YOMA BANK

ANTI MONEY LAUNDERING (AML) AND COUNTER FINANCING OF TERRORISM (CFT) POLICY

Board Approval Date : 26 June 2024

CHAIRMAN OF THE BOARD OF DIRECTORS

Contents

1. Policy Scope

By the very nature of its functioning, banks are most susceptible to the risk of money laundering and terrorist financing, and the possibility of its various services being unwittingly used as conducting and cycling the ill-effects of the tainted/illegal money by the launderers. Money laundering and terrorist financing are often mentioned in the same breath. Many of the controls that the bank should implement in this policy document is meant to serve the dual purposes of combating both money laundering and terrorist financing. The most basic difference between money laundering and terrorist financing involves the origin of the funds. The purpose of money laundering is to enable the dirty money to be used legally but for the terrorist financing, funds is aiming for an illegal terrorist purpose which means that the money may not necessarily derived from illicit proceeds.

This policy is intended to outline Yoma Bank's standard requirements to prevent money laundering and terrorist financing activities and ensure compliance with relevant local laws and regulations as well as recommendations and guidelines from international bodies. The Bank's aim is to drive best practice and risk-based approach to management of money laundering and combatting terrorist financing. This policy is in line with Business Integrity Policy to ensure compliance by every person working for the Bank without exception and the Subsidiaries of the Bank, if any, and their respective employees, Affiliates or any third party acting on their behalf or for their benefit, with all laws and regulations of the Republic of the Union of Myanmar, the OECD Convention Against Bribery, the UN Convention Against Corruption concerning business integrity, corruption and bribery, and, for the avoidance of doubt, and all Applicable Laws.

An executive summary of the scope of this policy is listed below:

- The Bank shall develop internal procedures and technology that would assist the Bank in monitoring transactions for the purpose of identifying possible suspicious activities;
- The Bank shall continue to update policies and procedures in line with the laws, regulations and regulatory guidelines. Compliance Division will be delegated the task of overseeing the Bank's policies and procedures by adding internal controls with regards to money laundering and terrorist financing;
- The Bank shall take all reasonable steps to ensure that Customer Due Diligence information is collected and up-to-date, and that identification information is updated in the event where the Bank comes to know about any changes with regards to the parties involved in the relationship;
- The Bank shall take reasonable steps to verify the identity of the customers, including the beneficial owners of corporate entities, and the principals behind customers acting as agents;
- The Bank shall ensure that the Internal and External Audit Teams shall conduct their audit on periodic basis and Compliance Team randomly observe audit requirements of KYC guidelines and verification of its implementation at branches and other operational units of the Bank;
- The Bank shall not tip-off its customers regarding suspicious transactions and/or any internal/external investigation being carried out on them;
- The Bank shall not maintain any relationship with shell companies;

- The Bank shall cooperate with any lawful request for information made by authorized government agencies/statutory bodies during their investigations;
- The Bank shall receive and collect reports on suspicious and prescribed threshold financial transactions and other information relevant to money laundering and financing of terrorist activities from government agencies, financial and non-financial institutions;
- The Bank shall provide suspicious and relevant information to the investigation department and other relevant authorities;
- The Bank shall ensure compliance by reporting entities with regard to their obligations under the law, rules and regulations;
- The Bank shall ensure that the training sessions on KYC, CDD, ECDD and AML/CFT procedures and guidelines are included in the training calendar of the bank on an ongoing basis. The Bank shall arrange to update and module these training sessions to make all the concerned fully understand the rationale behind these procedures and implement them consistently;
- In order to educate customers on KYC requirements and the need for seeking certain personal information from the customers/applicants for opening accounts and/or establishing any Business Relationship with the Bank, and as well to ensure transparency, the Bank shall publish this Policy in the Bank's website. It will be the primary duty and responsibility of Operational Staff to educate the customers and tactfully/convincingly explain the need for customer profile and its relevance in enabling the Bank/Branch to render better customer service;
- The Bank shall establish clear lines of internal responsibilities and reporting;

Review and Amendments of the Policy

Bank AML/CFT Policy is subject to annual review. New Directives of the CBM and the MFIU and the AML/CFT Law and Rules, regulations for KYC/CDD from time to time 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.

Whenever the Policy is reviewed and updated, the CCO/CRO/AML/CFT team shall conduct an enterprise-wide AML/CFT risk assessment every 12–18 months. A more frequent refresh will be performed if new or emerging risks that significantly change the bank's risk profile are identified.

Any amendments, if deemed necessary, to this policy shall be approved by the Board of Directors (BOD), except specifically mentioned in this policy. In case any confusion in the interpretation of this policy arises, the matter shall be referred to the BOD through Risk Oversight Committee and the decision made therein, shall be final and binding.

Authority to Formulate and Approve Guidelines or Operating Procedures

Appropriate guidelines, manuals and other operating procedures required for effective implementation of the

provisions laid down in this Policy, will be reviewed and provided feedback to cover all the regulatory and compliance aspect by the Compliance Division. Each Division needs to develop operation procedures that are related to their respective Divisions and adhere to the AML/CFT policy. Such procedures and any supplement to any guidelines shall be construed as part of this policy and shall be read in conjunction with the provisions contained in this policy.

Exceptions and Breaches Management

All staff are required to immediately report any exceptions or breaches to this policy to the AML/CFT Department. The AML/CFT team is accountable for assessing all exceptions or breaches, ensuring necessary mitigating actions have been implemented on a timely basis and, where necessary escalating to the Chief Compliance Officer or the Board.

The AML/CFT team will work with People Division and the relevant line manager of staff where any Code of Conduct Breaches are identified to document the non-compliance and ensure they will be reflected in RAG gateway.

Application

This policy is applicable to all branches, subsidiaries and their employees, affiliates or any third party acting on their behalf, and offices of the Bank. The policy should be read in conjunction with related Standard Operating Procedures (SOPs) and guidelines. The contents of the policy shall be subject to change as advised by the regulators and/or the Bank from time to time.

Regulatory Obligations

This policy and related procedures are subject to periodic reviews to ensure that they remains robust and comply with the regulatory requirements and international recommendations. The key laws and regulations are listed as follows:

- The Anti-Money Laundering Law 2014;
- Directive for the CDD Measures (Directive No. 18/2019);
- Reporting Obligation Guideline (Instruction No. 1/2019);
- Suspicious Transaction Report Guideline (Instruction No. 2/2019);
- The Counter-Terrorism Law (2014);
- The Anti-Corruption Law (2013);
- Financial Institution Law (2016);
- Various regulations and directives issued by Central Bank of Myanmar (CBM) and Myanmar Financial Intelligence Unit (MFIU);
- Financial Action Task Force (FATF) recommendations and other international agencies;
- Circulation of Order No (4/2023) of the Central Committee for Counter Terrorism;

- Announcement for nominee Directors and members as nominee Shareholders by DICA. (Directive 7-2023);

Any provision laid down in this policy will be superseded by changes to existing laws, regulations and directives or new and future provisions to related laws, regulations, and directives by the relevant authorities.

Revision History & Version Control

Serial Number	Title	Date of Commencement	Base Version
1	AML Program	Jan-2015	Version 1
2	AML Policy	Oct-2015	Version 1
3	AML Policy	Sept-2021	Version 2
4	AML Policy	April-2024	Version 3

2. Governance, Oversight and Accountabilities

Yoma Bank has established a clear risk management framework to ensure all material risks arising from execution of Yoma Bank's strategy, including those related to AML/CFT, are managed in line with Risk/Compliance appetite set by the Board.

Governance and Oversight

The Board is primarily responsible for overseeing the establishment by Management of a sound risk management culture with an operational structure and necessary resources to facilitate effective risk management throughout Yoma Bank.

The Risk Oversight Committee will have the following responsibilities for AML/CFT framework:

- Set Bank's risk appetite with respect to AML/CFT and ensure effective implementation of code of conduct/risk culture and clear accountabilities consistent with bank's three lines of defense;
- Approve and oversee implementation of enterprise-wide AML/CFT policy and its subsequent amendments from time to time;
- Ensure bank implements robust oversight over the status of implementation of Anti-Money Laundering and Counter Financing of Terrorism Laws and the provisions contained in the directives, instructions, regulations, and guidelines issued by regulatory bodies;
- Review and challenge the reports submitted by the Chief Compliance Officer with respect to the Bank's compliance with legislation and other requirements contained therein and provide directions to the Bank's Management as required;
- Review management's strategy to ensure adequate management resources are allocated to discuss on

setting up and improving mechanism to prevent identify and manage High Risk customers, customer's suspicious and abnormal transaction or money laundering based on the report submitted by the Chief Compliance Officer, and make necessary arrangements to this effect;

- This includes ensuring the bank appoints a qualified independent Chief Compliance Officer and continuously monitor the bank's resource allocation to ensure the bank has sufficient expertise, vendors, independent specialists, technology, and control systems dedicated to AML/CFT compliance.
- Risk Oversight Committee members are required to be suitably qualified and have clear understanding of AML/CFT best practices, to receive adequate up to date training on AML/CFT and are accountable for ensuring they remain informed of main compliance risks (including AML/CFT), accept key compliance risks, or plans to mitigate them and be informed of other AML/CFT matters, such as major compliance failures and corrective actions, in a timely and comprehensive manner.

Specific to product management, the Board has delegated accountability to the Product Committee to ensure that AML/CFT emerging risk is considered, before launching new products.

Reporting of the Bank's AML/CFT Risk Profile

Internal reporting of AML operational performance and output is critical to the AML/CFT risk management process. The Chief Compliance Officer has the authority to act independently and to report changes in the Bank's compliance profile. AML/CFT-specific reports, as a minimum, require the following key information:

- Significant AML/CFT regulatory changes and tracking of compliance;
- Regulatory examination and internal audit results and tracking of remediation actions;
- AML/CFT Risk assessment/bank risk profile changes;
- Statistical data on High Risk accounts;
- Statistics on the number of transactions monitored, alerts generated, cases created, and suspicious transaction reports (STRs) filed;
- Periodic Reviews;
- STR filing trends;
- Potential backlogs in timely STR or cash (currency) transaction report filings;
- Staffing levels and capability gaps and
- Potential impact of new products and service offerings in the pipeline.

AML/CFT related reports should be made available and commonly discussed during bank risk oversight committee or compliance operations meetings and include all relevant stakeholders, including senior executive management, first-line executives, CRO and CCO. The reports must be sufficiently detailed and cover main Key Risk Indicators (KRIs) to facilitate the management's assessment of the state of AML/CFT risk exposures. More importantly the reports must cover the effective operation of the AML/ CFT control environment.

All employees, including contractors must report all suspected or actual acts of ML/FT to the AML/CFT team. The AML/CFT team must ensure that all relevant matters reported by employees and contractors are investigated and where necessary report to CCO and the MFIU. CCO shall assign a person referred to as Head of AML/CFT department, who is responsible for overseeing the Bank's anti-money laundering activities and program and for filing reports of suspicious transactions with the MFIU.

Three Lines of Defense

At Yoma Bank, we drive top-down culture from the Board to C-level executives and cascading so on where "Risk is Everyone's Responsibility". Specific to AML/CFT, the accountabilities of each line are as follows:

- First line "risk owners" are accountable for managing their risks by setting a system of internal procedures and controls;
- Second line risk management and compliance teams provide policy and governance oversight, "review and assessment", training and required support to enable business, and
- Third line (Internal Audit) provides independent assurance that the Bank's first and second line accountabilities are appropriately implemented.

Internal Audit has the responsibility to test the adherence of the Bank's KYC and AML/CFT policy and procedures. Internal Audit will provide an independent evaluation including legal and regulatory requirements. Internal Auditor shall specifically check and verify the application of KYC and AML/CFT procedures at the branches and comment on any breaches. The findings/recommendations should be reported directly to the CCO and the Audit Committee.

The frequency and scope of Internal Audit's evaluation and any follow-up Audits will be set by the Audit Committee. As a general guidance the minimum scope of audits should include:

1) Governance;
2) Risk Identification, Assessment, and Mitigation;
3) Policies and Procedures;
4) Customer identification and Due Diligence;
5) Transaction Monitoring;
6) Reporting;
7) Communication and Training;
8) Evaluating/Assessing and Testing;

Roles and Responsibilities of AML/CFT Department

AML/CFT Department primarily responsible for overall monitoring of the implementation of the AML/CFT policy is also responsible for:

- Reviewing and approving the controlling, monitoring and reporting procedures formulated for the effective implementation of this Policy on KYC and AML/CFT;

- Escalating and reporting of the Bank's compliance with AML/CFT regulations within three months from the end of fiscal year. Further, a brief summary relating to this shall also be disclosed in the annual report of the Bank;
- Ensuring the policy meets prevailing laws and regulations;
- Ensuring records are kept properly in accordance with the Policy;
- Monitoring and reporting suspicious transactions, as required under the law;
- Liaising with AML/CFT external agencies including government agencies, regulating authorities; MFIU, CBM, Banks and other institutions, which are involved in the fight against money laundering and financing of terrorism;
- Providing internal reports on the
  - Measures taken to strengthen the bank's AML/CFT policies, procedures, systems and controls,
  - Results of any independent audit of AML/CFT including recommended remedial actions
  - Results of any onsite inspections conducted by the external agencies
  - AML/CFT policy implementation status, key risks and gap analysis of policy
- Training and educating on KYC and AML/CFT matters;
- Reviewing and approving High Risk customers and transactions;
- Accessing whether the first line staffs are compliant with AML/CFT laws, regulations, and bank policy independently.

3. AML/CFT Training and Awareness

Training is one of the most important ways to stress the importance of AML/CFT efforts, as well as educating employees about what to do if they encounter potential money laundering. The Bank shall not only undertake awareness and training for AML/CFT, explain the relevant AML/CFT laws and regulations but also cover the Bank's policies and procedures to mitigate money laundering risks. The bank shall outline who should receive AML/CFT training, the topics that should form the basis of that training and how, when and where that training should be delivered.

For an effective AML/CFT training program defining the target audiences such as customer-facing staff, operations, AML/CFT compliance team, independent testing staff such as risk and audit teams as well as senior management and Board of Directors is essential.

All staff who are employed and stated by the Bank as target audiences, shall be provided AML/CFT risk awareness training which covers:

- The Bank's obligations under the AML/CFT Laws, any rules and directives issued by the relevant regulatory authority;
- The consequences of non-compliance with the AML/CFT Laws;
- The type of ML/TF risks that the business faces and the potential consequences of such risks;

- The necessary documents and information including the reasons for document collection and why the bank needs to collect these from customers, especially for risk assessment and due diligence;
- What kind of suspicious activities they must be identify and report to the AML/CFT department in a timely manner;
- The specific processes and procedures provided for by the Bank's AML/CFT policy and procedures that are relevant to the work carried out by the employee.

E-learning is an effective and efficient way to deliver AML/CFT training program but there will be some classroom training since it is the best option to communicate and disseminate the message across the bank. The training should be ongoing and on a regular schedule. Existing employees should at least attend an annual training session but if there are new CBM regulations or instructions, the training content might be changed and may need to attend a new/refresher training course. New employees should receive appropriate training with respect to their job function and within a reasonable period after joining or transferring to a new role or job.

Track attendance (a record of the staff attendance) and completion of the training will be made, and disciplinary action taken for non-attendance or failure to complete the training in a reasonable time frame.

4. Secrecy of Information

Staff shall not disclose any of the reports, documents, records, details or information that have been prepared as per the requirement of AML/CFT legislation, rules, regulations, directives and guidelines, to the customer or to any other unauthorized person/agent unless the disclosure/act has been required for fulfillment of the responsibilities as per the provisions stated by the AML Law, Rule and Directives. The Bank and its directors, officers and employees should not practice improper or illegal act of notifying a suspect to any related parties that he or she is the subject of a suspicious transaction report or is otherwise being investigated or pursued by the authorities. In case the disclosures have been identified to be made against the AML legislations and this policy, the person shall be subject to disciplinary action as per the Code of Conduct Policy, Personal Data Protection Policy and Business Integrity Policy.

Information collected from the customers for the purpose of opening of an account and/or satisfying the KYC requirements shall be treated as confidential and details thereof shall not be divulged for any purpose to the unauthorized person/entity without the expressed permission from the customer unless disclosure is under the compulsion of law.

5. Retention of Record

Adequate records of identification, address verification, account opening, and transactions will be retained for at least 5 years, enabling to provide a clear audit trail in the event of need and investigation. The following documents and details will be retained, for the period as prescribed by law/policy after the Business Relationship has ended:

- Documents relating to the identification and verification of customers and related beneficial owner;
- Documents relating to domestic and international transactions;
- Documents relating to attempted transactions and Business Relationship;
- Records relating to suspicious transactions and suspicious activity reports (STR/SAR), and the supporting investigation material;
- Documents collected from employees such as employee information forms, employment contracts, education and professional certificates, identification, and copies of all records obtained through KYE process;
- The Bank's AML/CFT policy and copy of the director's approval of the AML/CFT policy;
- Documents pertaining to the prevention of ML/TF, including the AML/CFT monitoring reports made by the AML/CFT team and the action taken as a consequence;
- Records showing the dates of AML/CFT and KYC/CDD trainings and the names of the staffs receiving the training.

All records maintained should be available to the authorized persons promptly on request without any undue delays. AML/CFT team will document the non-compliance and monitor progress towards full compliance and that progress record will be reflected in RAG gateway.

6. Customer Due Diligence and Verification

The Bank shall establish and verify a customer's identity prior to the commencement of a Business Relationship in line with CDD procedures. The level and nature of due diligence undertaken should be commensurate with the type of customer and level of risk identified.

CDD should be completed before:

i. Opening an account;
ii. Undertaking any transaction or receiving any funds for an Individual or Enterprise which does not have a Business Relationship with The Bank.

The Bank shall undertake:

- To check the sanction lists (including Local, Lists in the Refinitiv World-Check or using similar vendor, as well as PEPs) for all types of customers. For Enterprises, Beneficial Owners will be screened;
- A risk assessment of all customers including verification of key information to determine the potential exposure to AML/CFT. For all customers identified as High-Risk, the bank shall apply Enhanced Customer Due Diligence (ECDD);
- To source original documentation and verify these documents in a face-to-face meeting with the Customer.

In the event that the Bank identifies customers who are not compliant with this policy, the situation will be reported to AML/CFT department which will review the Business Relationship and report to MFIU as

required by law. The Bank may elect to terminate the Business Relationship with the Customer.

Identification and Verification Principles for an Individual:

- The Bank shall accept the original documents to verify as evidence of a customer's identify:
- The Bank must ensure it takes reasonable measures to verify the accuracy of information contained in these documents provided by customers;
- The Bank must retain copies of all documents used for identification and verification of identity for a minimum of 5 years after the end of the Business Relationship, and have periodic reviews to ensure information held is up to date;
- On-boarding requirements for Individual Small Business Owners may be the same with those of Individual customers however risk assessments should be aligned to the profile of the customer, including their business activities, and purpose of accounts. For this segment customers may not open Enterprise Accounts unless exceptional approval is provided by AML/CFT department.

The bank shall verify the above information using reliable, independently sourced documents and data. Document verification procedures should include;

- Confirming the identification form is an unexpired official document that bears a photograph of the customers.
- Confirming the date and place of birth from an official document.
- Confirming the validity of the official documentation, Non-documentary verification procedures should also be included;
  - Contact the customer by telephone to confirm the information supplied after an account has been opened.
  - Sending an OTP code to the telephone number from the onboarding form as part of the validation step when opening the customer's mobile application.
  - Using an independent information verification process, such as accessing public registers or other reliable independent sources.

Identification and Verification Principles for an Enterprise:

- The Bank must perform CDD on the Enterprise, UBOs that meet the ownership requirements and any individual authorised to transact on accounts owned by the Enterprise;
- The Bank shall accept the original documents to verify as evidence of an Enterprise, UBOs and any individual authorised to transact on accounts owned by the Enterprise;
- The Bank must ensure it takes reasonable measures to verify the accuracy of information contained in these documents provided by customers;
- Copies of all documents used for identification and verification of identity must be retained for a

minimum of 5 years after end of Business Relationship and be subject to periodic reviews to ensure information held is up to date.

The bank shall verify the above information using reliable, independently sourced documents and data. Document verification procedures should include;

- Obtaining a copy of the certificate of incorporation, memorandum and articles of association, partnership agreement or any other document certifying the existence of the entity.
- Reviewing a copy of financial statements (audited, if available) for established corporate entities.

Non-documentary verification procedures include;

- Undertaking a company search and/or other commercial inquiries to ascertain that the legal person has not been, or is not in the process of being, dissolved or terminated;
- Using an independent information verification process, such as by accessing public corporate registers, private databases or other reliable independent sources (e.g., lawyers, accountants);
- Validating the legal entity identifier and associated data in the public access service;
- Visiting the corporate entity, where practical;
- Contacting the corporate entity by telephone or email.

Identification and Verification Principles for an Individual or Entity without a Business Relationship with the Bank:

For non-customer or walk-in customer, branches must verify the identification documents (NRC and Passport) before carrying out the transaction and record the copy of the identification documents of such customer.

Where the Bank does not have a Business Relationship with an Individual or Enterprise wishing to complete a cash transaction of 30 million Kyats or above, the Bank is required to complete additional due diligence as articulated in Branch operating procedures.

Periodic Reviews of CDD:

The Bank shall perform periodical reviews of customer information. The frequency of which will be based upon the customer's risk classification. The minimum review period is:

- High Risk -Yearly
- Medium Risk - Every 2 years
- Low Risk - Every 3 years

When undertaking a periodic review, the branches shall confirm all supporting documents are current and have not expired. If the document is no longer current, then the branches shall collect and verify new / current documents.

The Bank shall implement event-based triggers for ad-hoc EDD out with the minimum Review Period timeframes. An event-based trigger could be in response to suspicious transaction or an escalation in risk classification.

Determination of Ultimate Beneficial Owner (UBO)

A UBO is an individual/natural person who:

- Owns or controls directly or indirectly more than 20 percent of the Enterprise;
- Exercises control of the Enterprise through other means.

The Bank shall conduct the following for all UBOs:

- When dealing through an Authorised Person, the bank shall confirm the Authorised Person is acting on behalf of one or more UBOs;
- Collect and verify the identity of the UBOs by using relevant information or data obtained from a reliable source so that the Bank is satisfied that it knows the identity of the UBO;
- If the Enterprise is listed on a stock exchange, the Bank shall not require to identify and verify the identity of UBOs, provided the company is subject to adequate disclosure requirements to ensure transparency of UBOs. The Bank shall obtain and verify identification documents from the public registry. Where the Bank determines the disclosure requirements are inadequate, the Bank shall determine the UBOs following which it shall obtain and verify the documentation for each UBO.
- The Bank shall verify and prohibit nominee shareholders who are not officially registered in the company's records in accordance with the directives issued by the Directorate of Investment and Companies under the Ministry of Investment and Foreign Trade.
- Where the Enterprise has been classified as High Risk or escalated to High Risk status, identification and verification should be made to each individual shareholder who owns or controls directly or indirectly more than 10 percent of the Enterprise and perform enhanced due diligence (EDD).
- For Enterprise, the Bank shall conduct face-to-face KYC and CDD with the Enterprise's authorized person. The authorized person shall provide the information as requested by the bank. Where The Bank is unable to undertake a face-to-face meeting, the customer shall be automatically classified as High Risk.

Reliance on third parties to undertake CDD

The bank shall conduct its onboarding activities in strict adherence to Customer Due Diligence (CDD) if the Bank delegate part or all of the onboarding processes to a third party. The Bank will implement the following processes before establishing any new third-party onboarding relationships:

- If the Bank is delegating it's Know Your Customer (KYC) and Customer Due Diligence (CDD) to a third party, it is imperative for the Bank to establish rigorous controls and oversight mechanisms.

These measures are essential to ensure the precise and compliant execution of KYC and CDD tasks by the third party. The third-party onboarding process must adhere meticulously to all relevant financial and data protection regulations, encompassing strict adherence to reporting standards, independent evaluation for the purpose of the bank's risk management, and full compliance with all regulatory obligations.

- The bank is committed to maintaining the highest standards of Financial Crime Compliance (FCC) and, in this regard, shall extend training in AML/CFT, Sanctions Screening, and Record-Keeping to third-party entities. The bank shall also provide ongoing oversight of the third party's training program to ensure it aligns with internal resources' training standards. The bank shall establish mechanisms to ascertain that the third party's training program complies with the bank's requirements and maintains the level of quality expected to meet the standards of Financial Crime Compliance.

7. Customer Risk Assessments

- All customers must be rated as Prohibited, Low, Medium or High Risk based on Customer Risk Assessments (CRA) which may consider the following criteria:
  - Customer Risk: Defined based on factors such as the industry or occupation, legal arrangement, ownership structure, residence, source of funds, PEP, Domestic blacklist and other negative lists, negative media or local reputation and income or deposit amount of customers.
  - Geographic Risk: Consideration of both Myanmar regional risk profiles and/or Country risk profiles where banking transactions involve both foreign and domestic Individuals or Enterprises. Risk assessments may consider AML/CFT index, corruption and terrorism index as defined by credible sources from international organizations as well as specific High Risk regions defined by local regulators.
  - Product, service, and transaction risk: Defined based on factors such as product type, purpose of establishing the account, mode of transaction or payment, expected and actual transaction volumes or amounts, availability of information of the stakeholders of the product and parties involved in transactions, complexity of products, transactions, and payments patterns.
- The CRA and any supporting documentation shall be stored in line with the Bank’s procedures and Periodic Reviews undertaken in line with the risk classification schedule.
- The Bank shall use the outcome of the CRA to establish risk-based approach and manage the identified risks through appropriate systems and controls.
- The nature and extent of due diligence will depend on the risk classification. When preparing the customer profile, the bank should request information relevant to the risk category, no more and no less.

- At the time of on-boarding, the risk category of the account is based on the parameters available in the CRA. Periodic Reviews will be undertaken at differing intervals depending on the risk classification and / or following a trigger event (for example where a suspicious transaction has taken place, velocity and volume of the transactions, the type of transactions is suspicious). The risk will then be recalculated based upon the new information to hand.

Prohibited Parties and Industries

The Bank shall not engage in any Business Relationship nor cash transactions with Individuals or Enterprises who/which:

(1) are Sanctioned or a citizen of a sanctioned country (locals doing business in local currency to be excluded);
(2) appear on the CBM Blacklist;
(3) have been charged with a serious offence;
(4) are Shell Companies;
(5) are Red Light Business/Adult Entertainment/Prostitution/Massage Parlors;
(6) are Atomic Power;
(7) are in production of, use of, or trade in, Arms (i.e., Weapons, Munitions Products, primarily designated for Military Purposes).
(8) are Non-resident, non-citizen opening account if one of the below requirements is not met:
    - They have material investment in local business (>10%);
    - Individual opening account as required for investment in the local stock exchange and they have stock exchange approval to support the investment;
    - Individuals who have resided or established their primary business within the Union of Myanmar for a continuous duration of at least 183 days during the preceding twelve-month period, as well as companies, organizations, and offices that are lawfully established under domestic or foreign regulations within the Union of Myanmar;
    - Foreign incorporated or registered business entities must adhere to the specified documents, which necessitates the submission of notarized mandatory documents. These documents must be certified by the Ministry of Foreign Affairs and subsequently endorsed by the Myanmar Embassy.

Customers meeting the following criteria will **automatically be assessed as High Risk:**

- Non-resident, non-citizen, but if they meet one of the above requirements they may be allowed to open accounts but still shall be classified as High Risk;
- Individuals/Enterprises which are under PEP List;
- Individuals/Enterprises which are under one of the international sanction lists, in which such individuals/enterprises have committed several breaches of regulations and imposed penalty or other

legal enforcement by regulatory bodies. The Bank shall apply international sanction lists derived from Refinitiv World-Check or similar vendors for both domestic and international transactions and onboarding;

- Individuals/Enterprises accounts opened by lawyers, law offices or trustees on behalf of their clients;
- Individual/Enterprise which are from Private Banking;
- Trusts and casino industries are considered as a High Risk

Enhanced Customer Due Diligence (ECDD)

The bank's knowledge of the customer based on its activity shall better determine the actual risk presented by a customer. Higher risk customers, including those whose activity drives a higher risk rating, should be subject to enhanced customer due diligence (ECDD) to mitigate the risk including:

- For all High Risk Customers ECDD must be approved by AML/CFT department prior to onboarding and at each subsequent annual review;
- As general guidance, Enhanced Customer Due Diligence may consider the following, but AML/CFT team retains full discretion for full requirements for specific customers;
    a) Taking additional measures to understand customers' ownership structure and ensuring business structure is established for legitimate purposes rather than efforts to hide or misrepresent flow or purpose of funds;
    b) Taking additional measures to identify the purpose of establishing Banking Relationship and source of wealth and funds. This would include assessment of whether the quantum and nature of funds is commensurate with what would be reasonably expected for the customer in their employment or business;
    c) Seeking additional information on expected transactions and risk profile of key counterparties or entities that the customer is expected to regularly transact with;
    d) Seeking additional documentation evidence to verify the integrity and legitimacy of the customer's employment or business.
    e) Referring to additional third-party information about the customer to validate customer sourced information and scan negative media to assess potential risks. This information may be obtained through public domain searches, independent subscription databases such as World Check or CBM negative lists;
    f) For existing customers review of last 12 months transaction record to ensure its consistent with customer disclosures and is commensurate with what would be reasonably expected for the customer in their employment or business.
- Additional transaction monitoring must be implemented for High Risk Customers including customer specific transaction thresholds, increased frequency and pattern monitoring of the

transactions or activities to determine whether unusual or suspicious behaviour;.

- Transaction monitoring should consider apparent economic or lawful purpose and is not consistent with the bank knowledge on customer;
- The Bank shall carry out customer due diligence measures on the first transaction conducted through the account opened with the customer's name.

8. Political Exposed Persons (PEPs)

The Bank shall identify customers who are Politically Exposed Persons (PEPs) or connected with PEPs and conduct appropriate enhanced due diligence and monitoring on their related parties and transactions. PEPs can be either foreign or domestic. Foreign PEPs is defined as individuals who are or have been entrusted with prominent public functions by a foreign country (e.g., heads of state or of government; senior politicians; senior government, judicial or military officials; senior executives of state-owned corporations and important political party officials).

For domestic PEPs they are, individuals who are or have been entrusted domestically with prominent public functions (e.g., heads of state or of government; senior politicians; senior government, judicial or military officials; senior executives of state-owned corporations and important political party officials)
Predominantly, a PEP, is a person who holds (or has held, whether domestic, or foreign) a prominent public function by a state Government or their Departments or is a close associate of a person in such a position ('PEP Associates'), these include but are not limited to:

- Head of State or government;
- Senior government, judicial or military officials;
- Senior officials of political parties at a national level;
- Senior executives of state-owned enterprises;
- Senior members of ruling royal families;
- Senior people of religious organisations;
- Political parties or organisations;
- Senior management or individuals of international organisations.

Definition of a PEP does not include a middle-ranking or more junior official of any of the categories mentioned above (e.g., In the absence of other risk factors, for Myanmar government officials only officials of high rank or above would be classified as PEP).
"PEP Associates" in relation to the above includes:

- Immediate family members (spouse(s) and partners, parents, children, siblings, in-laws);
- Person who has close business relations with a PEP or who is the beneficial owner of an entity or trust that is setup for the benefit of PEP (i.e., Close Associate).

PEPs, due to the nature of their role and the influence they can bring to bear, are considered to be at higher risk for potential bribery and corruption, money laundering, and terrorist financing. Yoma bank shall not consider as a PEP after **3 years** of not being in prominent position. Yoma Bank shall adopt a risk-based approach to managing PEPs, including the initial customer due diligence steps; establishment of appropriate risk management systems to identify PEPs; and enhanced and ongoing monitoring of identified PEPs.

Enhanced Due Diligence for Politically Exposed Persons (PEPs)

In addition to the usual risk assessment factors of other customers, all PEPs will be subject to the following factors during enhanced due diligence to assess final risk level:

a) Taking all reasonable measures to identify the purpose of establishing Banking Relationship and source of wealth and funds. This would include assessment of whether the quantum and nature of funds is commensurate with what would be reasonably expected for the PEP current and/or prior roles;
b) Seeking relevant information from the customer such as country or jurisdiction in which the PEP is or was a public official and considering how country or jurisdictional factors impact the relative risk level;
c) Seeking relevant information on the responsibilities of the position that the PEP holds and/or the former position held and duration these positions were held. Assessments of the roles should be considered if this exposes the PEP to state assets or the PEP has critical decision- making authority in government or State-Owned Entities that could expose them to heightened risk;
d) For PEP associates consideration on the type of relationship held between the associate and PEP;
e) Referring to third party information about the customer to validate customer sourced information and scan negative media to assess potential risks. This information may be obtained through public domain searches, independent subscription database such as World Check, and internal bank PEP list of domestic PEP and/or negative lists, CBM negative lists;
f) Consideration of mitigating factors that PEP is not associated with the key risks of bribery and corruption, money laundering, and terrorist financing.

Following enhanced due diligence business shall obtain approval from AML/CFT department before establishing or continuing a Business Relationship with PEPs.

Required Risk Systems and Ongoing Monitoring

Yoma Bank shall adopt the following systems and infrastructure to assist with the management of PEPs:

a) Implementation of necessary infrastructure for customer risk scorecard specific to PEPs;
b) Implementation of necessary infrastructure for specific transaction monitoring thresholds and criteria for PEPs and event-based triggers for ad hoc enhanced due diligence;

c) Implementation of necessary infrastructure to report and manage Yoma Bank's portfolio- wide PEP exposure and related trends;
d) Performing, as minimum, annual reviews of all PEPs considering any changes in the PEPs position, activities, and historical transaction;
e) Hindsight screening of newly onboarded relationships to ensure PEPs have been identified and escalated for enhanced due diligence.

9. Correspondent Banking

Correspondent banking is vulnerable to money laundering since it is the provision of banking services by one bank (the correspondent bank) to another bank (the respondent bank). Correspondent Banking relationships are the Myanmar financial system's gateway to the global financial system. Efficient access to the global financial system is vital to Myanmar. However, this gateway potentially exposes the Bank to heightened AML/CFT risks

Correspondent Banking Due Diligence

The Bank shall undertake Correspondent Banking due diligence prior to establishing a Business Relationship and thereafter on an ongoing basis during the course of the Business Relationship. In addition to usual assessment criteria additional CRA should consider the following:

- Quality of the Correspondent Bank's management to deal with AML/CFT matters;
- Maturity of their AML/CFT policies and systems;
- Profile of their customer base;
- Document the responsibilities of each institution; mitigate risks associated with payable- through accounts and ensure accounts are not established for shell bank.

Before establishing a Business Relationship with a new correspondent bank, Treasury/Financial Institutions Department (FI) shall inform the AML/CFT team and source the required documents according to the Bank's procedures and checklist. All Correspondent Banking relationships must be reviewed and overseen by AML/CFT department prior to onboarding. The Bank shall not allow the followings:

- The Bank shall not allow to open an "Payable Through Account" for any purpose, any individual and any organization;
- The Bank shall not enter into or continue a correspondent or Business Relationship with a shell bank in a foreign country .

The Periodic Review of all Correspondent Business Relationships will be performed annually by AML/CFT department with the support of FI Department.

10. Transaction Monitoring

The Bank shall gather further information regarding a customer or his or her transaction before deeming it suspicious and filing an STR alongside with proper customer due diligence process. The Bank employees should watch for any activity that may be inconsistent with a customer's source of income or regular business activities.

The bank must sort through thousands of transactions each day, a system for monitoring and reporting suspicious activity should be risk-based and should be determined by factors such as the nature of its business, its location, the frequency and size of transactions and the types and geographical location of its customers. A system should also gather sufficient knowledge of a customer and their activity, so that their use of products and services can be monitored to detect any unusual activity, which may be suspicious and reportable under local law or regulation.

The core operating system of the bank maintains significant customer data and can also be utilized to generate certain internal reports that can be used to discover possible money laundering and terrorist financing. Some of the reports may include:

- Daily activity in excess of the CBM's reporting threshold;
- Daily cash activity just below the country's reporting threshold to identify possible structuring;
- Cash activity aggregated over a period of time (e.g., individual transactions over a certain amount, or totaling more than a certain amount over a 30-day period) to identify possible structuring;
- Wire transfer reports/logs with filters using amounts and geographical factors;
- Monetary instrument logs/reports;
- Check kiting/drawing on uncollected funds with significant debit/credit flows;
- Significant change reports;
- New account activity reports.

All Bank staff must report any red flags identified when accepting a customer or a transaction to the AML/CFT Department based on the following criteria but not limited to others:

- Unusual Customer Behavior;
- Unusual Customer Identification circumstances;
- Unusual Cash Transactions;
- Unusual Noncash Deposits;
- Unusual Wire Transfer Transactions;
- Unusual Safe Deposit Box Activity;
- Unusual Activity in Credit Transactions;
- Unusual Trade Financial Transactions;
- Unusual Employee Activity;
- Unusual Activity Indicative of Potential Terrorist Financing.

AML/CFT team will review a red flag that has been raised and:

- Require the branch to seek further information from the customer, and/or;
- Apply ECDD, and/or;
- Refuse to accept the transaction, and/or;
- Consider lodging a suspicious matter report with the MFIU.

The AML/CFT Department will review these 'red flags' annually to see if new flags should be added. Where transactions are identified as unusual, AML/CFT team will investigate all the recent transaction history of the customer to identify anything that is suspicious. If such transactions are identified, AML/CFT team will follow the suspicious activity reporting (STR) procedures. To conduct the above close monitoring and detect suspicious activities, The Bank shall install the third-party solution soon. If no suspicious activity report is lodged with the MFIU the AML/CFT team may still flag the customer for re-identification or to conduct enhanced due diligence.

The Bank is permitted to cease the CDD process if it has a reasonable belief that performing the CDD process will tip off the customer that his/her transaction may be considered as related to money laundering or the financing of terrorism. In such circumstances AML/CFT team may review in detail the transaction provided that it immediately submits a suspicious transaction report to the MFIU.

The Bank shall promptly report to the MFIU if the amount of transaction of money is equal to or exceeds the designated threshold or it has reasonable ground to believe that any money is obtained by illegal means or is related to ML/TF. The Bank has adequate policies, procedures, and systems in place to be able to provide the compliance reports to governmental agencies.

External Reporting

External reporting typically involves reporting of:

(i) Suspicious Transactions, and;
(ii) Threshold Transactions exceeding a certain threshold.

Suspicious Transaction Report (STR)

The Bank must report suspicious transactions and related findings to MFIU. All transactions must be categorized as either attempted transactions (suspicious activity) or completed transactions (suspicious transactions).
The AML/CFT Department must develop an effective suspicious activity monitoring and reporting policy and create a culture of compliance whereby policies, procedures, and processes are followed.

Where the branch has reasonable ground to believe that any transaction or attempted transaction may be related to AML/CFT, it must submit a STR/SAR report to AML/CFT department with the required documentation.
AML/CFT team will review the branch STR/SAR report based on the detailed assessments of the information provided, along with any subsequent decisions about whether or not to await developments or seek additional information, rationale for deciding whether or not to proceed with an external SAR/STR and if it has reasonable ground to believe that such transaction is suspicious, shall report to MFIU.

Threshold Transactions Report (TTR)

The Bank has specified threshold transaction limit for all transactions conducted through The Bank. Threshold Transaction Reporting (TTR) shall incorporate all transactions conducted at or above threshold limit within a day or as specified in the guidelines/directives issued by the regulatory bodies from time to time.

The Threshold Transaction may be a single transaction or several transactions that appear to be linked which exceed the threshold limit which is USD 10,000 or MMK 100 million. Details of the source/s of funds shall be obtained and recorded by The Bank for each threshold transaction.

The AML/CFT team shall submit TTR in the format issued by MFIU and as prescribed in the regulatory guidelines within the specified deadline of 24 hours if it is situated in an urban center or within 3 days if it is situated in a remote district. Head of AML/CFT or the designated officer shall ensure that the TTRs are duly submitted to MFIU.

11. Freezing/ Blocking the account

The Bank shall freeze a bank account/assist in seizure of financial assets at the behest of an authority (e.g., order of Anti-Corruption Commission under the Anti-Corruption Law, Central Committee for Counter Terrorism under the Counter Terrorism Law, Financial Intelligence Unit under the Anti-Money Laundering Law (AML Law), by Court or Police Order). For blocking or freezing accounts of incident or fraud related customers, the consultation and approval of AML/CFT team is required on a case-by-case basis and must be informed to Central Bank of Myanmar as well as the following considerations must be taken place:

- To cover the consumer protection acts or legal basis for blocking/ freezing an account;
- To highlight the significant or potentially reputational risk to the bank;
- To decide on freezing/ blocking bank account should be the result of an accumulation of aggravating factors and a lack of mitigation factors;
- To freeze/ block bank account, the purpose should be clearly stated and explained when there is an oversight from Central Bank of Myanmar;
- According to the Notification No. 22/2023 issued by the Central Bank of Myanmar (CBM), detailing the Standard Operating Procedure (SOP) for handling fraud cases, the bank is committed to the stringent enforcement of the prescribed controls as outlined in the SOP for the suspension of amounts or blocking of accounts.

12. Wire Transfer

Wire Transfers are transfers of money by electronic means from a financial Institution on behalf of an Individual or Enterprise to a beneficiary of another financial Institution. Wire Transfers include both cross-border, and domestic transactions including international remittance transactions.

The Bank should have effective risk-based preventative procedures for determining:

i. When to execute, reject or suspend a Wire Transfers;
ii. When to perform ECDD;
iii. When to report to the MFIU;
iv. Transaction monitoring as a control process.
v. The appropriate follow-up action which may include restricting or terminating Business Relationships.

The Bank shall perform the following before the wire transfer is initiated and posted:

- Name or sanctions screening of the customer and all related parties to the wire transfer transactions as well as sanctions screening of the payments or swift messages related to the trade finance transactions;
- The Bank should obtain a letter of authorization from the entity, authorizing the person to conduct transaction on behalf of the entity. The letter should have a letterhead specifying the name of the entity, its address and business registration number;
- The Bank shall obtain true identity of the beneficiary while making payment of the wire transfers, must record adequate details of the wire transfer including at least the date of the wire transfer, the type and amount of currency involved, value date, the detail of the wire transfer, accurate and meaningful originator, beneficiary and the beneficiary bank information;
- The Bank shall insist on complete originator and beneficiary identification before effecting the transfer, where the branch staff, initiating the wire transfer has reason to believe that a customer is intentionally structuring the wire transfers to below threshold limits to several or same beneficiaries in order to avoid documentation or reporting requirement. Where the customer is not cooperative, The Bank shall make necessary efforts to establish the identity and report suspicious transaction/activities report (STR/SAR) to the MFIU;
- With respect to the possession of foreign currency, the initiation and operation of foreign currency accounts, or any transactions involving foreign currency, shall apply the Foreign Exchange Management Law (12/2012) and regulation without limitation.

Requirements for Transaction as Intermediary Bank

When The Bank acts as an Intermediary Bank, The Bank shall pass on all messages and payment instructions received, including the originator's information. The Bank shall retain this information for at least five years starting from the transaction posted date.

Moreover, when a customer or the customer's proxy or beneficiary owner is identified as a national of a FATF non-cooperative countries, the staffs shall perform EDD in accordance with local laws and regulations. Such transaction shall be reviewed by Head of Operations and approved by Head of AML/CFT.

13. Know Your Employee (KYE)

A Know Your Employee (KYE) program means that the bank shall have a program in place that allows it to understand an employee's background, conflicts of interest and susceptibility to money laundering complicity. Policies, procedures, internal controls, job descriptions, codes of conduct and ethics, levels of authority, compliance with personnel laws and regulations, accountability, monitoring, dual control and other deterrents should be firmly in place. The People Division shall incorporate the following provisions of KYE in the recruitment process and undertake a Periodic Review of the information held:

- Bank shall establish screening procedures to ensure appropriate standards when hiring employees and such procedures shall be approved by the Board of Directors or such other management body of The Bank;
- Background screening of prospective and current employees, especially for criminal history, is essential to keeping out unwanted employees and identifying those to be removed;
- Background screening to prohibit any person who has been convicted of a crime involving dishonesty or money laundering from becoming or continuing as an institution-affiliated party; owning or controlling, directly or indirectly, an institution; or otherwise participating, directly or indirectly, in the conduct of the affairs of an institution without the prior written consent of the regulator (Consultants who take part in the affairs of the Bank shall be subject to this requirement too);
- The sensitivity of the position or the access level of an individual employee may warrant additional background screening, which should include verification of references, experience, education and professional qualifications;
- The Bank shall ensure that the details of employee's information remain current, these checks will be repeated for all employees every year.

Definitions

Business Relationship: means any business, professional or commercial relationship connected with the professional activities of a bank and which is expected to have an element of duration.

Correspondent Banking: means the provision by one bank (the correspondent) to another bank (the respondent) of credit, deposit, collection, clearing or payment services.

Customer: means a person involved in any of the followings:

(i) a person who transfers money, opens a bank account or makes a commitment;
(ii) a signatory to a transfer or an account;
(iii) a person assigned to transfer, a transferor, a person who has the right or responsibility to transfer;
(iv) a person who has the authority to transfer or control an account;
(v) a person who attempts to deal with the matters mentioned in clause (i) to clause (iv);

Customer Due Diligence (CDD): is the process through which the Bank develops an understanding of the customers and the ML/FT risks. CDD is the cornerstone of the AML/CFT program. It involves gathering and verifying information about a customer's identity, beneficial owners and representatives.

Enhanced Due Diligence (EDD): is the additional information collected on the customer to provide a deeper understanding of the customer's activities to mitigate associated risk. ECDD is required where the customer has been determined as High Risk. due to the customer profile and the way they utilize of the bank's products and services.

Financial Action Task Force (FATF): is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering and terrorist financing. These Recommendations also include international co-operation and preventive measures to be taken by financial institutions and others such as casinos, real estate dealers, lawyers and accountants. The FATF Recommendations are recognized as the global anti-money laundering (AML) and Combat financing of terrorism (CFT) standard.

Geographical Risk: means the area, region or country that related to money laundering, terrorist financing and sanctions those areas are specify as High Risk in geographical areas.

Know Your Customer (KYC): is a set of standards to identify the customer using reliable and independent information. KYC is an ethical requirement for those dealing with customers during the opening and maintaining of accounts and is regarded as the basic tool for AML/CFT. If the Bank is unable to apply appropriate KYC measures the Bank should consider closing the account and terminating the banking relationship after issuing due notice to the customer explaining the reasons for taking such a decision.

Know Your Employee (KYE): is a set of standards upon which the bank assesses all employee's background, any conflicts of interest and susceptibility to money laundering.

Local Blacklist: means the list which is provided by CBM, MFIU and other local/domestic AML/CFT authorities.

Money Laundering: is the participation in any transaction that attempts to conceal or disguise the nature or origin of funds derived from illegal activities such as, fraud, corruption, tax evasion, organized crime, or terrorism etc.,

Money Laundering is the process used to disguise the source of money or assets derived from criminal activity. To use the proceeds of their crimes, criminals need to 'clean' or 'launder' this money — making it appear to have come from legitimate sources. The crime of Money Laundering involves diverse and often sophisticated methodologies. It corrupts and intermingles with legitimate transactions in areas such as banking and finance, casinos and gaming, high-value assets like real estate and luxury vehicles, international trade, and international remittance and foreign exchange services.

- **Placement:** Involves placing the proceeds of crime in the financial system. It refers to the physical disposal of cash, often in the form of bank deposit, through a succession of small and anonymous transactions. The money launderers insert the illicit money into a legitimate financial institution.
- **Layering:** This stage involves converting the proceeds of crime into another form and creating complex nature of financial transactions to disguise the audit trails and the source and the ownership of funds. (e.g., buying and selling gold, stock, property etc.). It involves bank to bank transfers, wire transfers, several deposits and withdrawals, purchasing high value items etc.
- **Integration:** In this stage the money re-enters the mainstream economy in the legitimate looking form. It involves placing the laundered proceeds back in the economy under the veil of legitimacy.

Myanmar Financial Intelligence Unit (MFIU): was established on 16 January 2004 to prevent money laundering and terrorism financing activities in Myanmar. It is a central, national agency, responsible for receiving, processing, analyzing and disseminating financial information and intelligence on suspected money laundering and terrorist financing activities to the Investigation Department, other relevant law enforcement agencies and foreign FIUs.

Nested Accounts: occurs when a Bank/FI (third party BFI) gains access of the financial services offered by the correspondent bank by operating through the correspondent account belonging to another Bank/FI i.e., of a respondent Bank/FI.

Non-Compliance: means failure to act in accordance with Laws, Regulations, and internal policies and procedures.

Originator: means the account holder, or where there is no account, the person (natural or legal) that places the order with the bank or financial institution to perform a wire or electronic transfers.

Payable-through accounts: refers to correspondent accounts that are used directly by third parties to transact business on their own behalf.

Proceed of Crime: means money derived from illegal activities

Prohibited Parties and Industries: are the list of parties and industries which the bank is unable to do business with.

Politically Exposed Person (PEP): A PEP, is a person who holds (or has held, whether domestic, or foreign) a prominent public function by a state Government or their Departments or is a close associate of a person in such a position ('PEP Associates').

Red Flag: are warning signs, such as unusually large transactions, which indicate signs of money laundering activity and indicate EDD is required.

Reporting Organization: all entities who are required to report to the regulator as stipulated by AML Law.

Risk-based Approach: to AML/CFT means that countries, competent authorities and financial institutions, are expected to identify, assess and understand the ML/TF risk to which they are exposed and take AML/CFT measures commensurate to those risks in order to mitigate them effectively.

Risk Assessment: the process of identifying and evaluating the risks and assessing the potential impact of each risk.

Shell Entity: is an entity that has no active business and usually exists only in name as a vehicle for another company's business operations. In essence, shells are corporations that exist mainly on paper, have no physical presence, employ no one and produce nothing. Although they are legal entities that do have a legitimate function in business operations, shell companies are also utilized by criminals to facilitate fraudulent activities including money laundering.

Sanctions List: is a compilation of individual sanctions.

Suspicious Transactions: are transactions that may involve proceeds of crime or where the funds are intended to be used for illegal activities.

Suspicious Transaction Report (STR): is a report prepared by the Reporting Entity to the MFIU detailing suspicious transactions, transactions above the defined threshold or it has reasonable ground to believe that any money or property is obtained by illegal means or is related to money laundering or financing of terrorism or attempt to do so.

Terrorism Financing or Financing of Terrorism (TF/FT): refers to any activity that raises money to support terrorist activities. The money may have been raised from legitimate and/or criminal sources.
The financing of terrorism is where money or other assets are made available, directly or indirectly, with the sole intention to further terrorism. The primary goal is not necessarily to conceal the source of the money but to conceal the nature of the financed activity.

Trustee: should be understood as described in and consistent with Article 2 of the Hague Convention "Convention on the Law Applicable to Trusts and on their Recognition" and "the Trust Act, 1904" applicable to trusts and their recognition. Trustees may be professional (e.g., depending on the jurisdiction, a lawyer or trust company) if they are paid to act as a trustee in the course of their business, or nonprofessional (e.g., a person acting without reward on behalf of family).

Threshold Transaction Reports (TTR): is a report prepared by the Reporting Entity to the MFIU on details of transactions above certain amount. Threshold amount to report is designated by respective notifications of Central Control Board on Money Laundering, regarding Myanmar currency transaction, if the transaction amount is equal and or in excess of 100 million kyats, and although if it does not exceed 100 million kyats, if it is unordinary or it has suspicious ground to Money Laundering/Terrorist Financing it must be reported to FIU.

Ultimate Beneficial Owner (UBO): Directors and/or Shareholders who ultimately own or controls more than 20% of the Enterprise,

Wire or Electronic Transfers: any transaction carried out on behalf of an originator through a financial institution by electronic means, with a view to making an amount of funds available to a beneficiary person at a beneficiary financial institution, irrespective of whether the originator and the beneficiary are the same person. It also includes cross-border and domestic wire or electronic transfers.

Important Acronyms

AML	-	Anti-Money laundering CBM - Central Bank of Myanmar
CCO	-	Chief Compliance Officer
CDD	-	Customer Due Diligence
CDD Directive	-	Central Bank Customer Due Diligence Directive 18/2019
CFT	-	Counter Financing of Terrorism
CRA	-	Customer Risk Assessment
CRO	-	Chief Risk Officer
EDD	-	Enhance Due Diligence
EU	-	European Union
FATF	-	Financial Action Task Force
FCC	-	Financial Crime Compliance
FIs	-	Financial Institutions
KRIs	-	Key Risk Indicators
KYC	-	Know Your Customer
KYE	-	Know Your Employee
MFIU	-	Myanmar Financial Intelligence Unit
ML	-	Money Laundering
NRC	-	National Registration Card
OECD	-	Organization for Economic Co-operation and Development
OFAC	-	Office of Foreign Assets Control
OTP	-	One-time Password
PEPs	-	Political Exposure Persons
RAG	-	Red/Amber/Green
RMA	-	Relationship Management Accounts
SAR	-	Suspicious Activity Report
STR	-	Suspicious Transaction Report
TF/FT	-	Terrorism Financing or Financing of Terrorism
UBO	-	Ultimate Beneficiary Owner
UN	-	United Nations