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: 01

Effective Date: February 2020

Author: Compliance Unit

Review Date: January 2021

Amendment History (Where applicable):

Version Number	Effective Date	Brief description of amendments

Contents

I. List of Acronyms 1
II. Policy Statement 2
III. Definitions 2
IV. Policy objective 5
V. Purposes of the Policy 6
VI. Scope 6
VII. Applicability of the Policy 6
VIII. Obligation of the institution: 7
1. Documentation requirement 7
2. Ideologies of CDD 9
3. Verification of documents 11
4. Screening 11
5. Record updating and retention 11
6. Obligation to report suspicious/ Unusual Transaction 11
IX. Risk Profile 12
X. Supervisory Function 14
XI. Request for assistance 14
XII. Roles and responsibilities 15
XIII. Training and development 16
XIV. Confidentiality 16
XV. Breach of Policy 17
XVI. Reading with other documentation 17
XVII. Procedure Manual 17
XVIII. Review of Policy 18
XIX. Approval of Policy 18
XX. Annex 1 List of Policies, Guidelines and Acts 19
XXI. Annex 2 Determining the risks 20

I. List of Acronyms

AA	Approval Authority
AML	Anti-Money Laundering
AMLA	Anti-Money Laundering Act
ARC	Audit and Risk Committee
BDC	Bureau De Change
BO	Beneficial Owner
CDD	Customer Due Diligence
CEO	Chief Executive Officer
CFT	Counter Financing of Terrorism
CPF	Counter Proliferation Financing
EDD	Enhanced Due Diligence
FATF	Financial Action Task Force
FI	Financial Institution
FIA	Financial Institutions Act
FIU	Financial Intelligence Unit
IAD	Internal Audit Division
IC	Investment Committee
ID	Identification Document
IMF	International Monetary Fund
MER	Mutual Evaluation Report
ML	Money Laundering
NGO	Non-Governmental Organisation
P	Proliferation
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
TF	Terrorist Financing
The Bank	Central Bank of Seychelles
The Board	Board of Directors of the Bank

II. Policy Statement

The Bank recognises its role in combatting 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 AMLA, the PTA and all the international standards.

III. 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.	**Apostille**	An Apostille is a certificate that authenticates the origin of a *public document* (e.g., a birth, marriage or death certificate, a judgment, an extract of a register or a notarial attestation). The Apostille is attached to your original document to verify it is legitimate and authentic so it will be accepted in one of the other countries who are members of the Hague Apostille Convention.
3.	**Approval Authority**	shall mean: o for activities engaged through the procurement process and approval of license for Bureau de Change, it shall be the Governor; o for licensable activities (i.e., banks and financial leasing) it shall be the Board; o for approval of the following counterparts for investments and third-party service providers, i.e., Commercial and Investment Banks in the capacity of third-party service providers, Central Banks, commercial banks, other financial institutions and commercial entities of investment avenues and global custodians, it shall be the Board; o for issuers of sovereign, supranational and agency (SSA) securities, it shall be IC.
4.	**Beneficial Owner**	means a natural person or persons who ultimately owns or controls a customer or the natural person on whose behalf a transaction is being conducted and includes those persons

		who exercise ultimate effective control over a legal person or arrangement.
5.	**Counter Financing of Terrorism**	means the measures undertaken to tackle terrorist financing.
6.	**Counter Proliferation Financing**	are the measures being undertaken to prevent the use of the Financial system to finance proliferation of weapons.
7.	**Counterparty**	shall include but not limited to o Suppliers o Contractors o service providers o ministries o government agencies o commercial banks o pension funds o parastatal bodies o international financial organisation o investors and prospective investors o license applicants o international financial institutions that engage with the Bank in reserve management activities and any other person whose relationship, existing or prospective, with the Bank might expose the Bank to a range of risks. These risks include money laundering and terrorist financing. As the Bank acts as banker to the government, the beneficiary of the transactions in this instance shall fall under the definition of counterparty.
8.	**Counterparty Due Diligence**	means information or facts (these shall include but not limited to identification and verification of counterparties and monitoring of transactions) about a counterparty, that should enable the Bank to assess the extent to which the counterparty exposes the Bank to a range of risks. These risks include ML, TF and P.
9.	**Enhanced due diligence**	means heightened processes to assess the extent to which higher-risk counterparties expose the Bank to a range of risks. Counterparties that pose higher money laundering or terrorist financing risks present increased exposure to the Bank and its stakeholders. Due diligence policies, procedures, and processes should be enhanced as a result.

10. **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

11. **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.

12. **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.

13.	**Politically Exposed Person**	is an individual entrusted with a prominent public function, and includes any immediate family member or close associate of such an individual. It is important to note that both local and foreign PEPs are covered by this definition.
14.	**Proliferation**	is the manufacture, acquisition, possession, development, export, transhipment, 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.
15.	**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, transhipment, 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.
16.	**Simplified counterparty due diligence**	means the lowest level of due diligence that can be completed on a counterparty. This is appropriate where there is little opportunity or risk of the counterparty becoming involved in money laundering or terrorist financing.
17.	**Terrorism Financing**	is the process by which terrorists fund their operations in order to perform terrorist activity.

IV. Policy objective

The objective of the Policy is to highlight the obligation of the Bank to AML, CFT and CPF legislations and international standards. It is aimed at establishing an appropriate framework for the protection of the Bank against ML, TF & P.

V. Purposes of the Policy

The purposes are as below:

1. To establish the responsibility of the Bank under the AML, CFT and CPF legislations and standards;
2. To define the extent to which the Bank will take to carry out its Counterparty due diligence using the Risk Based Approach;
3. To establish the standards, approach and processes, in accordance with local and international standards and best practice;
4. To provide a baseline from which procedures should be developed by divisions on reporting of suspicious and/or unusual transactions and implementing AML, CTF and CPF framework.

VI. Scope

This Policy is applicable to the Board, all divisions, units and staff of the Bank. It establishes the full scope of work that the Bank will undertake to be compliant with domestic and international laws and standards for AML, CFT and CPF.

VII. Applicability of the Policy

This Policy shall be applicable to the following categories of activities ("the Identified activities"):

1. Obtaining services and goods from suppliers, consultants etc;
2. Procurement of Services from FIs;
3. Licensing of banks, bureau de change, financial leasing companies, Payment Systems Service Providers and other activities licensable by the Bank;
4. Effecting payment transactions for Government and all institutions holding an account with the Bank;
5. Management of Government securities;
6. The appointment of any person or entity to act on behalf of the Bank;
7. Engagement with firms for reserve management activities;
8. Acceptance of demonetised currency from public and institutions;
9. Sale of numismatic items to the public and institutions;
10. Any activity that can affect the Bank in terms of ML, TF and P.

VIII. Obligation of the institution:

1. Documentation requirement

In order to fulfil the due diligence requirement, the following documents need to be obtained in order to establish a business relationship.

#	Type of Counterparties	Information Required	Documents Required
1	Individuals / Sole proprietorship	• Full names and surname • Physical and postal address • Telephone numbers • Sources of income • Nationality	• Copy of national identity document or passport • Detail of business or employment proof • Copy of trading licence if applicable • Proof of residential address • Tax Clearance Certificate
2	Partnerships	• Name of Partnership entity • Full name and surnames of partners • Address of partnership entity • Telephone numbers	• Copies of ID / passport of all partners • Copies of ID for authorized signatories • List of authorized signatories along with power of attorney • Resolution authorizing intended transaction • Copy of latest financials of partnership • Tax Clearance Certificate • Partnership Agreement
3	Companies (Institutional & corporate)	• Name of company as well as trading name	• Copy of ID/passports of all directors and shareholders

		• Names and surnames of directors and shareholders • Registered address • Telephone numbers • Contact persons • Registered number and Tax Identity Number • Details of regulating or licencing entities • Return of particulars of directors as filed with the Registrar of Companies.	• List of all shareholders and ultimate beneficial owners of shares stating the name and address of respective shareholding. • Memorandum and articles of association • Board resolution authorizing to enter into a business relationship with the Bank • Certificate of incorporation/ commencement of business • List of authorized signatories along with copy of IDs • Copy of trading licence • Proof of residential address of all directors • Tax Clearance Certificate • Copy of financials
4	Clubs, Societies and Associations	• Name of club, society or association • Registered address of club, society or association • Telephone numbers (s) • Contact persons	• Board/governing body resolution for intended transaction • Copy of by-laws/rules and regulations • Copy of IDs for board members • Copy of certificate of registration

			• List of authorized signatories along with copy of IDs • Copy of financials
5	Trusts including, but not limited to, provident fund, gratuity fund, pension fund, mutual funds, fiduciary funds etc	• Name of trust, Fund etc • Full names and surnames of trustees • Address of trust/fund etc • Telephone numbers • Contact persons	• Copies of IDs of all trustees • Copy of trust deed • Trustee/governing body resolution for intended transaction • Copy of latest financials of trust or fund etc • List of authorized signatories along with copies of IDs
6	Executors and Administrators	• Name of entity for Executor/Administrator appointed • Name of Executor/Administrator • Address of entity & telephone numbers	• Copy of ID of Executor / Administrator • Copy of order of appointment letter of administration • List of beneficiaries

Note: All documents from foreign Counterparts must be accompanied with an Apostille certificate.

2. Ideologies of CDD

The Bank has developed strict rules for effective implementation of this Policy. These principles shall be applicable to all new and existing counterparties.

The following steps are to be taken:

a. CDD measures shall be enhanced for counterparties considered to be high risk. Factors to determine the risk rating of counterparties are demarcated in Annex 2 of this Policy.

b. For counterparties who are legal persons or for legal arrangements, the Bank is required to take reasonable measures to understand:
   i. the ownership and control structure of the company;
   ii. determine the individuals who own or control the company.

   This includes those persons who exercises ultimate effective control over a company.

c. The Bank must ensure that PEPs are identified when entering into a business relationship with a counterparty.
   i. Identification must take place during the following circumstances:
      - during the preliminary evaluation of a request for proposal (RFP);
      - during the submission of documents to seek approval for licensable activities;
      - during evaluation of choosing a counterparty engaging in reserve management activities;

   ii. In the case, where a PEP has been identified, the division/unit is required to undertake the following measures:
      - When entering into a business relationship with this category of counterparties, the division/ unit must consult their respective committee (i.e. IC or PC where applicable), who will in turn make recommendation to the AA, when seeking approval;
      - Where division/unit do not go before a committee, the division/unit shall make recommendation to the AA for approval or rejection where applicable;

   iii. As for existing relationship with a counterparty who has been identified as a PEP, the division/unit must ensure that they have obtained all the necessary CDD, implement EDD and apply on-going monitoring.

d. In the event the Bank 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.

3. Verification of documents

The Bank shall conduct verification of all documents in its possession. As such before undertaking the identified activities the Bank 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.

4. Screening

Screening is an integral part of CDD measures. Screening shall be done on individual names, Companies, Groups, etc. When screening, adverse media results and any results should be taken into consideration before eliminating or acceptance of counterparties.

The Bank shall:

a. screen using the available tools that it subscribes to (i.e., World Check/Accuity, etc.);
b. screen against financial sanctions databases;

5. Record updating and retention

CDD should not be contemplated as a one-time exercise at the time of entering into a relationship with the counterparty. CDD should be viewed as an ongoing process and should encompass monitoring of the risk profile of the counterparty using a risk-based approach. The Bank shall keep records regarding the identification data obtained through the CDD process, account files and business correspondence for at least 7 (seven) years in physical form and 30 (thirty) in electronic form, after the business relationship has ended.

6. Obligation to report suspicious/ Unusual Transaction

Should an employee become suspicious of a particular transaction, or find anything unusual about a proposed or existing transaction, the employee must report such transactions for further investigation to the immediate supervisor who will then report the same to the person overseeing the Division/Unit and Compliance Unit. Suspicious transactions are not limited to financial transactions. It shall include when entering into a relationship with a counterparty.

Where the Bank comes to have knowledge that a ML offence is being perpetrated or is of the suspicion that an offence is being committed, the Compliance Unit shall report the same to the FIU after it has established the suspicion.

IX. Risk Profile

The division/unit shall conduct an assessment of all counterparties to assign a risk profile. This will enable the division/unit to focus resources to ensure that measures to prevent or mitigate ML, TF and PF are commensurate with the risks identified.

The division/unit shall conduct an initial assessment of all existing counterparties. New counterparties shall be assessed and rated at on-boarding.

The risk rating are classified as low, medium or high, with low carrying the least risk and high carrying more risk

Annex 2 describe the how to determine the rating for each counterparties.

1. **Treatment of the different types of risk rating**

   Counterparties that have been identified as higher risk, the division/unit should ensure that the AML/CFT/CPF measures adequately addresses such risks. Where counterparties identify as lower risks, the division/unit may decide to allow simplified measures.

   The bank should adopt the following treatment for each rating:

   a. For high risk counterparties, that are defined as:
      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. A “counterparty” for this purpose includes any legal person/entity entering a business relationship or undertaking a one-off transaction with the Bank.

         The Bank 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. The Bank is allowed to rely on public information in determining whether persons are within the definition of "close associates" (for example, partners or joint ventures), and should conduct regular searches and checks for this purpose. Once a PEP has been identified, a business relationship can only be established with the appropriate approval, and the division/unit must take adequate measures to establish the source of wealth and the source of funds involved in any proposed relationship or transaction.

vi. Counterparties from or in countries where CDD and AML regulations are lax and are not sufficiently applying FATF recommendations and represents a high risk of crime and corruption; and

vii. Counterparties who have been declined by another regulatory institution, including professional bodies, conviction, (based on reliable and verifiable information from independent sources).

viii. Counterparties that are on the sanctions list or in a country on the sanctions list.

The division/unit is required to conduct EDD and enhance on-going monitoring.

b. For medium risk counterparties, the division/unit should apply the a slightly higher than average CDD measures.

c. For low risk counterparties, the division/unit may apply simplified CDD measures. A counterparty may be considered under low risk category, if the identity of the counterparty and the beneficial owner of a counterparty are publicly known or where adequate checks and controls exist.

d. Following cases 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.

2. Approval of the risk rating

Rating must be assigned to all counterparties by the technical staff and approved by the AA.

The Compliance Unit shall compile all ratings from the divisions/units and bring to ARC for sanction semi-annually.

X. Supervisory Function

The FIA and other legislation designate the Bank with supervisory functions. As per the AMLA, the Bank is empowered to supervise, monitor and enforce compliance with legislations on institutions that it regulates. The Bank shall act in accordance with AMLA in order to carry out its functions.

Where the Bank has

a. knowledge or 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 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 referred to in paragraph (a);
    ii. relevant to an investigation or prosecution of a person for an offence referred to in paragraph (a); or
c. of assistance in the enforcement of this Act or the Proceeds of Crime (Civil Confiscation) Act,

As per AMLA, every supervisory authority and its staff members shall report to the FIU about any suspicious activity or transaction that the supervisory authority or its staff, may encounter during the normal course of their duties

The division/unit, having ascertained the knowledge, formed the suspicion or received information of ML activities, must submit the STR to the Compliance Unit who will in turn forward it to the FIU on behalf of the Bank, within 2 (two) working days.

XI. Request for assistance

Any division/unit which receive a request for assistance in regards to the AML, CFT and CPF, must inform the Compliance Unit who will coordinate the collation and dissemination of the information. The Compliance Unit will engage with the appropriate

division/unit to gather the information and send a response within 2 working days of receiving the request.

XII. 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, as per point VIII (2) (c) of this Policy.

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. **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.

6. **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.

7. **Compliance Unit**

   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.

8. **IAD**

   Responsible for assessing the effectiveness and adequacy of internal ML controls and processes for ensuring compliance with the Act and other applicable legislations. They will also notify and advise the respective divisions/units and the compliance unit of any non-compliance with the AMLA and other applicable legislations, this Policy and related guidelines issued in terms of this Policy.

9. **All employees**

   The employees of the Bank are responsible for**:**

   a. reading and understanding this Policy;
   b. responsible for complying with this Policy and any other relevant guidelines.

XIII. Training and development

The content of and obligations contained in this Policy will be communicated by the Compliance Unit 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 AML compliance training on an on-going basis.

XIV. Confidentiality

Any information obtained in the course of fulfilling AML obligations, is confidential. Staff shall not divulge any information in regards to a suspicious transaction report filed or being filed or any information they come across in performance of their duties to any

members of the public. Disclosure to other staff shall be made on a need to know basis only.

Staff can make disclosure in the following circumstances:

1. for the purpose of the performance of his or her duties.

   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 Compliance Unit;
   d. Seeking clarification from Senior Management and HODs;

2. when required to do so before a Court of law or under any law.

Any person, who discloses the information or the identity of the source of such information is in contravention of section 54 subsections (1) and (2) of AMLA. They commit an offence, and is liable on conviction to a fine up to SCR200,000 or to imprisonment up to two years or to both.

No civil, criminal or disciplinary proceedings shall be taken against—

1. a reporting entity or supervisory authority of a reporting entity;
2. an officer, employee or agent of a reporting entity or supervisory authority of a reporting entity acting in the course of that person's employment or agency,

in relation to any action by the reporting entity or the supervisory authority or their officer, employee or agent taken in good faith under the provisions of this Act, or in compliance with the directions given by the FIU under the provisions of AMLA.

XV. Breach of Policy

Any employee who breaches this Policy and related guidelines shall be subject to disciplinary action as per Code of Conduct and possibly criminal prosecution.

XVI. Reading with other documentation

This Policy shall be read together with the other related policies, guidelines and legislations as listed in Annex 1. The annex will be updated as and when necessary to remain relevant.

XVII. 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.

XVIII. 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.

XIX. Approval of Policy

This Policy is approved by the Board of Directors.

XX. Annex 1 List of Policies, Guidelines and Acts

1. Anti-Money Laundering Act
2. Prevention of Terrorism Act
3. Proceeds of Crime (Civil Confiscation) Act
4. Procurement Policy
5. Licensing Guidelines for Banks and Bureau de Change
6. FATF Recommendation 2012
7. Wolfsberg Payment Transparency Standards
8. EU Regulations 2015/847
9. EU Directives 2018/843
10. Basel Committee on Banking Supervision – Customer Due Diligence

XXI. Annex 2 Determining the risks

When assessing risks, the Bank must consider risks that will arise from the following:

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

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 customer 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 the Bank'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 beneficial owner 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 customer 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 Bank 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 beneficial owners 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 Bank, 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 customer risk. These include but not limited to:

- Complex ownership structures than 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 identify 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 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 customers 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 customers 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.

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 productions and services to its counterparties, and how the relationships with counterparties and intermediaries are managed affects its susceptibility for ML or TF or PF. Divisions/units might want to consider the following when assigning 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 customer 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 Bank should consider factors such as whether the relationship with the customer is conducted indirectly through intermediaries or introducers, and whether it is capable of being controlled remotely by the customer.