AML Policy
&
AML Procedure

uab bank Limited

Version 4

1.
AML Policy

Table of Contents

1. Introduction

1.1 Overview

Money Laundering (ML) is considered as a potent threat to financial system of all countries. The magnitude of its' damage extends to a larger dimension in the form of loss of sovereignty and image of a country. This has been recognized globally and has culminated in concerted efforts to fight this activity by way of enactment of stringent laws, regulations and measures.

The financial activities in Myanmar is still predominantly ruled by cash-based transactions and/or transactions emanating from non-account holders. There is a significant part of economic activities, which are run through informal channels and mechanism and are not in direct control of law enforcement agencies. However, banks are at some level used in these informal channels to move/route funds inside country or between countries.

There is indeed a need to monitor, control and act against the practices that are directly helping individuals, group and organizations to evade taxes, drugs/human trafficking, finance terrorist activities and pose threat to national and international economy.

The uab bank Limited ("uab bank" or "Bank") is committed to:

a. Meeting its national and international regulatory obligations in the identification, treatment and management of Money Laundering (ML)/Terrorist Financing (TF) risk.
b. Protecting the bank from reputational risk and breaches of regulatory requirements that may lead to severe actions, fines and penalties.
c. Safeguarding the bank, its customers and employees from becoming a victim of or unintentional accomplice to ML/TF activities.

1.2 Definition of ML/TF

1.2.1 Money Laundering (ML)

Money Laundering means commission of any of the followings:

a. Converting or transferring of money and/or property, knowing or having reason to know that it is money and/or property obtained by illegal means for the purpose of disguising or concealing the source or for the purpose of assisting before or after commission of the offence to any person who is involved in the commission of any offence to evade the legal action;
b. Changing the true nature, source, location and disposition of money and property, knowing or having reason to know that it is money and property obtained by illegal means and conceal or disguise of ownership or rights of such money and property;
c. Acquiring, possessing or using money and property, knowing or having reason to know at the

time of receipt that it is money and property obtained by illegal means; and

d. Participating, facilitating, aiding, supporting, managing, counseling, being a member of an organised group in committing, attempting to commit or conspiring to commit any offences contained in clauses (a) to (c) by action or omission and pertaining by any other means.

as per Section 3(n) of The Anti-Money Laundering Law, 2014.

It is important for all employees of the Bank to be conversant and familiar with the money laundering process/stages (described below) as they must be vigilant at all times and should any of the aspects involved in money laundering process surface in our business they must be able to identify the warning signs and take appropriate actions.

Placement

The first stage of money laundering is successfully disposing of the physical cash received through illegal activity. The criminals accomplish this by placing it into a financial institution.

Layering

The second stage concentrates on separation of proceeds from criminal activity using various layers of monetary transactions. These layers are aimed at wiping audit trails, disguising the origin and maintaining anonymity for people behind the transaction. E.g. fraudulent letters of credit transactions, over invoicing for goods transshipped from another country, using high value credit cards to pay for goods/services etc.

Integration

The final link in money laundering process is called the integration stage. This occurs when the laundered or cleaned up money is legitimately brought back into financial systems operated by end user and when it is safe and insulated from enquiry by any agency. E.g. loan back technique or loan-default technique where the lender bank seeks to recover its assets (loans to money launderers) by attaching the securities held by Bank which exist in the form of dirty money.

1.2.2 Terrorist Financing

Terrorist financing provides funds for terrorist activity. The main objective of terrorist activity is to cause substantial property or human damage; or seriously interfering with or disrupting essential services, facilities or systems. There are two main sources of terrorist financing – financial support from countries, organizations or individuals. The second source, revenue-generating activities, which may involve drug trafficking, human smuggling, theft, robbery and fraud to generate money. Funds raised to finance terrorism usually must be laundered and thus anti-money laundering processes in banks are important in the identification and tracking of terrorist financing activities.

uab bank shall build measures to monitor, identify and report such funds received or sent using the uab bank's system. The Bank shall take caution while doing transaction, account opening or carrying banking activities if in any circumstances the name of any banned organization or individual (involved in terrorist activities) appears as payee/endorsee/applicant and report such transaction as and when detected.

The Bank shall endeavor to get the list of such organization/individuals to the best possible means or mechanisms.

1.3 Purpose

uab bank Anti-Money Laundering Policy broadly is based on following legislations:

- The Anti-Money Laundering Law, 2014;
- The Money Laundering Rules, 2015;
- The Counter Terrorism Law, 2014;
- The Counter Financing of Terrorism Rules, 2015;
- Directive for the CDD Measures, 2019;
- AML-CFT Risk Based Management Guidance Note, 2015;
- AML Order 45/2019 of President Office; and
- FATF 40 Recommendations

among others. Also, this Policy incorporates agreed international rules and regulations and best practices, which directs uab bank's banking activities to proactively comply with AML prudent practices.

The purpose of this policy is to establish governing standards to insulate the bank from being used as a component of financial system to launder money. In the light of above, the purposes of this Policy are:

a. To enable the Bank to conduct clean, commercial business, conforming to standards set by the industry; laws and regulations of the country/governing authorities;
b. To follow, the internationally accepted standards used for Know Your Customer (KYC) compliance, as far as practical;
c. To report and take suitable actions, upon detecting the suspicious activity involving money laundering as directed by Central Bank of Myanmar or any other laws formulated from time to time;
d. To make the employees and customers aware about the seriousness of the impact of ML activities;
e. To set-up administration processes within the Bank to implement the AML standards;
f. To comply with applicable laws in Myanmar with reference to ML and adhere to the standards accepted internationally by the financial world on the subject, as far as practical;
g. To train staffs so that they can identify ML-FT transactions;
h. To make Bank's staff aware of the AML Policies and Procedures;
i. To avoid the opening of anonymous, UN sanctions list and fictitious accounts; and

j. To provide the knowledge to staff to verify the identity of prospective customers before they can establish account relationship.

1.4 Scope

The four tenets covered in this AML Policy are:

a. Know Your Customer (KYC)
b. Risk Assessment of Accounts
c. Accounts Review
d. Suspicious and Large Value Transaction Monitoring and Reporting

This Policy intends to increase the awareness of money laundering activities amongst the staff, customers and general public and its ill effects and to effectively counter/guard against money laundering at all times.

Considering the sensitiveness of the matter on global arena the Bank has developed this Policy in order to be proactive in dealing with issues related with money laundering within the purview of the local law and guidelines of Central Bank of Myanmar.

Compliance and willing to adopt this Policy will be the primary goal while implementing it. All uab bank employees including employees of its Subsidiaries must comply with this Policy.

2. Governance for AML

Governance structure assigns responsibilities for the effective implementation of Bank's AML policies and monitoring structure and overall accountability. To align with our business requirements, it incorporates guidance from global standards, CBM circulars and directives and elements consistent with evolving best practices.

2.1 AML-CFT Governance

2.1.1 Board Responsibilities

The Board of Directors has supreme authority and responsibility to implement robust guidelines relating to AML-CFT in the Bank. Following are the main responsibilities of the Board of Directors:

a. Approving, enforcing AML Policy in the Bank;
b. Establishing and approving the organizational structure, roles and responsibilities in AML-CFT of individual department/unit;
c. Oversight on the risk management on AML-CFT;
d. Review the AML-CFT status of the bank on regular basis and provide feedback if any to the

management or Compliance Officer ("CO"); and

e. Any amendments/cancellation or revision in the Policy shall be at the discretion of the Board of Directors.

2.1.2 Board Risk Committee (Board Level) Responsibilities

a. Review and support AML Policy for the purpose of approval of Board of Directors;
b. Review the AML-CFT status of the bank on regular basis and forward to Board for further review;
c. Periodically review and update AML Policy; and
d. Monitoring AML-CFT related activities for the implementation of AML Policy.

2.1.3 Senior Management Responsibilities:

2.1.3.1 Chief Executive Officer

Chief Executive Officer is a head of the management of the bank who ensures that the Bank has implemented AML Policy and Procedures effectively. Following are the main functions of the Chief Executive Officer:

a. Ensuring that policies and procedures for AML-CFT Program are in line with the changes and developments in products, services and information technology of the bank as well as in line with development in modus for money laundering or terrorist financing;
b. Approving and enforcing AML/CDD Procedures of the Bank;
c. Ensuring that the implementation of AML-CFT Program is based on established policies and procedures;
d. Ensuring that all employees, particularly employees of related work units and new employees have participated in ongoing training related to AML-CFT Program;
e. Supervise the AML-CFT Unit work in implementing AML Policy and Procedure;
f. Based on the recommendation of CO for any action to respective staff for not complying AML Policy and Procedure, Chief Executive Officer shall take initiative for further action to such staff;
g. Ensuring that sufficient recourses, suitable workplace, required access to information, document and staff have been managed to do compliance function effectively and efficiently; and
h. Other discretionary authorities shall be exercised as delegated in the Policy or by the Board from time to time.

2.1.3.2 Compliance Officer (CO)

The CO shall be of a Senior Management grade of the Bank and who shall be the focal point for implementation of the AML Policy, Procedures and regulatory requirements relating to AML-CFT. The Bank shall have a separate AML-CFT Unit under CO, which shall implement CBM Directives, AML Act/Rules, CFT Act/Rules, AML Policy and Procedures etc. Bank may appoint Assistant Compliance Officer

(ACO), who shall assist in implementation of entire responsibilities of CO.

Rights of the CO

a. Direct access to any documents, transactions and document related to accounts;
b. Right to demand/acquire any information, details, account statements or documents from any staff of the bank; and
c. Direct access to any documents, information required for implementation of the AML-CFT Act, Regulations and Rules, CBM Directives/Circulars and Bank's Internal Policy and Procedures.

Responsibilities of CO

a. Effective policy, procedure and system shall be developed for the implementation of AML-CFT Program;
b. Suspicious Transaction Report, which is sent by Department, shall be reviewed/analyzed and sent to FIU;
c. Ensure timely reporting of Threshold Transaction Report (TTR) to FIU;
d. CO shall consult with another department or get specialist feedback, if needed;
e. CO shall prepare the report on the AML-CFT status of the Bank;
f. CO shall instruct to Bank's management / all departments for complying the AML Policy, Procedure, CBM Directives and related laws and regulations;
g. CO shall make recommendation to take actions to those staffs who have not provided required information, document and account details and/or who do not cooperate for the implementation of the AML Policy/Procedure to CEO and HR;
h. CO shall submit the report on AML-CFT status to Board Risk Committee. BRC shall submit those reports to uab bank Board on regular basis. uab bank Board shall review such report and provide feedback to Board Risk Committee or Management accordingly;
i. CO shall share the knowledge about the AML-CFT, its impact to the bank and other details to the Shareholders, Board Members, Top Level Management and Staffs. External resource person may also be used, if needed;
j. CO shall facilitate to provide regular training about the AML-CFT to the staff for enhancement of AML-CFT knowledge and effective implementation in the bank; and
k. As prescribed by Regulator.

2.1.4 Branch Compliance Officers

Service and Operations Managers of the respective branches shall act as Branch Compliance Officer("BCO"). BCO of respective branch will have primary responsibility to implement of AML Policy and related Procedures. The major responsibilities of BCO will be as follows:

For AML/CFT Compliance:

a. Ensure that the Bank's AML Policy is available at the Branch and understood by the staff
b. Ensure Customer Due Diligence (CDD) and Customer Identification process is followed in the opening an account
c. Ensure that Enhanced Customer Due Diligence is followed for high risk Customers
d. Report any suspicious transaction by filing a Threshold Transaction Report (TTR) to Myanmar Financial Intelligence Unit (MFIU)
e. Identify the Suspicious Transactions/Activities and report to CO/ACO

For other Compliance matters:

a. Policies, Procedures and instruction of the Bank are adhered to at all times.
b. Ensure that staff at the branch are adequately trained with regard to the Bank policies, procedures and instructions. Both training at the branch and Training School is encouraged.
c. All report to Central Bank, Regulatory Authorities or Head Office are accurately prepared and sent in timely manner.

2.1.5 Director-Finance

Following are the main responsibilities of Director-Finance:

a. The Director-Finance shall be responsible for ensuring proper implementation, control, monitoring and reporting of entire operation of the Bank; and
b. As directed by the AML/CDD Procedure.

2.1.6 Director- Operations

Following are the main responsibilities of Director-Operations:

a. To ensure proper implementation of AML-CFT Act, its Regulations and Rules, AML Policy and Procedures;
b. To instruct Branches to comply with AML-CFT Policy, Procedure, CBM Directives, etc.;
c. To instruct to respective branches and department for rectifying the discrepancies on AML-CFT related matters;
d. To make arrangement for digitalization of all customer information as per AML-CFT Law/CBM Directives;
e. To ensure proper resources, controls and best practices are advised to branches and Line departments; and
f. As directed by the AML/CDD Procedure.

2.1.7 Business Directors, Zone Heads and Head of the Departments

Following are the main responsibilities of Business Directors, Zone Heads and Head of the Departments:

a. Business Director, Zone Heads and Head of the Departments shall be responsible for respective Department/Zones/Units in ensuring proper implementation, control, monitoring and reporting activities designed to prevent Money Laundering and Terrorist Financing as per AML-CFT Law, Regulations and Rules, AML Policy, AML/CDD Procedure et al;
b. Responsible to reasonably assure that staffs under their control have required knowledge and are not involved in any money laundering and terrorist financing activities; and
c. As directed by the AML/CDD Procedure.

2.1.8 Branch Manager

Following are the main responsibilities of Branch Manager:

a. To ensure proper implementation, control, monitoring and reporting procedure across the branch under their control to prevent money laundering and terrorist financing;
b. To ensure that all customers on boarding process, transaction activities in the branches follow prescribed AML-CFT practices of the bank;
c. To ensure that all customer related documents of Account Opening/KYC form including transaction shall be kept in prescribed way and are provided to Compliance Department/AML-CFT Unit or Authorized Authority immediately or as and when required;
d. To ensure all staff of the branch have gone through in-house training on AML-CFT at least once every year. If not, Branch Manager shall escalate that information to uab Banking School for providing training to those staff.
e. Responsible to reasonably assure that staffs under their control have required knowledge and are not involved in any money laundering and terrorist financing activities;
f. Branch Manager shall be primarily responsible for monitoring high value and high-risk transactions, detecting suspicious activities and reporting suspicious transactions/activity to CO/ACO.
g. Approve onboarding of High-Risk customers; and
h. As directed by the AML/CDD Procedure.

2.1.9 Information Technology Department (IT)

IT Department is responsible for providing necessary data and support to AML and CFT Unit.

2.1.10 Internal Audit Department

Internal Audit is an independent body, which shall test whether bank has effectively followed the AML-CFT Law, Regulations and Rules, CBM Directives and AML/CDD Policy and Procedures of the Bank. Following are the main role and responsibility of Internal Audit Department:

a. Internal Audit Department shall independently review the compliance of AML Policy and AML/CDD Procedure;
b. Internal Auditor shall be responsible for conducting checks and reviews to ensure that the control and monitoring and reporting procedures under this Policy are followed;
c. Internal Audit shall independently check and verify the AML Policy and Procedure of the Bank, AML-CFT Law, Regulations and Rules and CBM Directives at Department/ Branch/Unit and report it accordingly; and
d. Compliance on AML-CFT and updated status of Department/Branch/Unit shall be provided to AML-CFT unit on quarterly basis.

2.1.11 Human Resource Department (HRD)

Following are the main role and responsibility of Human Resource Department:

a. To screen the staff from AML perspective (criminal activities, sanction list etc.) before recruitment of staff. It is also applicable for outsourced staffs;
b. HR shall ensure that the due diligence of all employees is updated regularly and recorded;
c. Transactions in all staff accounts shall be monitored by HR to identify money laundering activities;
d. Liaise with uab Banking School to arrange a training program related to AML-CFT to staffs on need basis; and
e. Departmental punishment/action as recommended by CO/CEO, shall be taken against those staffs that do not comply the AML-CFT Law, Regulations and Rules, CBM Directives and AML Policy and Procedures.

2.1.12 uab Banking School

Following are the main role and responsibility of uab Banking School:

a. To arrange trainings related to AML-CFT to all staff at least once a year; and
b. To facilitate to provide national and international training on AML-CFT to CO, staffs of AML-CFT Unit and any staffs who are directly involved in AML-CFT activities.

2.1.13 Individual employee

Following are the main role and responsibility of individual employees:

a. Individual employee shall be more vigilant to possibility of Money Laundering/Terrorist Financing risks through the use of Bank's products and services.
b. Any staff that comes to know about the involvement of Bank's staff or any of its customers in money laundering or terrorist activities must report same to the CO/ACO of the Bank.

3. Know Your Customer/ Employee

3.1 Know your customer (KYC)

KYC is the process of verifying the identity of clients. The term is used to refer to the Bank regulation, which governs these activities. Banks are increasingly demanding that customers provide additional information, to verify their probity and integrity. Know Your Customer policies are becoming important globally to prevent identity theft, financial fraud, money laundering and terrorist financing. uab bank shall not engage in business relationship with customers, whose identification and KYC has not performed.

3.1.1 Customer Acceptance Principles (CAP)

uab bank's Customer Acceptance Principles (CAP) lays down the criteria for acceptance of customers.

a. Account shall be opened only in the name of natural and legal person/organization, the name being the same as in the primary identifying document. Bank shall only open the account based on required document and information as prescribed in AML Act, Rule, CBM's Directive on the CDD Measures, and Bank's AML/CDD Procedure.
b. Account shall be opened after identification of customer and verification of required information/document. Necessary checks are done before opening a new account to ensure that the identity of the customer does not match with any person involved in money laundering or with banned entities such as individual terrorists or terrorist organizations etc.
c. P. O. Box addresses are not acceptable as a recorded residential address. (P. O. Boxes are acceptable as mailing address).
d. Accounts must not be opened or retained (or one-off transactions undertaken) where it is known or suspected that a customer or prospective customer is involved in money laundering or terrorist financing. In such circumstances the account opening process should cease and, where appropriate, attempted suspicious activity should be reported to CO or ACO.
e. The bank shall not open accounts for shell banks or hold alternate name/ anonymous name (altering form the primary identity document) or fictitious name or blank name or numbered/alphanumerical characters accounts.
f. Accounts shall not be opened, or one-off transactions undertaken, for sanctions list individuals or entities.
g. In case, power of attorney holders, beneficial owners, third party mandates or guarantors in a relationship, such persons should be identified in the same manner as the primary customer. The documents for such arrangement should be verified and the reason for the arrangement understood and recorded.

3.2 Purpose of KYC

a. To establish procedures to verify the identification of individuals or corporate or other institutional accounts;
b. To detect suspicious transaction;
c. To establish process and procedures to monitor high value and suspicious transactions; and
d. Establish systems for conduction of due diligence and reporting of such activities.

3.3 Mechanisms Deployed for KYC

The Bank shall use various mechanisms for Customer Due Diligence/ Know Your Customer. These activities shall be carried out at the time of account opening for all the types of accounts opened. uab Bank shall deploy all or the combination of any of the below mechanisms for KYC/CDD.

a. Customer Identification and Profiling
b. Risk Assessment
c. Documentary Evidence
d. Verification of Documents as per original
e. Identification of Beneficial Owner
f. Politically Exposed Person (PEP) verification
g. Restriction on Account Opening

3.3.1 Timeline for obtaining KYC

KYC of the customer can be obtained after establishing a business relationship or after doing any transactions in the following cases after approval of Branch Manager

a. when the verification can occur as soon as reasonably practicable
b. when it is not necessary to interrupt the normal conduct of business
c. when ML and TF risks are effectively managed

Bank will adopt the risk management procedures with respect to the conditions under which as customer may utilize the business relationship prior to verification. The procedures will include a set of measures such as a limitation of a number, types and/or amount of transactions that can be performed and the monitoring of large or complex transactions being carried out outside of expected norms for that type of relationship.

Notwithstanding anything contained above, KYC must be obtained prior to account opening/transaction in the following cases:

a. If the customer is a high risk or PEP or a family member or relative to a PEP.
b. If the customer or transaction seems suspicious and high value transaction.

3.4 Know your customer for High Risk account

Banks shall ensure whether the customers, beneficial owners and potential customer are high-risk customer or not. Risk management procedure for High Risk customer shall be described in the AML/CDD Procedure. In case of Local/Foreign customers who are vested with significant authority or PEPs or customers of foreign organization, which operate businesses categorized as high risk or in case of nationals who are high-risk customers, the following conditions shall be followed:

a. Approval of respective Branch Manager must be obtained before establishing business relation;
b. If the existing customer falls under high-risk customer, approval as per above clause (a) must be obtained immediately;
c. Bank shall identify the source of wealth/fund of high-risk customer or beneficial owner;
d. Ongoing monitoring of the business relation with the customers and their transactions; and
e. Conduct Enhanced Customer Due Diligence (ECDD) of such high-risk customer.

3.4.1 Enhanced Customer Due Diligence (ECDD)

Bank shall carry out the ECDD in following conditions:

a. High risk customer;
b. Customers of high-risk country and customers of countries, which have partially implemented FATF standards;
c. PEPs, his/her family members and close associate person;
d. Customer who make huge value of transaction, complicated and unnatural in nature and transaction, which have no clear financial or legal objective;
e. A customer who has business relation or transaction with individuals, companies or any legal entity that has not followed the FATF standards or such individuals/companies/legal entities belongs to high-risk country;
f. Customer who use the new technology, which has the potential risk for ML/TF;
g. Customer who is suspected of ML/TF; and
h. As prescribed by Regulator.

3.5 Provisions regarding KYC of existing customers

In case of existing customers maintaining account and/or doing transactions before implementation of this Policy, customer shall be identified, documents shall be reviewed and risk grading shall be done on the basis of customer and/or beneficial owner, business relations, transactions, manufacturing or service details, country or geographical region or its distribution methods as per this Policy.

3.6 Beneficial Owner

Beneficial Owner means the ultimate natural person who owns or controls money or property or

customer or (on whose interest the transaction is carried out). It also means the ultimate natural person who controls or exercises such powers to a legal person or arrangement. Identity of such beneficial owners must be established in line with the AML CDD Procedure on following conditions:

a. If the transaction is done on behalf of actual customer.
b. If bank identifies that the transaction is done by someone else other than the actual customer.

Bank shall open an account only if the beneficial owner can be identified. If the bank cannot identify the beneficiary owner or customer is unable to provide the information of beneficial owner, relationship with any person or entity shall not be established.

3.7 Know Your Employee (KYE)

uab bank shall have processes in place that provides reasonable assurance of the identity, honesty and integrity of prospective and existing employees as per CBM Directive. Human Resource Department shall incorporate the provisions of KYE in their recruitment process and the KYE of the employees shall be reviewed on regular basis.

4. Prevention of Money Laundering (ML)/Terrorist Financing (TF)

This Policy is for the prevention of ML/TF risk faced by the bank. The bank is committed to fully comply with the applicable AML/CFT rules and regulations of the country. The Bank also adopts not only the AML-CFT rules of existing country, but it shall adopt international best practice as applicable. Senior Management has fully committed to establish appropriate Policy and Procedure as per requirement of the AML-CFT Law, Regulations and Rules and CBM Directives/Circulars. Senior Management shall also facilitate to implement these policies and procedure in the Bank and make arrangement to monitor and control risk arising from money laundering/terrorist financing activities in its daily operation and business transactions. The Senior Management of the Bank shall promote compliance as a core value and culture of the bank and the bank will not enter, or maintain, business relationships that are associated with excessive Money Laundering/Terrorist Financing risk which cannot be mitigated effectively.

4.1 New Technologies

a. The Bank shall assess the money laundering and terrorist financing risk arising from new technologies and business practices on bank, non-face-to-face banking and new technologies.
b. Risk assessment in the above case must be done before implementing such new technologies, business practices or distribution system.
c. The Bank shall prepare proper method for the management of risk arising from the above process before implementing such new technologies in the bank.
d. The Bank shall develop a procedure for the mitigation of risk arising due to non-face-to-face

banking with customer.

5. Risk Assessment

a. Bank shall analyze the customer profile based on country of origin, geographical region, nature of business, occupation, type of customer, service or product, transaction and delivery channels for the risk assessment.
b. Bank shall also follow the basis of national risk assessment or risk assessment by regulatory authority after receiving national risk assessment report.
c. Bank shall identify the risk grade based on the above-mentioned section (a).
d. Bank shall record such assessment and report to regulatory authority, if required and also report such assessment when it is required by authorized body.
e. Bank shall categorize the customer in different category (High, Medium, Low) as per the risk level.

6. Suspicious and Large Value Transaction

This section of the document is intended to highlight about the suspicious transaction and large value transaction. The Bank will refuse any transaction which based on explanation offered by the customer or other information, reasonable grounds exist to suspect that the funds may not be from a legitimate source or are to be used for an illegal activity such as terrorism, human trafficking etc. The Bank shall use reasonable judgment in determining the suspicious transactions.

The understanding of customers' identity vis-à-vis his stated norms of dealings, services, etc. would also have a bearing on transactions before they are viewed as suspicious transactions hence cautious approach in the process is very essential. Under no circumstances, Bank will alert a customer about his transactions being considered suspicious or that reporting is underway. The Bank will make prompt report of suspicious transactions, or proposed transactions to Financial Intelligence Unit (FIU) through ACO/CO.

Bank shall report a suspicious transaction and large value transaction within given deadline. Bank shall report after identifying any suspicious customer, transaction or property in the following cases:

1. In case of any suspicion of any charges relating to money laundering and/or terrorist financing or suspected of any other charges or any other grounds for suspicion.
2. If a person or organization is suspicious of being involved in any Terrorist Financing or a part of any terrorist group or has done any financing related to terrorist activities.

Suspicious Transaction Reporting shall be done even in case of any attempt of doing transaction related to money laundering and/or terrorist activities. Additional provisions for suspicious transactions, format of suspicious transaction reporting, reporting methods and procedures shall be prescribed in the

AML/CDD Procedure.

7. Wire Transfer

Wire transfer is a method of electronic funds transfer from one person or entity to another. A wire transfer can be made from one bank account to another bank account within the national boundaries of a country or from one country to another. Wire transfers does not involve actual movement of currency, they are considered a secure method for transferring fund from one location to another. Detailed AML measures relating to wire transfer shall be prescribed in the AML/CDD Procedure.

8. Correspondent and Shell banks

8.1 Correspondent banks

The Bank shall implement risk based due diligence procedures that include, but are not limited to, the following – understanding the nature of the correspondent's business, its license to operate, the quality of its management, ownership and effective control, its AML Policies, external oversight and prudential supervision including its AML-CFT regime. The Bank shall conduct required due diligence while establishing SWIFT Relationship Management Application (RMA) with any correspondent banks.

Additionally, ongoing due diligence of correspondent accounts shall be performed on a regular basis or when circumstances change. Bank policies also ensure that we do not offer payable through accounts/pass through accounts. Senior Management of the bank shall approve all new correspondent-banking relationships.

8.2 Shell Bank/Company

A shell bank/company is a financial institution that does not have a physical presence in any country. uab bank shall not conduct business with shell bank/company.

9. Account and Transaction Monitoring

1. Banks shall carry out ongoing due diligence of customers, beneficial owners or transactions by performing the following actions:

    a. Checking whether the transaction has been done as per the description provided to the Bank regarding the business and its risk until the relationship lasts and obtain information about the source of income; if necessary.
    b. Updating the records through review in order to ensure that the documents and information about the Politically Exposed Persons (PEPs) are up to date.

c. Regular inspection of relationship with customer and their transactions related to cross- border wire transfer through correspondent banking.
d. Other functions prescribed by the regulatory authority.

2. The process (automated or manual) of monitoring transactions after the execution to identify unusual transactions, including monitoring single transactions as well as transaction flows, for subsequent review and, where appropriate, and reporting to the authorities. The purpose of transaction monitoring is to provide ongoing identification of suspicious activity from customer transaction data.

Bank shall give special care while executing the following transactions:

a. All transactions which are huge, complicated and unnatural in nature and which do not have clear financial or legal objective.
b. Customers of high-risk country and customers of countries, which have partially implemented FATF standards.
c. Any other transaction mentioned by the regulatory authority.

Investigations shall be done in case of above transactions and record of the same shall be kept.

10. Reporting Related to AML-CFT

If the bank suspects or has reasonable grounds to suspect that funds are proceeds of a criminal activity, or are related to terrorist financing, CO shall report the same to FIU. Concerned staffs are prohibited from disclosing the fact that a Suspicious Transaction Report (STR) or related information is being reported to the FIU. Process for raising the STR and report to FIU shall be described in the AML/CDD Procedure of the bank.

The Bank shall also generate TTR (Threshold Transaction Reports) and other reports related to AML-CFT and report it to FIU/Regulator as requested by them.

11. Provisions regarding restriction in transactions

Business relationship shall not be maintained, or transactions shall not be done in the case of the following customers:

a. Customer is not providing necessary information and documents regarding identification of customer as per AML/CDD Procedure.
b. Customer who could not be identified from the information and details obtained from the customer.
c. Beneficial owner cannot be identified.

d. Purpose and the intended nature of the business relationship cannot be identified.

Business relationship must be stopped in case the existing customers fall under any of the clauses mentioned above. If the bank is unable to obtain the proper KYC then it should not open the account, commence business relations or perform the transaction; or should terminate the business relationship; and should consider making a suspicious transactions report in relation to the customer.

12. Retention of Records

Bank shall maintain records of the following information:

a. Copies of all records obtained through the customer due diligence process;
b. Including documents evidencing the identities of customers and beneficial owners, account files and business correspondences, for at least 5 years after the business relationship has ended, or a transaction with a customer who does not have an established business relationship with the bank has been carried out;
c. All records of transaction, both domestic and international, attempted or executed for at least 5 years following the attempt or execution of the transaction. Such records must be sufficiently detailed to permit the reconstruction of each individual transaction; and
d. Copies of reports sent and related documents for at least 5 years after the date the report was made to Financial Intelligence Unit.

13. Confidentiality of Customer Information (Tipping Off)

Bank's staff shall not disclose the customer information such as report, document, record, statement and other information, which are prepared/maintained as per the AML-CFT Law, Regulations and Rules and CBM Directives/Circulars to other customer or any unauthorized persons. The concerned staffs shall take utmost precautions that they do not leak such confidential information. Tipping Off is a punishable offence.

14. Policy Compliance

14.1 Employee Training Program

Training shall be provided to business units that offer products and services that are subject to the legislative requirements. Staff involved in customer facing areas, remittance, SWIFT etc., of the bank shall receive periodic training and reminders on the detection and reporting process for suspicious activities. Communications of changes to AML-CFT legislation or any emerging risks will be communicated to the relevant staff.

In addition to the above, uab Banking School shall make sure that the training on AML/CDD is also be provided to all the staff using internal or external means.

14.2 Branches and subsidiary companies

a. Branches in Myanmar or any other country and all the subsidiary companies wherein the bank holds more than 50% of shares shall be liable to follow the AML Policies and Procedures formulated as per AML Acts and Rules & other regulatory instruction.
b. Following subject matters must be followed for the implementing AML- CFT:
    1. Conveying information regarding identification of customer and management of the risk related to money laundering and terrorist financing;
    2. Conveying information regarding programs related to customer, transactions, account, audit, compliance and AML & CFT; and
    3. Utilization and Confidentiality of the information conveyed as per above-mentioned clauses.

c. uab bank shall ensure that the provisions applicable to banks, which are mentioned above are also applied to branches and majority owned subsidiaries located abroad, especially in countries, which do not or insufficiently apply the FATF Recommendations, to the extent that local applicable laws and regulations permit. When local applicable laws and regulations prohibit this implementation, the foreign branches should inform competent authorities in the country of the parent institution.
d. If the provisions mentioned in clause (c) above are not enough to prevent money laundering and terrorist financing, then the branches and subsidiaries located in the country must be closed.

14.3 Amendment to the Policy

Circular/Directives of CBM and FIU and the AM/CFT Act and Rules of the country shall form integral parts of this Policy. If any section/sub- section/clause of this Policy contradicts with the country's laws, the later shall be valid to the extent of contradiction.

This Policy is subject to annual review. There shall be a separate AML/CDD Procedure formulated by the bank and implemented after approval of Board.

14.4 Compliance Measurement

CO or the designated officer will verify compliance to this Policy through various methods, using various tool, reports, internal and external audits, and feedback to the Policy owner. Banks auditors shall conduct programs of audits and compliance testing of this Policy and operational procedures applicable to AML. The frequency and scope of the audits and compliance tests are determined through a risk-based approach, where higher risks units/processes are audited and tested more frequently.

Similarly, AML-CFT Unit or Compliance Department may conduct assurance review in some branches/departments on sample basis for the compliance test of this Policy.

14.5 Exceptions

Any exception to this Policy must be acknowledged by CO and approved by the bank management.

14.6 Non-Compliance

An employee found to have violated this Policy might be subject to disciplinary action, as per the provisions in the prevailing Employee Handbook.

14.7 Repeal and Saving

14.7.1 Anti Money Laundering Policy Version 3 is here by repealed.

14.7.2 Activities carried out relating to AML monitoring, implementation, reporting etc., under Anti Money Laundering Policy Version 3 shall be considered as done under this Policy.

2.
AML Procedure

1. Introduction

1.1 Overview

Together with the Anti-Money Laundering Policy, this Procedure document is intended to assist in the implementation of AML/CFT Law, its Regulations and Rules, Directives and Circulars of Central Bank of Myanmar and AML Policy of the bank in a consistent manner, for all the units across the bank.

This document outlines a clear procedural guideline for account opening, risk categorization, list of documents required for opening various accounts, on-going account monitoring, record retention, threshold transaction reporting, detecting suspicious transaction, reporting suspicious transactions amongst others. This procedure sets minimum mandatory requirements for all units while conducting Customer Due Diligence (CDD) for anti-money laundering and terrorist financing prevention purposes.

An inadvertent association with the customers involved in the criminal activities could expose the bank to money laundering and terrorist financing risk hence the bank must try to obtain as much information about the customers.

1.2 Purpose

The purpose of this document is to establish a standard procedure for identification, monitoring and management of Anti Money Laundering and Combating Financing Terrorism / Customer Due Diligence issues that may arise during the banking operations conducted by the bank. This document incorporates the requirement set forth by the bank's Anti-Money Laundering Policy (AML Policy), Directives and Circulars issued by Central Bank of Myanmar and MFIU (Myanmar Financial Intelligence Unit) from time to time. This document is intended to assist in the implementation of AML-CFT Laws, its Regulations and Guidelines on Suspicious Transaction Reporting and Threshold Transaction Reporting Guideline of Central Bank of Myanmar and AML Policy of the bank in a consistent manner, for all the units across the bank.

1.3 Scope

The scope of this procedure includes all staff of the bank who are directly or indirectly in contact/relation with the client for selling bank's products and services.

2. Customer Due Diligence (CDD)

CDD information comprises the facts about a customer that should enable an organization to assess the extent to which the customer exposes bank to a range of risks. CDD measure shall comprise of the following:

a. Identifying the customer based on documents, data or information obtained from a reliable and independent source;
b. Identification of the beneficial owner of the client/customer to the possible extent and taking risk-based and adequate measures to understand the structure of ownership and control of the client/customer;
c. Obtaining information on the purpose and intended nature of the business relationship; and
d. Conducting ongoing monitoring of the business relationship including ensuring that the transactions being

conducted are consistent as per the nature of the business and details/data provided by the customer. The risk profiling shall be monitored/reviewed on timely basis including where necessary, finding out source of funds and keeping data/details or information up to date.

2.1 Know Your Customer (KYC)

KYC Stands for "Know Your Customer". Know Your Customer (KYC) is an important step developed globally to prevent identity theft, financial fraud, money laundering and terrorist financing. The objective of KYC is to enable us to know and understand our customers better to manage the risks prudently.

KYC is not only regulatory and legal requirement; but also, can form basis to have better business relationship with the client.

The process of KYC entails acceptance of the customer by identifying them. That is verifying the identity by using reliable and independent documents or information. Then after monitoring their transactions and managing the risk by risk profiling them.

Situations when KYC is required?

KYC must be carried by each unit/department/branch of the bank while dealing with customers. KYC procedure needs to be adhered to during following instances:

- While opening an account
- While providing loan
- While providing occasional transaction of customers who has not established relationship with the bank if the transaction amount is equal to or above the threshold of Kyat or any other currencies equivalent of (USD 1,000) non – customer (walk in customer). Further, if the amount exceeds USD 15,000 or equivalent in any currency enhanced due diligence shall be carried out.
- When there are not enough documents with the bank for existing account
- When additional authority has been given to a third person for operation of account.
- When there is change in signatory, beneficial owner and board of directors.
- When the bank feels it is necessary to obtain additional information from existing customers based on conduct of the account etc.

All staffs of Bank are accountable to perform KYC of its customers as per the instruction of CBM (Directive on the CDD Measures), Bank's AML Policy and Branch Management Guidelines Manual-Unit 2 (Page 47-73). Detailed procedure on KYC can be referred from Branch Management Guidelines Manual-Unit 2.

2.2 Enhanced Customer Due Diligence

The enhanced customer due diligence shall be applied by the bank for high risk customer and shall include:

a. Examining, as far as reasonably possible, the background and purpose of all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or lawful purpose.
b. Increasing the degree and nature of monitoring of the business relationship regarding the transactions or

performance prescribed in sub-article (a), in order to determine whether those transactions or activities appear unusual or suspicious.

c. Obtaining additional information on the customer (e.g. occupation, volume of assets,), and updating more regularly the identification data of customer and beneficial owner.
d. Obtaining additional information on the intended nature of the business relationship.
e. Obtaining information on the source of funds or source of assets of the customer.
f. Obtaining information on the reasons for intended or performed transactions.
g. Obtaining the approval of senior management to commence or continue the business relationship.
h. Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.
i. Carrying out customer due diligence measures on the first transaction conducted through the account opened with the customer's name.

Bank shall apply the enhanced customer due diligence measures to high risk customers at each stage of the customer due diligence process and on an on-going basis.

Enhanced customer due diligence measures for business relationships with customers not physically present for the purpose of identification should include the following:

a. certification of documents in line with relevant Laws and this Directives;
b. requesting additional documents and development of independent verification measures and/or contact with the customer.

2.3 Risk Assessment

This section of the documents deals with the risk assessment process to arrive at certain risk category of customer accounts for the purpose of Customer Due Diligence (CDD). All accounts must be assigned with risk category for CDD purpose. The risk category must be assigned prior to account opening. The risk level will determine the level of due diligence required to be performed in the account hence proper risk assessment in accounts is necessary and important. In case of existing customers maintaining account and/or doing transactions before implementation of this procedure, customer shall be identified, sufficiency shall be reviewed, and risk grading shall be done.

While assigning risk categories, bank shall give consideration to factors such as:

a. Customer risk;
b. Country or Geographic region risk; (i.e. countries or geographic areas in which customers operate or the place of origination or destination of transactions);
c. Products and services risks; (i.e. the risks that arise from the products and services offered) and
d. Delivery channel risk: (i.e. the risks that arise from the channels used to deliver products and services).

For the customers who are categorized 'Low and Medium Risk', standard KYC will be applied and for the customers who are categorized 'High Risk', enhanced customer due diligence will be applied. Customer risk grade must be categorized on the following basis:

- Based on information which has been provided by customer at the time of account opening such as PEPs

(Politically Exposed person) declaration (customer declaration), criminal activities, beneficial owner, high net worth etc.

- Based on Public information through public media or staff knowledge or bank's internal sources.
- Based on PEPs check database (PEPs check report) etc.

Note: If any customer makes a deposit of above MMK 300 million will be classified as a high net worth individual.

Three Risk levels are defined for customers as follows:

- Level 1 (LR, Low Risk)
- Level 2 (MR, Medium Risk)
- Level 3 (HR, High Risk)

Prior to opening Level 3 account, approval must be obtained from respective Branch Manager.

2.3.1 Low Risk Customers (LR)

The customers who fall under following criteria will be classified as LR

Criteria:

- Myanmar Citizens
- Resident in the country but are citizens of countries other than High Risk Countries

2.3.2 High Risk Customers (HR)

Criteria:

Customer Risk Factors:

a. The business relationship is conducted in unusual circumstances
b. Non-resident customers
c. Legal persons or arrangements that manage the assets of third parties
d. Companies that have nominee shareholders or shares in bearer form
e. Activities that are cash-intensive or susceptible to money laundering or terrorism financing
f. The ownership structure of the legal person appears unusual or excessively complex with no visible economic or lawful purpose given the nature of the company's business
g. Business relationships conducted in or with countries as identified by the Financial Intelligence Unit under section 31(a) of the Law
h. Politically exposed persons ("PEP") or customers linked to PEP
i. High net worth customers, or customers whose source of income or assets are unclear
j. Businesses/activities identified by the MFIU, the Central Board, the CBM or the FATF as of higher money laundering or financing of terrorism risk

Country or geographic risk factors:

a. Countries classified by credible sources, such as mutual evaluation reports or published follow-up reports, as not having adequate AML/CFT systems.
b. Countries identified by the Central Board, Myanmar Financial Intelligence Unit or CBM as high risk.
c. Countries subject to sanctions, embargos or similar measures issued by, for example, the United Nations.
d. Countries classified by credible sources as having significant levels of corruption or other criminal activity.
e. Countries or geographic areas classified by credible sources as providing funding or support for terrorist activities, or those have designated terrorist organizations operating within their country.

Product, service, transaction or delivery channel risk factors:

a. Private banking.
b. Anonymous transactions (which may include cash).
c. Accounts opened, business relationships or transactions conducted with customers that are not physically present for the purpose of identification.
d. Payment received from unknown or un-associated third parties.
e. Complex trade financing products.

Beside the above-mentioned criteria, Bank shall also identify the high-risk customer on following grounds:

- Bank branch through local knowledge may identify a PEP or identify through PEPs verification from PEPs check database such as Accuity software, publicly available information etc.
- Bank shall identify whether any of the existing customers turn to PEPs or not which shall be identified through AML System.
- Bank shall identify the family member or close associate of High-risk customer through available sources such as adverse news, PEPs database etc.

2.3.3 Medium Risk Customers (MR) – Personal Accounts

All other customers who do not fall in either Low Risk or High Risk should be categorized as Medium Risk.

2.3.4 Account Opening

2.3.4.1 Personal Accounts

- Full name, including any aliases
- National Registration Card/Citizen Scrutiny Card/Passport
  Sight the original document with a copy and retain copy with 'original seen' signed by Authorized Person
- Permanent and mailing address
- Date of birth
- Nationality
- Occupation

- Phone number (if any).
- Photo or Photo IDs

In the case of joint accounts, a bank/financial institution shall obtain the above information on all parties to the account.

2.3.4.2 Non-Personal Accounts (Other than NGO)

Legal persons and Legal Arrangements including partnerships, limited liability partnerships and Trusts

- Name of company
- Address of head office
- Full address (including phone, fax)
- Certificate of Incorporation, Memorandum of Association, Article of Association for entities incorporated before 17 December 2017. For entities incorporated on or after 17 December 2017, entities' constitution
  Sight the original document with a copy and retain copy with 'original seen' signed by Authorized Person
- Partnership Agreement
- Trust deed
- Name and address of Board of Directors (phone number, if available)
- Identification documents of Directors/Shareholders/Partners
- Identification documents of Settlors, Trustees, Protectors and beneficiaries with respect to trusts.
- Board resolution authorizing opening and operation of the account
- Authorization by Board of Directors to Chief Executive Officer or other officers for conducting financial transactions.
- Identification documents to identify the person authorized to represent the company/business in its dealings with the bank/financial institution.

Further, in case of trust account opening, branch staffs shall obtain following additional information;

a. Status of the trust
b. Information regarding the beneficial ownership of the assets of the trust

Branch staff shall verify the authenticity of the information provided by the company/business with the Directorate of Investment and Company Administration.

For foreign incorporated or foreign registered business entities, comparable documents should be obtained. Branch staff shall make all efforts to verify the documents supplied including requiring that they be certified by the Office of Foreign Affairs and endorsed by the Embassy of Myanmar.

2.3.4.3 Non-Government Organization (NGO)

- Name of Non-Government Organization.

- Address
- Certification of registration
- Sight the original document with a copy and retain copy with 'original seen' signed by Authorized Person
- Constitution of the NGO
- Name and address of Executive committee
- Telephone No.
- Executive committee's decision regarding opening of account
- Identification documents of directors/senior officers of the NGO
- Authorization for the operation of accounts financial transactions
- Identification documents to identify the person authorized to represent the NGO in its dealings with the bank/financial institution

2.3.5 Account Opening Restrictions

- P.O. Box addresses are not acceptable as a recorded residential address. (P.O. Boxes are acceptable as mailing address only)
- Accounts must not be opened or retained (or one-off transactions undertaken) where it is known or suspected that a customer or prospective customer is involved in money laundering or terrorist financing. In such circumstances the account opening process should cease and, where appropriate, a SAR (Suspicious Activity Report) must be raised.
- The bank must not open accounts for shell banks/company or quasi banks/company hold alternate name or anonymous or numbered accounts.
- Accounts must not be opened, or one-off transactions undertaken, for UN/US/UK/EU sanctions listed individuals or entities.
- The beneficial owners must be identified. Where the beneficial owners, in above of 20%, are not natural persons the structure should be unwrapped and examined until natural persons do emerge. It should then be established whether such natural person(s) hold a proportionate interest of 20% or more of the original applicant.

2.3.6 Identification of Beneficial Owners

Beneficial owner means the ultimate natural person who owns or controls money or property or customer or (on whose interest the transaction is carried out). It also means the ultimate natural person who controls or exercises such powers to a legal person or arrangement. Identity of such beneficial owners must be established. KYC of beneficial owner must be obtained.

However, if a customer is a company listed on a stock exchange, a Bank is not required to identify and verify the identity of any shareholder or beneficial owner of the company. In such a case, the bank should only obtain customer identification documents on the company itself and obtain the relevant identification data from public register or if not available from a public register, the reporting organization shall obtain the information from the customer.

For other customers that are legal persons or legal arrangements, reasonable measures must be adopted to

understand the ownership and control structure of the customer, including the ultimate natural person who owns or controls a legal person, including natural persons with a controlling interest as described below. With respect to companies, limited partnerships, or similar arrangements, identification should be made of each natural person that:

a. owns directly or indirectly 20 percent or more of the vote or value of an equity interest in;
b. exercises management of the company, limited partnership or similar arrangement; and
c. controls or exercises control of the legal person or arrangements

With respect to a trust or similar arrangement, identification of settler, trustee and beneficiary or of beneficiary or of persons in similar positions and any other person exercising ultimate effective control including through a chain of control/ownership.

2.3.7 Documentary Evidence

In very exceptional cases, the individual required to be identified is public figure/ high profiled "well-known" public figure and sighting of any document as mentioned above may not always be practical. Although all efforts should be made to obtain such documents, where this is not practical, reliance may be made on any publicly available documents containing photographs of the individual. The account opening officer should certify that the individual concerned is the same person and obtain approval from the delegated authorities as required since this type of account shall be treated/considered as a High-Risk Account.

The verification of source of wealth or income could be from actual documents provided by the customer (e.g. proof of sale of property), available public information surrounding the individual or, where appropriate, from a detailed due diligence report of the relationship manager that includes elements of external enquiry and detailed meetings with the customer. Such information gathered from meeting or external enquiry should be recorded. (Refer Appendix 4)

2.3.8 PEP-Politically Exposed Person

Definition – “Natural Persons who are or have been entrusted with prominent public functions and their immediate family members, or persons known to be close associates of such persons”

Domestic and foreign politically exposed person means a person who is prominent or has been entrusted with public functions within the country or in any foreign country and family members or close associates of such persons.

International politically exposed persons means a director, a deputy director, a member of the board of directors and a senior member of an international organization, a member who has the similar position or a person who has been entrusted with such function and family members or close associates of such persons.

2.3.9 Non-Face to Face A/C Opening

The customer can send or forward account opening request through internet/mobile banking or e-mail or other electronic means and must verify themselves at the branch at the time of their visit to the branch for any

purpose.

2.3.10 Loan Accounts

KYC of loan customers must be completed by respective RM/FLO at the time of account opening. KYC assessment application will be same as in Personal/Non-Personal Accounts case.

2.3.11 Certifying Documents

Where documents are used to verify KYC information, the original must be sighted, copies taken and certified 'original seen' by an authorized person. The copies must be retained in customer's file.

2.3.12 Sanction List

UN sanction list of individual, group and organization are uploaded in the web site of United Nation Security Council's website https://www.un.org/securitycouncil/ and https://www.mfiu.gov.mm/en on regular basis. This UN Sanction List must be checked by AML/CFT Unit at least once a month or as guided by Myanmar Financial Intelligence Unit (MFIU) and such list must be sent to IT Department to verify against bank's existing customers.

IT Department shall forward the name-matched report to AML Unit for further verification. Any true match found, it shall be forwarded to respective branches for account freeze/block and such blocked account report must be forwarded to Manager – AML/CFT Unit and Director-Risk & Compliance for their notification.

3. Account Monitoring and Review

3.1 Ongoing Account Monitoring

3.1.1 Change of Conditions

The accounts must be reviewed on following conditions:

- Change of Account Name
- Change of Shareholders
- Change of Authorized Signatories
- Change of Directors
- Activation of Dormant/ Where About Unknown (WAUN) accounts.
- Account's transaction reported as Suspicious to Myanmar Financial Intelligence Unit (MFIU)
- It is apparent that the customer has become a PEP
- Customer name has been alerted through public media, regulatory authority as investigation, Newspapers, Public Media, Home Ministry, UN Sanction list, Myanmar Police, Myanmar Financial Intelligence Unit (MFIU), Tax Office, CIAA, Tax, Revenue Investigation, etc.
- If the customer's account transaction/activities can't be matched as per the declaration, source of fund, purpose of account, transaction etc. in AOF/KYC.
- If the customers have made frequent huge amount of cash withdrawal through foreign ATM outlet

without providing valid document.

- If any foreign bank's customers' frequent ATM transaction through our ATM/POS outlet.
- If the customer information/document is not line as per current bank procedure/CBM Directive.
- If the customer information/document gives ground for suspicion.

3.1.2 Change of authorized signatories

Authorized signatories to the accounts are changed on customers request with receipt of appropriate document (as per 2.3.4 or Refer Appendix 2). At the time of request for change of signatories, Customer Services Department staff at the branches must do the following:

- Check for identification documents of the signatories.
- Review the names of the signatories in PEP database.
- If the name does not match, proceed for signature amendment.
- If the name matches with PEP list, follow procedures as on 'Review of High Risk (HR)' Accounts
- Obtain documents/information as per 2.3.4 if necessary.

3.2 Ongoing Review of Accounts

3.2.1 Ongoing Review of Medium Risk account (Level 2 A/Cs)

Medium Risk Accounts (MR) accounts must be reviewed once every 3 (Three) years:

- Review date must be keyed in CBS in all MR accounts after the completion/approval of review.
- BM/SOM/RMs must review a report of overdue account of Medium Risk account through Pumori Query report/AML System on a monthly basis
- Accounts must be reviewed by using account review form (Refer Appendix1).
- Branch shall review the customer account's transaction on the basis of customer occupation/business/source of fund/purpose of account opening etc. for ensuring that customer has not made any transaction related to money laundering/terrorist financing through the account and such details shall be recorded in account review form.
- Branch shall ensure that all required document/information as per the AML CDD procedure/CBM Directive have been obtained. If any, branch shall obtain such document/information.
- BM/SOM/RMs should contact customer, if the review requires additional details/information of the client/customer.
- Review of MR accounts must be completed within 1 (one) month from the review date. If concerned branch is not able to complete review within the set timeline of a month, dispensation can be requested for additional 15 days. For which, respective Zone Head and Director should support the request and Director-Risk and Compliance should approve.
- Input all the KYC information such as occupation, annual income, purpose of account open, source of fund, anticipated transaction amount and volume, KYC rectification status etc. in the CBS.
- BM/SOM/RMs must maintain record of the contact made to customer for tracking the MR account review details.
- Manager- Operation must approve account Review of MR accounts.

- After completion of the account review and approval, necessary information/details shall be sent to CIF Team for updating that customer information/account review information into Pumori System. If all the information/documents are intact, such information shall be inputted into Pumori System and future review date shall be changed.
- List of overdue MR accounts must be sent to respective branch under CC to Zone Head and Director-Operations by AML/CFT Unit on a monthly basis.
- Ongoing review of High Risk (HR) account (Level 3 A/Cs):
- High Risk (HR) Accounts must be reviewed once in a year.
- Keeping in view of the risk associated with HR accounts, account review must be carried out for HR accounts each year. Process as follows must be complied for HR account review:
- Review date must be inserted in CBS System in all HR accounts after the completion/approval of account opening/review.
- BM/SOM/RMs must review a report of overdue account of high-risk account through Pumori query report/AML System on a monthly basis.
- Accounts must be reviewed by using Account Review Form.
- Branch shall review the customer account's transaction on the basis of customer occupation/business/source of fund/purpose of account opening etc. for ensuring that customer has not made any transaction related to money laundering/terrorist financing through the account and such details shall be recorded in account review form.
- Branch shall ensure that all required Enhanced Customer Due Diligence (ECDD) and KYC documents have been obtained.
- Enhance Customer Due Diligence (ECDD) shall not be obtained in case of account categorized as high risk due to high net worth of the individual.
- BM/SOM/RMs should contact customer, if the review requires additional details/information of the client/customer.
- Review of HR accounts must be completed within 1 month from the review date. If concerned branch is not able to complete review within the set timeline of a month, dispensation can be requested for additional 15 days. For which, respective Zone Head and Director should support the request and Director-Risk & Compliance should approve.
- Respective Director must approve account Review of HR accounts. Director can delegate his/her authority official during the period of his/her leave/official visit.
- After completion of the account review and approval, necessary information/details shall be sent to CIF Team for updating that customer information/account review information into Pumori. If all the documents/information are intact, such information shall be inputted into Pumori and future and transaction review date shall be changed, otherwise it shall be notified to respective branch for updating such information.
- BM/SOM/RM must maintain record of the contact made to customer in account review form for tracking of HR account review details.
- List of overdue HR accounts must be sent to respective branch under CC to Zone Head and Director-Operations by AML/CFT Unit on a monthly basis.

3.2.2 Information/Documents for review of high risk accounts:

- Identify the linkage between customer account transaction and customer business/occupation.

- Identify the background of transaction and objective of transaction.
- Ongoing review for ensuring the transaction is not suspicious.
- Verify whether the KYC and document as per latest bank procedure/CBM Directive is obtained or not. If not arrange to obtain required document/KYC.
- PEPs report shall be obtained of all related party such as Directors/Head of the organization/Signatories/Beneficial owner etc.
- Obtain KYC and related document if any customer have beneficial owner.
- Further transaction details shall be obtained if necessary.
- Transaction limit shall be setup if necessary.
- Verify the document for their genuineness through other sources if necessary.
- First withdrawal shall be made from the enhanced customer due diligence account only.
- Account review form shall be kept along with the respective account opening form, which shall be provided to audit or capable officials if required.
- Source and purpose of fund deposit and purpose of fund withdrawal of all transaction in high-risk accounts shall be identified.
- Approval from Branch Manager shall be obtained after review the high-risk account for continuing/terminating relationship. Based on the customer details and transaction, decision for continuing relationship with customer shall be obtained from Director.

3.3 Revision of Risk Level

After carrying out review of HR accounts, the risk level may be reduced to lower risk on the following conditions:

- In MR accounts, balance is less than MMK 200M/1200M (Personal/Non-Personal A/C) for last one year.
- Signatories/Directors/Head of the Organization/Shareholders/Beneficial Owners are no longer PEP for more than 5 years.
- Resident/Operating Address is no longer under High Risk Countries
- Nature of business no longer falls under High Risk Business

Approval of respective Director or his/her delegates in his/her absence must be obtained for lowering of risk in all accounts.

4. Transaction Type

4.1 Wire Transfers

Particular attention must be paid to the adequacy of information contained in records relating to electronic fund transfer instrument, that is both for inward and outward/domestic and international wire transfers. These offer money launderer the opportunity to speedily disperse funds to different jurisdictions making subsequent tracing and investigation difficult.

Each Transaction from/to tax heaven country shall be reviewed before transmitting/crediting in the account. Details

of sender in case of Outward Telegraphic Transfer and receiver in case of Inward Telegraphic Transfer and source of fund and purpose of fund sending shall be identified prior to transmitting/crediting.

4.1.1 Cross Border International Inward & Outward Wire Transfers

All electronic cross border international inward and outward wire transfers must contain the following information:

- accurate originator and recipient information;
- full name of the originator;
- the originator account number where such an account is used to process the transaction;
- the originator's address, or customer identification, or date and place of birth;
- the name of the recipient and the recipient account number where such an account is used to process the transaction.

Bank shall not route any international inward and outward transaction in the absence of above-mentioned information. If there is any ground for suspicion due to lack of information or any other reason, transaction of those wire transfer must be stopped immediately and report STR to AML/CFT Unit.

International Outward Wire transfer through wire/electronic media must be avoided if the remitter does not maintain an account with us.

The beneficiary of Cross Border International Outward Wire Transfer should not be in the sanction list.

Bank shall screen the Swift transaction such as Inward Telegraphic Transfer and Outward Telegraphic Transfer through Swift Sanction Screening Software. Bank shall screen the sanction list of UN, UK, EU and US. Sanction match information shall be verified by Swift Department on daily basis. If there is any true match between the transaction and sanction list, Swift Department shall stop such transaction and report to Director-Risk and Compliance, Director-Operations and Manager – AML CFT immediately.

Wire transfers that are not accompanied by complete originator information on the basis must be identified of perceived risk of money laundering and terrorist financing. In such case, the bank must request the missing originator information from the financial institution that sent the wire transfer. If the missing information is not forthcoming, the bank should consider whether, in all the circumstances, the absence of complete originator information creates or contributes to suspicion about the wire transfer or a related transaction. If the wire transfer is deemed to be suspicious, then it should be reported to AML CFT Unit. In addition, bank may decide not to accept the wire transfer.

Issuance of drafts to non-account holder must not be encouraged. In case, such drafts are to be made on exceptional cases, it can be done by obtaining KYC Details of the respective customer and after approval from Director-Operations. The full customer details must be obtained of a person/firm requesting such drafts.

4.1.2 Domestic Inward & Outward Wire Transfers

For domestic wire transfers, transactions should include the originator information required for cross border

wire transfers, unless such information can be made available to the beneficiary institution and competent authorities through other means. In such cases, bank need to only include the originator's account number or where no account number exists, a unique transaction or reference number that allows the transaction to be traced back to the originator or the beneficiary.

For incoming wire transfers, a bank shall verify the identity of the beneficiary, if the identity has not been previously verified, and maintain this information in accordance with the record keeping requirements.

Domestic inward wire transfer relating to pay upon proper identification should be completed after having proper identification document along with proper address of the beneficiary.

4.2 One-off transactions

"One-Off" transactions means any transaction carried out by a customer who does not maintain an account with the bank e.g. a single customer make foreign currency transaction or related transactions that exceed USD 15,000 or equivalent, KYC details of such persons such as his/her complete name, names of spouse/father/grandfather, current address, permanent address, telephone, number, mobile number, email address etc. and identification document such as NRC or valid Passport must be obtained prior to making such transaction. Effort, however, must be made to discourage such transactions.

4.3 Correspondent Relationships

In addition to verifying the identity of a bank, steps must be taken to ascertain whether correspondents have internal anti-money laundering procedures in place. It is particularly important to determine that prospective correspondents take steps to thoroughly identify their own clients on whose behalf we may be conducting transactions. It is also essential in order to identify any potentially suspicious activity to understand the type of business undertaken by the correspondent and therefore the normal or expected use of the account.

Bank will not establish or continue a correspondent banking relationship with a bank incorporated in a jurisdiction in which the bank has no presence, and which is affiliated with a shell bank.

Care should also be exercised where the respondent allows direct use of the correspondent account by third parties to transact business on their own behalf (i.e. payable through accounts). In such case the Bank must be satisfied that the respondent bank has performed the customer due diligence for those customers that have direct access to the accounts of the correspondent, and that the respondent is able to provide relevant customer identification information on request of the correspondent.

Bank shall follow the national and international best practices for avoiding the risk of AML CFT at the time of making correspondent banking relationship.

For banks in Financial Action Task Force member countries, it can be relied that appropriate money laundering controls including adequate KYC procedures are in place.

For branches or subsidiaries of banks outside FATF countries, that have their Head Office in an FATF country, a declaration must be sought from the Head Office that the branch or subsidiary in question follows money laundering

prevention and KYC procedure equivalent to FATF standards for all units.

Following documents must be obtained at the time of establishing relationship with foreign banks (for VOSTRO Accounts):

- Obtain firm registration, banking license
- Obtain shareholding structure of the bank along with the details of Board of Directors and Management staff
- Obtain the details of Board of Directors.
- Obtain business details of foreign bank
- Identify the status of money laundering and terrorist financing status of the foreign bank and identify the penalty on AML/CFT if any.
- Ensure that foreign bank is not involved in any money laundering and terrorist financing activities.
- Full Address of main office.
- Policy/Process/Procedure for anti-money laundering, KYC & anti-terrorist financing.
- Foreign country's rule/act regarding the AML & Terrorist Financing
- Purpose of account opening.
- Obtain latest Annual Report
- Obtain Anti-Money Laundering Questionnaire
- Memorandum of Article and Article of Association/Constitution

After obtaining the above-mentioned documents/information, approval from Director-Business must be obtained prior to establishing relationship with them.

Treasury and FI team shall review the cross border corresponding relationship and transaction to ensure the compliance to AML/CFT measures.

However, AML/CFT status of corresponding bank (for NOSTRO Account including local NOSTRO Account) shall be obtained through Bank AML questionnaire on yearly basis (Refer Appendix 3).

Transaction on behalf of shell bank/company and with the shell bank/company shall not be allowed.

5. Reporting of AML/CDD issues

5.1 Threshold Reporting Requirements

A Threshold Transaction Report (TTR) is a report that financial institutions are required to file to MFIU for each deposit, withdrawal, exchange of currency, or other payment or transfer, by, through, or to the financial institution which involves a transaction 100 million MMK and more. In FCY case, which involves a transaction of USD 10,000 or more (or equivalent). Further, report of TTR must be sent in where originator's information is incomplete or unavailable.

Threshold Transaction Reports (TTRs) are very important to develop the data bank of customers/clients' profile for future use in case such transactions happen to relate to money laundering and terrorist financing offences. TTR

helps to form a link chart during the analysis of a STR and helps the investigator to find the criminal elements involved in the transactions and convert the financial information into financial intelligence by adding value in it.

The Bank must submit the particulars of transactions in MMK or USD(or the equivalents in foreign currency) of afore-mentioned threshold or in excess of such threshold within 1 working day (3 working day for the units located at rural areas) from the date of transaction to the MFIU through electronic medium.

5.2 Suspicious Transactions Reporting

5.2.1 Detecting Suspicious Transactions

Suspicious Transactions Reports (STRs) include detailed information about transactions that are or appear to be suspicious. The goal of STRs filings is to help the Myanmar Financial Intelligence Unit (MFIU) to identify individuals, groups and organizations involved in fraud, terrorist financing, money laundering, and other crimes. The purpose of a STR is to report known or suspected violations of law or suspicious activity observed by financial institutions subject to the provision related Anti-Money Laundering Law, 2014. In many instances, STRs have been instrumental in enabling law enforcement to initiate or supplement major money laundering or terrorist financing investigations and other criminal cases. Information provided in STR forms also presents FIU with a method of identifying emerging trends and patterns associated with financial crimes. The information about those trends and patterns is vital to law enforcement agencies and provides valuable feedback to financial institutions.

Each STR must be filed in prescribed format with the given deadline of the initial determination to MFIU. With the assistance of branch/department, AML CFT Unit shall lodge STR to MFIU.

5.2.2 Detection of Suspicious Transactions using two kinds of information

1. Individual Account's History

   a. Threshold based detection
   b. Situation/activity-based detection

2. Transaction information from other accounts in peer group

5.2.3 Transaction of Suspicious or Large Value in Nature

For identification of suspicious transaction, the bank shall take the precautions, which would be exercised by a person of normal prudence. Some of the indicators of suspicious transaction shall be:

- Involvement of funds for illegal activity.
- Intending to hide or disguise assets derived from illegal activities.
- Intention to evade AML guidelines
- Customer has no business or apparent lawful purpose and has no linkage with such business.

5.2.4 General Characteristics of Suspicious Financial Transactions

- Transactions having unclear economical and business target.

- Transactions conducted in relatively large amount cash and/or conducted repeatedly and unnaturally.
- Transactions conducted differently from that of usually and normally conducted by the relevant customer.
- Huge, complex and unusual transaction.

5.2.5 Elements of Suspicious Transactions

1. Transaction deviating from:
    - the profile;
    - the characteristics; or
    - the usual transaction pattern of the relevant customer.

    - Transaction reasonably suspected to have been conducted with the purpose of evading the reporting that must be conducted by the relevant reporting entity.
    - Financial transaction conducted using fund alleged to be attributable to predicate offences.

5.2.6 Indicators of Suspicious Transactions

5.2.6.1 Cash

a. Cash transactions conducted in an unusual amount from that of usually conducted by the relevant customer.
b. Transactions conducted in a relatively small amount but with high frequency (structuring).
c. Transactions conducted by using several different individual names for the interest of a person (smurfing).

5.2.6.2 Economically irrational transactions

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

5.2.6.3 Fund transfers

a. Fund transfers to and from high-risk offshore financial centers without any clear business purposes.
b. Receipts of fund transfer in several phases and once accumulated the funds are subsequently transferred entirely to other account.
c. Receipts and transfers of funds at the same or approximately the same amount and conducted in a relatively short period (pass-by).
d. Receipts/payments of funds made by using more than one (1) account, either in the same name or

a different one.

e. Fund transfers using the account of reporting entities' employee in an unusual amount.

If multiple inward or outward remittance transaction is conducted with the person from the country or region where terrorist organizations operate. Behaviors of the Customer are:

a. Unreasonable behaviors of the relevant customer when conducting a transaction (nervous, rushed, unconfident, etc.).
b. Unusual curiosity about internal system, control and reporting.
c. Customer/prospective customer gives false information with respect to his/her identity, sources of income or businesses.
d. Customer/prospective customer uses identification document that is unreliable or alleged as fake such as different signature or photo.
e. Customer/prospective customers are unwilling or refusing to provide information/documents requested by the officials of the relevant reporting entity without any clear reasons.
f. Customer or his/her legal representative tries to persuade the officials of the relevant reporting entity in one way or another not to report his/her transaction as a Suspicious Financial Transaction.
g. Customer opens account for a short period.
h. Customer is unwilling to provide right information or immediately terminating business relationship or closing his/her account at the time the officials of the relevant reporting entity request information with respect to his/her transaction.
i. If anyone, for no apparent reason, often comes for transaction at pick hour or only in crowd.
j. If anyone tries to maintain close relation unnecessarily or unnaturally with the employees.
k. If anyone automatically unnecessarily clarifies or tries to clarify legality of amount or transaction.
l. If customer-conducting transaction looks confused, nervous, hurried, or wants to remain reserved at the time of transaction.

Miscellaneous grounds for suspicion

a. If it is evident that any one is earning wealth (including cash) by evading tax, custom duty, land revenue, electricity bill, and water bill, phone bill and any other revenue or government fees.
b. If anyone lives unusual lifestyle compared to his/her economic strength, profession/business.
c. If unreasonable economic growth or economic strength is evident.
d. If no information about the source of income is disclosed or stated or information about the source of income is not satisfactory.
e. If any act or transaction is not found reasonable or is found to have been conducted with irrelevant party or where the transaction has no justifiable purpose.
f. If it is evident that the asset is earned from the offences committed by organized criminal group;
g. If it is evident that the asset is earned from the offences relating to sexual exploitation including sexual exploitation of children;
h. If it is evident that the asset is earned from the offences relating to infringement of the Intellectual Property Right (offences relating to Intellectual Property);
i. If it is evident that the asset is earned from the offences relating to environmental crime;
j. If it is evident that the asset is earned from the offences relating to tax evasion and other tax crimes;

k. If it is evident that the asset is earned from the offences relating to privacy;
l. If it is evident that the asset is earned from the offences relating to terrorism;
m. If it is evident that the asset is earned from the offences relating who is the first to know the information by using the said information himself or providing it to another person and market manipulation;
n. If it is evident that the asset is earned from the committing of any offence punishable with imprisonment for a term of a minimum of one year and above under any existing law of the State;
o. If it is evident that the asset is earned from the offences prescribed by the Union Government that are applicable to this Law by notification from time to time;
p. If it is evident that the asset is earned from the participating, abetting, supporting, providing, managing, advising and being a member of an organized criminal group and other related offence by action or omission in committing, attempting to commit or conspiring to commit any offence contained in sub-sections (f) to (o).

5.2.7 Governed by Law

Any other transaction the reporting institution finds the grounds for suspicious transaction reporting as per the prevailing law. The bank will refuse any transaction where based on explanation offered by the customer or other information, reasonable grounds exist to suspect that the funds may not be from a legitimate source or are to be used for an illegal activity such as terrorism. The staff will use reasonable judgment in determining the suspicious transactions. The understanding of customers' identity vis-à-vis his stated norms of dealings, services, etc. would also have a bearing on transactions before they are viewed as suspicious transactions hence cautious approach in the process is very essential. Under no circumstances, staff will alert a customer about his transactions being considered suspicious or that reporting is underway.

The Bank will make prompt report of suspicious transactions, or proposed transactions to MFIU through Director-Risk & Compliance. The Branches/Units on suspicion of any transactions will fill up Suspicious Transaction Report and submit CO/ACO. Director-Risk and Compliance has authority to investigate the transactions and can withheld the report from being reported to MFIU if enough ground exist to prove transactions not being of suspicious in nature else ACO shall report suspicious transaction activity to FIU in prescribed form.

6. Record Retention

To assist the authorities on investigation of cases of suspicious money laundering, it is essential that evidence of customer identification, address, and transactions details are retained by the bank as mandated by the regulators. Such records must be archived in a secure area under the custody of a dedicated custodian. Access to such records must be made available only with due approval from Director-Operations or authorized staff by him/her. Records of every transaction undertaken for/by a customer must be retained for 5 years.

7. Internal Mechanism

- Human Resource Department shall prepare the procedure for appointing the high level official.

- Independent audit on AML shall be performed by the internal audit department. AML/CFT unit shall review the branches/department on AML prospective. All the observation during audit/review shall be recorded.
- Bank shall analyze the AML CFT risk to the Bank on yearly basis and record the same within subsequent of first quarter and update it in AML Policy and/or Procedure if necessary.

8. Procedure Compliance

8.1 Compliance Monitoring

Compliance Department/AML CFT Unit shall ensure that any system or services deployed by the bank has the requirement of this document incorporated. Compliance Officer, Internal Audit Department or the designated officer from the AML CFT Unit will verify compliance to this procedure through various methods, such as business tool reports, internal and external audits, and feedback to the procedure owner.

8.2 Compliance Officer

Director-Risk & Compliance or any other senior grade staff appointed by the CEO, will also work as Compliance Officer (CO) responsibilities of CO are defined in the AML Policy.

8.3 Confidential information

Bank's staff shall not disclose the customer information such as report, document, record, statement and information which are prepared as per the AML/CFT Law, its Regulations and Rules and CBM Directives to other customer or any other unauthorized persons. The concerned staffs shall take utmost precautions that they do not leak such confidential information. Tipping Off is a punishable offence.

8.4 Training

uab Banking School shall make sure that the training on AML/CFT shall also be provided to all staff of uab using internal or external or computer based resources regularly or as and when there are changes in AML/CDD Policy/procedure or there are new developments in the AML trends worldwide.

8.5 Amendment of the Procedure

CBM and MFIU issued AML related circular/directives from time to time and the KYC/AML/CFT acts and laws of the country shall form integral parts of this procedure. If any section/sub-section/clause of this policy contradicts with the country's laws, MFIU/CBM's directives, circulars; the latter shall be valid to the extent of contradiction.

8.6 Exceptions

Due to the way in which these procedures are implemented technically, there cannot be any exceptions to this procedure for users.

CEO must approve any exception to this procedure.

8.7 Non-Compliance

An employee found to have violated this procedure may be subject to disciplinary action, as per the provisions in the prevailing uab bank Employee Bylaw.

APPENDIXES

Appendix 1

Account Review Form

Client Code (CIF):
Name of the Account Holder:
Address:
Reason for Review:

☐ Change of Account Name ☐ Change of Shareholders ☐ Change of Directors
☐ Change of Authorized Signatory ☐ It is apparent that customer has become PEP

Ongoing Review (As per AML/CDD Procedure)

☐ Ongoing review of Level 2 Account ☐ Ongoing review of Level 3 account
☐ Ongoing review of Level 2 Account ☐ Dormant/WUAN account
☐ Others, Please Specify

Transaction Monitoring Status (Please tick mark as appropriate, details of the transaction must be written)

a. Threshold within as per KYC Declaration
b. Threshold limit breach as per AML/CDD Procedure
c. Details of the transactions

……

……

AOF and KYC Document Status…….

Contact made to the Customer Record

Date	Customer View

Recommendation for (Please tick and write as appropriate)

1. Risk level movement details:
   a. Downgrade (L1 to L2)/ (L2 to L3)/ (L1to L3)
   b. Upgrade (L3 to L2)/ (L2 to L1)/ (L3 to L1)
   c. No Movement
2. Risk Categories ☐ Level 1 ☐ Level 2 ☐ Level 3
3. Future Review Date……/……/…… Transaction Review Date ……/……/…….
4. STR send to CBM due to ……
5. We will obtain new/updated KYC within ……. days.
6. Others, Please Specify……
7. Future Action……

Completed by Checked/Reviewed by

…….. ……

Signature
Name:
Date:

Signature
Name:
Date:

Appendix 2

A. Natural persons

1. Full name, including any aliases
2. National Registration Card/Citizen Scrutiny Card/Passport
3. Permanent and mailing address
4. Date of birth
5. Nationality
6. Occupation
7. Phone number (if any)
8. Photo
9. Name and account numbers of two introducers (existing account holders)

In the case of joint accounts, a bank/financial institution shall obtain the above information on all parties to the account.

B. Legal persons and Legal Arrangements including partnerships, limited liability partnerships and Trusts

1. Name of company
2. Address of head office.
3. Full address (including phone, fax)
4. Certificate of Incorporation, Memorandum of Association, Article of Association
5. Partnership Agreement
6. Trust deed
7. Name and address of Board of directors (phone number, if available)
8. Identification documents of Directors/Shareholders/Partners.
9. Identification documents of Settlors, Trustees, Protectors and beneficiaries with respect to trusts.
10. Board resolution authorizing opening and operation of the account
11. Authorization by Board of directors to Chief Executive Officer or other officers for conducting financial transactions.
12. Identification documents to identify the person authorized to represent the company/business in its dealings with the bank/financial institution.

Banks and financial institutions shall verify the authenticity of the information provided by the company/business with the Directorate of Investment and Company Administration. For foreign incorporated or foreign registered business entities, comparable documents should be obtained. Banks and financial institutions shall make all efforts to verify the documents supplied including requiring that they be certified by the Office of Foreign Affairs and endorsed by the Embassy of Myanmar.

C. Non-Government Organization (NGO)

1. Name of Non-Government Organization.
2. Address
3. Certification of registration
4. Constitution of the NGO
5. Name and address of Executive committee
6. Telephone No
7. Executive committee's decision regarding opening of account
8. Identification documents of directors/senior officers of the NGO
9. Authorization for the operation of accounts financial transaction
10. Identification documents to identify the person authorized to represent the NGO in its dealings with the bank/financial institution

Appendix 3

AML/CFT Correspondent Banking Questionnaire

I-General Information

1. Contact Details	
Legal Name:	
Legal Name:	
Registered Address:	
Operating Address:	
Address of Corporate Office: (If different from above)	
Phone Number:	
Fax Number:	
Number of Branches:	
Type of Institution:	
Type of Product and Services offe	
Website:	

2. Company Registration Details	
Authority issuing the license:	
License No:	
Corporate Identification Number/I	
Corporate Identification/Regist Type	
Country of Incorporation a registration	
Date of Incorporation	
Regulator Details: Banking and Prudential Matters: AML/CFT Matters: (Insert name and web address)	
Is your Institution a Shell Bank?	
Please state the areas of organization covered by Questionnaire	
Is your institution publicly owned? If Yes, please provide the name of the stock exchange	

Ownership and Executive Management

Please attach additional sheets if necessary.

3.	**Details of Board of Directors**			
S. No.	Name	Address	Nationality	Position

4.	**Details of Senior/Executive Management**			
S. No.	Name	Address	Nationality	Position

5. Kindly, list below all individuals or legal entities that own 10% or more share of your institution. Please, attach additional sheets if necessary.

S. No.	Name	Ownership Interest (%	Nature of Ownership (Direct/Interest)

If the legal entities are listed above, please list the individual shareholders of the entities (> 10%), their nationalities, percentage ownership and nature of ownership.

Entity Name	Shareholder Name	Ownership Interest (%	Nature of Ownership (Direct/Indirect)

Description	**Yes/No**

6. Has your institution been subjected to sanctions or punitive actions in relation to anti-money laundering and anti-terrorism financing by regulators/law enforcement in past 5 years? If Yes, please provide the details	
7. Has your institution appointed senior officer responsible for your institution's day to day anti-money laundering and anti-terrorism financing program?	

II Framework

Description	Yes/No
8. Have the laws and regulations for the prevention of money laundering and terrorist financing been formulated by your country?	
9. Is your institution subject to such laws/regulations?	
10. Have the laws and regulations for the prevention of money laundering and terrorist financing been formulated by the country wherein your parent company is located.	
11. What is the name of the regulatory authority of your country responsible for overseeing the AML Laws/Regulations?	

III General AML Policies, Practices and Procedures

Description	Yes/No
12. Does your institution have written policies, procedures and controls in place to prevent money laundering and terrorist financing?	
13. Are your AML policies and procedures approved by Board or Board Committee?	
14. Are AML policies and procedures applicable to head office, all branches and subsidiaries? If no, please provide a list of the branches and/or subsidiaries that are excluded, including the name and the location of the institution. _____ _____	
15. When was your AML policies and procedures last reviewed?	
16. Does your institution have policies and procedures covering relationship with PEPs, their family, close associates consistent with relevant regulatory requirements and industry best practices?	
17. Does your institution maintain any correspondent banking relationship and conduct business with any shell banks? (A shell bank is defined as a bank incorporated in a jurisdiction in which it has not physical presence and is unaffiliated with a regulated financial group)	

18. Does your institution permit opening of anonymous account by customers?	
19. Does your institution allow third parties to directly or indirectly use Your account(s) with any bank, i.e. in the form of "payable through accounts"? If Yes, has your institution formally identified and monitored these third parties?	
20. Does your institution have written AML policies and procedures to prevent, detect and report suspicious or unusual activity?	
21. Does institution have policies to reasonable ensure that it only operates with correspondent banks that possess the license to operate in their country of origin?	
22. Does your institution maintain customer record of customer profile and transaction? If yes, for how long?	
23. In addition to regulatory inspection, does your institution have any internal audit function or other independent third party that assess the AML/CTF policies and procedures on regular basis? If Yes, how often are they conducted?	

IV. KYC, Due Diligence and Enhanced Due Diligence

Description	**Yes/No**
24. Does the institution have customer due diligence (CDD) and enhanced customer due diligence (ECDD) program in place to identify and verify your customer's identity?	
25. Do you undertake the customer due diligence, including: a. Verification of identity of: i. Customers; and ii. The natural person(s) who control the customers and the beneficiary of the transaction; and b. Obtain enough understanding of the customer's financial and business circumstances to evaluate the reasonableness of transactions and legitimacy of the source of funds used in transactions?	
26. Does your institution have customer risk rating/grading process? If Yes, Please, describe the process and methodology.	
27. Does your institution apply enhanced due diligence policies and procedures in connection with high risk customers?	
28. Does your institution focus on high risk customers, including politically	

exposed persons, correspondent banking relationships and customers from risk countries?	
29. Does your institution have process to review and where appropriate, update customer information?	
30. Does your institution ensure that effective anti-money laundering and anti-terrorist controls are in place on new technologies, and when you are dealing with non-face to face customers or through intermediaries?	

V. Transaction Monitoring Report

Description	Yes/No
31. Does your institution monitor customer accounts and transaction in order to detect unusual and suspicious activities?	
a. Is this process automated or manual?	
b. What type of transactions do you monitor (e.g. large value transaction, wire transfers, cash withdrawals, cash deposits)?	
c. Is there an established method of reporting unusual and suspicious activities and transaction to the appropriate authorities	
32. Does your institution have an established program that includes policies and procedures that include a process (manual or automated) to periodically review customer accounts for large or unusual transactions?	
33. Does your institution have an established program that includes policies and procedures for review of wire transfer activity?	
34. Does your institution conduct any kinds of banking transactions with non-established customers or walk-in customers (non-account holders) If Yes, please mention the control mechanism:	
35. Has your institution reported any suspicious transactions in the past year? If Yes, please provide the number of such transactions:	

VI. Sanction Compliance

Description	Yes/No
36. Does your institution conduct sanction screening against your customers and their transactions?	
37. Does your institution have a sanction screening IT System?	
38. Is the sanction screening internally developed? If No, please provide the name of the external vendor.	

39. What sanction lists are included within the system?	
40. Describe the controls to ensure complete originator/beneficiary information in payments?	

VII. AML Training and Others

Description	**Yes/No**
41. Does your institution conduct periodic training to relevant employees that include the detection, monitoring and reporting of suspicious transactions to the relevant authority? If Yes, does your institution retain records of its training materials and attendance records?	
42. Does your institution communicate new AML related act, regulation or changes to relevant employees?	
43. Is there any system to ensure that the staffs who have not received any training regarding AML Policies can be identified and trained as soon as possible?	
44. Who is responsible for managing the training program and its records? Name: Designation:	
45. What is the delivery method for AML training in your institution?	

DOCUMENTS TO BE ENCLOSED

A.	Certified Copy of Certificate of Incorporation	
B.	Certified Copy of License	
C.	List of Branches and Subsidiaries and their respective jurisdiction	
D.	List of Ultimate Beneficial Owners	
E.	Organizational Chart	
F.	Organization Chart of Compliance Depart	
G.	AML/CFT Policy of the Bank/FI	
H.	AML Audit Certificate and/or latest Audit Report	
I.	List of shareholders with shareholding percentage (>10 %)	

I confirm that the information provided in the above questionnaire is current, accurate and representative of the anti-money laundering and anti-terrorist financing policies and procedures that are established in my institution.

Name:	
Position:	
Address:	
Telephone:	
E-mail:	
Signed:	
Date:	

Appendix 4

Customer Interaction Form

Date:
Time:
CIF No:
Name of the Customer:

Following information needs to be obtained through the meeting or external enquiry:

a. Purpose behind opening an account.

   _____
   _____
   _____
   _____
   _____

b. What would be the primary source of fund and net worth?

   Source of Fund:_____
   Net Worth:_____

c. Any other relevant information

   _____
   _____
   _____
   _____
   _____
   _____

Signature
Staff Name: