers.

- Use of intermediaries without good reason
- Avoidance of personal contact for no good reason
- Reluctance to disclose information, data and documents that are necessary to enable the execution of the transaction - Use of false or counterfeit documentation
- The client is a business entity that cannot be found when conducting searches on open sources e.g. internet web searches
- The relationship between the client and counter parties - ties between the parties of a family, employment, corporate or any other nature generate doubts as to the real nature/ reason for transaction
- Multiple appearances of the same parties in transactions over a short period of time
- The parties attempt to disguise the real owner or parties to the transaction
- The natural person acting as a director or representative does not appear to be a suitable representative
- The parties, their representatives, the beneficial owners or intermediary companies in the chain of ownership of legal entities, are native to, resident in, or incorporated in a higher ML/TF risk country, and the transactions or connections appear to be illogical or do not make business sense.

Real Estate Agents/House Agents/Housing Developers

- Customer purchases property in the name of a nominee such as an associate or a relative (other than a spouse), or in the name of minors or incapacitated persons or other persons who lack the economic capacity to carry out such purchases.
- Customer does not want to put their name on any document that would connect them with the property or uses different names on offer letters to Purchase; or closing documents and deposit receipts.
- Customer attempts to hide the identity of the beneficial owner or requests that the transaction be structured to hide the identity of the beneficiary.
- Buyer is a shell company and representatives of the company refuse to disclose the identity of the beneficial owner.
- Address given by customer is unknown, believed to be false, or simply a correspondence address.
- Customer does not satisfactorily explain the last-minute substitution of the purchasing party's name.
- Customer pays substantial down payment in cash and balance is financed by an unusual source or offshore bank.
- Customer purchases property without inspecting it.
- Customer purchases multiple properties in a short time period, and seems to have few concerns about the location, condition and anticipated repair costs, etc., of each property.

- Customer pays rent or the amount of a lease in advance using a large amount of cash.
- Customer is known to have paid large remodelling or home improvement invoices with cash, on a property for which property management services are provided.
- Transaction does not match the business activity known to be carried out by the customer.
- Transaction is entered into at a value significantly different (much higher or much lower) from the real or market value of the property.
- Property is sold in a series of successive transactions each time at a higher price between the same or connected parties.
- Buyer takes on a debt significantly higher than the value of the property.
- Customer suddenly cancels/ aborts transaction and requests refund either back to himself/herself/itself or to a third party.

Dealers in Precious and Semi-Precious Stones and Metals

- Transactions that are not consistent with the usual profile of a customer:
- Transactions that appear to be beyond the means of the customer based on his/her stated or known occupation or income; or
- Transactions that appear to be more than the usual amount for a typical customer of your business.
- Transactions where customer does not consider the value, size and/or colour of the precious stone, precious metal, or precious product.
- Unusual payment methods, such as large amounts of cash, traveller's cheques, or cashier's cheques.
- Large or frequent transactions that are in a foreign currency.
- Numerous transactions by a customer, especially over a short period of time, such that the amount of each transaction is not substantial (e.g. below the regulatory threshold for customer due diligence), but the cumulative total of which is substantial.
- Payments received from a third party, who is not the owner of the funds, without legitimate business purpose;
- Precious stones/metals product delivered to a third party, who is not the owner or payer of funds, without legitimate business purpose.
- The customer enquiry about refund policies and requests for large refunds subsequently.
- The customer is suspected to be using forged, fraudulent or false identity documents for due diligence and record keeping purposes.
- The customer is unusually concerned with the AML/CFT policies and procedures.
- The customer pays for precious metals, precious stones or precious products with cheques, but noted on the cheque that the payment is for something else.

- **The Gambling Sector (Casinos /Betting Shops/ Lotteries)**

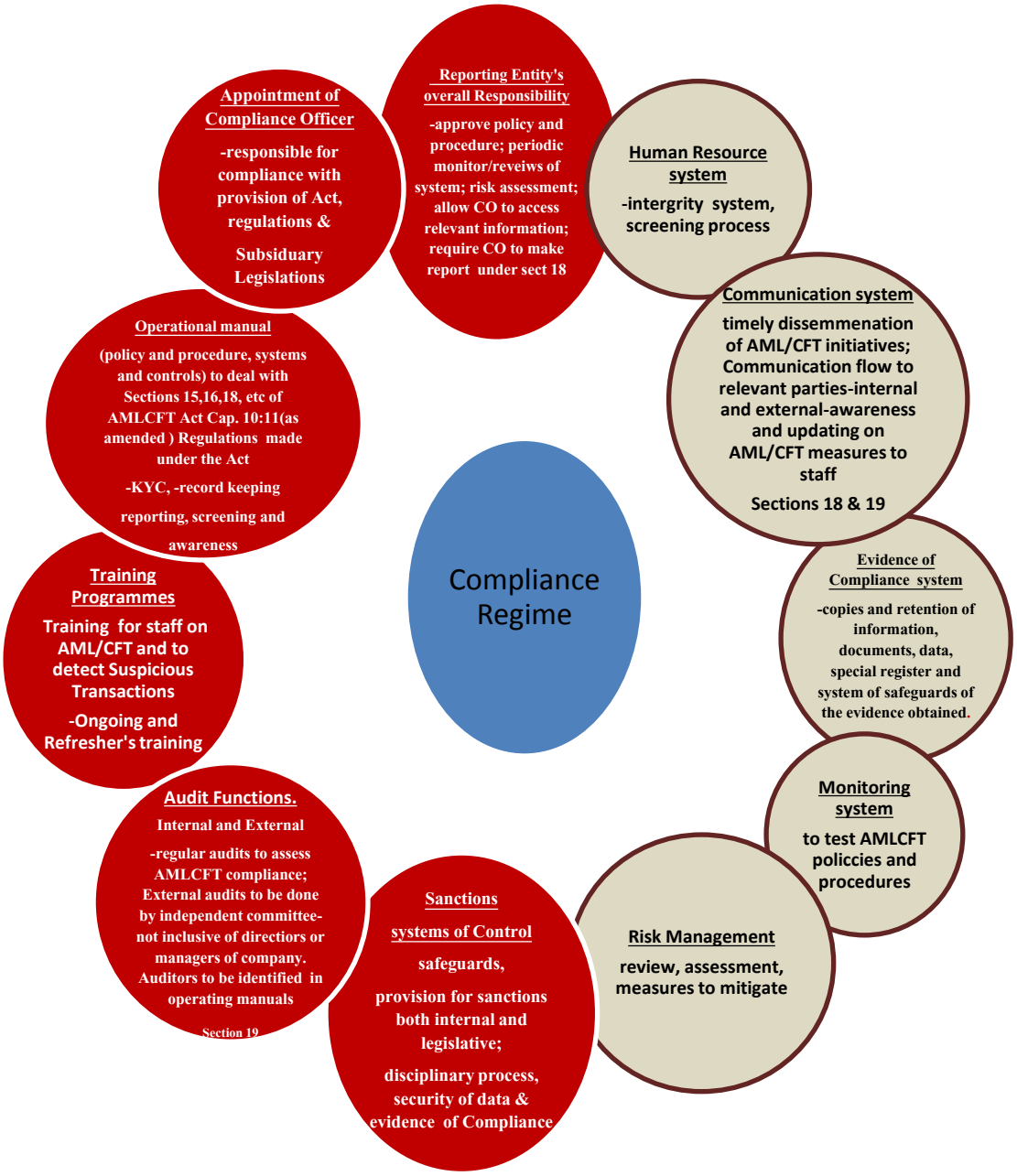
- Gamblers who don't gamble much despite large purchases of chips which are usually returned for a refund payable via a check;
- Not willing to offer personal information when asked;
- Make bets that cancel each other out such as betting on both red and black at the same time in roulette.

- **Used Car or Car Parts Dealers**

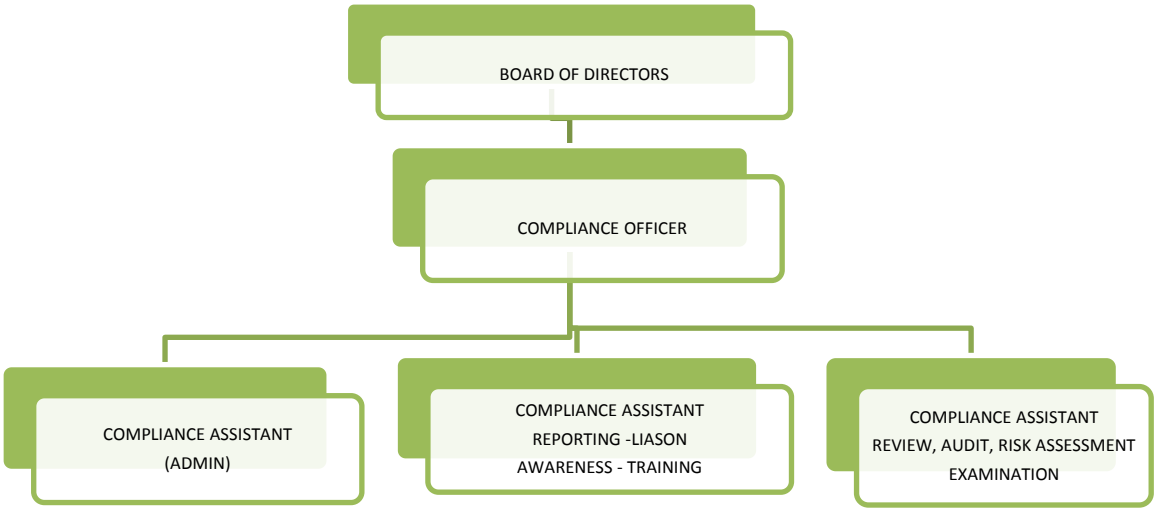
- Customer attempts to purchase vehicle with a significant amount of cash.
- Customer is reluctant or refuses to produce personal identification documents for the transaction to be completed.
- Customer pays substantial down payment in cash and balance is financed by an unusual source for example a third party or private lender.
- Purchases carried out on behalf of persons who appear to lack the economic capacity to make such purchases.
- Last minute cancellation of order, which means that funds would have to be reimbursed to the customer via a business cheque.
- Customer purchases vehicle without inspecting it.
- Customer purchases multiple vehicles in a short time period, and seems to have few concerns about the type, cost, condition, etc.
- Customer purchases vehicles and registers them for “Rental”.
- Customer is known to have a criminal background or to be an associate of known criminals.
- Customer uses or produces identification documents with different names.
- Customer does not want to put his/her name on any document that would connect him/ her with the purchase of the vehicle.
- Purchase appears to be beyond the means of the Customer based on his/her stated or known occupation or income.

Appendices

Diagram Showing the main features of an AMLCFT Compliance Regime



Sample: Structure of Compliance Department- (Medium to large reporting entity)



Sample -Structure of Compliance Department (small reporting entity)