



**ANTI-MONEY LAUNDERING, COUNTER
FINANCING OF TERRORISM AND
COUNTERING PROLIFERATION
FINANCING POLICY**

2020

Policy Control Sheet

Title: Anti-Money Laundering, Counter Financing of Terrorism and Countering Proliferation Financing Policy

Version: 02

Effective Date: April 2022

Author: Compliance Unit

Review Date: January 2023

Amendment History (Where applicable):

Version Number	Effective Date	Brief description of amendments
2	April 2022	Elaboration and alignment of provision to the AMLCFTA 2020 and PTA 2021 and the BO Act 2020 and international standard.

Contents

I.	List of Acronyms	1
II.	Definitions	2
III.	Policy Statement	6
IV.	Policy objective	6
V.	Purpose of the Policy	6
VI.	Scope of the Policy	6
VII.	Applicability of the Policy	6
VIII.	Performing Due Diligence	7
	1. Process of performing Due diligence	7
	2. Documentation requirement	7
	3. Specificities of documents	8
	4. Verification of documents	9
	5. Screening	9
IX.	Risk Profile	9
	1. Risk Assessment	9
	2. Approval of the risk rating	9
	3. Treatment of the different types of risk rating	9
X.	Sanctions	11
XI.	Obligation to monitor counterparty activities and transactions	12
XII.	Retention of Records	13
XIII.	Obligation to report suspicious/ Unusual Transaction	13
XIV.	Opening and maintaining of business relationship in legal name	14
XV.	Business relationship with other entities	14
XVI.	Obligation to cease transaction	14
XVII.	Tipping off	15
XVIII.	Terrorist Financing	16
XIX.	Proliferation Finance	16
XX.	Request for information	16
XXI.	Roles and responsibilities	17
XXII.	AML/CFT Enterprise Wide-Risk Assessment	18
XXIII.	Reporting to the ARC	18
XXIV.	Training and development	18
XXV.	Confidentiality	18
XXVI.	Breach of Policy	18
XXVII.	Procedure Manual	18
XXVIII.	Review of Policy	18
XXIX.	Approval of Policy	19
	Annex 1 Assessment of risks	20
	Annex 2 Definition and treatment of Politically Exposed Person	23
	Annex 3 Determination of a beneficial owner	24
	Annex 4 Guidance on financing of terrorism	27

I. List of Acronyms

AML	Anti-Money Laundering
AMLCFTA	Anti-Money Laundering and Countering the Financing of Terrorism Act 2020
ARC	Audit and Risk Committee
BDC	Bureau De Change
BO	Beneficial Owner
BOA	Beneficial Ownership Act 2020
CDD	Counterparty Due Diligence
CEO	Chief Executive Officer
CFT	Countering Financing of Terrorism
CPF	Counter Proliferation Financing
CPU	Compliance Unit
DBS	Development Bank of Seychelles
EDD	Enhanced Due Diligence
FATF	Financial Action Task Force
FI	Financial Institution
FIA	Financial Institutions Act
FIU	Financial Intelligence Unit
HFC	Housing Finance Company
IAD	Internal Audit Division
IC	Investment Committee
ID	Identification Document
IMF	International Monetary Fund
KYC	Know Your Counterparty
MER	Mutual Evaluation Report
ML	Money Laundering
NGO	Non-Governmental Organisation
PC	Procurement Committee
PEP	Politically Exposed Person
PF	Proliferation Financing
PTA	Prevention of Terrorism Act
RBA	Risk-Based Approach
RMC	Risk Management Committee
RMU	Risk Management Unit
SDD	Simplified Due Diligence
TF	Terrorist Financing
The Bank	Central Bank of Seychelles
The Board	Board of Directors of the Bank

II. Definitions

1. **Anti-Money Laundering** refers to a set of laws, regulations, and procedures intended to prevent criminals from disguising illegally obtained funds as legitimate income.
2. **Approval Authority**
 - shall mean:
 - a. The Board shall approve:
 - license of operations of Financial and Non-financial institutions (i.e. banks, financial leasing, payment service providers and,), and Non-Bank Credit Institutions;
 - External asset managers in G-7 countries with client asset in excess of US\$ 1,000 million or equivalent for the purpose of managing part of the reserves;
 - Global custodians with assets under custody in excess of US\$ 1,000,000 million for safe-keeping of assets held in the reserves.
 - b. The Governor and in the absence of the Governor, the CEO shall approve:
 - license of BDC and appointment of administrators;
 - Approval of new activity of existing financial institution
 - counterparties base on recommendation of the PC.
 - c. PC shall approve:
for activities that have gone through the procurement process, who in turn will recommend approval to the Governor or Board.
 - d. IC shall approve the following:
 - Central banks, commercial banks, other financial institutions and commercial entities as providers of investment products and services, within eligible asset classes and risk limits specified by the Investment Policy;
 - Brokers listed in the list of primary dealers of the central banks or governments, relating to the eligible asset classes specified by the Investment Policy, such as the Federal Reserve Bank of New York;
 - Issuers of Sovereign, Supranational and Agency (SSA) Securities in line with the eligible asset classes and risk limits specified by the Investment Policy;
Other commercial and investment banks in the capacity of third-party service providers, in line with the eligible asset classes and risk limits specified by the Investment Policy.
3. **Beneficial Owner** means a natural person or persons who ultimately owns or controls a counterparty or the natural person on whose behalf a transaction is being conducted and includes those who exercise ultimate effective control over a legal person or arrangement. See **Annex 3** for further details.
4. **Counterparty** shall include but not limited to
 - suppliers
 - contractors
 - consultants
 - service providers
 - government ministries
 - government agencies
 - entities regulated by the Bank
 - pension funds
 - parastatal bodies
 - international financial organisation
 - investors and prospective investors

- international financial institutions that engage with the Bank in reserves management activities.

and any other person whose relationship, existing or prospective, with the Bank might expose the Bank to risks associated to ML, TF and PF. These risks include ML and TF. As the Bank acts as banker to the government, the beneficiary of the transactions in this instance shall fall under the definition of counterparty.

5. Counterparty Due Diligence

The divisions/units shall apply due diligence measures in respect of counterparties, business relationships and transactions, and conduct ongoing monitoring of business relationships.

These measures include:

- identifying the counterparty identity on the basis of documents, data or information obtained from a reliable and independent source or any other source that the reporting entity has reasonable grounds to believe and can be relied upon to identify and verify the identity of the counterparty;
- obtaining the identity of the beneficiary of the investment-related policies managed by the Bank, benefactors under the policy and the verification of person or a legal person or a legal arrangement shall be carried out and if the division/unit is unable to obtain such information, it shall prepare and submit a suspicious transaction; and send to CPU for onward transmission to FIU;
- where the counterparty is not the BO, identify the BO, and take reasonable measures, on a risk-sensitive basis, to verify the identity of the BO, including, in the case of a legal person, partnership or trust through the following information:
 - i. the identity of the natural person who ultimately has a controlling ownership interest;
 - ii. the identity of the natural person exercising control through other means;
 - iii. the identity of the relevant natural person who holds a senior management position;
- obtaining information on the purpose and intended nature of the business relationship and to establish details of the business of the counterparty or a BO to enable the division/unit to identify:
 - i. complex or unusual large transactions;
 - ii. unusual patterns of transactions which have no apparent economic or visible lawful purpose; or
 - iii. any other activity which may be, by its nature, likely to be related to ML, financing of terrorism or other criminal conduct; and
- take reasonable measures to ascertain the purpose of a one-off transaction and the origin and ultimate destination of funds involved in a one-off transaction or transfer as part of a business relationship.

6. Enhanced due diligence

means heightened processes the Bank must implement to counteract the risk associated with higher-risk counterparties. Counterparties that pose higher ML or TF risks presents an increased risk exposure to the Bank and its stakeholders. Due diligence policies, procedures, and processes should be enhanced as a result.

7. Financial sanctions

are restrictions put in place, e.g. by the UN, EU, UK or US, to achieve a specific foreign policy or national security objective.

They can:

- limit the provision of certain financial services;
- restrict access to financial markets, funds and economic resources.

Financial sanctions are generally imposed to:

- coerce a regime, or individuals within a regime, into changing their behaviour (or aspects of it) by increasing the cost on them to such an extent that they decide to cease the offending behaviour;
- constrain a target by denying them access to key resources needed to continue their offending behaviour, including the financing of terrorism or nuclear proliferation;
- signal disapproval, stigmatising and potentially isolating a regime or individual, or as a way of sending broader political messages nationally or internationally; and/or
- protect the value of assets that have been misappropriated from a country until these assets can be repatriated.

8. International Organisation

International organisations are entities established by formal political agreements between their member States that have the status of international treaties; their existence is recognised by law in their member countries; and they are not treated as resident institutional units of the countries in which they are located. Examples of international organisations include the United Nations and affiliated international organisations such as the International Maritime Organisation; regional international organisations such as the Council of Europe, institutions of the European Union, the Organization for Security and Cooperation in Europe and the Organization of American States; international military organisations such as the North Atlantic Treaty Organization (NATO), and economic organisations such as the World Trade Organisation or the Association of Southeast Asian Nations, etc.

9. Key controller

Key Controller is someone who is elected or appointed to exercise direct control over the counterparty entity, by participating in the governance or senior executive activities of the counterparty.

Key Controllers typically set the strategic direction of the entity. The title given to a Key Controller varies according to the type of entity, Country of Operation, and Country of Incorporation/ Registration/ Formation. Most commonly, a Key Controller will include the Chief Executive Officer (CEO), Chief Financial Officer (CFO), Managing Partner, Chairman of the Board and Directors. Usually, control is exercised jointly with other Directors/senior executive management.

10. Legal Arrangement

means a partnership of persons, a trust or similar arrangement or any person holding assets in a fiduciary capacity and any other similar entity or arrangement.

Legal Arrangement being:

- a. A resident trustee of an international trust under the International Trusts Act;
- b. A general partner of a limited partnership under the Limited Partnerships Act.

11. Legal Person

means any entity other than a natural person that can establish a counterparty relationship with a financial institution or otherwise own property and the term legal entity shall be construed accordingly.

Legal person being:

- a. A company including overseas company;
- b. An association;
- c. An international business company;
- d. A protected cell company;
- e. A company incorporated under Companies (Special Licenses) Act;
- f. A partnership;
- g. A foundation.

12. Money Laundering

is the processing of criminal proceeds to disguise their illegal origin. The goal of a large number of criminal acts is to generate a profit for the individual or group that carries out the act. This process is of critical importance, as it enables the criminal to enjoy these profits without jeopardising their source. (FATF)

13. Payment Service Providers

Shall mean an entity providing the following services

- a. services enabling cash deposits and withdrawals;
- b. execution of payment transactions;
- c. issuing and/or acquisition of payment instruments;
- d. money remittances; and
- e. any other services functional to the transfer of money. This shall also include the issuance of electronic money and electronic money instruments. The term does not include the provision of solely online or telecommunication services or network access.

14. Politically Exposed Person

is an individual who is or has been, during the preceding three years, entrusted, with a prominent public function, and includes any immediate family member or close associate of such an individual. This includes foreign PEPs, domestic PEPs and persons entrusted with a prominent function by an international organisation.

15. Proliferation

is the act to manufacture, acquisition, possession, development, export, transshipment, 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 national laws or, where applicable, international obligations. Includes technology, goods, software, services or expertise.

16. Proliferation Financing

is the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, transshipment, 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 national laws or, where applicable, international obligations. (FATF)

17. Sanction Screening

is a control employed to detect, prevent and manage sanctions risk. Screening should be undertaken as part of an effective due diligence program, to assist with the identification of sanctioned individuals, organisations and countries, as well as the illegal activity to which FIs may be exposed. It helps identify areas of potential sanctions concern and assists in making appropriate compliant risk decisions.

18. Simplified due diligence

means the level of due diligence that can be completed on a counterparty which is commensurate with a lower level of risk of ML or terrorist financing.

19. Terrorist Financing

The international Compliance Association describe it as the provision or collection of funds with the intention that they should be used (or in the knowledge that they are to be used) to carry out acts that support terrorists or terrorist organisations or to commit acts of terrorism. (ICA)

III. Policy Statement

The Bank recognises its role in combating ML, TF and PF activities. The Bank holds itself to the highest standards of integrity in the conduct of its engagements to fulfil its role as an accountable institution and a supervisory body in terms of the AMLCFTA, the PTA, the BOA and the international standards.

IV. Policy objective

The objective of the Policy is to document the commitment of the Bank to the fight against ML, FT and PF.

V. Purpose of the Policy

The aim of the policy are as follows:

1. To establish the responsibility of the Bank in terms of AML and TF control measures;
2. To align control measures of the Bank to the obligations of reporting entities under the AML, CFT and CPF legislations and standards;
3. To define the extent to which the Bank will carry out its CDD using the Risk-Based Approach;
4. To establish the standards, approach and processes, in accordance with best practice specified in local and international standards;
5. To provide a baseline from which procedures should be developed by divisions/units on reporting of suspicious and/or unusual transactions and implementing AML, CTF and CPF framework.

VI. Scope of the Policy

This Policy is applicable to the Board, all divisions, units and staff of the Bank and shall be applied in all relevant activities and engagements by the Bank.

VII. Applicability of the Policy

This Policy shall be applicable to the following categories of activities:

1. Procurement of services and goods from suppliers, consultants etc;
2. Procurement of services from FIs;
3. Licensing of banks, BDC, financial leasing companies, payment systems service providers and other activities licensable by the Bank;
4. on all transactions being processed by the Bank.
5. Issuance and management of securities being issued by the Bank;
6. Appointment of any individual or entity to act on behalf of the Bank;
7. Engagement with firms for reserves management activities;
8. Acceptance of demonetised currency from public and institutions;
9. Sale of numismatic items to the individuals and entities;
10. Any activity that presents a risk of ML, TF and PF.

VIII. Performing Due Diligence

1. Process of performing Due diligence

Due diligence has to be performed before or during the course of establishing a business relationship or carrying out a one-off transaction in respect of the counterparty, the business relationships and transactions. It should not be contemplated as a one-time exercise.

The due diligence process includes the following:

- a. Obtain documents to identify the counterparty and verify the identity of the counterparty.
- b. Obtain information on the purpose and intended nature of the business relationship or the one-off transaction.
- c. Ascertain the origin and the ultimate destination of funds in a one-off transaction or transfer as part of a business relationship.
- d. Screen all parties to ensure that they are in good standing and to find any adverse information.
- e. Conduct ongoing monitoring of the business relationship to observe any change in status and the level of risk to the Bank.
- f. Assign a rating to implement RBA. CDD measures for each counterparty shall be commensurate with the rating assigned. Factors to determine the risk rating of counterparties are demarcated in **Annex 1** of this Policy.
- g. Take reasonable measures to understand:
 - i. the ownership and control structure; and
 - ii. determine the individuals who own or control the legal person or legal arrangement. This includes those who exercise ultimate effective control over a company.
- h. Identify PEPs when entering into a business relationship or carrying out a one-off transaction with a counterparty.
 - i. Identification shall take place during the following circumstances:
 - o Before on boarding a PEP as a counterparty;
 - o Before processing any transaction;
 - o Prior to initiating and during the preliminary evaluation of a procurement process;
 - o during the submission of documents to seek approval for licensable activities;
 - o during evaluation of choosing a counterparty engaging in reserves management activities;
 - ii. Once a PEP has been identified, a business relationship can only be established with the appropriate approval, and the division/unit shall take adequate measures to establish the source of funds (where applicable) involved in any proposed relationship or transaction.
 - iii. Where a PEP is identified, the division/unit shall apprise their respective committee (i.e. IC or PC where applicable), for approval for the engagement.
 - iv. As for existing relationship with a counterparty who has been identified as a PEP, the division/unit shall ensure that they have obtained all the necessary CDD, implement EDD and apply ongoing monitoring.

Annex 2 provides a detailed definition of PEP.

In the event the division/unit is not able to satisfy itself with the required CDD measures, business relationship should not be established and business transaction should not be carried out. Similarly, relationship with existing counterparty should be terminated if CDD is found to be unsatisfactory.

2. Documentation requirement

In order to fulfil the due diligence requirement, the potential counterparty or counterparty shall submit the following documentation.

#	Type of Counterparties	Documents Required
1.	Individuals / Sole proprietorship	<ul style="list-style-type: none"> i. Copy of valid ID (ID card or passport) ii. Business registration certificate iii. Copy of trading licence (if applicable) iv. Tax Clearance Certificate v. Proof of address
2.	Partnerships	<ul style="list-style-type: none"> i. Copies of ID of all partners, authorised signatories, and any Key Controllers. ii. List of authorised signatories iii. Tax Clearance Certificate iv. Copy of trading license and/or business registration certificate v. Proof of address
3.	Companies	<ul style="list-style-type: none"> i. Copy of ID/passports of all authorised signatories and Key Controllers. ii. List of all shareholders and ultimate BOs of shares stating the name and address. iii. Certificate of incorporation/ commencement of business iv. List of authorised signatories v. Copy of trading licence vi. Tax Clearance Certificate vii. Certificate of good standing from Registrar of Companies viii. Proof of Address.
4.	Clubs, Societies and Associations	<ul style="list-style-type: none"> i. Copies of ID for all Key Controllers and authorised signatories ii. Copy of certificate of registration iii. List of all board members stating the name and address iv. Proof of address
5.	Executor	<ul style="list-style-type: none"> i. Copy of ID of Executor ii. Copy of order of appointment

Note:

- Explicit requirement (such as it being notarised) of the division/unit must be adhered to at all times.
- Refer to **Annex 3** for determination of who is of a BO.

3. Specificities of documents

i. Identification document:

- a. For the types of Identification document, it shall be either the national ID card or passport in the case of a person based in Seychelles.
- b. In the case of a foreign person it shall be the passport.
- c. The identity document shall show clearly the picture and the number.
- d. The identity document shall still be valid and not have expired.

ii. Proof of address:

In the event that proof of address is required:

- a. The proof of Address shall be a utility bill or equivalent.
- b. It shall be where the entity operates.
- c. If the company operates at a residential domicile, it shall be of that.
- d. In the event that the company does not have a specific address of operation, the proof of address of the BO should be obtained.
- e. The proof of address of the BO should be obtained when required.
- f. The proof of address shall not be older than 3 months.
- g. The proof of address shall not be a postal order box number.

- h. The proof of address shall be a utility bill in the name of the company and/or the BO.
- i. In the event that the proof of address is not in the name of the BO (e.g. when renting), the owner of the accommodation shall certify that the entity/BO is renting the accommodation.

4. Verification of documents

The division/unit shall:

- a. verify the copies of all documents, where relevant, with the issuing authority in the country of issue;
- b. verify the given or mentioned references in the application with the said individual or entity;
- c. verify the source or existence of funds for transactions (where applicable).

The list is not comprehensive. The division/unit shall do the necessary verification as per their own procedural manuals in addition to the above.

5. Screening

Screening is an integral part of CDD measures.

The division/unit shall:

- a. carry out screening before and during the course of establishing a business relationship or carrying out a one-off transaction. The frequency of the screening shall depend on the risk profile.
- b. screen individual names, companies, groups, etc.;
- c. screen using the available tools available (i.e., World Check/Accuity, etc.);
- d. conduct an online search, especially for persons based in Seychelles as their information might not be available on World Check/ Accuity;
- e. analyse and record the results of the screening and review the risk profile of the entity or individual;
- f. Escalate the results and the analysis to the relevant approval authority for them to make an informed decision on the business relationship.

IX. Risk Profile

1. Risk Assessment

The division/unit shall assess all counterparties and assign a risk rating in accordance with **Annex 1**.

The assessment shall be conducted for new counterparties upon on-boarding and for existing counterparties at the earliest.

The risk ratings are low, medium or high, with low carrying the least risk and high carrying more risk. The division/unit will be able to focus resources to ensure that measures to prevent or mitigate ML, TF and PF are commensurate with the risks identified.

2. Approval of the risk rating

The divisions/units shall assign a rating to all counterparties and submit to the respective AA for approval.

3. Treatment of the different types of risk rating

The level of measures adopted is commensurate to the level of risk the entity presents. E.g. divisions/units shall adopt EDD measure for Counterparties that have been identified as higher risk, and SDD measures where counterparties identify as lower risks.

The division/unit should adopt the following treatment for each rating:

a. High risk counterparty:

A High-risk counterparty includes but is not limited to:

- i. Non-resident counterparty;
- ii. Non-legal persons or arrangements including non-governmental organisations (NGOs) and Trusts/ charitable trusts;
- iii. High net worth counterparties;
- iv. Counterparty dealing in high-value items;
- v. PEPs: EDD and enhanced ongoing monitoring (on a risk-sensitive basis) are required whenever a counterparty, or any BO of a counterparty, is or becomes a PEP. The division/unit should have a risk management system in place to determine if prospective or existing counterparties are PEPs. That determination is complicated by the fact that the definition of a PEP includes close family members and associates, who may have different names and may not publicise the fact of their association with the relevant individual. **Annex 2** provides an elaborated definition of PEP.
- vi. Counterparties from or in countries where CDD and AML regulations are lax and have significant strategic deficiencies in their regimes to counter ML, TF, PF, drug trafficking, human trafficking, corruption and other crimes (financial or otherwise);
- vii. persons from, and transactions in, countries which do not apply or fully apply the Financial Action Task Force Recommendations.
- viii. Counterparties who have been declined by another regulatory institution, including professional bodies, conviction, (based on reliable and verifiable information from independent sources); and
- ix. Counterparties that are on the sanctions lists or are based in a country on the sanctions lists, or have embargoes or similar measures issued e.g. by the UN.

The division/unit is required to conduct EDD and enhanced ongoing monitoring for the counterparties listed above.

EDD and Ongoing monitoring of a business relationship entails:

- i. Scrutinising all documents that have been provided and verification is at the utmost important;
- ii. Scrutinising transactions undertaken throughout the relationship to ensure that the transactions are consistent with the division/unit's knowledge of the counterparty, the business and risk profile and the source of funds of the counterparty; and
- iii. Keeping the documents, data or information obtained for the purpose of applying CDD measures up to date;
- iv. The division/unit shall apply on a risk-sensitive basis EDD measures and enhanced ongoing monitoring in any other situation which by its nature presents a higher risk of ML, terrorist financing activities or other criminal conduct on the basis of the national risk assessment;
- v. The division/unit shall review the profile every year at a minimum.

Examples of EDD:

- o obtaining additional identifying information from a wider variety or more robust sources and using the information to inform the individual counterparty risk assessment;
- o carrying out additional searches (e.g., verifiable adverse media searches) to inform the individual counterparty risk assessment;
- o commissioning an intelligence report on the counterparty or BO to ascertain whether the counterparty or BO may be involved in criminal activity;
- o verifying the source of funds or wealth involved in the business relationship to be satisfied that they do not constitute the proceeds from crime;
- o seeking additional information from the counterparty about the purpose and intended nature of the business relationship.

b. Medium risk counterparty

The division/unit should apply normal CDD.

Normal CDD entails:

- a. Obtaining all the documents before entering into a business relationship
- b. Verification and screening is done before entering into a business relationship.
- c. Verification can be done obtaining information from local and reputable sources.
- d. Understanding the source of funds (where applicable).

Examples of medium risk:

- o might be where the profile of counterparty is uncertain and/or doubtful and not all information is immediately verifiable.
- o Where not all information are readily available upon request or in the submission.

c. Low risk counterparty:

For low risk counterparties, the division/unit may apply simplified CDD measures in relation to a particular business relationship or transaction if it determines that the business relationship or the transaction presents a low degree of risk of ML and TF activities.

Where there is a suspicion of ML and terrorist financing activities, reporting entities shall not apply SDD measures.

A counterparty may be considered under low risk category, if the identity of the counterparty and the BO of a counterparty are publicly known or where adequate checks and controls exist.

The division/unit are recommended to review the profile every four (4) years at a minimum.

The following Counterparties may be considered as low risk, for application of simplified or reduced CDD:

- i. Financial institutions, provided they are subject to requirements to combat ML and TF and are supervised for compliance with those requirements; and
- ii. Public listed companies on the stock exchange that are subject to regulatory disclosure requirements, Government administrations/ entities.

Examples of SDD measures include:

- o Verifying the identity of the counterparty and the BO after the establishment of the business relationship (e.g. if it is a well-known company and no negative information that is public knowledge).
- o Reducing the frequency of counterparty identification updates.
- o Reducing the degree of ongoing monitoring and scrutinising transactions, based on a reasonable monetary threshold.
- o Not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but inferring the purpose and nature from the type of transactions or business relationship established.

X. Sanctions

The Bank prohibits and will not facilitate any activity with governments or parties within certain geographies targeted under the sanction programs of the United Kingdom (UK), the European Union (EU), the United States (US) or the United Nations (UN).

The Bank shall not engage in any transaction that involves (directly or indirectly) or is for the benefit of any sanctioned parties. Sanctioned parties are defined as:

- a. parties that any one or more of the UK, EU, US or the UN has listed as the target or subject of sanctions; or
- b. parties which have been internally identified as presenting an unacceptable level of sanctions risk to the Bank.

In order to fulfil this obligation, divisions/units must:

- a. Screen counterparties and transactions against the sanctions lists issued by the UN, the EU, and/or the US.
- b. not engage or process transactions that:
 - i. may violate the applicable sanctions laws, whether directly or indirectly.
 - ii. involve individuals, entities or vessels listed on an official sanctions list by the UN, EU, OFAC or the local regulatory sanctions list whether directly or indirectly.
 - iii. involve individuals or entities residing in, or operating from a sanctioned country/location.
 - iv. may potentially circumvent applicable sanctions laws or contravene the spirit of such sanction laws.
- c. Block or reject transactions where the Bank is obligated to do so or where the transactions are not within the risk appetite of the Bank¹.

Counterparties may be required to furnish the Bank with additional information as and when necessary for the Bank to fulfil this requirement.

XI. Obligation to monitor counterparty activities and transactions

Reporting entities are obligated to conduct ongoing monitoring of a business relationship. This requires that they:

- i. scrutinise transactions undertaken throughout the relationship to ensure that the transactions are consistent with the reporting entity's knowledge of the counterparty, the business and risk profile and the source of funds of the counterparty; and
- ii. keep the documents, data or information obtained for the purpose of applying counterparty due diligence measures up to date.

Accordingly, the Bank shall also monitor the activities and transactions of its counterparties.

- a. The divisions/units shall pay special attention to:
 - i. any complex, unusual or large transaction;
 - ii. any unusual pattern of transactions;
 - iii. business relations and transactions with persons in jurisdictions that do not have adequate systems in place to prevent or deter ML or financing of terrorism;
 - iv. electronic funds transfers that do not contain complete originator information;
 - v. examine as far as possible the background and purpose of the transactions or business relations and record its findings in writing; and
 - vi. upon request, make available such findings to the FIU or to the Attorney-General to assist them in assessing an offence of ML or TF activities.
- b. The divisions/units shall screen cross-border payments.

Screening cross-border payments prior to completing the transaction is common practice and known as screening in real-time. By contrast, screening domestic payments in real-time may be unnecessary where, the entities are subject to the same local regulatory requirements, including the jurisdictions' local sanctions and KYC requirements when on-boarding clients. The Bank is adequately equipped with screening tools and these should be taken advantage of. An e.g. of cross-border screening would be done when uploading the payment instruction through SWIFT which automatically screens all mentioned entities and beneficiaries.

¹ The Bank recognises that the Government has to make stipend payment for students on Government scholarships and tuition fees in Cuba. The Bank will assist the Government with these payments provided

- a. the receiving bank or beneficiary in Cuba is not a sanctioned entity or linked to a sanctioned entity; and
- b. the correspondent banks are willing to conduct the transaction.

XII. Retention of Records

- I. The division/unit shall maintain records of:
 - a. CDD measures, including account files, business correspondence and copies of all documents evidencing the identities of counterparties and BOs; including the records and the results of any analysis undertaken in accordance with the provisions of the AMLCFTA;
 - b. all transactions carried out both domestically and internationally by it and correspondence relating to the transactions as is necessary to enable any transaction to be readily reconstructed at any time by the FIU or the Attorney-General, and the records shall contain particulars sufficient to identify:
 - i. the nature and date of the transaction;
 - ii. the type and amount of currency involved;
 - iii. the type and identifying number of any account with the entities involved in the transaction;
 - iv. if the transaction involves a negotiable instrument other than currency, the name of the drawer of the instrument, the name of the institution on which it was drawn, the name of the payee (if any), the amount and date of the instrument, the number (if any) of the instrument and details of any endorsements appearing on the instrument;
 - v. the name and address of the reporting entity, and of the officer, employee or agent of the reporting entity who prepared the record;
 - c. all reports made to the FIU; and
 - d. enquiries relating to ML and TF activities.
- II. The records mentioned in subsection (I) shall be kept for a minimum period of **7 years** (physical) from the date:
 - a. on which evidence of a person's identity is obtained;
 - b. of any transaction or correspondence relating to a counterparty; or
 - c. on which the business relationship ceases.
- III. Notwithstanding any other law, the records mentioned shall be kept for a period of **30 years** in digital form, from the date on which the business relationship ceases.
- IV. The records established and maintained for purposes of (I)(b) shall be:
 - a. sufficient to enable the transaction to be readily reconstructed at any time by the FIU or the Attorney-General to provide, if necessary, evidence for the prosecution of any offence;
 - b. maintained in a manner and form that will enable the reporting entity to comply immediately with requests for information from the law enforcement agencies or the FIU.
- V. Where any record is required to be kept under AMLCFTA, a copy of it with the appropriate back-up and recovery procedures shall be kept:
 - a. in a machine-readable form, if a paper copy can be readily produced from it; or
 - b. in an electronic form, if a paper copy can be readily produced from it and in a manner that enables appropriate authentication.
- VI. The records maintained under subsection (I.) shall be made available upon request to the FIU or the Attorney-General.

XIII. Obligation to report suspicious/ Unusual Transaction

Where a staff has:

- a. reasonable grounds to suspect that any service, or transaction may be related to the commission of criminal conduct including an offence of ML or of TF activities; or to money or property that is or represents the benefit of criminal conduct;
- b. information that may be:
 - i. relevant to an act preparatory to an offence or to money or property;
 - ii. relevant to an investigation or prosecution of a person for an offence;
 - iii. of assistance in the enforcement of this Act or the Proceeds of Crime (Civil Confiscation) Act;

the staff shall submit a suspicious transaction report to the CPU. The CPU receives and review reports of suspicious transactions, or suspicious activities made by the staff and, if sufficient basis exists, report the same to the FIU **within 2 working days** of ascertaining the reasonable grounds, forming the suspicion or receiving the information.

Notwithstanding the above, the AML/CFT Unit has been designated as the function to conduct the work of the Bank as the supervisory authority under the AMLCFTA, shall report directly to the FIU on any suspicious activity or transaction that the supervisory authority or its officers may encounter during the normal course of their duties. For the purposes of this section, transaction includes an attempted transaction, regardless of the amount of the transaction.

XIV. Opening and maintaining of business relationship in legal name

- a. Account shall be opened in legal names:
No accounts shall be opened, in fictitious and anonymous names and the Bank shall know the BO of the accounts or transactions at all time.
- b. All transactions shall be carried out in the name of the true name of the person requesting the transaction. Any transaction being requested on behalf of someone else, appropriate measures need to be undertaken to establish the relationship between the two persons and to ensure the person is authorised to act on the other person's behalf.

XV. Business relationship with other entities

The division/unit shall be aware of the following:

- a. It is prohibited to open and maintain accounts for unauthorised/unlicensed banks .
- b. It is prohibited to maintain accounts and carry out business relationships with shell banks.
- c. It is prohibited to transact or have a business relationship with another entity that provides services to shell banks.
- d. It is prohibited to open and maintain accounts for Section 311 designated entities².

For the purpose of this paragraph, a shell bank is a bank, or an institution engaged in equivalent activities that:

- a. is incorporated in a country in which it has no physical presence involving meaningful decision making and management; and
- b. is not subject to supervision by the Bank or a foreign regulatory authority, by reason that it is not affiliated to any financial services group that is subject to effective consolidated supervision;

XVI. Obligation to cease transaction

² Section 311 of USA PATRIOT Act grants the US Secretary of the Treasury the authority, upon finding that reasonable grounds exist for concluding that a foreign jurisdiction, institution, class of transaction, or type of account is of "primary ML concern," to require domestic financial institutions and financial agencies to take certain "special measures" against the entity of ML concern.

- a. Where a division/unit is unable to apply CDD measures for a counterparty, the division/unit shall:
 - i. not carry out a transaction with or for the counterparty through a bank account;
 - ii. not establish a business relationship or carry out a one-off transaction with the counterparty;
 - iii. terminate any existing business relationship with the counterparty.
- b. Where the division/unit is unable to undertake ongoing monitoring with respect to a business relationship, it shall terminate the business relationship.
- c. Where subsections (a) or (b) applies in relation to any counterparty, the division/unit shall submit a suspicious activity report.
- d. Subsections (a) and (b) shall not apply to the extent where the division/unit is acting:
 - i. in the case of a suspicious transaction report, with the consent of the FIU; or
 - ii. in the case of a disclosure under the Prevention of Terrorism Act, with the consent of the Commissioner of Police.

XVII. Tipping off

- I. A staff who, knowing or suspecting that:
 - a. a suspicious transaction report or a direction of the FIU has been or may be made or that further information has been given;
 - b. the Bank has formed a suspicion in relation to a transaction;
 - c. any other information from which the person to whom the information is disclosed could reasonably be expected to infer that a suspicion has been formed or that a suspicious transaction report has been or may be made;
 - d. a search warrant is to be issued or has been issued;
 - e. an application is to be made, or has been made, under the AMLCFTA for a production order;
 - f. an investigation has commenced concerning the circumstances that gave rise to the suspicious transaction report, the warrant or the production order; or
 - g. makes any disclosure, which could or may or be likely to prejudice the implementation of the warrant, the making available of the material in accordance with the production order, or the investigation

commits an offence and is liable on conviction to imprisonment up to six months or to a fine not exceeding SCR200,000 or to both, as per the AMLCFTA.
- II. In proceedings against a person for an offence under this section it shall be a defence to prove that the person had lawful authority or reasonable excuse for making the disclosure.
- III. Subsection I shall not apply to disclosures made to:
 - a. an officer or employee or agent of the reporting entity for any purpose connected with the performance of that person's duties;
 - b. a legal practitioner, attorney or legal adviser for the purpose of obtaining legal advice or representation in relation to the matter;
 - c. the supervisory authority of the reporting entity for the purpose of carrying out the supervisory authority's functions.
- IV. No person referred to in subsection (III)(b) to whom disclosure of any information has been made, shall disclose that information except to another person mentioned above in subsection (III), for the purpose of:
 - a. the performance of his duties; or
 - b. obtaining legal advice or representation in relation to the matter.

- V. No person referred to in subsection (III)(c) to whom disclosure of any information to which that subsection applies has been made shall disclose that information except to a person referred to in that subsection for the purpose of giving advice or making representations in relation to the matter.

XVIII. Terrorist Financing

The Bank adopts a policy to not allow its financial system to be used for the purpose of financing terrorism.

The facilitation of the financing of terrorism is a different process to that of ML. In many cases, funds used to finance terrorism will have been legally acquired or donated from charities, proceeds of legitimate business, self-financed internally within the organisation or by sympathisers, state sponsors. In other words, ML is the process of making dirty money appear clean, whereas TF often involves clean money being used for criminal purposes.

ML and TF have a number of features in common:

- i. The source of the funds and destination of money used to support terrorism has to be disguised.
- ii. They will require assistance of the financial sector.
- iii. Terrorist groups are known to have links to the criminal organisations and in many cases derive funding from such organisations.
- iv. The techniques used to disguise destination of terrorist funds are identical to those used to launder the proceeds of crime.

In this regards, the division/unit must ensure to do the proper screening as required.

XIX. Proliferation Finance

United Nation Security Council resolution 1540 requires jurisdiction should take effective measures to establish domestic controls to prevent the proliferation of nuclear, chemical or biological weapons and their means of delivery. Recommendation 7 of the FATF, require countries to set up prevention measures that are necessary and unique in the context of stopping the flow of funds or other assets to entities or person undertaking such acts, or for the use in proliferation. Proliferation ultimately involves the transfer and export of technology, goods, software services or expertise that could be used in nuclear, chemical or biological weapon-related programmes, including delivery system.

Proliferation may use both the formal and informal sector of the international financial system and may also deal in cash. Proliferation support networks use the international financial system to carry out transactions and business deals, often acting through illicit intermediaries, front companies and illegal trade brokers. Proliferation differs from ML in several respects. The fact that proliferators may derive funds from both criminal activity and/or legitimately sourced funds means that transactions-related to proliferation financing may not exhibit the same characteristics as conventional ML. The number of customers or transactions-related to proliferation activities is likely to be markedly smaller than those involved in other types of criminal activity such as ML.

The Bank remains vigilant of such transactions, as they would be harmful to the reputation of the jurisdiction and hence seek to prevent its financial system to be used for such acts by implementing the measures adopted in this policy.

XX. Request for information

A division/unit which receive a Request For Information (RFI) directly, in regards to the AML, CFT and CPF, where the transaction or information has been processed or held by the Bank, shall inform the CPU, who will coordinate the collation and dissemination of the information. For better co-

ordination, the CPU will engage with the appropriate division/unit, supervisory authority or agency to gather the information and send a response at the earliest.

Notwithstanding the above, the AMLCFT unit shall handle the RFIs in relation to the supervisory authority responsibilities of the Bank under the AMLCFTA.

XXI. Roles and responsibilities

1. **The Board** Accountable to stakeholders and ultimately responsible for directing and monitoring the entire process of risk management, which includes the implementation of an effective AML, CFT and CPF framework to guide the Bank with regulatory requirements and internal policies. The Board shall approve counterparties that have been identified as PEP.
2. **ARC** Assists the Board in fulfilling its oversight responsibilities of the financial reporting process, the systems of risk management and internal control, the audit process (both internal and external). Also reviews the Bank's process of monitoring compliance with legislation, international standards and internal policies.
3. **RMC** Assists the Board in overseeing the implementation, development and monitoring of the Risk Management Framework (RMF) and the Business Continuity Management Systems (BCMS). The Committee is responsible for the review of strategies, policies, frameworks and guidelines for the RMF and BCMS prior to Board approval.
4. **IC** The Board delegates the operationalisation of the Investment Policy and oversight of reserves management to IC guided by a Terms of Reference as approved by the Board. IC approves the Due Diligence guidelines of reserve management activities.
5. **PC** The PC has oversight of the procurement activities in the Bank as mandated by the Procurement policy.
6. **Management** Management is responsible for:
 - a. Ensuring day-to-day compliance with obligations on AML within the areas for which they are responsible for;
 - b. Ensuring that all employees in their respective departments are trained on ML control measures;
 - c. Assisting in the development and maintenance of appropriate procedures for the implementation of this Policy and related guidelines within the areas for which they are responsible for; and
 - d. Ensuring that any unusual or suspicious transaction in the area which they are responsible for are promptly reported.
7. **RMU** Assist in identifying risks, identify mitigation solutions, aid the divisions/units to put in place the mitigations and raise the issues to RMC. This is done through yearly risk assessment and by risk reporting events. They ensure that matters are discussed at the ARC level and given the proper attention.
8. **CPU** Assist the divisions/units to identify, assess and manage compliance risk and appraise Senior Management and Board on the management of compliance risk. They shall conduct monitoring of the Bank's activities to determine if activities are being conducted in accordance with the regulatory requirements. Furthermore, the Unit shall ensure that each division/unit is aware of new Acts and regulations, international standards and procedures that will affect their duties.
9. **IAD** Responsible for assessing the effectiveness and adequacy of internal ML controls and processes. They will inform the CPU of their findings.
10. **All employees** The employees of the Bank are responsible for:
 - a. reading and understanding this Policy;

- b. complying with this Policy and any other relevant guidelines.

XXII. AML/CFT Enterprise Wide-Risk Assessment

The CU shall carry out an enterprise wide-risk assessment annually to identify and understand the risks of the divisions/units on AML/CFT.

XXIII. Reporting to the ARC

The CU shall report to ARC on the status and progress of the implementation of the policy, which includes, the risk assessments conducted by divisions/units, the RFIs and any related AML/CFT issues. This report shall be produced twice a year.

XXIV. Training and development

The content of and obligations contained in this Policy will be communicated by the CPU on an ongoing basis to all employees of the Bank. The Board, Management and all employees who work in areas in which ML can potentially occur shall receive specific mandatory AML compliance training on an ongoing basis.

XXV. Confidentiality

Any information obtained in the course of fulfilling the obligations of this policy, is confidential. Disclosure to other staff shall be made on a need to know basis only.

For the purpose of this Policy, disclosure shall be done as follows:

- a. seeking legal advice from Legal Unit;
- b. seeking legal advice from the external legal professional through Legal Unit;
- c. seeking assistance from IAD and CPU;
- d. Seeking clarification from Senior Management and HODs.

XXVI. Breach of Policy

Any employee who breaches this Policy and related guidelines shall be subject to disciplinary action as per the Code of Conduct and Ethics and may lead to a criminal prosecution.

XXVII. Procedure Manual

Every division/unit shall develop their own procedural manual and put into practice the content of this Policy where applicable to their duties. The division/unit shall review and amend their manual to reflect changes in their procedures and the regulatory requirements. All procedure manuals shall be approved by the AA.

XXVIII. Review of Policy

This Policy shall be reviewed annually to ensure its relevance.

Notwithstanding the above, the Policy may be reviewed at any time where there is a material need for amendment.

XXIX. Approval of Policy

This Policy is approved by the Board of Directors.

Annex 1 Assessment of risks

The division/unit shall consider the following factors/criteria when determining the counterparty's risk classification:

- Counterparties;
- Products and/or services;
- Delivery channels;
- Geographic areas of operations;
- Adverse information.

The higher the level of risk, the greater the control measures need to be. Senior Management and the relevant divisions/units should be actively involved in determining the risks posed by ML and TF within the areas for which they have responsibility.

Various risk factors are interrelated. A high-risk counterparty will adversely affect the risk profile of an otherwise low-risk product and geographical risks can affect all normal low-risk factors. A low-risk product will change its profile when the product is delivered remotely with no face-to-face contact.

Different counterparts, products and services carry different levels of ML risk that need to be managed effectively within division/unit's policies and procedures. The Higher the risk, the greater the due diligence that is required, and the higher the level of monitoring required to manage the risk.

1. Assessing product and service risk

No product or service, including low-risk products, is immune from the attention of criminals. In practice, however, some products and services are more attractive for ML and TF than others. The divisions/units need to consider the following:

- Whether the product facilitate payment to third parties that may mask the true BO of the funds or assets being handled or the illegal origins of the funds;
- Whether the product involves receipts and payment in cash which is a preferred exchange medium of criminals;
- Whether the product allows for counterparty anonymity, i.e., permitting criminal's identity to remain unknown.

2. Assessing counterparty risk

Some categories of counterparties pose a higher risk of ML, TF or PF. The division/unit should consider the following when assessing counterparty risk:

- Counterparties involved in occasional or one-off transactions (particularly where these can be structured below a particular national threshold);
- Counterparties involved in cash-intensive businesses, which may be used by criminals to mask illegally obtained funds;
- Counterparties who use complex business or organizational structures that offer no apparent legal or economic benefits (including those whose only purpose is for aggressive tax avoidance or evasion purposes);
- Counterparties who are PEPs, including corporate entities whose BOs or controllers are, or include, one or more PEPs;
- Counterparties involved in business sectors with high levels of corruption or links to organized crime, e.g. construction, extractive industries, arms dealing or gambling;
- Counterparties whose origin of wealth and/or source of funds cannot be easily verified or where the audit trail appears to be broken, or unnecessarily complex, or lacking in transparency;
- Counterparties who request excessive amounts of secrecy or abnormal levels of confidentiality;
- Counterparties who conduct business through, or are introduced by, accountants, lawyers of other 'gatekeepers';
- Counterparties for whom the business relationship is conducted online, by phone or otherwise entirely non-face-to-face;

- Counterparties who are charities or other non-profit organisations, particularly those involved in conflict zones or who are providing humanitarian aid;
Counterparties of a type that has been identified in National or Sector Risk Assessments as 'high risk'.

In contrast, some counterparties can generally provide a lower indication of risk, including:

- Counterparties who are employed and generally only receive a regular income from one known source;
- Counterparties with a long-term and active business relationship with the division/unit, whose profile generally remains relatively static and for whom CDD information is complete and up-to-date;
- Counterparties who are only supplied with low-risk products or services;
- Counterparties who are themselves regulated for AML/CFT/CPF purposes in a jurisdiction without strategic AML/CFT/CPF deficiencies.

Generally, any form of legal entity or related services that enables individuals to divest themselves of ownership of property while retaining an element of control over it is vulnerable and will increase the counterparty risk. These include but not limited to:

- Complex ownership structures that can make it relatively easy to conceal underlying beneficiaries and where there is no legitimate commercial rationale;
- Companies incorporated in jurisdictions that do not require the identity of the ultimate underlying principles to be disclosed;
- Certain forms of trust or foundation, including blind trusts, dummy settlors trusts and settlor-directed trusts where knowledge of the identity of the true underlying principals or controllers cannot be guaranteed;
- Certain trusts under which a 'protector' may be appointed who can override certain key elements of the trust;
- Companies nominee shareholders have been appointed;
- Companies issuing bearer shares.

3. Assessing geographical risk

The jurisdiction with which a financial sector or professional firm or individual is connected, or does business, or in which its home base is located, will affect its overall AML/CFT business risk. Likewise, the jurisdiction with which counterparties are connected will affect their risk rating including the geographical sphere of their business activities.

Countries are generically assessed as 'high', 'standard' or 'lower' risk. Factors such as illicit drug production or drug transit, presence of high levels of organized crime, vulnerability to corruption and inadequate AML frameworks or supervision will affect the risk posed by relationships connected with such jurisdiction. Country risk is closely associated with counterparty risk. Where an organization has a high concentration of in a higher-risk jurisdiction, this will affect its overall AML/CFT/CPF business risk profile.

Where a jurisdictional risk is high, additional measures, including EDD, are required. In some extreme cases, FATF countermeasures may need to be applied or transactions with particular jurisdictions may be prohibited. Conversely, where jurisdictions are assessed as lower risk, domestic legislation or regulations may permit the due diligence checks to be reduced. Many countries will, of course fall within the standard risk category.

The MER provided by FATF, FATF Style-Regional Bodies (FSRBs) and IMF and any follow-on reports provide a useful starting point for the assessment. Other sources can also be used to inform the geographical risk of a jurisdiction, as follows:

- FATF list of high-risk and non-cooperative jurisdictions³
- FATF mutual evaluation reports
- European Union AML and tax blacklists

³ <https://bit.ly/1RA355J>

- Basel AML Index⁴
- United Nations Office on Drugs and Crime (UNODC)⁵ reports
- Transparency International Corruption Perceptions Index⁶
- Know Your Country reports⁷
- Trusted and independent media sources
- United Nations sanctions, embargoes or similar measures

In assessing geographical/country risk, organisations should also use their in-house knowledge as this is often one of the most reliable indicators of risk. This includes familiarity with a country, including knowledge of its local legislation, regulations and rules, the structure and extent of regulatory oversight and the compliance culture within its FIs.

4. Assessing delivery channel risk

The way a business supplies its products and services to its counterparties, and how the relationships with counterparties and intermediaries are managed affects its susceptibility for ML, TF or PF. Divisions/units might want to consider the following when assigning a rating:

- The way the transactions are conducted, i.e., via the internet or face-to-face;
- The way the business operates, i.e., through indirect relationship (intermediaries or through pooled accountants);
- whether the intermediaries or accounts are regulated;
- the method being used to process transactions, i.e., does the transfer of funds take place through new payment products.

Generally, there is considered to be a lower risk of handling criminal proceeds where the counterparty has been met face-to-face. Photographic evidence can be physically checked and an impression of the counterparty's age and lifestyle gained. Certainly, the risk of identity fraud is lowered in face-to-face relationship where original identity documents are obtained and closely checked for discrepancies.

Otherwise, the division/unit should consider factors such as whether the relationship with the counterparty is conducted indirectly through intermediaries or introducers, and whether it is capable of being controlled remotely by the counterparty.

5. Assessing adverse information

Adverse media checks, also known as negative news checks, is the process of screening a counterparty against news articles, legal prosecution or similar content that may affect the counterparty's final risk by revealing their involvement in ML, terrorism, fraud, tax evasion, or other types of crimes.

In the international sphere, the Financial Action Task Force (FATF) in its Risk-Based Approach Guidance identifies adverse media searches as a part of Due Diligence practice concerning individual risk assessment.

⁴ <https://index.baselgovernance.org/>

⁵ <http://www.unodc.org/>

⁶ <https://bit.ly/2BJaDBF>

⁷ <https://www.knowyourcountry.com/>

Annex 2 Definition and treatment of Politically Exposed Person

Where the division/unit knows or has reasonable grounds to believe that a counterparty, or a BO of a counterparty, residing in or outside Seychelles is or becomes a PEP, the reporting entity shall apply EDD measures and enhanced ongoing monitoring.

1. A PEP means:
 - a. an individual who is or has been, during the preceding three years, entrusted with a prominent public function in —
 - i. Seychelles; or
 - ii. any other country; or
 - iii. an international body or organisation;
 - b. an immediate family member of a person referred to in paragraph (a); or
 - c. a close associate of a person referred to in paragraph (a).
2. prominent public function includes:
 - a. heads of state, heads of government, ministers and other senior politicians;
 - b. senior government or judicial officials;
 - c. ambassadors and chargés d'affaires;
 - d. persons appointed as honorary consuls;
 - e. high-ranking officers in the armed forces;
 - f. members of the Boards of Central Banks;
 - g. members of the Boards of state-owned corporations; and
 - h. influential political party officials.
3. immediate family member of a person specified in paragraph (1) includes:
 - a. a spouse;
 - b. a partner, that is an individual considered by his or her national law as equivalent to a spouse;
 - c. their child/children and that of spouse's or partner's child/children as defined in paragraph (b);
 - d. parents; and
 - e. siblings.
4. close associates of a person includes —
 - a. any person who is known to have joint beneficial ownership of a legal person, partnership, trust or any other close business relations with that legal person, partnership or trust; and
 - b. any person who has sole beneficial ownership of a legal person, partnership or trust which is known to have been set up
5. In determining whether a person is a close associate of a PEP, the division/unit shall have regard to public information or such information that the reporting entity has in its possession
6. A "counterparty" for this purpose includes any legal person/entity entering a business relationship or undertaking a one-off transaction with the Bank.

Annex 3 Determination of a beneficial owner

1. A BO in relation to a legal person or legal arrangement includes but is not limited to:
 - a. one or more natural persons who ultimately have a controlling ownership interest in a legal person or legal arrangement; and
 - b. to the extent that there is doubt under sub-regulation (1)(a), the natural person or persons, if any, exercising control of the legal person or legal arrangement through other means; or
 - c. if no such person exists or such person may be identified under sub-regulation (1)(a) and (b), the natural person or persons who holds the position of a senior managing official of the legal person or legal arrangement, as the case may be.
2. A BO of a legal person (except the BO of a foundation), shall:
 - a. be a natural person or persons, who ultimately owns or controls, whether directly or indirectly, ten percent or more of controlling ownership interest including the shares or voting rights of the said legal person;
 - b. hold the right directly or indirectly, to appoint or remove majority of the board of directors of the said legal person.
3. Exercising control through other means includes, but is not limited to:
 - a. the right to appoint or remove the majority of the board of directors or general partners of a legal person or legal arrangement, as the case may be
 - b. where the person with controlling ownership interest is dominated by another person because of a familial or employment relationship;
 - c. where another person holds certain powers in relation to the legal person or legal arrangement which are likely to be used in practice to affect the decisions taken by that person with the controlling ownership interest; or
 - d. any control over a legal person or legal arrangement other than the control by ownership of any interest.
4. A BO in the case of a foundation shall be a natural person or persons:
 - a. who holds, whether directly or indirectly, absolute decision or veto rights in the conduct and management of the foundation;
 - b. who holds the right, directly or indirectly to appoint or remove majority of the councillors of the foundation;
 - c. who is a beneficiary in whom an interest is vested;
 - d. who is the default recipient of the assets of the foundation in the event of its termination; or
 - e. any other person, who benefits from the foundation.
5. The BO in the case of a partnership with legal personality shall be a natural person or persons who:
 - a. ultimately owns or controls, whether directly or indirectly, absolute decision or veto rights in the conduct or management of the partnership;
 - b. holds the right, directly or indirectly to appoint or remove majority of the general partners of the partnership; or
 - c. is entitled to the assets of the partnership in the event of the dissolution of the partnership.
6. The BO in the case of a trust and other legal arrangements shall be a natural person or persons who is:
 - a. the trustee or, in the case of a legal arrangement other than a trust, any person in an equivalent or similar position of a trustee;
 - b. the settlor or in the case of a legal arrangement other than a trust, any person in an equivalent or similar position of a settlor;
 - c. the protector, if any or in the case of a legal arrangement other than a trust, any person in an equivalent or similar position of a protector;
 - d. the beneficiaries or class of beneficiaries or in the case of a legal arrangement other than a trust, any person in an equivalent or similar position of a beneficiary or class of beneficiaries;
 - e. any other natural person exercising ultimate effective control over the trust or the legal arrangement, including any person who has, under the trust deed of the trust or any similar document, power to:
 - i. appoint or remove any of the trustees of the trust;

- ii. direct the distribution of funds or assets of the trust;
 - iii. direct investment decisions of the trust;
 - iv. amend the trust deed; or
 - v. revoke the trust; and
 - f. any other person, known by the resident agent of the legal arrangement, who is exercising control over the legal arrangement.
7. In the case of a legal person or legal arrangement, which is in insolvent liquidation, administration or receivership proceedings, the natural person who has been appointed as a liquidator, administrator or receiver of the legal person or legal arrangement, shall be the BO.
 8. In the case of a receiver being appointed over ten percent or more of the shares or voting rights in a legal person or legal arrangement, the creditor who appoints the receiver shall be the BO.
 9. In the case of a deceased shareholder in the legal person, the natural person or persons acting as executor or a personal representative of the deceased's estate shall be the BO.
 10. A person shall not be treated as a BO only by reason of:
 - a. having the benefit of a security interest over the shares or voting rights in a legal person or legal arrangement; or
 - b. having commercial exposure to the financial performance of a legal person or legal arrangement pursuant to financial derivatives or similar contractual arrangements.
 11. Where two or more persons hold any interest jointly as joint owners, then each such joint owner shall be treated as a separate BO.
 12. For the purpose of these regulations, a legal person is a subsidiary of another legal person, if the parent entity:
 - a. holds, directly or indirectly, ninety percent or more beneficial interest in the shares of the subsidiary;
 - b. hold, directly or indirectly, more than ninety percent of the voting rights in the subsidiary; or
 - c. irrespective of percentage has direct or indirect interest.
 13. Holding shares:
 - a. Holding shares in a legal person means holding a right to share in the capital or, as the case may be, profits of that person.
 - b. Holding ten percent or more of the shares in that legal person means holding a right or rights to shares in ten percent or more of the capital or, as the case may be, profits of that person.
 14. Voting rights:
 - a. voting rights refers to the rights conferred on shareholders in respect of their shares or, in the case of a legal person not having a share capital, on members or officers, to vote at general meetings of the legal person or legal arrangement on all or substantially all matters.
 - b. In relation to a legal person or legal arrangement that does not have general meetings at which matters are decided by the exercise of voting rights:
 - i. exercising voting rights means to exercise rights in relation to a person or persons that are equivalent to those of a person entitled to exercise voting rights in a company; and
 - ii. exercising ten percent or more of the voting rights in the legal person or legal arrangement means to exercise the right under the constitutional document of the legal person or legal arrangement to effect changes to the overall policy of the legal person or legal arrangement.
 15. Shares or rights held:
 - a. by a legal person, which is under the control of an individual; or
 - b. by multiple legal persons, which are under the control of the same individual, shall be an indication of indirect ownership by such individual.
 16. For avoidance of doubt, the reference of right to appoint or remove majority of the board of directors of a legal person in these regulations refers to the right to appoint or remove directors holding majority of the voting rights at the meetings of the board on all or substantially all matters.

17. Shares held by a nominee on behalf of a nominator shall be treated as if the shares were held by the nominator.

Annex 4 Guidance on financing of terrorism

Any person who carries out the below act, shall be guilty of the offence of financing if:

1. Any person who provides or collects, by any means, directly or indirectly, any funds intending, knowing or having reasonable grounds to believe that the funds will be used in full or in part to carry out a terrorist act
2. Any person who, directly or indirectly, collects property or provides, invites a person to provide, or makes available, property or financial or other related services -
 - a. intending that they be used, in whole or in part, for the purpose of committing or facilitating the commission of a terrorist act or for the purpose of benefiting any person who is committing or facilitating the commission of a terrorist act; or
 - b. knowing that in whole or in part, they will be used by, or will benefit, a terrorist group.
3. Any person who -
 - a. uses property, directly or indirectly, in whole or in part, for the purpose of committing or facilitating the commission of a terrorist act; or
 - b. possesses property intending that it be used or knowing that it will be used, directly or indirectly, in whole or in part, for the purpose of committing or facilitating the commission of a terrorist act,
4. Any person who knowingly enters into, or becomes concerned in, an arrangement which facilitates the retention or control by or on behalf of another person of terrorist property
 - a. by concealment,
 - b. by a removal out of jurisdiction,
 - c. by transfer to a nominee, or
 - d. in any other way,
5. Any person who knowingly -
 - a. deals, directly or indirectly, in any property that is owned or controlled by or on behalf of a terrorist group;
 - b. enters into, or facilitates, directly or indirectly, any transaction in respect of property referred to in paragraph (a); or
 - c. provides financial or other services in respect of property referred to in paragraph (a) at the direction of a terrorist group,
6. Any person who knowingly, and in any manner -
 - a. solicits support for, or gives support to, any terrorist group, or
 - b. solicits support for, or gives support to, the commission of a terrorist act,
7. Any person who knowingly offers to provide, or provides, any weapon to -
 - a. a terrorist group;
 - b. a member of a terrorist group;
 - c. to any other person for use by, or for the benefit of, a terrorist group or a member of a terrorist group,
8. Any person who in Seychelles -
 - a. knowingly promotes or facilitates the doing of any act in a foreign State for the purpose of achieving any of the following objectives whether or not the objective is achieved-
 - i. the overthrow, by force or violence, of the government of that foreign State;
 - ii. causing, by force or violence, the public in that foreign State to be in fear of death or bodily injury;
 - iii. causing death of, or bodily injury to a person who –
 1. is the Head of State of that foreign State; or
 2. holds or performs any of the duties of a public office of that foreign State;

- b. recruits another person to become a member of, or to serve in any capacity with a body or association of persons the objectives of which are, or include, the objectives referred to in paragraph (a);
- c. accumulates, stockpiles or otherwise keeps, any weapons for the purpose of doing any act referred to in paragraph (a);
- d. trains or drills, or participates in the training or drilling of, any other person in the use of weapons or in the practice of military exercises or movements to prepare that person to do any act referred to in paragraph (a);
- e. allows himself or herself to be trained or drilled in the use of weapons or
- f. in the practice of military exercises or movements for the purpose of doing any act referred to in paragraph (a);
- g. gives any money or goods to, or performs services for, any other person or body or association of persons for the purpose of doing an act referred to in paragraph (a); or
- h. receives or solicits money or goods or the performance of services for the purpose of promoting or supporting the doing of an act referred to in paragraph (a).