



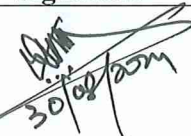

Empowering The Nation

ANTI MONEY LAUNDERING & COUNTER FINANCING OF TERRORISM POLICY

Policy Number: POB-AML-004

Next Review Date: 1 YEAR FROM THE APPROVAL DATE

Version : 6.0

	Name	Designation	Signature
REVIEWED BY	Rohan Fernando	Manager Risk & Compliance	 30/08/2014
APPROVED BY	Gishan Illangakoon	Chief Executive Officer	 30/08/2014

Contents

1. INTRODUCTION
2. SCOPE OF THE POLICY
3. RISKS IN ML/TF
4. POB OBLIGATIONS
5. STAGES OF MONEY LAUNDERING
6. STAGES OF TERRORIST FINANCING
7. KNOW YOUR CUSTOMER PROGRAM
8. CUSTOMER RISK RATING
9. ENHANCED DUE DILIGENCE
10. ULTIMATE BENEFICIAL OWNER
11. ONGOING PERIODIC REVIEWS
12. SANCTIONS
13. RECORD KEEPING
14. CASH TRANSACTION REPORT
15. ELLECTRONIC FUND TRANSFER REPORTING
16. ONGOING TRANSACTION MONITORING
17. SUSPICIOUS TRANSACTION REPORTING
18. INTERNAL CONTROLS
19. ROLES & RESPONSIBILITIES
20. TRAINING

INTRODUCTION

The policy shall be named as “AML/CFT Policy” and shall come in effect from the date of approval of the Board of Pan Oceanic Bank Limited (“POB”).

The policy has laid down appropriate framework addressing the requirements stipulated in the following; Laws, Regulations & Directives;

- Money Laundering & Proceeds of Crime Act 2010
- Counter Terrorism Act 2009
- Prudential Guideline – No.18
- Prudential Guideline – No.19
- Prudential Guideline – No.16
- Prudential Guideline – No.17
- FATF Guidelines

The main guiding principles of POB’s AML/CFT framework is as below;

- To do business only with customers whose identity is fully known to the bank
- To determine and record the identity, background and business of all clients
- To regularly monitor the relationship in order to identify unusual or suspicious activity to be able to take appropriate action, if required.

SCOPE OF THE POLICY

This policy is applied to all staffs, bank functions and structures (including departments and branches) of POB. If any department, branch or business unit of the Bank is unable, to apply the standards set by this policy, such activities or transactions are not tolerated by bank

Money Laundering: Money laundering is the process by which criminally obtained money or other assets (criminal property) are exchanged for ‘clean’ money or other assets with no obvious link to their criminal origins. The money earned from drug trafficking, tax evasion, extortion, smuggling, fraud, bribery etc. are examples of dirty money.

Financing of Terrorism: is a financial support, as the solicitation, collection or provisions of funds with the intention that they may be used to support terrorist acts or organizations. The primary goal of individuals or entities involved in the financing of terrorism is therefore not necessarily to conceal the sources of the money but to conceal both the financing and the nature of the financed activity.

RISK OF MONEY LAUNDERING AND FINANCING OF TERRORISM TO POB

Reputational Risk: The reputation of a business is usually at the core of its success. The ability to attract good employees, customers, funding and business is dependent on reputation. Even if a business is otherwise going on the right track, if customers are permitted to undertake illegal transactions through that business, its reputation could be irreparably damaged. A strong policy helps to prevent a business from being used as a vehicle for illegal activities.

Operational Risk: This is the risk of direct or indirect loss from faulty or failed internal processes, management and systems. In today's competitive environment, operational excellence is critical for competitive advantage. If AML policy is faulty or poorly implemented, then operational resources are wasted, there is an increased chance of being used by criminals for illegal purposes, time and money is then spent on legal and investigative actions and the business can be viewed as operationally unsound.

Legal Risk: Risk of loss due to any of the above risk or combination thereof resulting into the failure to comply with the Laws and having a negative legal impact on the Bank. The specific types of negative legal impacts could arise by way of fines, confiscation of illegal proceeds, criminal liability etc.

Financial Risk: Risk of loss due to any of the above risks or combination thereof resulting into the negative financial impact on the Bank.

POB OBLIGATIONS

POB has a responsibility to;

- Create Policies and Procedures that address money laundering risks
- Appoint Compliance Officer for the day to day Operations of the AML program
- Conduct ongoing training to employees
- Conduct periodical audits to ensure that AML/CFT program is functioning effective
- Adopts a risk based approach towards AML/CFT and conducting due diligence

STAGES OF MONEY LAUNDERING

There are three main stages of money laundering: staging, layering, and placement. These three stages can be implemented over time or simultaneously.



Placement: In the initial placement stage of money laundering, 'dirty money' is introduced into the financial system. This is often done by breaking up large amounts of cash into less

conspicuous smaller sums to deposit directly into a bank account or by purchasing monetary instruments such as checks or money orders that are collected and deposited into accounts at other locations.

Layering: After the funds have entered the financial system, the layering stage occurs, with the launderer moving the funds around to distance them from their source and disguise the money trail. The funds could be channelled through the purchase and sales of investments, a holding company, or simply moved through a series of accounts at banks around the globe. Widely scattered accounts are most likely to be found in jurisdictions that do not cooperate with AML investigations. In some instances, the launderer could disguise the transfers as payments for goods or services giving them a legitimate appearance.

Integration: In the final stage of money laundering, funds are integrated into the legitimate economy. To use the funds to buy goods and services without attracting attention from law enforcement or the tax authorities, the criminal may invest in real estate, luxury assets, or business ventures.

STAGES OF TERRORIST FINANCING

The terrorism financing cycle involves three stages that terrorist organisation may use to support a terrorist network, organisation, or cell.



- Donations
- Self funding
- Criminal activity

- To a terrorist network
- To a terrorist organization
- To a terrorist cell

- Purchase weapons or bomb-making equipment
- Payments for recruitment & training
- Finance living expenses of terrorists

Raising Funds: Raising funds is about how funds are raised to support terrorism financing and that can be done via legitimate or criminal activities.

- Donations
- Self-funding
- Criminal activity.

Transferring Funds: Transferring funds is about how funds are transferred to a terrorist network, organisation, or cell, and money laundering is often associated with this stage of the terrorism financing cycle.

Funds need to be stored at each stage of the terrorism financing process. Storage methods can range from hiding cash in a private residence or in a sandooq (cash box), to depositing funds in a bank account or other financial product.

Money laundering may be a part of the transferring funds process, when dealing with funds that have been sourced via criminal activity, used to make those funds look like they have come from a legitimate source.

Using Funds: Using funds is about how funds can be used for direct and indirect support of terrorist activities carried out by the terrorist network, organisation, or cell.

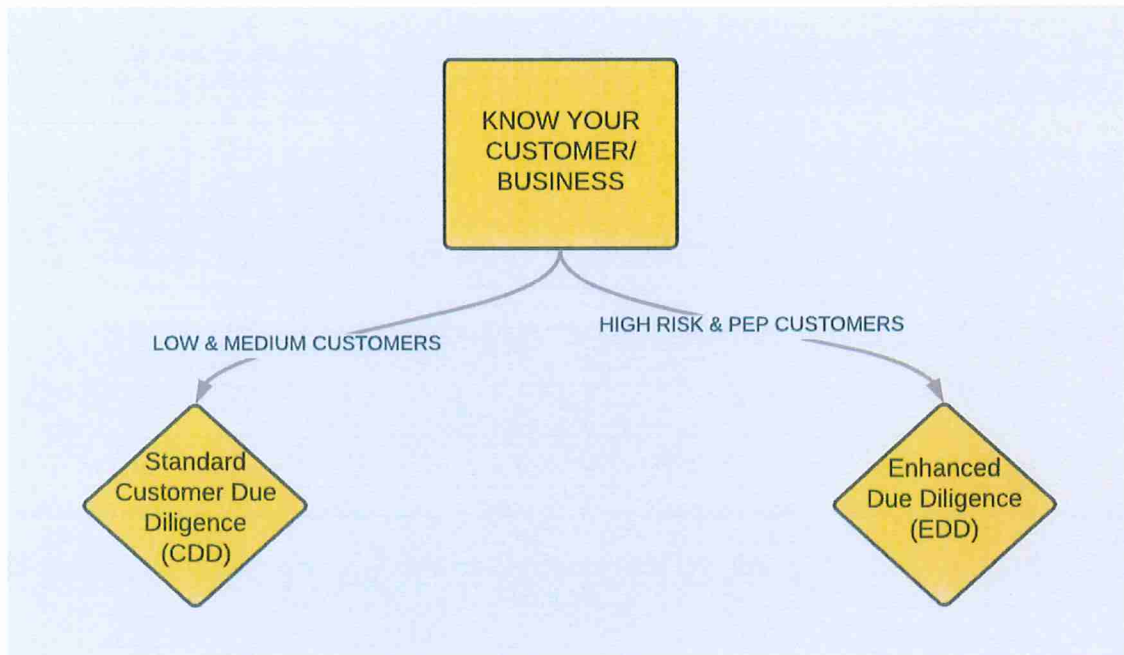
- Purchasing weapons or bomb making equipment
- Payment to insurgents
- Covering living expenses for a terrorist cell.

KNOW YOUR CUSTOMER PROGRAM

KYC (Know Your Customer) is today a significant element in the fight against financial crime and money laundering. KYC check is the mandatory process of identifying and verifying the client's identity when opening an account and periodically over time.

CUSTOMER DUE DILIGENCE (CDD) is a process undertaken by POB staff in order to KNOW YOUR CUSTOMER. CDD can be mainly classified into two categories.

1. **Standard Customer Due Diligence (CDD)** - This practice is applicable for **Low & Medium** risk customers. In short, this entails obtaining minimal basic KYC documents to on board the customer.
2. **Enhanced Due Diligence (EDD)** This practice is applicable for **HIGH** risk customers. In short, this entails obtaining additional details to verify the customer.



CDD is expected to be undertaken on the following circumstances;

- Establishing business relations
- Carrying out occasional transactions: Above USD 3000
- There is a suspicion of money laundering or terrorism financing, or
- The financial institution or DNFBP has doubts about the veracity or adequacy of previously obtained customer identification data.

For further guidance on the KYC Program, we expect the staff to refer to the KNOW YOUR CUSTOMER POLICY (**POB-KYC-002**)

CUSTOMER RISK RATING

Customer risk scoring is part of the Know Your Customer (KYC)/Customer Due Diligence (CDD) pillar of an AML framework. The goal of any customer risk scoring procedure is for Pan Oceanic Bank to understand the risk that a customer (or potential customer) poses to their organization both when they on-board with the bank and across the entire customer lifecycle.

The Current practice is that, Customer Risk Rating is carried out manually using the Risk Matrix F2[POB-CRR-002]. Customers are risk scored **on a scale of 1 to 3** with the following breakdown;

Legend		
0.01	1.50	LOW RISK
1.51	2.20	MEDIUM RISK
2.21	3.00	HIGH RISK

For Individuals account risk rating, following risk components are considered using the corresponding risk weightages applied;

CUSTOMER RISK SCORING- INDIVIDUAL CUSTOMERS				
RC NO	RISK COMPONENTS	SELECTION	RISK SCORE	WEIGHTAGE GIVEN
1.00	TYPE OF PRODUCT			7%
2.00	COUNTRY OF NATIONALITY			40%
3.00	COUNTRT OF RESIDENCE			27%
4.00	EMPLOYMENT			5%
5.00	SOURCE OF FUNDS			8%
6.00	EXPECTED TRANSACTION MONTHLY			13%
7.00	PEP STATUS			
8.00	WORLD CHECK HIT			
9.00	ADVERSE MEDIA HIT			

For Entities account risk rating, following risk components are considered using the corresponding risk weightages applied;

CUSTOMER RISK SCORING- CORPORATE CUSTOMERS				
RC NO	RISK COMPONENTS	SELECTION	RISK SCORE	WEIGHTAGE GIVEN
1.00	TYPE OF PRODUCT			7%
2.00	COUNTRY OF INCORPORATION			40%
3.00	COUNTRT OF INCORP (PARENT CO)			20%
4.00	LINE OF BUSINESS			12%
5.00	SOURCE OF FUNDS			8%
6.00	EXPECTED TRANSACTION MONTHLY			13%
7.00	10% OR MORE OWNED BY PEP			
8.00	WORLD CHECK HIT			
9.00	ADVERSE MEDIA HIT			

Risk Rating should be performed by the Operations staff responsible for the account opening. The ultimate responsibility to feed in the risk rating in the Core Banking system is with the Authorising Officers. Risk Rating should be performed on the following circumstances;

- Account Opening
- Dormant Activation
- Ongoing Review
- Remediation
- As and when required by Compliance

ENHANCED DUE DILIGENCE

Enhanced Due Diligence (EDD) is a risk-sensitive form of Customer Due Diligence (CDD). Requires more detailed information about the customer in addition to the basic Customer Due Diligence (CDD) requirements.

At POB, the following EDD measures are taken, but not limited to;

- Obtaining additional information on the customer;
- Obtaining additional information on the intended nature of the business relationship, and on the reasons for intended or performed transactions;
- Obtaining information on the source of funds or source of wealth of the customer; and
- Conducting enhanced monitoring of the business relationship, potentially by increasing the number and timing of controls applied, and identifying patterns of transactions that warrant additional scrutiny

When a customer is identified as High Risk customer the following form should be filled for Obtaining Senior Management Approval for commencing the business; If any additional documents are required for On-boarding, Compliance will instruct the operations to do so on a case by case basis. (Appropriate measure will be decided by Compliance on a case by case basis for High Risk Customers)

HIGH RISK & PEP FOR NTB IND	F3[POB-HRP-003]
HIGH RISK & PEP FOR NTB ENT	F4[POB-HRP-004]

ONGOING KYC REVIEW/ PERIODIC REVIEWS

One of the most important part of effective KYC program is making sure the customer information available within the bank is up to date and current.

Ongoing KYC Reviews forms an integral part of POB's Anti Financial Crime Control. Information obtained during the client on boarding and account opening may not be up to date. Therefore, obtaining current information about the existing clients is one of the important pillar in fighting against Financial Crime.

Ongoing KYC reviews should be conducted in the following intervals.

Risk Type	Interval
High	Once a Year
Medium	Once in Two Years
Low	Once in Three Years

IT IS THE ULTIMATE RESPONSIBILITY OF THE OPERATIONS THAT CUSTOMERS ARE REVIEWED TIMELY WITHOUT ANY LAPSES. INTERNAL AUDIT SHOULD MAKE SURE THAT ONGOING REVIEWS ARE CARRIED OUT AS EXPECTED.

POB must ensure at the time of ongoing review, that all the documents obtained at the time of account opening are active and valid.

ULTIMATE BENEFICIAL OWNER (UBO)

A UBO is a company's ultimate beneficial owner or the individual who effectively controls the organization. Individuals who possess more than 10% shares of a company is considered as UBO.

In order to identify UBO for the customer of POB, the operations should undertake the following steps;

Receive Company Vitals;

Collect and verify an accurate company record such as identification number, company name, address, status or key management personnel, depending on jurisdictional requirements and the organization's fraud prevention standards. Input that information into workflows.

Analyse the ownership structure and percentage

Determine who has an ownership stake, either through direct ownership or through another party.

Identify Beneficial Owners

Calculate the total ownership stake, or management control, of any person and determine if it crosses the threshold for UBO reporting.

Conduct AML/KYC Checks

Perform AML/KYC procedures, including UBO screening on everyone identified as a UBO. The checks do not limit to PEP screening, adverse media screening, and sanctions screening.

POB PRODUCTS AND SERVICES SHOULD NOT BE OFFERED UNDER ANY CIRCUMSTANCES IF POB COULD NOT ASCERTAIN THE OWNERSHIP STRUCTURE OR THE BASIC KYC DETAILS OF THE ULTIMATE BENEFICIAL OWNERS.

SANCTIONS

WHAT IS SANCTIONS?

Sanctions screening is a control employed within Pan Oceanic Bank ("POB") to detect, prevent and manage sanctions risk. Screening should be undertaken as part of an effective Financial Crime Compliance (FCC) programme, to assist with the identification of sanctioned individuals and organisations, as well as the illegal activity to which POB may be exposed. It helps identify areas of potential sanctions concern and assists in making appropriately compliant risk decisions.

Prohibiting customer relationships, or engaging in transactions or business activity, involving certain countries, territories or Governments, including;

- Iran and the Government of Iran;- – The Bank does not undertake any transaction involving Iran, any party in Iran, or the Government of Iran or any of its political subdivisions, agencies, or instrumentalities;
- North Korea and the Government of North Korea;- The Bank does not undertake any transaction involving North Korea, any party in North Korea, or the Government of North Korea or any of its political subdivisions, agencies, or instrumentalities;
- Syria and the Government of Syria;- The Bank does not undertake any transaction involving Syria, any party in Syria, or the Government of Syria or any of its political subdivisions, agencies, or instrumentalities;
- The Crimea Region;- The Bank does not undertake any transaction involving Crimea, or any of the occupied regions known as Donetsk People's Republic (DNR) and the Luhansk People's Republic (LNR), the areas of the Kherson oblast and of the Zaporizhzhia oblast that are illegally occupied by the Federation of Russia or any party in the five (5) aforementioned regions
- The Government of Venezuela; The Bank does not undertake any transaction related to the provision of financing for or any other dealing involving the Venezuelan Government, including entities owned (50% or more) or controlled by the Venezuelan Government, or any Venezuelan political subdivisions, agencies, or instrumentalities, or those identified by the U.S. or Canada as close associates of the Maduro regime; and

- Cuba and the Government of Cuba – relationships and transactions are prohibited to the extent that they involve a US nexus (that is, the US financial system, US persons or US-origin goods).

Restricting certain transactions and business activity involving, directly or indirectly, certain countries, governments, individuals, entities or industry sectors, including:

- Belarus – prohibiting the direct funding of the Government of Belarus;
- Libya – freezing of assets of certain Libyan entities (and any subsidiaries owned 50% or more or controlled by these entities) held outside Libya as at September 2011;

Russia – engaging in transactions or business activity involving:

- the Russian military, intelligence or defence or related materiel sector;
- the provision of goods, technology and services in support of certain Russian energy projects;
or
- debt and equity of certain entities operating in the Russian financial, energy and defence sectors; and

Zimbabwe – prohibiting the direct funding of the Government of Zimbabwe.

WHEN SHOULD THE SANCTIONS SCREENING BE PERFORMED & WHAT DATAS MUST BE SCREENED

To manage sanctions effectively POB is required to screen their customers in the following situations, It must be noted, that all related parties in the below mentioned criteria are required to be screened against Sanctions List;

- Account Opening
- At the time of applying for credit facility
- Choosing new products
- Dormant Activation
- Performing Periodical Reviews
- Transaction Screening
 - Initiating Outward Transactions (Above USD 3000)
 - Inward Transfers (Above USD 3000)
 - Trade Transactions (Above USD 3000)
- Transaction Monitoring
- As and when required by the Compliance
- **ONGOING SCREENING**

ASSET FREEZING

All department heads, interacting with customers including third party vendors should be screened against the list of designated terrorists and terrorist organizations, including those issued by the United Nations Security Council, Office of Foreign Asset Control of the US, Her Majesty's treasury, and European Union using world check one screening system. Department heads may seek necessary clarification from Compliance if required. In case some customers are identified whose names are similar or close to the names of the designated terrorists and terrorist organizations, each branch / department shall obtain further information on the identity of the customers and report Compliance Department with immediate effect. Such transactions and customer relationship will be on hold and will be notified to SIFIU for further guidance.

Accounts and or relationship other than above mentioned cases, will be frozen only upon a court or regulatory order.

ONGOING SCREENING (OGS) - INDIVIDUALS

As an additional measure to ensure the effectiveness of Sanctions Compliance, the existing customer base of POB is screened against the sanctions database on a daily basis. For individual customers, Solomon Islands Nationals rated as Low Risk as per the risk rating model will be exempted from the Daily Screening.

ONGOING SCREENING (OGS) - ENTITIES

All entities are fed into the OGS database regardless of the risk type posed, however, the in order to apply OGS for the connected parties of the entities, the following matrix must be used. The following list is a non-exhaustive list. Risk Based Approach should be applied while deciding the application of OGS. If in the event the screening personnel finds anyone other than the one mentioned below should also be fed into the OGS, then it is expected to be done so.

For further guidance on the KYC Program, we expect the staff to refer to the TRANSACTION MONITORING POLICY (POB-SCP-003)

RECORD KEEPING

Records of all transactions with customers and beneficial owners, STR and TTR should be retained for at least five years from the date of transaction unless any longer period recommended by regulatory authority. The necessary records on transactions, both domestic and international, for at least five years following completion of the transaction. The records obtained through CDD measures, account files and business correspondence, and results of any analysis undertaken, for at least five years following the termination of the business relationship or after the date of the occasional transaction. The CDD information and transaction records are available swiftly to domestic competent authorities upon appropriate authority. This provision applies whether the account has been closed. Retention may be in the form of original documents, discs, tape or microfilm.

In situations where the records relate to ongoing investigations or transactions that have been the subject of disclosure, they should be retained till conclusion of the investigation subject to minimum retention period of five years. Detail of all transactions should be retained in such a way that these could be evidence in case of court case. Transaction records should contain at least following: -

- a) Customer Name (including beneficiaries) and address
- b) Transaction's nature and date
- c) Transaction currency and denomination.
- d) Account number involved and its type.
- e) Record of identification e.g. Copies or records of official identification documents like passports, identity cards, driving licenses or similar documents), account files and business correspondence.

The information collected from the customer should be treated as confidential and details thereof are not to be divulged for cross selling or any other like purposes. Staffs should, therefore, ensure that

information sought from the customer is relevant to the perceived risk, is not intrusive, and is in conformity with the SIFIU guidelines issued in this regard. If any information to be provided to court as evidence, approval from Chief Executive Officer should be obtained.

CASH TRANSACTION REPORTING (CTR)

A Cash Transaction Report (CTR) is a report of deposits, withdrawals, exchange of currency, or other payment by, through, or to the bank which involves a transaction more than SBD 50,000 in a day. The threshold amount may be reached by a single transaction or by a series of transactions in cash into a single account or by a single customer over a period of one working day. It is an aggregate transaction in cash exceeding the prescribed threshold.

Cash does not include negotiable instrument, nor does it include a transfer of funds by means of cheques, bank draft, electronic funds transfer, wire transfer or other written order that does not involve the physical transfer of cash. These methods of transferring funds do not fall within threshold reporting obligation.

In the case of cash transactions involving foreign currency, the CTR must be submitted to the FIU within two (2) working days, otherwise if the cash transaction only involves local currency (SBD), the CTR must be submitted within fifteen (15) calendar days.

ELECTRONIC FUND TRANSFER REPORTING (EFTR)

For any electronic funds transfer of SBD 30,000 or more (or its equivalent in foreign currency), a reporting entity is obliged to lodge an EFTR with the FIU. In the case of electronic funds transfers involving foreign currency, the EFTR must be submitted to the FIU within two (2) working days, otherwise if the electronic funds transfer only involves local currency (SBD), the EFTR must be submitted within fifteen (15) calendar days.

ONGOING TRANSACTION MONITORING

AML-Compliance ensures that an "ongoing transaction monitoring" is conducted to detect transactions which are unusual or suspicious compared to the customer profile.

Transaction Monitoring at POB is conducted on two levels; AML User (Level 1) and AML Officer (Level 2).

The alerts investigation at Level 1 can be escalated to level 2 in the event if it is found unusual. The level 2 will then conduct its investigations and file suspicious transaction Report in the event Level 2 finds transactions are suspicious.

Sources of Transaction Monitoring

Transaction Monitoring does not necessarily have to originate from the TM system, TM could also be initiated in the following situations;

1. Court Orders
2. Unusual Activity Reports
3. FIU Enquiries
4. Whistle Blower Notifications

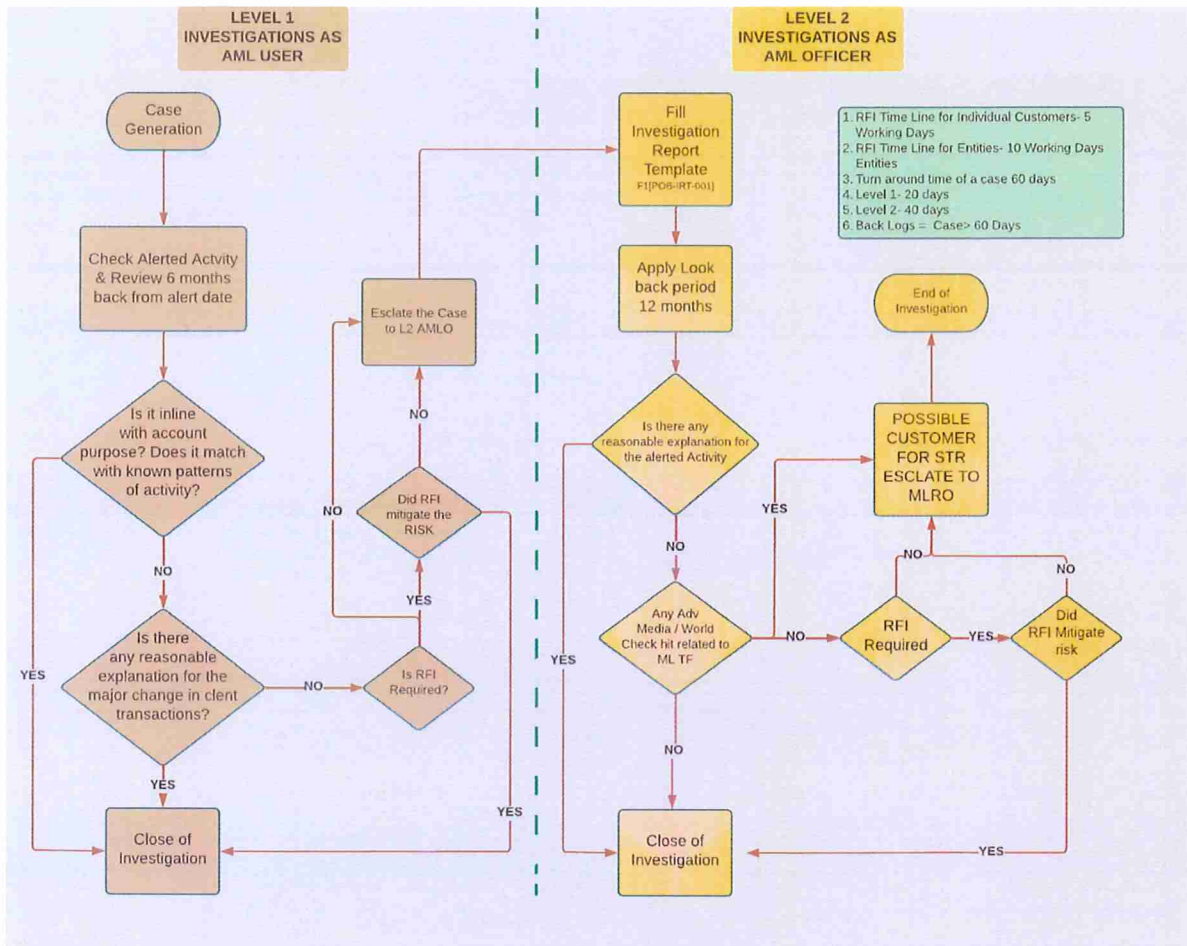
Level 2 Post Investigation Actions

Post Investigation Action (PIA) is a measure that is taken once after the investigation is completed by the Level 2. The following PIAs are taken at the POB;

1. KYC Repair Referral

2. PAB Referral (Personal Account for Business Purpose)
3. STR Filing
4. No Further Action

The below diagram demonstrates the work flow of end to end investigation of alerts.



For further guidance on the KYC Program, we expect the staff to refer to the TRANSACTION MONITORING POLICY (POB-TMP-001)

SUSPICIOUS TRANSACTION REPORTING

This section is intended to highlight situations that may suggest that money laundering is taking place. The customer shall clarify the economic background and purpose of any transaction of which the form or amount appear unusual.

Suspicious Transaction arises from the suspicion created by a specific transaction, which creates the knowledge or belief that the transaction may relate to the legitimization of proceeds from ML/FT activities. Suspicious Activity arises from suspicion relating to general behaviour of the customer in question which creates the knowledge or belief that they may be involved in ML/FT activities out of which revenue might be generated.

All staff should report any suspicious activities/transactions to the Compliance Department using the Unusual Activity Report (“UAR”) template. While reporting, the branches should clearly mention the account name, account number of the customer, amount of the suspicious transaction, nature of transaction (Deposit or Withdrawal) and the reasonable grounds regarding why the transactions are considered suspicious.

INDICATORS OF SUSPICIOUS TRANSACTIONS

Cash

- Cash transactions conducted in an unusual amount from that of usually conducted by the relevant customer.
- Transactions conducted in a relatively small amount but with high frequency (structuring)
- Transactions conducted by using several different individual names for the interest of a particular person (smurfing).
- The purchase of several insurance products in cash in a short period of time or at the same time with premium payment entirely in a large amount and followed by policy surrender prior to due date.

Economically Irrational Activity

- Transactions having no conformity with the initial purpose of account opening.
- Transactions having no relationship with the business of the relevant customer
- Transaction amount and frequency are different from that of normally conducted by the customer

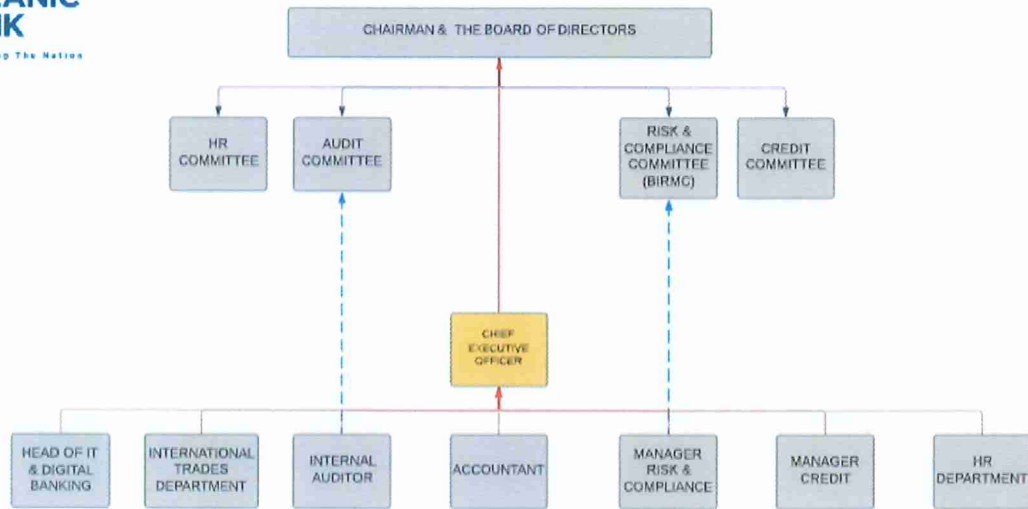
Fund Transfers

- Fund transfers to and from high-risk offshore financial centres without any clear business purposes.
- Receipts of fund transfers in several phases and once accumulated the funds are subsequently transferred entirely to other account.
- Receipts and transfers of funds at the same or approximately the same amount and conducted in a relatively short period (pass-by).
- Receipts/payments of funds made by using more than one (1) account, either in the same name or a different one.
- If multiple inward or outward remittance transaction is conducted with the person from the country or region where terrorist organizations operate.

INTERNAL CONTROLS

In order to perform effective management of AML/FT risks, board level BIRMC Committee of the Bank shall provide governance and oversight of the adequacy and effectiveness of management of ML/FT risks

They will also ensure that AML/CFT programs are aligned with relevant legal and regulatory requirement and AML/CFT strategy is optimally aligned with international best practices. The AML/CFT management of the bank shall be carried out on the structure as depicted in following Organogram.



MANAGER RISK & COMPLIANCE (MRC)

MRC is appointed for implementation of this policy in the bank. Name, Designation, Address, Qualification, contact number, email address of the AML/CFT Chief Compliance Officer shall be informed to FIU for correspondence. MRC is responsible to ensure proper reporting to FIU.

Following tasks should be performed by Manger Risk & Compliance:

- The MRC shall prepare quarterly report on the compliance of AML/CFT Act/Rules/directives issued by Solomon Islands Financial Intelligence Unit and report to BIRMC
- The MRC shall conduct Enterprise Wide AML Risk Assessment on a yearly basis and share it with BIRMC for review
- The MRC shall file Suspicious Activities directly to the Solomon Islands Financial Intelligence Unit

AML/CFT Department

The Bank has created AML/CFT Department under Manager Risk & Compliance with necessary staffs as per requirement. The AML/CFT Department will look after the overall compliance of AML/CFT policies and procedures, with direct reporting to BIRMC (Board Integrated Risk Management Committee)

INTERNAL AUDIT DEPARTMENT

Internal audit department should conduct independent audit function to test the effectiveness of AML/CFT program. The Audit Scope shall cover the following areas but not limited to;

- KYC RISK ASSESSMENT
- TRANSACTION SCREENING
- TRANSACTION MONITORING

- ACCOUNT OPENING
- CASH TRANSACTION REPORT
- TRAINING
- SUSPICIOUS ACTIVITY REPORT
- ONGOING PERIODICAL REVIEWS

ROLES AND RESPONSIBILITIES

Roles and Responsibilities of Board

The Board of Directors shall be responsible for approving the policies ensuring the appropriateness, sufficiency and effectiveness of the policies adopted by the bank based on the overall risk level of the bank on prevention of money laundering and financing of terrorism.

Roles and Responsibilities of Department Heads

Department Heads are responsible for setting the right tone for compliance and ensuring that all business units of the bank is complied with AML & CFT regulations with the assistance of Manager Risk & Compliance. Also they are responsible for taking appropriate actions to resolve concerns raised & reported to them by Compliance Department.

In carrying out the above responsibilities, Department Heads will be assisted by the MRC.

Roles and Responsibilities of Manger Risk & Compliance

- Function as focal point to perform tasks in accordance with the Act, these Rules and the Directives,
- Cause to maintain secure record of transaction,
- Provide information about suspicious or other necessary transaction to the FIU through letter or electronic means of communication like fax, email,
- Provide information about transaction of the branch offices to the FIU in a regular basis.
- Work as a link, counsel and guide for bank management and staffs on AML/CFT Department.
- Ensure that KYC/CDD properly conducted, risk well managed.
- Ensure that staffs are well aware and trained on AML/CFT and most particularly on CDD,
- Risk management and STR detection.

Roles and Responsibilities of Compliance Department

- Implementation and periodic review of the policy. Dealing with any queries on its interpretation.
- Providing AML/CFT compliance related reports like suspicious transaction reports, Cash transactions reports, self-evaluation questionnaire, bank related data etc. to regulatory authority on a timely manner
- Keeping abreast of all technical and regulatory developments on money laundering related matters and advising concerned staffs of any changes required in the policy or SOP.
- Ensuring that all are aware of their responsibilities and obligations, adequately trained in relevant aspects of anti-money laundering processes.
-

Roles and Responsibilities of Operations Department

- Ensure KYC is conducted up to the standards, taking in to consideration of obtaining proper identification documents, understanding the purpose of account, identifying source of funds and wealth
- Ensure Accounts are periodically reviewed and updated with accurate information of the customer
- Identify any loopholes in the day to day operational matters and inform timely to the Senior Management for remediation
- Work in close coordination with AML/CFT department for any related matters

Roles and Responsibilities of Every Employees

- It shall be the responsibility of every individual employee of the bank to remain vigilant to the possibility of money laundering / terrorist financing risks through use of bank's products and services.
- Any staffs who come to know about the involvement of bank's staff or any of its customers in money laundering or terrorist activities must report to the higher management of the bank following standard procedure framed under this policy and shall be mandatory role of all staffs of the bank.

TRAINING

Asp per Money Laundering Proceeds of Crime Act of Solomon Islands and Industry wide best practices, employees must be trained periodically on AML/CFT standards. The key objectives of the AML/CFT training is to;

- To make the employees aware of Money Laundering / Terrorism Financing methods and typologies that are relevant to the organisation
- To help the employees understand AML policies, procedures systems & controls put in place by the organisation
- To help the staff members acquire the skill to identify suspicious activities & unusual behaviour of customers and report them to the AML compliance officer/ Money Laundering Reporting Officer (MLRO)
- To make the employees understand the responsibilities and role of each individual in the organisation towards countering money laundering and financing of terrorism

MAJOR THINGS TO BE INCLUDED IN AML/CFT TRAINING

- The organisation's obligations as per the Solomon Islands AML-CFT Law, Regulations and Directives.
- The consequence of not complying with the AML-CFT Law in the Solomon Islands.
- Major ML-FT risks to which the company is vulnerable and the consequences of such risks
- Steps to be taken to meet the AML obligations as well as identify, manage, and counter ML-FT risks
- Penalties to incur for failing to comply with the AML laws
- How should the employees respond when they detect any suspicious transaction or client

- Case studies based on true circumstances may include how the threat was detected and how it was dealt with proper strategies.
- Providing details regarding the activities and areas within a company that may be highly prone to money laundering and financial terrorism risks

TARGET EMPLOYEES

The leaders of the organisation must ensure that all the relevant employees of the company have received AML training. Employees must be provided with AML training irrespective of whether employed on a permanent or temporary basis. The Manager Risk & Compliance should also train all the new employees as well at a reasonably convenient time. The following types of employees must be included under training scope.

- Customer Facing Staff
- AML/CFT Compliance Staff
- Senior Management and Board of Directors

FORMS & RECORDS

Form Name	Form Number	Form Purpose
UNUSUAL ACTIVITY REPORT FORM	F1[POB-UAR-001]	TO RAISE CONCERNS OF ANY UNUSUAL ACTIVITY OR SUSPICIOUS ACTIVITIES TO COMPLIANCE DEPARTMENT

REVISION HISTORY

VERSION	REVISED BY	REVISED DATE	REVISED ELEMENTS
2 ND REVIEW	DILIP KRISHNASAMY	05 TH NOVEMBER 2018	NOT APPLICABLE
3 RD REVIEW	DILIP KRISHNASAMY	27 TH MARCH 2020	NOT APPLICABLE
4 TH REVIEW	KOGULAN KANSHANATHAN	22 ND DECEMBER 2022	POLICY TEMPLATE WAS CHANGED INCLUDED POB OBLIGATIONS CUSTOMER RISK RATING METHODOLOGY DEFINED UBO RULE INCLUDED ONGOING TRANSACTION MONITORING DEFINED AML GOVERNANCE STRUCTURE
5 th Review	Rohan Fernando	02 nd November 2023	MINOR CHANGES TO THE DOCUMENT.
6 th Review	Rohan Fernando	30 th August 2024	No Changes

THIS POLICY IS MANDATORILY SUBJECT FOR REVIEW YEARLY.

****END OF POLICY****

