



HABIB BANK  
හබිබ් බැංකුව  
ஹபீப் வங்கி

Anti-Money Laundering (AML) / Combating Financing of Terrorism  
(CFT)/ Combating Proliferation Financing (CPF) & Sanctions  
Procedures Version 5.0

Habib Bank Limited  
Sri Lanka Compliance

Anti-Money Laundering (AML) / Combating Financing of Terrorism (CFT) & Sanctions Procedures – HBL Sri Lanka	
APPROVAL SHEET	
Document Owner – HBL SL Compliance	
Document Version – Version 5.0	
Implementation Responsibility - Compliance - HBL Sri Lanka	
Custodian - HBL SL Compliance	
Operating Jurisdiction - HBL Sri Lanka	
Review Frequency – 01 Year or earlier if required	
Review Responsibility - Compliance - HBL Sri Lanka	
Last Approval Date – November 2023	
Approved Date:	
Effective Date: Immediately after approval	
Next Review Date: 01 year after approval date	
Prepared by:	Reviewed by:
 <b>Shashikala Kandage</b> Manager Compliance – Sri Lanka	 <b>Hasitha Ganegama</b> Regional Head of Compliance- Sri Lanka & Maldives
Recommended by:	
 <b>Sujeenie Gunasekera</b> Country Manager – Sri Lanka	
Reviewed and concurred by (HBL - PAKISTAN)	
 <small>majid aziz (Jun 24, 2025 11:45 GMT+5)</small> <b>Majid Abid Aziz</b> Head - International Compliance	
Approved by:	
 <small>Syed Saad Uddin Ahmed (Jun 24, 2025 11:47 GMT+5)</small> <b>Syed Saad Uddin Ahmed</b> Chief Compliance & Conduct Officer	

‘Compliance is my responsibility’

## Table of Contents

<b>ANTI-MONEY LAUNDERING (AML) / COMBATING FINANCING OF TERRORISM .....</b>	<b>1</b>
Document Version Tracker.....	8
DEFINITIONS.....	9
<b>1. INTRODUCTION .....</b>	<b>12</b>
1.1 OBJECTIVE .....	12
1.2 SCOPE .....	12
<b>2. SANCTION SCREENING.....</b>	<b>12</b>
2.1 WHO IS SUBJECT TO SANCTIONS? .....	13
2.2 HBL SL APPROACH TOWARDS SANCTIONS.....	13
2.3 DETECTION REVIEW PROCESS .....	13
2.4 DETAILS OF SANCTIONS SCREENING FILTER - SAFEWATCH: .....	14
2.5 SANCTIONS LISTS AS PER HBL GLOBAL SANCTIONS POLICY.....	14
2.6 PRIVATE LIST MANAGEMENT AND NAME ADDITION PROCESS: .....	15
2.7 SELECTION OF LISTS FOR PAYMENT SCREENING AND ONBOARDING .....	15
2.8 LIST UPLOADING IN SW 4.0:.....	15
2.9 FOUR EYE PRINCIPLE: .....	16
2.10 PAYMENT SCREENING .....	16
2.10.1 Swift Payments.....	16
2.10.2 Domestic Wire Transfers .....	17
2.10.3 Guidance on Payments Sanctions Screening through SSW .....	18
2.10.3.1 Sanctions Screening Performed by Compliance team on SWIFT .....	18
2.10.3.2 Reporting / MISs.....	20
2.10.3.3 Procedure for SWIFT Payment Sanctions Screening/ Onboarding .....	20
2.11 CUSTOMER ONBOARDING .....	20
2.11.1 Compliance Role and responsibilities .....	21
2.11.1.1 Compliance Role and responsibilities - Vendor screening and screening of third-party employees outsourced from Vendors .....	22
2.11.2 United Nations Security Council Resolutions relating to The Prevention and Suppression of Terrorism and Terrorist Financing .....	23
2.11.3. United Nations Security Council Resolutions relating to the prevention of Proliferation Financing (PF).....	24
2.12 SANCTIONS & SCREENING ADVISORY.....	25
2.12.1 Sanctions Countries.....	25
2.12.2 Trade department .....	25
2.12.3 Sanction Screening of bank's customer portfolio: .....	25
2.12.4 Freezing / Suspension Orders.....	26
<b>3. KNOW YOUR CUSTOMER (KYC) .....</b>	<b>27</b>
CUSTOMER DUE DILIGENCE (CDD).....	28
ENHANCED DUE DILIGENCE (EDD) .....	28
3.1 CUSTOMER RISK RATING METHODOLOGY .....	29
3.2 CUSTOMER DUE DILIGENCE (CDD).....	30
3.2.1 Information to Be obtained at the time of establishing relationship .....	30

3.2.2 Identification of the Customer.....	30
3.2.3 Verification of the Identity .....	31
3.2.3.1 Identification and Verification of Natural Persons Acting on behalf of Customer (power of attorney).....	31
3.2.4 Identification and Verification of Beneficial Owners .....	32
3.2.4.1 Beneficial owner(s) of a legal person .....	32
3.2.4.2 Beneficial owner(s) of a legal arrangement (i.e. legal arrangement includes an express trust, a fiduciary account or a nominee).....	33
3.3. CDD MEASURE FOR OCCASIONAL CUSTOMER / WALK-IN CUSTOMERS AND ONLINE TRANSACTIONS .....	34
3.4. INFORMATION ON THE PURPOSE AND INTENDED NATURE OF BUSINESS RELATIONSHIP .....	35
3.5 TIMING OF VERIFICATION.....	35
3.6 JOINT ACCOUNTS .....	35
3.7 DORMANT ACCOUNTS.....	35
3.8 CIRCUMSTANCES WHERE CDD MEASURES ARE NOT COMPLETED: .....	35
3.9 ANONYMOUS OR FICTITIOUS ACCOUNT .....	36
3.10 PROHIBITION OF PERSONAL ACCOUNTS FOR BUSINESS PURPOSES .....	36
3.11 ENHANCED DUE DILIGENCE.....	36
3.12 SPECIALIZED ENHANCED DUE DILIGENCE (SEDD) FOR ULTRA HIGH NET WORTH INDIVIDUALS .....	38
3.13 PERIODIC AND EVENT DRIVEN/TRIGGER BASED REVIEW: .....	39
3.13.1 Periodic Review: .....	39
3.13.2 Procedure to perform periodic reviews: .....	40
3.14 WIRE TRANSFERS/ FUND TRANSFERS.....	40
3.15 CORRESPONDENT BANKING RELATIONSHIPS.....	42
3.15.1 Types of relationships .....	42
3.16 RECORD RETENTION PERIOD.....	43
3.17 AML / CFT/ CPF, SANCTIONS AND TBML TRAININGS .....	44
3.18 CUSTOMER SELECTION FOR EXIT MANAGEMENT .....	44
<b>4. AML ADVISORY, POLICIES AND PROCEDURES.....</b>	<b>45</b>
4.1 AML ADVISORY .....	45
4.1.1 Associations, Clubs, NGOs, NPOs, Societies and Trusts: .....	45
4.1.2 Important considerations for first line of defense / branch level compliance: .....	45
4.1.3 Clearance Regarding Associations, Clubs, NGOs, NPOs, Societies and Trusts: .....	45
4.1.4 Politically Exposed Persons (PEPs) - Guidelines for Identification and Assessment of Politically Exposed Persons (PEPs) .....	46
4.1.4.1 Introduction.....	46
4.1.4.2 Definition.....	46
4.1.4.3 Categorization of PEP .....	47
DOMESTIC PEPS .....	48
FOREIGN PEPS .....	51
4.1.4.4 Minimum measures for identification of a PEP or their “family member or close associates” .....	51
4.1.4.5 PEP Risk Assessment Process .....	51
4.1.4.6 Identification of PEP for NTB and ETB Customer .....	52
4.1.4.7 Compliance Management Information Reports .....	53
<b>5. TRANSACTION MONITORING .....</b>	<b>53</b>

5.1	SYSTEM BASED TRANSACTION MONITORING.....	53
5.2	FCCM MODULES.....	54
5.3	ACCESS RIGHTS, ROLES AND ALERTS DISTRIBUTION .....	54
5.4	ALERT SCORING .....	54
5.5	ACTIVE AML SCENARIOS .....	55
5.6	CUSTOMER SEGMENTATION .....	61
5.7	ALERT MANAGEMENT .....	61
5.8	CASE MANAGEMENT .....	62
5.9	ACTIONS AVAILABLE .....	62
5.10	ROLES & RESPONSIBILITIES.....	64
5.11	REQUEST FOR INFORMATION (RFI) FOR ALERT MANAGEMENT .....	64
5.12	ALERT HANDLING PROCESS .....	65
5.13	ROLES & RESPONSIBILITIES.....	66
5.13.1	Role and Responsibility of Compliance Team along with Turn Around Time of Alert Resolution .....	66
	Role of Maker (Alert Management Analyst) .....	66
	Role of Checker .....	66
	Roles, Responsibilities & Authorities of Stakeholders along with levels of escalation .....	66
5.14	STAFF ACCOUNTS .....	67
5.15	MIS REPORTS IN FCCM .....	67
5.16	REPORTING OF STRs/CTR/EFTs/IFTs TO FIU .....	68
5.16.1	Procedures for STRs.....	68
5.16.2	Procedures for CTRs, EFTs & IFTs .....	69
<b>6.</b>	<b>TRADE COMPLIANCE ADVISORY .....</b>	<b>70</b>
6.1	MAIN METHODS OF TBML .....	71
6.1.1	Over Invoicing:.....	71
6.1.2	Under Invoicing:.....	71
6.1.3	Multiple Invoicing:.....	71
6.1.4	Short Shipping: .....	71
6.1.5	Over Shipping: .....	71
6.1.6	Deliberate obfuscation of the Type of Goods .....	71
6.1.7	Phantom Shipping .....	71
6.2	DUE DILIGENCE CHECKS.....	72
6.2.1	Identification of Customer's Line of Business: .....	72
6.2.2	Identification of Clients Dealing in Defense or Dual Use Goods: .....	72
6.2.3	Goods Description and Pricing Factor of Goods:.....	73
6.2.4	Determination of Movement of Goods:.....	73
6.3	REVIEW & ADVISE RELATED TO SANCTIONS .....	73
6.4	REVIEW & ADVISE RELATED TO TBML RED FLAGS.....	73
6.5	ROLE OF TRADE FINANCE TEAM .....	73
6.6	FILING OF STRs: .....	74
	Annexure I – World Check Format .....	75
	Annexure II – CRRM Methodology.....	75
	Annexure III – Beneficial Ownership declaration.....	75
	Annexure IV – High Risk Profile forms .....	75
	Annexure V – Periodic KYC SOP** .....	75

Annexure VI – Suspicious Indicators .....	75
Annexure VII - Compliance Management Information Reports .....	76
Annexure VIII - RFI.....	76
Annexure IX – PEP Approval forms .....	76
Annexure X – STR reporting manual .....	76
Annexure XI – Identification of Beneficial Ownership, Drill Down process .....	76
Annexure XII- STR Reporting Format for Branches .....	77
Annexure XIII- TBML red flags .....	77
<b>**ANNEXURE V- PERIODIC KYC SOP .....</b>	<b>78</b>
Scope of Periodic KYC Reviews .....	78
Objective .....	78
Why Periodic KYC reviews? .....	78
When to Perform .....	78
Responsibility of Branch Operations Manager (BOM) .....	79
Responsibility of HBSL Compliance Team .....	81
Periodic KYC Review Process.....	81
Maintaining updated records of Resident Visa / Permit – Non-Nationals .....	82
Annexures .....	84

**Document Version Tracker**

Version	Date	Revision History	Name
1.0	31/10/2019	New Document	Anti-Money Laundering (AML) / Combating Financing of Terrorism (CFT) & Sanctions Procedures
2.0	31/05/2021	1st Revision	Anti-Money Laundering (AML) / Combating Financing of Terrorism (CFT) & Sanctions Procedures
3.0	02/08/2022	2 <sup>nd</sup> Revision	Anti-Money Laundering (AML) / Combating Financing of Terrorism (CFT) & Sanctions Procedures
4.0	11/2023	3 <sup>rd</sup> Revision	Anti-Money Laundering (AML) / Combating Financing of Terrorism (CFT) & Sanctions Procedures
5.0		4 <sup>th</sup> Revision	Anti-Money Laundering (AML) / Combating Financing of Terrorism (CFT) & Sanctions Procedures



## DEFINITIONS

1. “Beneficial owner” As per the Rule 99 of the CDD Rules issued by FIU, “beneficial owner” of the legal person or legal arrangement is a natural person who ultimately owns or controls a customer or the person on whose behalf a transaction is being conducted including the person who exercises ultimate effective control over a person or a legal arrangement. According to Rule 49, controlling ownership interest means an interest acquired by providing more than ten percent (10%) of the capital of a legal person.
2. “Beneficiary” means the person to whom or for whose benefit the funds are sent or deposited in bank;
3. “Beneficiary institution” means the financial institution that receives the funds on behalf of the wire transfer or fund transfer beneficiary;
4. “Control” in relation to a legal person, means the power to exercise a controlling influence over the management or the policies of the undertaking, and, in relation to shares, means the power to exercise a controlling influence over the voting power attached to such shares;
5. “Correspondent bank” means the bank in Sri Lanka which provides correspondent banking services to bank or financial institution situated abroad and vice versa;
6. “Correspondent banking” means provision of banking services by one bank (correspondent) to another bank (respondent) including but not limited to opening and maintaining accounts in different currencies, fund transfers, cheque clearing, payable through accounts, foreign exchanges services or similar other banking services;
7. “Cross-border wire transfer” means a wire transfer where the ordering institution and the beneficiary institution are located in different countries or jurisdictions;
8. “Cash Transaction Report or CTR” means a report under section 6 of the Financial Transactions Reporting Act, No. 6 of 2006.;
9. “Customer” means a person having relationship with the bank which includes but not limited to holding of deposit / or any instrument representing deposit/placing of money with a bank, availing other financial services, locker facility, safe deposit facility, or custodial services from the bank;
10. “Customer due diligence or CDD” in broader terms includes;
  - a) identifying the customer and verifying the customer’s identity on the basis of documents, data or information obtained from customer and/or from reliable and independent sources;
  - b) identifying, where there is a beneficial owner who is not the customer, the beneficial owner and taking adequate measures, to verify his identity so that the bank is satisfied that it knows who the beneficial owner is, including, in the case of a legal person, trust or similar legal arrangement, measures to understand the ownership and control structure of the person, trust or arrangement;
  - c) understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship; and
  - d) monitoring of accounts/transactions on ongoing basis to ensure that the transactions being conducted are consistent with the banks knowledge of the customer, their business and risk profile, including, where necessary, the source of funds and, updating records and data/information to take prompt action when there is material departure from usual and expected activity through regular matching with information already available with bank.

11. “Domestic wire transfer” means any wire transfer where the originator and beneficiary institutions are located in Sri Lanka regardless the system used to affect such wire transfer is located in another jurisdiction;
12. “FATF Recommendations” means the Recommendations of Financial Action Task Force as amended from time to time
13. “FIU” means financial Intelligence unit established under the Financial Transaction Reporting Act (FTRA);
14. “Fund transfer/wire transfer” means any transaction carried out by financial institution on behalf of originator person by way of electronic means or otherwise to make an amount of money available to beneficiary person at another beneficiary institution, irrespective of whether the originator and the beneficiary are the same person;
15. “Intermediary institution” is an intermediary in the wire transfer payment chain; that receives and transmits a wire transfer on behalf of the ordering institution and the beneficiary institution, or another intermediary institution;
16. “Online transaction” means deposit or withdrawal of cash using different branches of a bank through electronic means;
17. “Ordering institution” means the financial institution that initiates a wire transfer on the instructions of the wire transfer originator in transferring the funds;
18. “Originator” means the person who allows or places the order to initiate a fund transfer/wire transfer or an online transaction;
19. . “Payable-through account” means an account maintained at the correspondent bank by the respondent bank which is accessible directly by a third party to effect transactions on its own (respondent bank’s) behalf;
20. “Politically exposed persons or PEPs” are individuals who are entrusted with prominent public functions either domestically or by a foreign country, or in an international organization, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations/departments/autonomous bodies. This does not intend to cover middle ranking or more junior individuals in the foregoing categories;
21. For the purposes of the PEP definition, “international organizations” are organizations established by formal political agreements between its member countries, where such agreement has the status of an international treaty, and the organization is recognized in the law of the member countries. The examples of international organizations provided by FATF include:
  - a) the United Nations and its affiliates such as the International Maritime Organization;
  - b) regional international organizations;
  - c) international military organizations such as the North Atlantic Treaty Organization;
  - d) economic organizations such as the World Trade Organization, International Monetary Fund, World Bank, Asian Development Bank, etc.
22. “Respondent bank” means the bank or financial institution outside Sri Lanka to whom correspondent banking services in Sri Lanka are provided and vice versa;
23. “Shell bank means a bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial group that is subject to effective overall supervision. The physical presence constitutes being located within a country performing a management function with meaningful mind and the mere existence of a local agent or non-managerial staff does not constitute a physical presence;
24. “Suspicious transaction report or STR” means a report of a suspicious transaction or attempted transaction as per section 7 of the FTRA.

25. "Senior management" means the Head of Business, Head of Operations, Head of Compliance and Regional General Manager.
26. "Occasional transactions" means any transaction, in relation to cash and electronic fund transfer, that is conducted by any person other than through an account in respect of which the person is the customer.
27. "Money laundering" means the offence of money laundering in terms of section 3 of the Prevention of Money Laundering Act, No 5 of 2006;
28. "Terrorist financing" means an act constituting an offence connected with the financing of terrorism under the Convention on the Suppression of Terrorist Financing Act, No. 25 of 2005
29. "Source of wealth" refers to the origin of the customer's entire body of wealth (i.e., total assets).
30. "Source of funds" refers to the origin of the particular bank.
31. "Numbered accounts" refer to accounts that the ownership is transferrable without knowledge of the Financial Institution and accounts that are operated and maintained with the account holder's name omitted.
32. Other terms used in the procedures that are not defined here, shall have the same meaning as ascribed to them in AML/CFT laws, other relevant laws, rules, regulations or international standards prescribed by the relevant global bodies e.g., Basel Core Principles, FATF Recommendations/ Guidelines etc.
33. Specialized Enhanced Due Diligence (SEDD) for Ultra High Net Worth individuals is required as per Head Office Internal Circular No. A/INST/2025/02 dated January 29, 2025.
34. Ultra-High-Net-Worth Individuals (UHNWI) are defined as those individuals that hold any kind of depository relationship in local or FCY currency more than the aggregate balance of USD 750K.

Note: Any other definition not provided above conveys the same meaning as per AML / CFT/ CPF Regulations by FIU, Wolfsberg & FATF.

# **1. INTRODUCTION**

## **1.1 Objective**

The objective of Anti-Money Laundering (AML) / Combating Financing of Terrorism (CFT) & Sanctions Procedures is to ensure that the products and services of Habib Bank Limited - Sri Lanka (also referred as Bank in this document) are not channelized or used to facilitate or assist financial crime and that management and its staff are aware of their obligations and the need for vigilance to combat Money Laundering (ML) and Terrorist Financing (TF) and the financing of proliferation of weapons of mass destruction. This procedure is stemming from the Global AML-CFT, CPF & KYC Policy and Sanctions Compliance policy of the bank and any amendment in the document will be raised in line with instructions provided in AFPAD.

## **1.2 Scope**

These procedures are developed to meet the requirements and processes applicable to all HBL Sri Lanka branches and departments and sets out appropriate procedural details for complying with the regulatory requirements in day-to-day business activities. Where the regulatory requirements in Sri Lanka are different from those mentioned in the Group procedure, more stringent of the two standards to be followed by HBL SL.

Note: All departments and functions of HBL SL will be required to prepare their SLAs or any relevant procedure considering HBL Global Anti-Money Laundering, Combating Financing of Terrorism, Countering Proliferation Financing & Know Your Customer (KYC) Policy, Sanctions Compliance Policy and Trade Based Money Laundering (TBML) Procedure and the same must be approved from all stakeholders.

AML/CFT/CPF and sanction related circulars and guidelines issued by Financial Intelligence Unit of Sri Lanka (FIU) are incorporated in this procedure. Further, as per the Compliance program of HBL SL, any new directions guidelines/ Circulars issued by regulator (Including AML/CFT & sanction related directions) will be sent to the concerned functional heads immediately.

In the event if there are any significant regulatory changes related to AML/CFT & Sanctions, this procedure document will be revised and approved in line with the "latest Approval Framework for Policy and Associated Documents (AFPAD).

In addition to guidelines issued by FIU and Central Bank of Sri Lanka (CBSL), HBL Sri Lanka Anti-Money Laundering (AML) / Combating Financing of Terrorism (CFT)/ Combating Proliferation Financing (CPF) & Sanctions Procedures are aligned with SBP AML CFT CPF Guidelines, Bank's Global AML/CFT/CPF/KYC Policy, Sanctions Compliance Policy and international standards including Financial Action Task Force (FATF), Wolfsberg Guidelines.

# **2. SANCTION SCREENING**

HBL SL Compliance team (With the assistance of FCC at HBL - Pakistan) provides sanctions and screening related guidance, advisory & services to the first line including business units and other

functions related to the aspects such as, majorly relating to customers onboarding screening, bank's periodic portfolio screening, payments screening, sanctions advisory etc.

Previously, the safe watch screening was limited to payment screening in HBL Sri Lanka. However, with the Business transformation implementation in year 2020, SafeWatch payment screening was implemented in HBL Sri Lanka, along with the addition of Real-time Customers On-boarding Sanction Screening. Further in the 2022 SafeWatch delta screening was implemented in HBL Sri Lanka. Wherein delta screening was noted as the existing customers being screened daily against the updated sanction list (it includes but not limited to amended UNSCR lists and local lists).

## **2.1 Who is subject to Sanctions?**

Entities, individuals or countries generally become vulnerable to UN sanctions inter-alia to OFAC / EU etc. or country specific sanctions lists due to their involvement in activities the government deems in violation of UN resolution. Examples of such activities may include, but are not limited to, the development and trade of weapons of mass destruction, political and military regimes acting against the norms of human rights, terrorist activities, either indulging in practices involving Money Laundering (ML) and/ or having tax laws to control ML and Terrorist Financing Activities, Human trafficking and Narcotics trafficking. Sanctions are normally imposed against persons who are known or suspected to be proscribed individual and entities. In Sri Lankan context, Special Designated Nationals and entities list published by FIU of Sri Lanka act as the domestic sanction list.

## **2.2 HBL SL approach towards Sanctions**

The Bank currently does not permit, having an account relationship nor processing any transaction with countries that are under Sanctions in line with Sanctions Compliance Policy and Financial Crime Country Risk Guidelines. Sanctions is an evolving issue where frequent changes are taking place; hence these guidelines may be revised by the Bank as and when required and the same will be circulated to all stakeholders.

## **2.3 Detection Review Process**

- A hit/alert will be considered as False Positive, if there is Full/complete name differs / Partial name match with violation.
- A hit/alert will be considered as False Positive, if there is Jurisdiction / Location differs with violation.
- A hit/alert will be considered as False Positive, if there is invalid hit/alert i.e. Individual vs entity, individual vs vessel, address field vs entity, match on father name only etc.
- A hit/alert will be considered eligible for further investigation as True match, if hit/alert details match with complete name and jurisdiction/Location available in the message/ transaction. In this scenario further investigation w.r.t Date of Birth, Father name, NIC, Passport, Nationality, Place of Birth, Profile of customer etc. will be carried out in order to determine, whether the hit/ alert is a True Match or not. If a True Match is confirmed, then the payment will be rejected/ blocked, and action will be taken as per available AML/CFT/CPF guidelines / AML law.
- In cases of Non-Resident customer, copy of the Passport with valid visa is obtained.
- Currently four eye principle is observed for live Swift transactions where the detections are reviewed by the level 1. Level 1 will input its comments and release the transaction to Level 2 queue. Level 2 will review the comments provided by level 1 and if details do not match will release the detection

as false positive, and if they match will block the detection as an exact match. If Level 2 requires further information, it will be sent back to Level1 with the comment for further actions to be taken. In order to determine a hit / alert as “True /Exact” match the following parameters should be assessed with the alerted names. System may generate multiple Alerts on Single detection.

- A percentage of accuracy 88% is considered for screening which is set by HBL-Pakistan.
- Customer’s further information will be scrutinized through the database / profile maintained in Misys or in case of further RFI, inquiry will be sent to the relevant Branch.

Matching full name with the customer and the search result- The hit should be considered as valid and true when the first and last name or on entirety the name has visible and viable matching along with a secondary unique matching (e.g., DOB, Nationality etc.).

Matching of Government issued ID number - When there is a similarity in NIC/Passport Number/ Driving License Number / National Tax Number/ Company Registration Number or IMO number in reference to vessels, the entity is considered as a true/ exact match.

Matching of Father’s Name - When the father’s name of the customer and the hit result matches in full the same is considered as a true/ exact match.

Matching of Nationality - If the nationality of the customer matches with the search results, the same can be determined as a true/ exact match. This is also very effective when assessing the proscribed Vessels where the change of flag with the vessels name may subject to change, but the IMO and country of sanctions remain the same with no alteration.

Matching of Date of Birth - One of the key factors in determination of match is the similarity of Date of Birth. If the same matches with the customer and the search result, it can be considered as a true/ exact match.

Note: During the assessment, it should be noted and considered that the matching of details may vary from case to case.

## **2.4 Details of Sanctions Screening Filter - SafeWatch:**

To ensure that HBL Sri Lanka channel is not being used by blacklisted individuals /entities for ML/TF/PF activities, HBL Sri Lanka has taken support of technology and has implemented SafeWatch filter 4.0 for screening customer’s names against Sanction lists and other watch lists. Details of sanctions/watch lists which are embedded in SafeWatch filter is given in the next Section.

## **2.5 Sanctions Lists as per HBL Global Sanctions Policy**

Sanctions team based at the HBL Head Office, Karachi, Pakistan shall carry out thorough review of the Global Sanctions regimes on annual basis and identify the sanctions lists which are required to be maintained and updated in the bank systems for screening purpose. Examples of mandatory Sanctions lists are:

- a) The United Nations (UN) Security Council consolidated sanctions list.
- b) The UK HM Treasury (HMT), Office of Financial Sanctions Implementation (OFSI), “consolidated list of targets”.

- c) The EU's consolidated list of persons, groups and entities.
- d) The US Department of the Treasury, Office of Foreign Assets Control (OFAC) sanctions lists.
- e) The US Department of the Treasury, Financial Crimes Enforcement Network (FinCEN) list.
- f) National Counter Terrorism Authority, (NACTA)
- g) And other related sanctions list.
- h) Other measures as issued by FIU of Sri Lanka - United Nations Security Council Resolution (UNSCR) 1373

## 2.6 Private list management and name addition process:

HBL Sri Lanka locally maintains "SLK Blacklist" in Safewatch. Compliance Staff will add /upload names in the SLK Blacklist through List Explorer Option in List Management module. There may be multiple sources of names. For example, STRs/SARs/Bank's internal escalation/ Head Office/ Media/FIU of Sri Lanka etc. Once name(s) are added/uploaded by the Supervisor (Level 2 user) the same will be validated by another Level 2 user or Level 1 user in Compliance department to adhere 4 eye principle and ensure that names are updated accordingly. Safewatch system audit trail of the validation performed by the level 2 user/level 1 user to be retained for Audit/future reference. Further an annual review would be performed on the list by a User in Compliance Department.

## 2.7 Selection of Lists for Payment Screening and Onboarding

To ensure that the selection of list set is appropriately selected on Safewatch for the source systems i.e. for transaction screening of SWIFT and Name Checker, below lists will be selected. For Customer's onboarding, following list set will be used.

S. No.	Source Systems	Lists Used for On-Boarding
1	MQ Connector	i. World-Check Sanctions List ii. Sri Lanka Blacklist/ Private list

For Transaction Screening of SWIFT, following list set will be used.

S. No.	Source Systems	Lists Used for On-Boarding
1	SWIFT	i. World-Check Sanctions List ii. Sri Lanka Blacklist/ Private list

## 2.8 List uploading in SW 4.0:

In SSW 4.0, the Sanctions list for each of the source systems will automatically be updated from the vendor's (World Check-Thomson Reuters) source system. HBL Sri Lanka blacklist is updated manually by HBL Sri Lanka Compliance promptly on receipt of new information by compliance officer.

## **2.9 Four Eye Principle:**

To ensure 4 eye principles two staff should review all searches for which audit trail is available.

**Maker:**

Whenever any notification or communication is received for addition/change or amendment from the FIU of Sri Lanka the same will be search in Customers database by the HBL Sri Lanka Compliance team.

Maker/ Compliance Assistant Manager will search name(s) in Safewatch database to make sure it is added in the Safewatch (World-Check sanctions list).

Up on completion of the search exercise Maker will send confirmation email to checker with the results of the SafeWatch name searches i.e if already updated/ available in SafeWatch Sri Lanka private list or what information needs to be added Additionally if any comparison made between the new list against the previous list shall also be provided to checker for list updating purposes.

Further in the email the maker should provide details such as the time period within which the searches were performed Audit trail obtained from the SafeWatch of the searches performed by the Maker to be shared with the checker/saved in the relevant folder.

**Checker:**

Checker/ Compliance Manager or Country Head of Compliance will review the results to ensure that all names are properly searched and concluded. Based on the information provided in the email by the Maker, the Checker will amend/do nothing to the private list. Further a random check to be performed on name searches where no change/amendment is required. Audit trail obtained from the SafeWatch of the amendments and searches performed by the Checker to be saved in the relevant folder to confirm the completion of the exercise. An email communication to be shared among the Compliance team once this exercise is completed.

Maker- Once the Checker performs the additions/deletions to the Private list, Maker shall verify the validity of the additions/deletions performed in the system by the check. The Maker shall search for the information/data modifications done by the Check. Once this exercise is performed by the Maker, an audit trail should be taken from the system and saved for evidence. Further email confirmation should be shared with the Compliance team to confirm the completion of the exercise.

**True positive**

If any match is found as true positive from HBL Sri Lanka database for the existing customer, immediate action(s) must be taken as per Bank's policy and Local Law which may include Freezing of the relationship and reporting of STR to FIU.

## **2.10 Payment Screening**

### **2.10.1 Swift Payments**

As a pro-active approach SWIFT transaction where there is a potential match on remitter and beneficiary of funds, country, vessel, financial institutions on any other party related to the transaction are routed to Compliance team via safe watch applications for clearance from sanctions



perspective. To maintain uniformity a percentage of accuracy 88% and above is considered for assessment and as potential. The said screening is conducted for both HBL customer and for the beneficiaries who do not have accounts in HBL conducting transaction using the bank as a “correspondent bank”. However, SWIFT messages on behalf of third-party Banks should not be entertained as instructed in the internal circular A/INST/2019/20 dated 22.08.2019. The steps for SWIFT transaction screening are as mentioned below.

- All SWIFT transactions incoming/outgoing & across/outside HBL network are routed through Safe Watch (SW) 4.0 filter where transactions are automatically screened.
- If there is a potential name match on remitter & beneficiary including location/jurisdiction, vessel names or any other parties relevant to the message, alert will be generated and raised to Compliance Team and transaction will be held until the alert is cleared.
- If the matches are determined as a false hit, Compliance Analyst has to release the alert after incorporating his comments & Compliance reviewer has to verify Analyst comments and release the Alert.
- In case of a partial match and Non-HBL Remitter or beneficiary, Compliance Analyst sends the RFI (request for information) to respective business unit to arrange details like: Full Name, Date of Birth, Place of Birth, Nationality, NIC, Passport, Profession & Address.
- If there is any exact match on Remitter, Beneficiary, Country, Jurisdiction & Correspondent Bank, the same is investigated by Compliance Analyst and reviewed by Compliance Reviewer through scrutinizing the core banking system i.e. Mysis. Based on the review, Compliance Reviewer blocks or releases the transaction. On need basis sanction related hits on correspondent Bank, Vessels, countries etc. will be referred to Compliance Sanction Advisory Team in HBL Pakistan for obtaining sanction clearance.
- The same is communicated to relevant stakeholders about the blocked payment.
- Once a payment message is blocked due to exact violation, STR will be filed in line with AML, CFT, CPF and sanctions regulations of SL.
- There can be multiple alerts against one detection.

### **2.10.2 Domestic Wire Transfers**

Incoming & outgoing local wire transfers including Sri Lanka Inter Bank Payments System (SLIPS) and Real Time Gross Settlements (RTGS) transactions are screened as mentioned below.

- Beneficiaries, ordering customers for Outgoing and incoming Local wire transfers are screened as per below,

#### **RTGS**

As RTGS is linked to SWIFT alliance it goes through the Safewatch filter system hence the screening is performed through the Safewatch filter system.

#### **SLIPS**

##### **Inward SLIPS**

Our customer is screened through the delta screening which is done on a daily basis. However, our counterparty cannot be screened due to the inadequate information of the counterparty.

##### **Outward SLIPS**

Our customer is screened through the delta screening which is done on a periodic manner. World check screening is conducted on the counterparty.

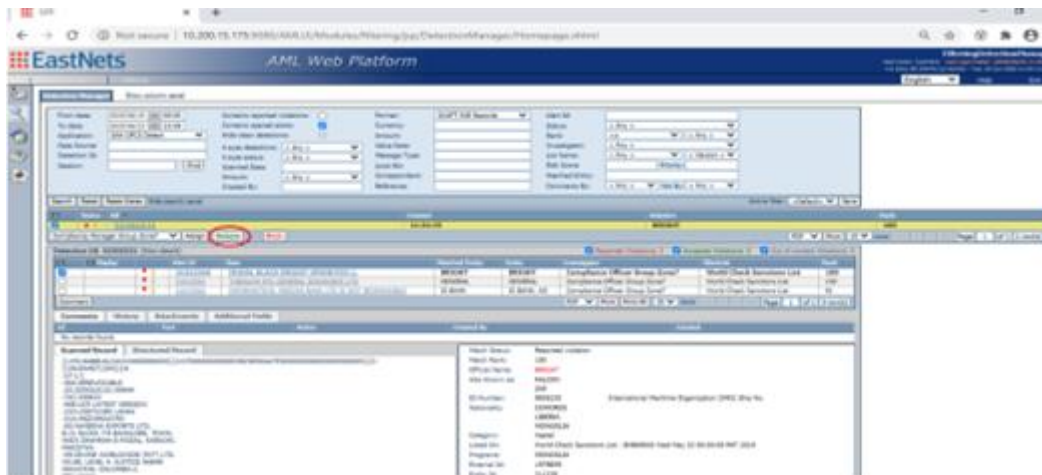
- If there is a match against the remitter/beneficiary and where the Branch is unable to discount the hit the Branch must obtain Compliance clearance in order to process the transaction.
- If the match is determined as false positive, Compliance will clear the transaction, and Branch can go ahead with the transaction.
- In case of a partial match the Compliance team will request for further information from respective business unit to arrange details like: Full Name, Date of Birth, Place of Birth, Nationality, NIC, Passport, Profession & Address.
- If there is any exact match on Remitter, Beneficiary the Compliance team will instruct the respective business unit to block the transaction.
- If the transaction is blocked due to exact match related to sanctions, STR will be filled to FIU of CBSL in line with AML, CFT, CPF and sanctions regulations of SL.

### 2.10.3 Guidance on Payments Sanctions Screening through SSW

Payments Sanction Screening will be performed on all swift transactions on a real time basis through SafeWatch Server 175 (Incoming and Outgoing). Screening of Payments is performed Automatically through SafeWatch.

#### 2.10.3.1 Sanctions Screening Performed by Compliance team on SWIFT

a) Level-1 Compliance Assistant Manager will review the matched results in the SafeWatch Payments screening filter and provide appropriate comments / remarks [Refer to General Guideline 7 (ii) below].



b) In case of False positive/ Invalid match, Level-1 Compliance Assistant Manager will release the alert along with the necessary comments. Through an RFI, Compliance needs to obtain relevant supporting documents/clarifications (e.g: Full Name, Father Name, Identity No., Address, Place etc.) from Business if required and the same will be attached in the Alert being reviewed.

The screenshot shows the 'Detection Manager' interface in the EastNets AML Web Platform. The top navigation bar includes the EastNets logo and 'AML Web Platform'. The main area is titled 'Detection Manager' and shows a list of detections. A red box highlights the 'Compliance Manager Group Zone?' dropdown menu, which is currently set to '< None >'. Below the dropdown, there are buttons for 'Confirm Release', 'Cancel', and a note '(\*) mandatory field'. The table below shows details for a specific detection, including 'Alert ID', 'Data', 'Matched Entry', 'Entry', 'Investigator', 'Checklist', and 'Rank'.

Alert ID	Data	Matched Entry	Entry	Investigator	Checklist	Rank
51112569	INDIAN BLACK BRIGHT SPURVED L	BRIGHT	BRIGHT	Compliance Officer Group Zone?	World Check Sanctions List	100
51112569	INDIAN BLACK BRIGHT SPURVED L	BRIGHT	BRIGHT	Compliance Officer Group Zone?	World Check Sanctions List	100
51112569	INDIAN BLACK BRIGHT SPURVED L	BRIGHT	BRIGHT	Compliance Officer Group Zone?	World Check Sanctions List	91

C) If a sanction hit/element is found on an alert, the same should be referred to Compliance sanctions Advisory team in HBL-Pakistan for obtaining clearance by the level -1 user.

d) Level-2 Supervisor – Compliance Manager or Head of Compliance verify the supporting details / provided comments by Level-1 Compliance Assistant Manager, insert the comments and release the alert

The screenshot shows the 'Detection Manager' interface in the EastNets AML Web Platform. The top navigation bar includes the EastNets logo and 'AML Web Platform'. The main area is titled 'Detection Manager' and shows a list of detections. A red box highlights the 'Template' dropdown menu, which is currently set to '< None >'. Below the dropdown, there are buttons for 'Confirm Release', 'Cancel', and a note '(\*) mandatory field'. The table below shows details for a specific detection, including 'Alert ID', 'Data', 'Matched Entry', 'Entry', 'Investigator', 'Checklist', and 'Rank'.

Alert ID	Data	Matched Entry	Entry	Investigator	Checklist	Rank
51112569	INDIAN BLACK BRIGHT SPURVED L	BRIGHT	BRIGHT	Compliance Manager Group Zone?	World Check Sanctions List	100
51112569	INDIAN BLACK BRIGHT SPURVED L	BRIGHT	BRIGHT	Compliance Manager Group Zone?	World Check Sanctions List	100
51112569	INDIAN BLACK BRIGHT SPURVED L	BRIGHT	BRIGHT	Compliance Manager Group Zone?	World Check Sanctions List	91

In case of RFI, Level-1 Compliance Assistant Manager or Level-2 Supervisor /Compliance Manager or Head of Compliance will seek additional information (E.g.: Full Name, Father Name, Identity No., Address, Place etc) from the related Business unit.

e) All the rejected / real violations will be communicated by the Compliance to the respective Business and Operations team with copy a through an email to relevant unit, Regional General Manager for their information and reviewing the relationship with HBL Sri Lanka. Respective Business and Operations teams will communicate their findings on clients' relationship with HBL Sri Lanka to the Compliance team within 3 working days.

f) If any match is found as true positive from HBL Sri Lanka database for the existing customer, immediate action(s) must be taken as per Bank's policy and Local Law which may include Freezing of the relationship and reporting of STR to FIU.

#### **2.10.3.2 Reporting / MISs**

Safe-Watch Level-1 Compliance Assistant Manager will submit a monthly MIS of Total cases screened/positive matches and false positives to the international Compliance for review via Monthly Country Compliance Management Information (CCMI- Formerly known as Compliance Performance report)

Moreover, if there are True matches found following steps will be ensured.

- Compliance team will consider filing of STR of positive/ real violations to FIU of Sri Lanka.
- Compliance will also communicate to the business the concerns on the real/ positive violation and to reassess the risk of the customer for continuing the relationship with HBL Sri Lanka.

#### **2.10.3.3 Procedure for SWIFT Payment Sanctions Screening/ Onboarding**

The procedure for SWIFT Payment / onboarding Sanctions Screening, in order not to leave any unattended alerts as the BOD/EOD Process are as follows:

- The date range should be selected from the 1<sup>st</sup> of the month to the current date so that no alerts are left unattended both by Analyst/ Compliance Manager. At least a two preceding weeks date may be selected at the beginning of each day.
- No "Assign" will be used, all alerts must be "Release" by Analyst/ Compliance Manager.
- Level 2 Manager user will confirm from the detection manager and Alert List report at the EOD that no Alert has been left unattended in new state and generate a Nil status email date range can be as mentioned in preceding point 2.
- A pending/ under investigation/ RFI with aging MIS or email also needs to be circulated at the EOD along with the proper reason of pending.
- Level 2 Manager will further verify the genuineness of the pending/ under investigation/ RFI of the Alert that the initiated inquiry was valid alert inquiry.

### **2.11 Customer Onboarding**

As a proactive approach all branch banking accounts that are opened on a daily basis are screened through World check for Possible PEP and any adverse media news to maintain uniformity. This will be conducted in addition to the Real time sanctions screening conducted through Safe watch which was implemented with the Business Transformation exercise. The said screening is conducted for HBL Accountholders, and all individuals/ entities linked to such accountholder including but not limited to Joint account holders, financial supporter, Mandate holder, Directors, Partners, Proprietor, Authorized signatory, Ultimate Beneficial owners etc. (fuzzy logic – 88%)

- Prior to onboarding customers, Branches should send the duly filled WC format (annex I) to World Check users in first line through email in order to screen the customer.
- Additionally, for Customers rated as High Risk, Branch should do a public search as instructed in the attached format (Annex I).
- World Check user will manually screen the customer based on the information provided by the branch and screening results are provided to the respective branch.
- If the screening results shows a positive match, further investigations are conducted in case of potential matches by the respective branch and referred to SL Compliance. Based on the findings SL Compliance team will instruct the branch either to establish the relationship or not to proceed with onboarding.
- For all positive results which match the sanctions list of proscribed individual / entity, STR is filed to FIU by SL Compliance team. Branches will be advised with the appropriate actions to be taken case by case basis as such cases to be handled in accordance with the SL legal framework. Provisions are only given in UNSCR regulations to freeze accounts.
- If the customer available data is inadequate to take decision on the violation, same is further referred to branch for the required clarity and further due diligence.
- If the true matches are found on PEPs or High-risk categories, branch will be instructed to conduct a PEP risk assessment/ High Risk profile assessment prior onboarding.
- World Check (WC) application automatically identifies false positive and ignore the hits. Further if unresolved hits are identified as false positive and comments shall be placed by the analyst.
- Customers On-boarding Sanction Screening will be performed on real-time basis through SafeWatch Server 171 on customers for example, account holders/ joint account holder(s), ultimate beneficial owner, partners, directors, authorized signatories, power of attorney holder and shareholders, all other type of customer.

Following Screening steps shall be performed at the time of customer on boarding using SSW:

- Accounts opened on daily basis will automatically be screened on Real time basis through Safewatch 4.0.
- Safewatch will perform automated screening and generated detections on potential matches.
- Branch User (Account opening officer -Maker) will create CIF and Branch Supervisor (Branch Manager / Branch Operations Manager)- Checker will authorize the same, post review of details.
- Details of CIFs will be screened for Sanction hits through Side Safe watch at branch level by Account opening officer.
- Branch users (Maker and supervisor) will be notified via Pop up in Mysis that Sanction Screening is in progress, CIFs where no match found in Safewatch will be treated as STP (straight through process) and Branch user will be notified automatically on the Misys screen appears as "Pass". Branch users will proceed for Account opening as per HBL Sri Lanka process. In case of any match /alert then same will be parked in Compliance queue for sanction screening (release or block).
- A percentage of accuracy 88% is considered for screening which is set by HBL - PAKISTAN.

### **2.11.1 Compliance Role and responsibilities**

Application "MQ Connector" must be selected by Safewatch Users.

Level 1- Analyst / Compliance Assistant Manager

- Level-1 Compliance Assistant Manager (Maker) will review the matched results and provide appropriate comments / remarks with regards to the Hit. Maker will release the hit/ alert post comments to Level-2 Supervisor – Compliance Manager or Head of Compliance, if found alert as false match.
- RFI will be sent to Business/Related HBL Sri Lanka Staff by Level 1 for further information if required such as Date of birth, Location, father's name, place of birth etc. to discount the Hit/alert. (Turnaround time is: 1 Day)
- Level-1 Analyst (Maker) will block Alert with necessary comments, if found alert with exact match and True Positive post review of Hit details.

#### Level-2 Supervisor – Compliance Manager or Head of Compliance

- Level-2 Supervisor (Checker) will release the Hit/alert after reviewing the comments of Level 1 Analyst if Hit / alert qualifies as "False positive."
- If Level-2 Supervisor (Checker) is not satisfied with the provided comments / explanation given by Level-1 Analyst, the Level-2 Supervisor will assign back the Hit/ alert to Level -1 for further clarity or to obtain necessary information.
- Level-2 Supervisor (Checker) cannot release the blocked alert. Blocked alert must be assigned to Level -1 Analyst (maker) for further review (if required).

#### Note:

If there are True matches found following steps will be ensured.

- All Real violations will be communicated to the Business with Copy to Business Head and Regional General Manager for their information and reviewing the relationship with HBL Sri Lanka. Respective business team will share their findings with Compliance on connected / related accounts relationships with HBL Sri Lanka within 3 business days or the case will be escalated to Business Head.
- Compliance team will consider filing of STR of positive/ real violations to FIU of Sri Lanka. Compliance team will also file STR for the positive / real violations if identified at branch level and escalated through Internal STR to Compliance team.
- Compliance will also communicate to the business the concerns on the real/ positive violation and to reassess the risk of the customer for continuing the relationship with the HBL Sri Lanka.
- All overdue alerts to be reported to Head IC HBL - PAKISTAN through monthly CCMI.

#### **2.11.1.1 Compliance Role and responsibilities - Vendor screening and screening of third-party employees outsourced from Vendors**

1. Vendor Screening involves Screening of the Vendors and their Directors/Shareholders/UBOs when Outsourcing activities by the Bank to such Vendors.

1.1 If a Vendor agrees to open an account/onboard at the time of entering/ subsequent to establishing outsourcing relationship with HBL Sri Lanka, usual process of onboarding a customer to be followed on the Vendor. Ongoing/delta screening of the vendors and their Directors/ Shareholders/ UBOs will be performed through Safewatch 171 screening platform.

1.2. If a vendor decides not to open an account with HBL Sri Lanka but to proceed only with outsourcing arrangement, GAD is required to communicate through an email the vendor details

(vendor name, directors, UBOs and shareholders) to Compliance department SL to process screening through SSW. Outcomes/results of the screening performed should be communicated to GAD through an email within an agreed TAT. Further, the Compliance department will perform fortnightly screening of vendors and their Directors, UBOs and shareholders based on the information provided by GAD department until an automated process is in place.

2. Screening of third-party employees hired from Vendors under Outsourcing arrangements.

2.1 If third-party employees from vendors are being used under outsourcing arrangements, the Bank should request such vendors to onboard (open accounts for) their employees with the Bank on need basis. If the Vendors and their third-party employees agree to Onboard, sanction screening would be automated as in the case of a customer at the time of onboarding and on an ongoing basis.

2.2 If third-party employees do not opt to open accounts with the Bank, Manual screening process to be followed by GAD and Compliance. GAD should inform the Compliance department through an email the details of the third-party employees who need to be screened in SSW. Accordingly, Compliance department will screen the provided details and respond the results of the screening to GAD through an email within a pre-agreed TAT. Further GAD is required to communicate through an email the details of the third-party employees to Compliance department to process ongoing screening through SSW. Compliance department will perform fortnightly screening of the third-party employees based on the information provided by GAD department until an automated process is in place.

### **2.11.2 United Nations Security Council Resolutions relating to The Prevention and Suppression of Terrorism and Terrorist Financing**

Refer to circular no. 02/14 - Financial Intelligence unit, Central Bank of Sri Lanka, following guidelines were issued for the measures related to Terrorist Financing.

Sri Lanka is required to implement targeted financial sanctions prescribed in the Gazette Notification No. 1758/19 to comply with the United Nations Security Council Resolution (UNSCR) 1373 (2001) and its subsequent resolutions which require countries to freeze funds, financial assets or economic resources of designated individuals and entities, and to ensure that no such funds, financial assets or economic resources are made available to or for the benefit of such designated persons or entities or their beneficiaries. Accordingly, every Licensed Bank/Licensed Finance Company is obliged to have measures in place to immediately freeze funds, financial assets or economic resources of such designated persons and entities who have been initially listed in the Extraordinary Gazette Notification No. 1854/41 and may be amended by any future Gazette notifications by the Competent Authority.

The list of designated individuals and entities (referred to as List in section 4(2) of the said Regulation) has been published in Extraordinary Gazette Notification No. 1854/41 dated 21 March 2014. The Licensed Banks shall maintain a database of names and particulars of individuals/entities in the List to ensure efficient detection of suspected financing of terrorism.

As and when amendments to the List are published in gazette by the Competent Authority, the FIU will notify all compliance officers of Licensed Banks/Licensed Finance Companies via E-mails.

Licensed Banks shall update the database of designated individuals/entities which is maintained by them on receipt of the notifications from the FIU.

Licensed Banks shall ensure that the name(s) of the prospective customers do(es) not appear in the List before entering into any new business relationships. Further, Banks shall scan all existing business relationships to ensure that no business relationship is held by or linked to any of the entities or individuals included in the List.

In case, the match of any of the customers with the particulars of designated individuals/entities, the Licensed Banks shall prevent designated persons from conducting any transactions and freeze all funds, other financial assets and economic resources without delay.

Licensed Banks shall bring the provisions of the United Nations Regulation No 1 of 2012 to the notice of the staff concerned and ensure strict compliance. The Compliance Officers are responsible for the establishment and maintenance of written internal procedures and systems to implement UNSCR 1373 (2001) and all current and future subsequent resolutions to UNSCR 1373

### **2.11.3. United Nations Security Council Resolutions relating to the prevention of Proliferation Financing (PF)**

There are no specific set of rules/regulations issued by CBSL/local regulator on PF. However, HBL SL, being a part of a global bank, is required to adhere to global standards. Accordingly, United Nations Security Council Resolutions (UNSCR) 1540 and 1718 and the FATF recommendations are the key regulations governing Proliferation Financing.

Proliferation Financing as defined by the FATF involves providing funds or financial services to support the development, acquisition or use of weapons of mass destruction (WMD) and their means of delivery. This includes activities related to nuclear, chemical or biological weapons as well as related technologies and dual use goods. UNSCR 1540 requires all States to refrain from providing any form of support to non-State actors that attempt to develop, acquire, manufacture, possess, transport, transfer or use nuclear, chemical or biological weapons and their means of delivery. UNSCR 1718 imposes a series of economic and commercial sanctions on the Democratic People's Republic of Korea (the DPRK, or North Korea) in the aftermath of DPRK's claimed nuclear test

There are key FATF recommendations and immediate outcomes governing PF. Recommendation 1 requires assessing & applying a risk based approach to PF. Recommendation 2 requires National cooperation & coordination, Recommendation 7 requires implementation of TFS related PF (this includes freeze without delay the funds or other assets of, and to ensure that no funds and other assets are made available directly or indirectly to or for the benefit of any person or entity designated by the UNSC) and Recommendation 15 requires deals with regulating new technologies (Virtual assets and VASPs)



## **2.12 Sanctions & Screening Advisory**

### **2.12.1 Sanctions Countries**

As per the Global AML, CFT, CPF & KYC Policy and Sanctions Compliance Policy of the Bank, Trade/Branches/all operational units are mandated to obtain prior SL compliance clearance for any transactions related to sanctioned countries. If deemed not applicable as per the bank's policy, then Compliance team will communicate via e-mail to the concern business unit not recommending for further processing. If deemed applicable for processing, then concurrence is accorded on e-mail for processing.

Business/Trade/ all operational units' remittance transactions related to sanctioned countries are referred to SL Compliance team for concurrence before execution if there are any clarifications required on the particular sanctioned country.

### **2.12.2 Trade department**

Local Trade department act as an additional layer of control to screen all inbound / outbound foreign currency payments. They perform screening of payments through World-check to mitigate sanctions risk for all outbound foreign currency remittance transactions.

- The trade department is the first line of defense to perform sanctions screening.
- During screening, once they find any exact match/match related to prohibited country, they refer to Compliance team for concurrence via e-mail.
- SL Compliance team will review the referred match for any possible Sanctions as well as applicability as per Bank's policy. If any further information/confirmation is required to assess the match, a Request for Information (RFI) is sent to Trade to obtain such information/confirmation.
- If deemed applicable for processing, then concurrence accorded on e-mail for processing.
- If deemed not applicable as per the bank's policy, then an email is sent to Trade not recommending any further processing.

### **2.12.3 Sanction Screening of bank's customer portfolio:**

The existing customers are being screened daily against the updated sanction list (it includes but not limited to amended UNSCR lists and local lists) and this is noted as Delta screening.

To ensure that delta screening is performed for the existing customers, the following steps are performed:

- a. Updates are sent to List Management Unit through SAS Analyzer Online portal service from time to time. These updates contain names of individuals, entities, vessels etc. whose name or information have been updated.  
Further HBL Sri Lanka blacklist is updated manually by HBL Sri Lanka Compliance promptly on receipt of new information by compliance officer.
- b. Level-1 Compliance Assistant Manager will review the matched results in the SafeWatch Delta screening filter and provide appropriate comments / remarks.

- c. In case of RFI, Level-1 Compliance Assistant Manager will seek additional RFI (E.g.: Full Name, Father Name, Identity No., Address, Place etc) from the related Business unit and same will be attached in the Alert being reviewed.
- d. Level-2 Supervisor – Compliance Manager or Head of Compliance verify the supporting details / provided comments by Level-1 Compliance Assistant Manager, insert the comments and release the alert.
- e. In case of RFI, Level-2 Supervisor /Compliance Manager or Head of Compliance will seek additional RFI if required (E.g.: Full Name, Father Name, Identity No., Address, Place etc) from the related Business unit and same will be attached in the Alert being reviewed.
- f. In case of an exact match, the Compliance will communicate through an email to the respective Business and Operations team with a copy to the relevant unit, Regional General Manager for their information and reviewing the relationship with HBL Sri Lanka. Respective Business and Operations teams will communicate their findings on clients’ relationship with HBL Sri Lanka to the Compliance team within 3 working days.
- g. If any match is found as true positive from HBL Sri Lanka database for the existing customer, immediate action(s) must be taken as per Bank’s policy and Local Law which may include Freezing of the relationship and reporting of STR to FIU.

#### **2.12.4 Freezing / Suspension Orders**

CBSL / FIU issues Freezing orders to its regulated entities for taking necessary action. These freezing orders, in addition to other requirements, require banks to:

“Freeze without delay the bank accounts, funds and other financial assets or economic resources of these individuals, groups, undertakings and entities, including funds derived from property owned or controlled, directly or indirectly by a proscribed/ designated individual/ entity, or by individuals acting on their behalf or at their direction, and ensure that neither these nor any other funds, financial assets or economic resources are made available, directly or indirectly for such individuals’ benefit”

- Upon receiving the Freezing / suspension order issued by FIU, the Compliance team shall Immediately acknowledge the suspension orders by way of an email to the FIU.,
- The compliance team shall immediately confirm the suspension order with details of all business relationships maintained along with the balances available as at the date of suspension, immediately to the FIU. TAT given for this activity is 5 working days. The compliance team will perform a check against the customer portfolio through the country operations team (Core Banking system).
- If any matches are identified (As per the statement above), the Compliance department will instruct Head - Branch Operations to freeze the account/s with immediate effect. Relevant branch operations manager should ensure to mark “adverse indicia” field in the frozen account as “Yes” in Mysis. The Compliance Department will communicate to FIU or relevant regulatory body.
- In the event if there are no matches, the Compliance team will inform FIU or the relevant regulatory body accordingly.
- Compliance shall obtain a confirmation from the FIU before releasing any suspended accounts.
- Receipt of salary/pension to suspended accounts shall be notified to the FIU along with suspension confirmation.
- During the period of suspension of transactions, Bank should not allow any transaction (including any statutory payments, standing orders, etc.) except for credit transactions into a suspended account. Any debit transaction, whether it is statutory or otherwise, should be communicated by Operations

team to Compliance enabling Compliance to communicate to FIU, and should await the High Court order permitting such transaction prior to debiting the account suspended.

- Bank may inform the customer about the suspension of his/her transactions only upon an inquiry by the customer and in the same manner the inquiry is made.
- Every customer subjected to a suspension order should be considered as of high-risk customers on all occasions in implementing the requirements under the provisions of the FTRA and CDD rules and any other rules and regulations issued under the FTRA.
- Compliance will update the freezing order details in the “Name list screening” excel to ensure that branches/employees are informed of the order details. Accordingly, prior to any new customer onboarding and processing transactions, details are screened against the said list/excel.

### **3. KNOW YOUR CUSTOMER (KYC)**

The Compliance team provides KYC-related guidance and advisory services to the first line i.e. business units and other support functions as and when it is needed for all aspects relating to customers KYC including Customer Due Diligence, Enhanced Due Diligence, customer documentation related to AML/CFT requirements etc.

The primary requirement for HBL SL is to be satisfied that it has adequate process to establish true identity of prospective customers, or users of the Bank’s products and services and that sufficient KYC information is collected to understand the risks involved in the relationship with the customer. Based on the due diligence/ enhanced due diligence conducted and the information obtained as a result of the same, the Bank would carry out risk profiling of its customers from Money Laundering (ML) perspective and ensure that the information obtained as a result of the due diligence activity is reviewed and updated periodically. This periodic review would be based on the risk level assigned to the customer, i.e.; low, medium and high. However, if any abnormality in account behavior is noted or if warranted by circumstances, the accounts should be reviewed as per need basis, including but not limited to upgradation of the overall risk rating or submitting a suspicious transaction report.

The risks associated with a customer are managed within the bank using the three lines of defense model. As such, the risk is to be managed between three lines of defense as follows:

- Responsibility of First Line (Business & Ops): The management of compliance risk lies primarily with the first line of defense/relevant business segment. This includes the responsibility to develop and update systems, policies, processes and procedures to manage compliance risk inherent in their day-to-day activities. For instance, meeting the customer, ensuring all the relevant information pertaining to their KYC is obtained, verified, complete and recorded.
- Responsibility of Second Line (Compliance): Is responsible for assisting line managers/departments in designing and implementing adequate controls to manage risks of non-compliance with regulatory instructions, guidelines, international standards and best practices.
- Responsibility of Third Line (Internal Audit): is responsible for providing independent assurance to board or its audit committee on the quality, effectiveness and adequacy of 1st and 2nd lines of defense.

To manage compliance risk associated to the banks' core business, it is necessary to have an in-depth understanding of the banks' customers. This in-depth understanding is a result of the bank conducting a KYC of its customers.

"KYC" refers to the steps taken by the Bank to:

- Establish the identity of the customer and ultimate beneficial ownership.
- Understand the nature of the customer's activities (primary goal is to satisfy that the source of the customer's funds is legitimate)
- Monitor the customers' financial activities to assess money laundering risk associated with the customer, ensuring that the activities are consistent with the available information and the account usage is as per the declared purposes.

Section 4 of the Global policy should also be followed when performing KYC.

## **CUSTOMER DUE DILIGENCE (CDD)**

Customer Due Diligence (CDD) is the process of Identifying the customer and verifying customer's identity by obtaining their source of income, identifying the nature and scope of relationship between the bank and the customer and other areas in order to identify and assess the risks posed by the customer vis-à-vis Money Laundering (ML) and / or Terrorist Financing (TF). It is to be applied when:

1. Establishing a business relationship.
2. When dealing with occasional / walk in customers desirous of conducting transactions with the bank
3. providing money and currency changing business for transactions involving an amount exceeding rupee two hundred thousand or its equivalent in any foreign currency
4. providing wire transfer services as referred to in Rules 68 to 83 of the CDD Rules No 01 of 2016
5. In case of suspicion of ML / TF, regardless of the amounts involved
6. When there are doubts on the authenticity / veracity of the previously obtained information.

CDD is not a one-time process but an ongoing process where the customer information is reviewed periodically or on a need basis.

## **ENHANCED DUE DILIGENCE (EDD)**

While Customer Due Diligence (CDD) is mandatory for each customer of the bank, Enhanced Due Diligence (EDD) is deemed advisable when additional information is required in order to adequately identify, understand and mitigate the risks associated with a customer. Hence, EDD is essentially information collected for high-risk customers or customers that pose a higher-than-average risk to the bank due to the nature of their location, source of funds, activities etc. in order to obtain a deeper understanding of customer profile and customer activities to mitigate associated risks.

Enhanced Due Diligence is an additional due diligence process required for all High-Risk Customers and where the Bank needs more information on the customer in order to determine the level of risks involved in the customer relationship.

Enhanced Due Diligence is mandatory for customers, both natural and legal, rated as High Risk as per the Customer Risk rating methodology of the Bank. Similarly, transactions conducted with / by such customers are also subject to EDD in order to enable the bank to identify the risks associated with such customers and transactions. Section 4.3 of the Global policy should also be followed when performing EDD.

### **3.1 Customer Risk Rating Methodology**

In determining what level of due diligence is appropriate (CDD v. EDD), a relationship manager should apply risk-based approach and look for “red flags” relating to:

- Location of the business
- Occupation or nature of business
- Purpose of the business transactions
- Expected pattern of activity in terms of transaction types, volume, and frequency
- Expected origination of payments/ transactions and method of payment/ transactions
- Articles of incorporation, partnership agreements and business certificates (where applicable)
- Understanding of the customer’s customers (where applicable)
- Identification of beneficial owners of an account or customer
- Details of other personal and business relationships the customer maintains
- Approximate salary or annual sales/ business turnovers
- AML policies and procedures in place (where applicable)
- Local market reputation through review of media sources

HBL Sri Lanka has adopted Risk Based Approach (RBA) while applying CDD/AML/CFT/CPF measures in line with Central Bank of Sri Lanka (‘the Regulator’) guidelines /International Standards and Best Practices including relevant recommendations of Financial Action Task Force (FATF). Customer Risk Rating Methodology is based on the following assessment models:

1. Rule Based Assessment Model: where specific customers are identified to be marked as High Risk by default and the Front line shall conduct EDD of the Customer.
2. Algorithm Based Assessment Model: where the customers shall be evaluated based on the following parameters:
  - Customer profiles;
  - Geographical risks;
  - Delivery channels; and
  - Products & Services

Considering all the above parameters, risk ratings shall be calculated and allocated to the customer as High, Medium or Low. Customer Risk rating methodology is a fully automated process with the implementation of the Business transformation exercise in HBL Sri Lanka except for legacy entity customers at the moment which will also be automated with rectification of technical issues in the system in near future. Detailed methodology used in assessing the customer Risk rating is explained in the attached Customer Risk Rating Methodology document (Annexure II)

## **3.2 Customer Due Diligence (CDD)**

### **3.2.1 Information to Be obtained at the time of establishing relationship**

For identity purposes, at the minimum following regulatory information should be obtained and in line with Rule No. 27 (SCHEDULE-list of information obtained from customers) of CDD Rules No. 01 of 2016 other than the requirements stipulated in post Business transformation Account Opening Process - BT AOP procedures. The information to be recorded in the Account Opening Forms, CIF as well as in the system.

- Full name as per identity document;
- NIC/Passport/Driving License number or where the customer is not a natural person, the registration/business registration number (as applicable);
- Existing residential address, registered or business address (as necessary), contact telephone number(s) and e-mail (as applicable);
- Date of birth, incorporation or registration (as applicable);
- Nationality or place of birth, incorporation or registration (as applicable);
- Nature of business, geographies involved and expected type of counter-parties (as applicable); (For ex, retail, wholesale, manufacturing, import export, services, etc. for nature of business; high risk areas as identified by FATF or other bodies, high risk areas as per the bank, intercity, intra city, national, international etc. for geographies; general public, retailers, distributors, manufacturers etc. for counterparties)
- Purpose of account; (Savings, business, investments, etc.)
- Type of account; (Current, savings, pension, investment etc.)
- Source of earnings; (Salary, business, agricultural, rental, pension, etc.)
- Expected monthly credit turnover (amount and No. of transactions); and
- Normal or expected modes of transactions. (Cheques, cash, remittances, etc.)

First Line of Defense / Business Team(s) are required to ensure that all account opening procedures have been completed /all documents have been examined to ensure that they are valid and complete. This shall also include verifying the validity of the Trade license (including approvals taken from BOI (Board of Investments), EDB (Export Development Board) etc.)/ verifying declared business operations against the nature of business specified in Articles of Association of the entity. Further, Bank shall not rely on any third-party financial institution, non-finance business or any other party to conduct CDD measures on behalf of the Bank.

### **3.2.2 Identification of the Customer**

Identity of every prospective customer must be ensured by the first line of defense i.e. business units. Relationship with the customer will not be established until the identity of a potential customer is satisfactorily established and otherwise the bank may consider marking the account as high risk and filing an STR with the FIU. In case, the customer refuses to provide the requested information the relationship should not be established. Likewise, if the requested follow-up information is not forthcoming (for example, documentary evidences requested against an unusual / complex / large transaction as a part of the transactional due diligence, or where proof of business that is in addition to an already declared business is requested but the customer declines to provide the same), the bank should consider marking the account as high risk and filing a STR with FIU.

In case the bank is unable to comply with the relevant CDD measures, in such instances bank shall,

- (a) in relation to a new customer, not open the account or enter into the business relationship or perform the transaction; or
- (b) in relation to an existing customer, terminate the business relationship, with such customer and consider making a suspicious transaction report in relation to the customer.

### **3.2.3 Verification of the Identity**

The identities of the customers (natural persons), and in case of legal persons, identities of their natural persons exercising control or beneficial ownership (including Directors who are neither beneficial owners nor signatories) where such natural persons have been issued a verifiable identity document from relevant authorities shall be verified against the Original Identification documents., In case of Foreign Nationals other reliable, independent sources should be referred and records / copies of all reference documents used for identification and verification shall be retained. These sources may include but are not limited to, in case of natural persons, consulates issuing visas or Passport issuing authorities, and in case of entities, relevant regulatory bodies permitting operations of the entity. The verification shall be the responsibility of the business for which the customer should neither be obligated, nor the cost of such verification be passed on to the customers.

#### **3.2.3.1 Identification and Verification of Natural Persons Acting on behalf of Customer (power of attorney)**

All persons acting on behalf of a Customer / Legal Entity or Beneficial Owner in relation to a customer will have to be identified and verified. Branches shall obtain copies of NICs/Passport/Driving License and verify the identities of all Authorized Signatories, Mandate-holders, Partners, Attorneys, Directors, Trustees, settlors, protectors (if any), beneficiaries and class of beneficiaries, Members of Governing Bodies, Members of Executive Committees etc. and or any other arrangements in place, as per the Type of Customer Relationship. Copies of all reference documents used for identification and verification of these persons should be retained in the bank's record.

The authority of such person to act on behalf of the customer shall be verified through documentary evidence including specimen signature of the persons so authorized.

The information of directors, Partners, Authorized signatories; Mandates; Members; Governing Body members; UBOs; Executive Committee; Attorney, Trustees, Settlers, Protectors (if any), Beneficiaries or class of beneficiaries etc. will be recorded onto the system and into the account opening form as per the document provided by the customer.

All beneficial owners (either natural or legal) associated with the account i.e. Customer(s), Mandate, Attorney holders, Directors, Partners, Trustees, Settlers, Protectors (if any), Beneficiaries or Class of Beneficiaries, Members, Executive Committee, Governing Body Members etc. shall be screened against the list of proscribed individuals and entities as per procedure of Screening defined above.

Moreover, it must be ensured to seek information on powers (legal basis or authority) that regulate and bind the legal person or arrangement, as well as the names of the relevant persons having a senior management position in the legal person or arrangement. (Directors, signatories and organizations' CEO and his direct reportees with copies of NIC or Passport in case of foreign nationals). The authority of such persons to act on behalf of the legal person or arrangement shall

also be obtained in documentary form (Board Resolution, List of Authorized Signatories etc.) for the banks' records.

The list of senior management shall also be screened against the lists of proscribed individuals and entities as per the process described in section 2.4 of the process document.

### **3.2.4 Identification and Verification of Beneficial Owners**

It must be inquired to ensure whether there exists any beneficial owner in relation to a customer or transaction. In case of beneficial owner(s) in relation to a customer, actual identity of the beneficial owner must be ensured and verified by the business using the relevant information or data obtained from a reliable source. (reliable sources include but are not limited to physically visiting the workplace for verification by the banks' officers, search engines like Google for publicly available information, resources like World Check, Lexis Nexis, Bloomberg, Reuters etc.)

#### **3.2.4.1 Beneficial owner(s) of a legal person**

In the process of identifying beneficial owner(s) of a legal person (i.e any entity other than a natural person that is able to establish a permanent customer relationship with a financial institution or otherwise owns property and includes a company, a body corporate, a foundation, a partnership or an association), the Bank should consider three main elements:

- a) Which natural person(s) owns or controls more than ten percent (10%) of the customer's equity?
- b) Which natural person(s) has "effective control" of the legal person?
- c) On behalf of which natural person(s) the transaction is being conducted

The beneficial owner(s) of a customer (legal person) may satisfy one or more of the three elements identified above. Accordingly, it would not be sufficient to simply apply only the ownership element in determining beneficial ownership.

Business has to understand the nature and the scope of customer activity based on the customers' business and scope of operations, unwrap ownership and control structure of the customer using all available constitutional/ legal documents for obtaining information and determining the natural person(s) who ultimately own or control the customer. Controlling ownership or interest means an interest / ownership acquired by providing / acquiring more than ten percent (10%) of the capital / controlling stake of a customer. In this regard, unwrapping of the customers till the natural person identification has to be performed as per approved HBL Sri Lanka AML, CFT, CPF & KYC Policy Addendum.

The identity of the natural persons (if any) exercising effective control of the legal person or arrangement should be identified and verified through other means.. Refer annexure XI - UBO direction issued by CBSL ( Guidelines for Financial Institutions on Identification of Beneficial Ownership, No. 04 of 2018) section 17 and 18 on identifying parties having effective control of the legal person.

The person on whose behalf a transaction is being conducted is another aspect of the definition of beneficial ownership. This may be the individual who is an underlying client of the customer. An example is, if the Bank knows that person 'A' is conducting an occasional transaction on behalf of



person 'B', and then person 'A' and person 'B' should be identified and verified along with any other beneficial owners that may be a party to transaction. Refer annexure XI - UBO direction issued by CBSL ( Guidelines for Financial Institutions on Identification of Beneficial Ownership, No. 04 of 2018) section 19.

### **3.2.4.2 Beneficial owner(s) of a legal arrangement (i.e. legal arrangement includes an express trust, a fiduciary account or a nominee)**

All trusts have the common characteristic of causing a separation between legal ownership and beneficial ownership. Legal ownership always rests with the trustee. Beneficial ownership can rest with the author of trust, trustees or beneficiaries, jointly or individually.

FIs should identify and take reasonable measures to verify information about a trust, including, the identities of the author of the trust, the trustees, the beneficiary or class of beneficiaries and any other natural person exercising ultimate effective control over the trust (including those who control through the chain of control or ownership).

Bank is required to obtain trust documents (e.g. deed of trust, instrument of trust, trust declaration, etc.) and the provisions of the trust document must be fully understood within the context of the laws of the governing jurisdiction. The FIs should take reasonable measures to verify trust document through independent means (e.g. Registry of Trust, Notary)

Example: Person 'A' is the author of a trust for the benefit of his child. The trustee seeks to establish a relationship with a financial institution to help manage the assets of the trust. Even though the trustee is the controller of the assets of the trust he may not be the ultimate beneficial owner and the main focus of CDD should include person 'A' as well.

Once the Bank establishes who the beneficial owner(s) of a customer is/are, the Branch must collect at least the following information in relation to each individual beneficial owner as mentioned below and under rule no. 27 of the CDD Rules No. 01 of 2016.

- ✓ full name
- ✓ official personal identification or any other identification number
- ✓ permanent/ residential address

For the verification of beneficial ownership, some of the documentation that Bank can rely on may include (but not limited to) the following:

- a) Share register,
- b) Annual Returns,
- c) Trust deed,
- d) Partnership agreement,
- e) The constitution and/or certificate of incorporation for an incorporated association,
- f) The constitution of a registered co-operative society,
- g) Minutes of the board of director's meetings,
- h) Information available through open-source search or commercially available databases.

In case of foreign legal persons and arrangements, the Bank should also take additional measures such as verification through mother company or branches, correspondence bank, other agents of the bank, corporate registries etc.

Bank should periodically review the adequacy of information obtained in respect of beneficial owners to ensure that the information is up to date. The review period should be the KYC review period.

However, any material/significant change in customer circumstances may necessitate a review of beneficial ownership. Some examples of material/significant changes include:

- a. a public company is taken private;
- b. a shareholder or group of shareholders takes effective control of voting shares;
- c. a new partner is added, or an existing partner is removed;
- d. change in management positions;
- e. new trustees are appointed;
- f. a trust is dissolved;
- g. a new account is opened for the same customer;
- h. transactions are attempted that are inconsistent with the customer's profile

Branches must obtain a declaration for Ultimate Beneficial Ownership from all customers prior to establishing a banking relationship. Declaration format is attached as annex III

Note: Identification of Ultimate beneficial owners should be in line with Guidelines provided by the Central Bank of Sri Lanka

### **3.3. CDD Measure for Occasional Customer / Walk-in Customers and Online Transactions**

Bank will ensure compliance for the Occasional Customer / Walk-in Customers and Online Transactions as per the AML/CFT regulations issues by CBSL/SBP

Accordingly, with regard to transactions or series of linked transactions exceeding rupees two hundred thousand or its equivalent in any foreign currency conducted by occasional customers, one-off customers or walk-in customers, Bank should conduct CDD measures and obtain copies of identification documents.

All cash deposits exceeding rupees two hundred thousand or its equivalent in any foreign currency made into an account separately or in aggregate by a third party customer, have on record the name, address, identification number of a valid identification document, purpose and the signature of the third party customer provided that, clerks, accountants, employees, agents, or authorized persons of business places who are authorized to deal with the accounts shall not be considered as a third party.

Further, if there are reasonable grounds to suspect that the transaction or series of linked transactions are suspicious or unusual, the Branch shall obtain such information irrespective of the amount specified above.

### **3.4. Information on the Purpose and Intended Nature of Business Relationship**

Customers information related to the purpose and intended nature of business relations shall be obtained. This information shall be obtained through various fields in AOF and KYC such as purpose of account, type of account, Expected Credit/Debit turnover and expected mode of transactions etc.

### **3.5 Timing of Verification**

Verification of the identity of the customers and beneficial owners shall be completed before business relationships are established including verification of identity documents such as NIC/Passport/DL/Business Registration etc. wherever required for customers under these requirements.

### **3.6 Joint Accounts**

In the case of joint accounts, CDD measures on all of the joint account holders shall be performed as if each of them was individual customers of the Bank.

### **3.7 Dormant Accounts**

For customers who are having “in-active” status, credit entries are allowed without changing the dormancy status of such accounts. When accounts are dormant, Debit transactions/ withdrawals shall not be allowed until the account holder requests for activation in writing and produces attested copy of his/her valid identity document. Before activation of the account, it must be ensured that the customer due diligence (CDD) record is updated, and it is in line with the current source of income and whereabouts of the customer.

In relation to the above, it may be noted that transactions e.g. debit under the recovery of loans and markup etc. any permissible bank charges, government duties or levies and instruction issued under any law or from the court will not be subject to debit or withdrawal restriction.

### **3.8 Circumstances where CDD measures are not completed:**

In case branch is not able to satisfactorily complete required CDD measures, account shall not be opened, or any services provided. Such cases might require the branch to raise a UAR (Unusual Activity Report) to the Compliance Department.

If CDD of an existing customer is found unsatisfactory, the relationship should be treated as high risk and reporting of suspicious transactions may be considered as per law and circumstances of the case. For this purpose, such cases should be immediately reported to Compliance Department by the respective branches / parties handling such cases as per the approved reporting process.

### **3.9 Anonymous or Fictitious Account**

Bank shall not open or maintain anonymous accounts, any account in a false name or accounts in the name of fictitious persons or numbered accounts. Customer on boarding procedure discussed in section 2.11 must be followed for all account opening with no exceptions.

### **3.10 Prohibition of Personal Accounts for Business Purposes**

Personal accounts should not be used for business purposes except proprietorships, small businesses and professions where constituent documents are not available, and the business is satisfied with KYC profile of the account holder, purpose of relationship and expected turnover of the account keeping in view financial status & nature of business of that customer.

The business transaction in the personal account of proprietors may only be permitted by linking it with account/ business turnover.

### **3.11 Enhanced Due Diligence**

Enhanced due diligence (EDD) is a process of “digging deep” into a customer / transaction. It’s a process of applying measures that are over and above the standard CDD procedures already in place and are effective and commensurate to the level of risks.

Following EDD measures shall be applied as per applicability on different high-risk elements/scenarios:

- Obtaining additional information on the customer (beneficial owner profile identification, instrument wise expected transaction details, details of Source of wealth, proof of source of income etc.);
- Reducing interval for updating and reviewing customer risk profile; including updating the identification data of customer and beneficial owner;
- Obtaining information on the reasons for intended or performed transactions;
- Obtaining the approvals as per the matrix mentioned in the AML, CFT, CPF & KYC Policy addendum of HBLSL for High-Risk Accounts (Refer Annex IV) to commence or continue the business relationship;
- 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;
- Documentary evidence may be sought to support the transaction where possible, e.g. purchase of property, inheritance etc.
- Obtaining additional information on the customer (occupation, volume of assets, address, information available through public databases, internet, etc.);
- Obtaining additional information on the intended nature of the business relationship;
- Obtaining additional information on the sources of funds or sources of wealth of the customer;

The Bank must, however, consider assigning relatively higher weightages to the following types of customers, while taking into consideration the risk determinants as per the CRRM and Rule Based Circular for high-risk accounts and approvals will also be obtained.

- Politically Exposed Persons;
- Trust / Clubs / Association / NGO / NPO / Religious Entities / Charity / Foundation / Masjid;
- Housewife\*
- Student \*
- Minor\*

- Sole proprietors or Self Employed engaged in the business of Arts Galleries, Gems Dealers, Jewelers, Gold Importers, Restaurants, Real Estate Agents, Travel Agents, Car dealers
- Sole Proprietor \*
- Self-Employed \*
- Foreign citizen / legal entities / Sri Lankan Nationals residing in High-Risk Countries under FATF and Basel – AML index and as per Bank's classification / local regulations i.e. CDD Rule 57 & 58.
- High-net-worth customers with no clearly identifiable source of income;
- Legal persons or arrangements that are personal asset holding vehicles;
- Embassies, Consulates & Foreign Missions of countries;

Additionally, the following are also critical aspects which are required to be taken into consideration for higher weightage:

- Online transactions
- Non-resident customers
- Customers with links to offshore tax heavens i.e., they are citizens, residents or have business interests including counterparties with offshore tax havens.
- Account holders who have given mandates to another person above customers are classified under high-risk categories based on the threshold values defined in the CRRM guidelines & Rule based circular.

Apart from the approval matrix defined in AML, CFT, CPF & KYC Policy addendum, as mentioned above, accounts of PEPs and NGO/NPO/Charities/Trusts/Welfare Organizations/Associations are subject to prior clearance from Regional Compliance Head, Business Head and approval from Country Manager. First line shall ensure all international and national level foreign funded voluntary social services organizations/ NGOs are re-registered with the National Secretariat for NGOs and monitor and immediately report any NGOs,

- a) not registered with the National Secretariat for Non-Governmental Organizations,
- b) registered with any other institution including the District Secretariat or the Divisional Secretariat or any other institutions and
- c) receives direct foreign funds / remittances into their accounts.

to Compliance Department enabling submitting reports in line with Section 7 of the Financial Transactions Reporting Act, No. 6 of 2006.

Further, NGO/NPO and Charities shall open accounts in the name of the relevant NGO, NPO or Charity as per title given in the constituent documents. The individuals who are authorized to operate the accounts and members of their governing bodies shall also be subject to enhanced CDD measures. Bank shall ensure that the aforesaid persons are not affiliated with any entity or person designated as a proscribed entity or person, whether under the same name or a different name. Bank should not allow personal accounts of the members of the governing bodies of a NGO, NPO or Charity to be used for charity purposes or collection of donations. Branches must review and monitor all existing relationships of a NGO, NPO or Charity to ensure that those organizations, their authorized signatories, members of their governing bodies and the beneficial owners are not linked with any entity or person designated as a proscribed entity and person, either under the same name or a

different name. In case of any type of suspicion, bank shall file a Suspicious Transaction Report or take other legal action or both.

In addition to the above, SL HBL will categorize the following business type as high risk & conduct EDD as well as have these relationships approved by HBL SL – Head of Compliance, Group Head of Business & Country Head before establishing relationship.

- Hedge funds
- Private equity/ Venture capital business
- Investment advisor
- Mutual funds
- Credit card services companies
- Offshore entities
- Commodity Operator / Commodity Trade Advisors
- High risk customer as per Global AML/CFT/CPF and KYC Policy

### **3.12 Specialized Enhanced Due Diligence (SEDD) for Ultra High Net Worth Individuals**

Ultra-High-Net-Worth Individuals (UHNWI) are defined as those individuals that hold any kind of depository relationship in local or FCY currency more than the aggregate balance of USD 750K. This may be at the time of Account Opening or any point during the course of the relationship. Once the defined limit is crossed, the relationship will be marked as 'High', and it will trigger the Enhanced UHNWI KYC review.

On a best-effort basis, the E-UHNWI KYC review will include the following additional steps in addition to the regular High-Risk KYC and may be obtained through documentation or documented in a call memo:

- I. Obtaining names of all Immediate Family members.
- II. For customer & immediate Family members:
  - a. Conduct Name Screening (Politically Exposed Persons "PEP", Sanctions and Adverse Media).
  - b. Obtain employment & business information, including geographic exposure and potential sanctions exposure (all businesses).
- III. For customers, if there are representatives involved, i.e., business advisor or mediator, they should also be subjected to SEDD i.e., steps 1 and 2 to be followed.
- IV. Where the business is unable to satisfactorily complete the SEDD, the customer should be exited in line with the bank's exit process after serving appropriate notices to the customer.

Immediate family members for this section are defined as 1) Parents 2) Spouse 3) Siblings and 4) Children.

In exceptional circumstances, where due to cultural sensitivities, regulatory or legal restrictions, names of the spouses, siblings, children, or parents are not easily available, dispensation should be obtained from Head International and Chief Compliance & Conduct officer (CCO) by the Country Manager/RGM.

### **3.13 Periodic and Event Driven/Trigger based review:**

As per the CRRM, the re-review of the risk rating shall be based on, Periodic reviews and event driven based Reviews. The periodic review will be conducted based on Customer Risk Rating Module, as per the existing risk rating of the customer, which is as follows:

- a) In case of High-Risk Customer, the update of customer KYC and risk rating shall be conducted annually.
- b) In case of Medium Risk Customer, the update of customer KYC and risk rating shall be conducted every 2 years.
- c) In case of Low-Risk Customer, the update of customer KYC and risk rating shall be conducted every 3 years.

Event driven/Trigger based review is conducted whenever any significant transaction or change in customer profile is observed including at the time of dormant account activation, which impacts the KYC of the customer and in turn, may impact the risk rating.

#### **3.13.1 Periodic Review:**

The purpose of periodic reviews of the KYC / CDD of customers is to examine customer transactions in light of the customer profile for unusual, large or complex transactions or transactions with no visible lawful or economic purpose. It is to be ensured that the results of these examinations are documented and kept as per the bank's record retention policy. In addition, the purpose of periodic reviews is to ensure that customer information is reviewed and updated on a timely basis and that the financial activity of the customer is as per the available information. In case of any changes in the customer profile or financial activities, the same is updated in the bank's records.

Customer KYC / CDD profile will be reviewed and / or updated on a pre-defined frequency in accordance with the risk profile of the customer. The frequency of such reviews is as under:

Table — 1: Frequency of KYC/CDD Periodic Reviews

High Risk	Once in every 12 months or event driven*
Medium Risk	Once in every 24 months or event driven*
Low Risk	Once in every 36 months or event driven basis*

\*In case of any material change in the relationship or deviation from customer profile, CDD will be conducted, and customer profile will be updated immediately. Accordingly, the next review date will then be calculated and reflected in the system from the date of the last review and taking into account the risk rating assigned.

**Responsibility:**

It is the responsibility of First line of defense i.e. Business to update customer's KYC information periodically as per the mentioned frequency. Business is instructed to conduct periodic reviews in accordance with the requirements of Bank's AML, CFT, CPF & Sanctions guidelines & Procedures. In this regard, management should ensure compliance. Compliance team will monitor the Expired KYC reviews and update same in monthly Country Compliance Management Information report to be submitted to international compliance department HBL - PAKISTAN. Further, the Compliance team will follow up with branches to complete the Expired KYC reviews.

### **3.13.2 Procedure to perform periodic reviews:**

This process will periodically update the customer's KYC information using risk-based approach. A review of the account statement and financial activity will be conducted, and this activity will be compared with the information available in the existing KYC records of the customer. In case of a satisfactory review, branches will update and take a print of the existing and updated KYC. In case the staff conducting the KYC has queries or reservations on the transactions and account activity, information will be sought from the customer regarding the same and the KYC will be revised as necessary. However, in case the staff conducting the KYC is not satisfied with the clarification obtained from the customer or if no information is being provided, the branch may consider marking the account as high risk and raising an STR to the Compliance Department as per the bank's defined procedures. -

Additionally, if the staff conducting the KYC has suspicions that the account under review is being used for money laundering / terrorist financing purposes and have reasons to believe that approaching the customer for information may tip off the customer, they are advised to raise an STR to Compliance Department without conducting any CDD process.

The detailed process on Periodic KYC reviews is attached as annexure V.

### **3.14 Wire Transfers/ Fund Transfers**

The Bank while acting as an Ordering, Beneficiary or Intermediary Institution for processing wire transfers/fund transfers shall obtain necessary information about the originator / beneficiary and other transactional details as required under the regulatory requirements and shall comply with the requirements mentioned under Rules 68 to 83 of the CDD Rules No 01 of 2016 as explained below.

Bank shall ensure that all cross-border wire transfers to be always accompanied with the following when acting as the Ordering Institution: -

- a) originator information: -
  - i. name of the originator;
  - ii. originating account number where such an account is used to process the transaction or in the absence of an account, a unique transaction reference number which permits traceability of the transaction; and



iii. originator's address, national identity card number or any other customer identification number as applicable;

b) beneficiary information: -

- i. name of the beneficiary; and
- ii. the beneficiary account number where such an account is used to process the transaction or in the absence of an account, a unique transaction reference number which permits traceability of the transaction.

If the bank fails to comply with the requirements in respect of a wire transfer, such Financial Institution shall not proceed with the wire transfer unless directed to do so by the Financial Intelligence Unit and shall consider reporting the relevant transaction as a suspicious transaction to the Financial Intelligence Unit

Where several individual cross-border wire transfers from a single originator are bundled in a batch file for transmission to beneficiaries, the batch file shall contain required and accurate originator information, and full beneficiary information, that is fully traceable within the beneficiary country and shall include the originator's account number or unique transaction reference number.

As "Beneficiary Institution", must ensure the following:

- To verify the identity of the beneficiary;
- the beneficiary account number where such an account is used to process the transaction or in the absence of an account, a unique transaction reference number which permits traceability of the transaction.
- Complete originator or beneficiary information, if not, then it may be considered as a factor in assessing whether to execute or terminate the transaction, and in assessing whether the transaction is suspicious and merits reporting to the FIU;
- Refrain from business relationship or transact with non-compliant institutions as set out in the standards for wire transfers.

**As an "Intermediary Institution", must ensure the following.**

- Keep a record of all the information onward and payment instructions, originator and beneficiary information received from the ordering financial institution or another intermediary;
- Identify cross-border wire transfer messages with lack of originator and beneficiary information and follow reasonable measures, which are consistent with straight-through processing. These measures may include rejecting the transaction or suspending the transaction until complete information is obtained. Maintain all originator and beneficiary information accompanying the wire transfer.
- It should be ensured that regardless of the role of the bank (Originator / Beneficiary / Intermediary), the information related to the originator and the beneficiary is available in the instructions throughout the payment chain. The minimum information contained in the instructions is as under:
  1. The name of the originator
  2. The originators' account number or the unique reference number for the transaction
  3. Originators' address or NIC / passport number

4. The name of the beneficiary
5. The beneficiary's address or NIC / passport number

It is pertinent to note that these requirements do not apply to wire / fund transfers between FIs for transactions executed between them, for example repo / reverse repo transactions, currency swaps etc.

### **NBFIs (Non-Banking Financial Institutions)**

Non-Banking Financial Institutions pose unique risks as customers of a bank due to the fact that may be classified broadly into two categories:

- a) Where an NBFI avails correspondent banking services with HBL SL
- b) Where an NBFI maintains account(s) with HBL SL that are not related to correspondent banking services.

Where an NBFI avails correspondent banking services, the account due diligence will be conducted as per the procedures defined in section 3.12 and 3.13 covering correspondent banking relationships.

Where an NBFI does not avail correspondent banking services from HBL SL and maintains accounts with HBL SL for their financial needs, the account will be treated as a high risk, non-individual account and all procedures applicable to such accounts including unwrapping of beneficial ownership to identify natural persons controlling the entity, identification of PEP individuals in beneficial owners / senior management, approvals for opening of account with PEP elements, screening of entity and beneficial owners / management on proscribed lists etc. will be as per applicable processes defined in sections 3 and 4 of this document.

## **3.15 Correspondent Banking Relationships**

Correspondent banking is the provision of banking services by one bank (the "correspondent bank") to another bank (the "respondent bank"). Large international banks typically act as correspondents for thousands of other banks around the world. Respondent banks may be provided with a wide range of services, including cash management (e.g. interest-bearing accounts in a variety of currencies), international wire transfers, cheque clearing, payable-through accounts and foreign exchange services.

Correspondent banking does not include one-off transactions or the mere exchange of SWIFT Relationship Management Application keys (RMA) in the context of non- customer relationships, but rather is characterized by its on-going, repetitive nature. However, transaction level risk has to be assessed with respect to sanctions, volume and underlying nature of transaction/goods.

### **3.15.1 Types of relationships**

- VOSTRO - A VOSTRO account is an account a correspondent bank holds on behalf of another bank. These accounts are an essential aspect of correspondent banking in which the bank holding the funds acts as custodian for or manages the account of a counterpart.
- NOSTRO – A NOSTRO account refers to an account that a bank holds in another bank. NOSTRO are frequently used to facilitate foreign exchange and trade transactions.

- RMA (Relationship Management) - The SWIFT RMA is a messaging capability enabling SWIFT members to exchange messages over the network and can create a non-customer relationship in particular cases of cash management, custody, trade finance, exchange of messages with payments and securities markets infrastructure entities, e.g., exchanges depositories.

As a clarification, Nostro and Vostro accounts are essentially referring to the same account, but from different perspectives. For example, if bank A is the correspondent and bank B is the respondent bank, then the account maintained by bank A will be referred by bank A as a Vostro Account whereas Bank B will refer to the same account as a Nostro Account.

As per the regulatory requirements and international best practices, all correspondent banking relationships are to be established only with banks that have a physical presence in the jurisdiction they are licensed in. Therefore, the bank will not establish business relations with banks, which have no physical presence in the jurisdiction in which they are licensed (Shell Banks). Additionally, the Bank must not knowingly establish relations with the banks that have relations with shell banks. To ascertain that no relationships are maintained with shell banks or with banks that have relationships with shell banks, the bank will ensure the following:

Bank has a separate procedure approved for FI CDD operations namely “Customer Due Diligence Procedures – Financial Institutions – HBL International Branches (Excluding HBL China)” which shall be followed for all FI CDD matters. Enhanced CDD measures shall be applied when entering into or continuing correspondent banking relationships with banks or Financial Institutions which are located in high-risk countries, referred to in Rule 57.

### **3.16 Record Retention Period**

The minimum retention periods to comply with CBSL/SBP Regulations are:

- Banks shall maintain all necessary records on transactions, both domestic and international, for a minimum period of ten years from completion of the transaction.
- The records should be sufficient to permit reconstruction of individual transactions as advised under FTRA (Sec 4) including the nature and date of the transaction, the type and amount of currency involved and the type and identifying number of any account involved in the transactions so as to provide, when necessary, evidence for prosecution of criminal activity. The transactions records may be maintained in paper or electronic or microfilm form, provided it is admissible as evidence in a court of law.
- The records of identification data obtained through CDD process like copies of official identification, account opening forms, KYC forms, verification documents, periodic KYC reviews and other documents along with records of account files and business correspondence shall be maintained for a minimum period of ten years after the business relationship is ended. The identification records may be maintained in documents as originals or copies subject to bank’s attestation.
- Bank shall, however, retain those records including STR records for longer period where transactions, customers or accounts involve litigation, or it is required by court or other competent authority.
- Bank shall satisfy, on timely basis, any enquiry or order from the relevant competent authorities including law enforcement agencies and FIU for supply of information and records as per law.

### **3.17 AML / CFT/ CPF, Sanctions and TBML trainings**

HBL SL Compliance should focus on the subject trainings on an ongoing basis and also conduct capacity analysis and allocate more resources towards trainings to ensure awareness of staff and their responsibilities to combat financial crime risks.

#### **Awareness Raising and Training**

- SL Compliance will be responsible for the preparation of the training material.
- Training material will be updated as and when required due to a change in Regulatory/legal framework, any change in Minimum AML/KYC standards or when felt necessary by Compliance Group
- In order to effectively implement the regulatory requirements and banks own policies and procedures relating to AML/ CFT/ CPF, suitable training program for relevant employees shall be carried out on annual basis.
- Further it is the duty of the relevant staff to duly complete the E-learning (Computer Based Training - CBT) assigned.

#### **The Bank's AML training will include:**

- Explanation of the Bank's AML, CFT, CPF & KYC Policy and Sanctions Policy and Applicable Laws, Regulations and International Standards
- Procedure for identifying and verifying customers.
- Understanding in prevention, detection and reporting ML / TF / PF / Sanctions & TBML
- Record Keeping and Reporting Requirements
- Guidance on how to identify suspicious activity, structured transactions, red flags and raising of UARs.
- Further, during the training, the knowledge levels of the attendees are tested through assessments. Where a pre assessment is conducted prior to the training and a post assessment is conducted post training. Thus, the results of the pre assessment and post assessment are analyzed to evaluate the impact of the training conducted. Also, the statistics are presented by the Compliance Team during the Compliance Committee Meeting. It is the responsibility of the participants to complete the pre-and post-assessment questionnaires in a timely manner when the Compliance department provides such assessments during and after the training. Any nonadherence will be notified to HR with a copy to the Country Manager (CM) for required actions.

#### **Compliance and Training Records:**

In relation to training, records of names of staff along with the dates of the AML/CDD/CFT/CPF training will be maintained by both SL Compliance and Human Resources Department.

### **3.18 Customer Selection for Exit Management**

The Compliance department identifies during an investigation/event driven review/course of its operations that ML/FT and PF risk posed by a customer to the bank is significant or beyond the risk appetite of the Bank, it may recommend to Business to exit the relationship with the customer in addition to reporting of SAR to the regulator where deemed necessary. This shall be communicated in writing by Head of Compliance to Head of Business.

## **4. AML ADVISORY, POLICIES AND PROCEDURES**

### **4.1 AML Advisory**

Compliance department of Sri Lanka provides guidance / advisory services to the businesses and other functions related to the details mentioned below.

#### **4.1.1 Associations, Clubs, NGOs, NPOs, Societies and Trusts:**

First line of defense must ensure that Enhanced Due Diligence is mandatorily conducted while dealing with the subject entity types in order to ensure that these relationships / accounts are used for legitimate purposes only and the transactions are commensurate with the stated objectives and appropriate approvals are in place prior to onboarding of such customers / relationships.

Sufficient information must be obtained by the first line of defense relating to Associations, Clubs, NGOs, NPOs, Societies and Trusts to understand the nature of their business, purpose of existence and organizational structure based on the minimum criteria given below prior to onboarding.

#### **4.1.2 Important considerations for first line of defense / branch level compliance:**

- Customer accounts must be opened as per the title given in the constituent documents of the entity.
- The individuals who are authorized to operate these accounts and members / directors of their Governing Body should also be subject to EDD checks.
- First line of defense should also ensure that the Trustees / Members /Signatories / Donors / Governing Body Members /Office bearers etc. must not affiliated with any proscribed linkage as defined in the above section, whether under the same name or any different name at the time of screening of such customers.
- Approval should be obtained from Regional Head of Compliance SL, Business Head and the Country Manger prior opening subjected account categories.
- In case of advertisements through newspapers or any other medium, especially where bank account number is mentioned for Donations, branches should ensure that the Title of the Account is the same as that of the entity soliciting Donations. In case of any difference, immediate caution should be marked on such accounts and the matter should be considered for filing SAR / STR under the SAR / STR process in the above section.
- Personal accounts cannot be used for charity purposes or collection of donations.
- Further, the first line should ensure at the time of on-boarding and also during the relationship that.
  - The entity has operations in line with the articles /trust deed /rules etc
  - The funds are utilized in the manner and in the area as was stated in the documents and recorded at the time of CDD.

#### **4.1.3 Clearance Regarding Associations, Clubs, NGOs, NPOs, Societies and Trusts:**

The following process must be followed in the account opening for the subject account categories which will also require clearance / review / approval at the following levels:

1. Branch must perform adverse media searches; Google searches results on all High-Risk customer names Trustee/Member/Signatories/Donors/Governing Body Members/Office bearers etc. identified in the relationship / account of the subject account categories. The branch must request World Check users in the first line to conduct screening in World check through email by providing all necessary details. Further these entities will be automatically screened through the SSW system as per the account opening process.
2. Branch will submit the duly filled High Risk profile form with required supporting documents to the applicable stakeholders for prior approval.
3. The stake holders must review the High-Risk profile form and provide necessary approvals / rejections within 5 calendar days. (On a case-by-case basis, relevant stake holders may seek further extensions upon informing the business & other stake holders involved in this process)
4. To further strengthen the oversight on Charitable Organizations in addition to the approvals required as per the approval matrix, CCO approval will also require when onboarding new Charitable Organizations or providing any new accounts, products or services to existing Charitable Organizations
5. In the event of a rejection, the compliance department at its disposal may file a STR with FIU through its web portal subject to the gravity of the reason for rejection.

#### **4.1.4 Politically Exposed Persons (PEPs) - Guidelines for Identification and Assessment of Politically Exposed Persons (PEPs)**

##### **4.1.4.1 Introduction**

In terms of Global AML, CFT, CPF & KYC Policy and Sanctions Compliance Policy, bank is required to identify customers who are Politically Exposed Persons (PEPs), including their close relatives or close associates and perform Enhanced Due Diligence (EDD) on the account of PEPs mandatorily and to classify them as High Risk and also assess or evaluate the impact of the PEP on the overall non-individual relationships (whether as customer or beneficial owner) this includes asset customers. In this regard, the following guidelines are required to be compliant along with the PEP Risk assessment forms.

##### **4.1.4.2 Definition**

PEPs are individuals who are or have been entrusted with prominent public functions either domestically or by a foreign country, or in an international organization, for example but not limited to Heads of State or of government, politicians, senior government officers, judicial or military officials, senior executives of state-owned corporations/departments/autonomous bodies, etc. This does not intend to cover middle-ranking or more junior individuals in the foregoing categories. The involvement of a PEP in the management of an entity-based relationship could increase the risks involved in establishing or maintaining a relationship with such an entity. Moreover, accounts for trusts, personal investment companies, foundations, operating companies etc., if established for the specific benefit(s) of a PEP, Close Family Member or Close Associate, will also be classified as PEP.

Requirements for PEP should also be applied to the close family members or close associates of PEPs with a separate PEP Risk assessment form and identification of the same is also the first line responsibility.

- Family members of PEP includes: PEP's direct family members, their spouse, their children and their spouses, parents and the siblings of the PEP

- Close Associates of PEP: Close business colleagues and personal advisors / consultants to the PEP, as well as persons who are expected to benefit significantly by being close to such a person.

Accordingly, PEPs can be identified under the following categories.

- a) Domestic PEPs: individuals who are entrusted with prominent public functions in Sri Lanka.
- b) Foreign PEPs: individuals who are entrusted with prominent public functions by a foreign country.
- c) International organization PEPs: persons who are entrusted with a prominent function by an international organization.
- d) Immediate Family members: individuals who are related to a PEP either directly (on grounds of consanguinity) or through marriage or similar (civil) forms of partnership.
- e) Close associates: individuals who are closely connected to PEP, either socially or professionally.

Immediate family members of PEPs include any of the following relations:

- i. spouse (current and past);
- ii. siblings, (including half-siblings) and their spouses;
- iii. children (including stepchildren and adopted children) and their spouses;
- iv. parents (including stepparents);
- v. grand children and their spouses.

Close associates of PEPs or their family members includes;

- i. a natural person having joint beneficial ownership of legal entities and legal arrangements, or any other close business relationship with any PEPs or immediate family members of PEPs
- ii. a legal person or legal arrangement whose beneficial owner is a natural person and is known to have been set up for the benefit of such person or his immediate family members of PEPs or immediate family members of PEPs
- iii. a PEP's widely- and publicly known close business colleagues or personal advisors, in particular, persons acting in a financial fiduciary capacity.

The PEP definition specifically excludes identifying middle ranking or junior individuals as PEPs. However, there should be awareness that middle ranking and junior officials could act on behalf of a PEP to circumvent AML/CFT controls. These less prominent public functions could be appropriately taken into account as customer risk factors in the framework of the overall assessment of risks associated with the business relationship in accordance with CDD Rules when they are acting on behalf of a PEP.

#### **4.1.4.3 Categorization of PEP**

Bank considers a range of factors while determining whether a particular holder of public office function has the requisite seniority, level of authority or exercise influence the individual has over government activities / funds, prominence or importance, etc. to be categorized as PEP.

While considering the facts certain positions are exposed to the possibility of corruption or the abuse of their position to a certain degree, those holding senior, prominent or important positions, with substantial authority over policy, operations or the use or allocation of government-owned resources, have much more influence and therefore normally pose greater risks for a bank and should accordingly be categorized as PEPs and below categories may also extend subject to frontline

knowledge for the purposes of control and oversight frameworks and categorized as PEP as well with the strong justifications and will be considered once a PEP is always PEP.

However, providing a definitive list of who could be classified as PEP is difficult, as the criteria is quite broad. Relevant factors could include assessing the nature of the Sri Lanka's political and legal system and its vulnerability to corruption & influence of the surroundings as per various publicly available position or information, independent indices, the official responsibilities of the individual's function, the nature of the title (honorary or salaried political function), the level of authority the individual has over governmental activities and over other officials, whether the function affords the individual access to significant government assets and funds or the ability to direct the awards of government tenders or contracts and whether the individual has links to an industry that is particularly prone to corruption.

At the minimum, following persons or beneficial owners of the account, should be identified and marked as PEP in the system including the non-individual relationships (where required), whether they are existing clients or new. The below list is not exhaustive and any person who fits in the definition of PEPs must be marked as PEP in the system post relevant approvals, subject to the knowledge of any first line staff and same needs to be properly documented in the PEP Risk assessment forms along with other documentation for audit trail.

## DOMESTIC PEPs

A.	1	The President
	2	The Prime Minister
	3	The Speaker and the Deputy Speaker of the Parliament
	4	Cabinet Ministers, Non-Cabinet Ministers, State Ministers, Deputy Ministers
	5	Members of Parliament
	6	Leaders of Political Parties
B	7	Governors of Provinces
	8	Chief Ministers of Provinces
	9	Mayor, Chairman of Municipal Councils
	10	Chairman of Provincial Councils
	11	Members of Municipal Councils/ Provincial Councils / Local Government Bodies
	12	Commissioners/ Secretaries to Municipal Councils/ Provincial Councils / Local Government Bodies
C	13	Chief Justice
	14	Attorney General
	15	Judges of Supreme Court



	16	Judges of the Court of Appeal
	17	Solicitor General of the Attorney General's Department
	18	Judges of High Courts/Provincial High Courts
	19	Judges of District Courts
	20	Judges of Magistrate Courts
	21	Registrar of Supreme Court
	22	Registrar of the Court of Appeal
	23	Registrars of Judges of High Courts/Provincial High Courts
	24	Registrars of District Courts
	25	Registrars of Magistrate Courts
D	26	Ambassadors /High Commissioners
	27	Consul-General/ Deputy Head of Mission/Charge d'affaires/Honorary Consul
	28	Ministers plenipotentiary and Envoys Extraordinary
	29	Representatives of UN agencies and Heads of other international organizations
E	30	Secretary/ Senior Additional Secretaries/ Additional Secretaries to the President
	31	Secretary/ Senior Additional Secretaries/ Additional Secretaries to the Prime Minister
	32	Secretary /Senior Additional Secretaries/ Additional Secretaries to the Cabinet of Ministers, Non-Cabinet Ministers, State Ministers, Deputy Ministers
	33	Deputy Secretary to the Treasury
	34	Secretary/ Senior Additional Secretaries /Additional Secretaries/ Deputy Secretaries to Ministries
	35	Members of the Monetary Board
	36	Governor / Deputy Governors / Assistant Governors and Heads and Additional Heads of Department of the Central Bank of Sri Lanka
	37	Advisors to the President/ Prime Minister / Ministers/ Ministries
	38	Chief of staff of presidential secretariat
	39	Auditor General
	40	Secretary General of Parliament
	41	District Secretaries/ Government Agent and Secretaries
	42	Heads and Senior Officials of Government Departments

	43	Chairmen and Senior Officials of State Enterprises
	44	Chairmen and Senior Officials of State Corporations / Statutory Boards/ Authorities/ Public Corporations
F	45	Field Marshall / Admiral of the Fleet/ Marshal of the Air Force
	46	Chief of Defense Staff
	47	General of Sri Lanka Army/Admiral of Sri Lanka Navy/ Air Chief Marshal of Sri Lanka Air Force
	48	Officers in the Rank of Lieutenant Colonel and above of Sri Lanka Army
	49	Officers in the Rank of Commander and above of Sri Lanka Navy
	50	Officers in the Rank of Wing Commander and above of Sri Lanka Air Force
	51	Inspector General of Police
	52	Police officers above the rank of Asst. Superintendent of Police
	52	Police officers above the rank of Asst. Superintendent of Police
G	53	Chairman/ members and senior officers of the Public Service Commission
	54	Chairman/ members and senior officers of the National Police Commission
	55	Chairman/ members and senior officers of the Human Right Commission
	56	Chairman/ members and senior officers of the Commission to Investigation Allegations of Bribery or Corruption
	57	Chairman/ members and senior officers of the Finance Commission
	58	Chairman/ members and senior officers of the Election Commission
	59	Members of Constitutional Council
	60	Chairman/ members and senior officers of the Audi Service Commission
	61	Chairman / members and senior officers of the Delimitation Commission
	62	Chairman / members and senior officers of the National Procurement Commission
	63	Members of Cabinet appointed committees
	64	Chairman, Members and senior officers of University Grant Commission
	65	Chairman, members of University Councils
	66	Chancellor
	67	Vice Chancellor

	68	Registrar of Universities

## FOREIGN PEPs

I	69	Officials of international organizations who hold or have held, in the course of the last 5 years, management positions in such organizations (directors, heads of the boards or their deputies)
	70	Officials of international organization who perform or performed any other management functions on the highest level, particularly in international and intergovernmental organizations,
	71	Members of international parliamentary assemblies,
	72	Judges and management officials of international courts

Note: Guidelines on Identification of Politically Exposed Persons No. 03 of 2019 - issued by FIU of Sri Lanka should be complied with in identification of PEPs

### 4.1.4.4 Minimum measures for identification of a PEP or their “family member or close associates”

The following measures at minimum would be appropriate and effective to identify and to assess the PEP risk:

- Making enquiries regarding the PEP status of prospective customers during the account opening process and completing the KYC
- Screening of prospective customers and key principals of the overall customer relationship on ongoing basis as per bank’s process.
- Searching for publicly available information from independent sources such as Google Searches, Lexis Nexis, etc. but not limited to the knowledge of frontline staff only.

### 4.1.4.5 PEP Risk Assessment Process

Identification of PEP, Close Associate and Family members of the PEP is the responsibility of first line (Business i.e., Branch manager/branch ops manager/ Relationship Managers/any responsible person) in addition to completion of all formalities including the PEP Risk assessment forms (Refer Annex IX). Business will be responsible for performing Adverse Media searches provide updates and make recommendations for onboarding and retaining of the customer in case of adverse media. Subsequently the same will be forwarded to the Compliance Team to conclude its decision based on the screening results provided by the first Line and post analysis and re-assess the risk associated with the PEP profile.

Relationship with PEPs shall be established with the necessary approval from the Country Manager, Head of Compliance and Head of Business as bank’s senior management approval. Periodic review will be performed as per the process.

First line staff should apply the following procedures, while doing/performing the risk assessment

- Understanding and documenting occupation, source of income, source of wealth source of funds and further information and analysis of the PEP customer.
- conduct enhanced ongoing monitoring of business relationships with the politically exposed person.
- Understanding and documenting the length of PEP's holding position,
- The title or position and country in which the PEP holds, or held, political exposure.
- If the individual customer is a close family member or close associate, the relationship of the person to the PEP and background of the individual customer must be documented in the PEP Risk assessment form.
- In case the customer is determined to be a domestic/international organization PEP, then FIs should gather sufficient information to understand the particular characteristics of the public functions that the PEP has been entrusted with and, in the case of an international organization, the business model of that organization. Information on international organizations, for example, may be found on their respective websites.

#### **4.1.4.6 Identification of PEP for NTB and ETB Customer**

New Bank Customers (NTB): Bank has risk-based procedures to determine whether a customer is a PEP, before establishing the relationship. Once a new customer is determined to be a PEP, the Bank should risk assess the customer and categorize as rule based.

Existing to Bank Customers (ETB): KYC is the responsibility of the first line where the Bank (business team) becomes aware that an individual has become a PEP under event driven or Periodic review, then the same standard process should be followed.

Following are some instances where institutions are required to update its customer status relating to PEPs.

- a. when a customer spontaneously submits a new declaration of political exposure.
- b. when ongoing monitoring reveals activities or information that deviate significantly from the customer and/or account profile in a manner that suggests previously unknown political exposure.
- c. When an election is held that affects any of the customer's PEP statue.
- d. whenever the FIs becomes aware, through any means, of the need for such an update.

#### **Important Notes:**

The approval trial should be kept and attached with the account opening documents for record purpose and for any further reference and audit trail at branch end, where the archiving will be done.

In case of NTB, until the account is reviewed and approved by the authorized parties, as mentioned above, the Account shall not be opened / activated, and no transactions shall be allowed until activation. In case of existing customers account will be treated as overdue KYC until the account is reviewed and approved by the authorized parties, as mentioned above.

Compliance may request additional documents / information, if required such as income proof in case of individual PEPs etc.

Where the level or type of activity in the business relationship is different from what can be reasonably explained, given the knowledge of a PEP's sources of funds and sources of wealth, bank should undertake a further assessment on the business relationship to establish whether to:

- a. continues with or terminate the business relationship; or
- b. file a suspicious transaction report to the FIU.

#### **4.1.4.7 Compliance Management Information Reports**

In order to Continuously monitor and evaluate critical and high-risk areas, it is very important to have a well-structured Compliance Management Information Reports in place. For taking rational decision, timely and reliable information is essential and is procured through a logical and well-structured method of information collecting, processing and disseminating for decision making. HBL Sri Lanka has documented a procedure for Compliance information reports which is annexed in this procedure as Annexure VII.

## **5. TRANSACTION MONITORING**

The Compliance department HBLSL monitors customer transactions including customer's behavior and patterns of transactions among others detailed as below. Compliance is also a focal point for internal SARs / STRs within the bank for analyzing the suspicions and concerns for onward reporting to the FIU.

### **5.1 System Based Transaction Monitoring**

To mitigate the financial, reputational and regulatory risk and in order to safeguard the Bank against money laundering & terrorist financing activities and to comply with requirement laid down in bank Global AML, KYC, CPF & KYC policy, HBL has come up with the automated system named FCCM to facilitate proper alerts and case management and ensure sufficient audit evidence. The system, based on the calibration performed by the bank, is generating AML alerts which have to be resolved using the workflows implemented.

Compliance will be responsible to review and analyze system generated transaction monitoring alerts through FCCM application which is an Anti-Money Laundering Solution that uses sophisticated data mining and pattern detection techniques to identify possible money laundering and suspicious behavior.

Compliance will review the effectiveness / revision of the scenarios & thresholds on an ongoing basis (minimum once every 2 years) and request will be forwarded to international Compliance upon recommendation of Country Compliance Head for onward approval of Chief Compliance Officer to make necessary changes in the system.

## 5.2 FCCM Modules

FCCM is composed of the following components which are relevant for this document:

- Behavior Detection – a module that uses pattern recognition techniques to identify behaviors of interest, or scenarios that are indicative of potentially interesting behavior. A pattern is a specific set of detection logic and matches generation criteria for a particular type of behavior. When one or more data records equal a scenario's pattern of behavior, a match is created. Records that contribute to the exhibition of behavior are associated to the match as matched records are displayed in the Alert Management as building blocks. The Alert Management generates an alert to package one or more matches for analysis and action.
- Alert Management – a module that provides a user interface and workflow for managing alerts, reporting and searching business data.
- Case Management – a module that manages and tracks the investigation and resolution of Cases related to one or more business entities involved in potentially suspicious behavior.
- Analytical Reports – a dynamic reporting tool with predefined MIS reports.

## 5.3 Access rights, roles and alerts distribution

The system has a mechanism to assign alerts to a predefined owner. When performing alert assignment, the module fetches new, unowned alerts for a given product and assigns them to FCCM Users based on pre- defined criteria. One of the basic principles supporting quality is the four-eyes principle. FCCM permits dual control that requires an authorized user (for example, a supervisor) to approve actions of other users prior to those actions taking full effect on the alert (for example, closing the alert).

## 5.4 Alert Scoring

All transaction monitoring system alerts are generated with alert risk score based on predefined risk scoring criteria. Alert Risk Score provided the following benefits.

- time reduction and resource focused on alerts with higher risk attributes
- increase the possibility that potential suspicious activity is detected if the alert is flagged as “High risk” and appropriate investigation efforts are allocated
- reduced time to detect suspicious activity and submit SAR, as alerts are prioritized based on their probability of resulting in a SAR
- enabled to estimate the remaining risk in the backlog and more efficient processing of it optimized the effort put into the investigation of an alert.

Category	Score Range
Low Risk	0 – 39
Medium Risk	40 – 56
High Risk	57 – 100

## 5.5 Active AML Scenarios

HBL SL is currently using the following FCCM AML Scenarios as per their assigned frequencies:

Scenario	Scenario Description	Frequency
HR Trans – Fo- cal HRE	Financial institutions must apply enhanced scrutiny to transactions involving high-risk entities, as such activity that may subject the institution to a greater risk of money laundering or fraud. Any account, customer, correspondent bank, or external entity found on a watch list is considered to be a high-risk entity. This scenario monitors transactions to and from high-risk entities during a specified Lookback Period.	Daily
Journal Bet Unrelated	<p>Money launderers may establish a number of accounts within a single institution, often establishing relationships at multiple branches using aliases or slightly different identifying information. They then move their money between accounts as part of a layering strategy, often consolidating the funds in a single account before removing them from the institution. Without a known link, institutions have an extremely difficult time identifying these relationships. This scenario detects an account that conducts journal transactions to one or more unrelated accounts.</p> <p>A journal transaction is considered unrelated when the transaction occurs between accounts that do not share tax identifiers, do not share a customer, are not in the same household, and are not known to have a formal relationship. The aggregated value for all transactions must be higher than a specified threshold, and the transactions must be conducted within a specified Lookback Period (for example, 14 calendar days).</p>	Fortnightly
CIB - Previous Average Ac- tivity	A sudden change in transaction activity may be suspicious and warrant additional investigation. The large number of various types of transactions within an account including funds transfers, checks presented, cash deposits, etc. on daily basis makes it very difficult to detect changes or anomalies in account activity. The product monitors transaction activity and detects significant changes from the typical activity of an account. This scenario identifies accounts and correspondent banks that may be considered to be at risk by monitoring electronic funds transfers, check,	Monthly

	monetary instrument, cash and journal activity and detecting significant changes from the average of previous monthly transaction activity.	
CIB - Previous Average Activity	A sudden change in transaction activity may be suspicious and warrant additional investigation. The large number of various types of transactions within an account including funds transfers, checks presented, cash deposits, etc. on daily basis makes it very difficult to detect changes or anomalies in account activity. The product monitors transaction activity and detects significant changes from the typical activity of an account. This scenario identifies accounts and correspondent banks that may be considered to be at risk by monitoring electronic funds transfers, check, monetary instrument, cash and journal activity and detecting significant changes from the average of previous monthly transaction activity.	Monthly
CIB - Previous Average Activity	A sudden change in transaction activity may be suspicious and warrant additional investigation. The large number of various types of transactions within an account including funds transfers, checks presented, cash deposits, etc. on daily basis makes it very difficult to detect changes or anomalies in account activity. The product monitors transaction activity and detects significant changes from the typical activity of an account. This scenario identifies accounts and correspondent banks that may be considered to be at risk by monitoring electronic funds transfers, check, monetary instrument, cash and journal activity and detecting significant changes from the average of previous monthly transaction activity.	Monthly
CIB - Product Utilization	A sudden change in transaction activity may be suspicious and warrant additional investigation. The large number of various types of transactions within an account including funds transfers, checks presented, cash deposits, and so forth on daily basis makes it very difficult to detect changes or anomalies in account activity. The product monitors transaction activity and detects significant changes from the typical activity of an account. This scenario identifies accounts and correspondent banks that may be considered to be at risk by monitoring for changes in the types of products that are utilized by the account, (product utilization shift)	Monthly



	among electronic funds transfers, check, monetary instrument, cash, and journal transactions.	
Rapid Mvmt Funds - All Activity	Money launderers typically move funds between accounts to help integrate the funds and give the appearance of legitimacy. One possible indication of money laundering activity is the rapid movement of funds into and out of an account. The scenario detects both new ac- counts/customers and more seasoned accounts/customers that move transactions of all types in and out of an account or accounts within a specified Lookback Period. The scenario can take into account the amount or velocity of funds through the account relative to the account balance or net worth.	Monthly
Escalation Inactive AC	Money launderers may open accounts, deposit illicit funds, conduct a small number of transactions to test the system, and then leave the ac- count alone for a period to avoid raising suspicions. They then remove a significant portion of the balance of the account, often leaving the remaining balance behind to avoid detection. This scenario generates an alert for accounts that are inactive for a predefined period and then have a sudden escalation in activity. It identifies accounts that may be considered to be at risk based on the number, amount, or a large portion of recent transactions in contrast to its previous dormant status. The client's risk exposure is greater for outgoing funds relative to incoming funds. The system then monitors significant withdrawal activity at more stringent thresholds than deposit activity.	Daily
Lg. Depreciation Acct. Value	A large and sudden debit, or series of debits, from an account causing a significant depreciation in the account's net worth could signal account takeover or other type of fraudulent activity. This scenario identifies ac- counts that experience a significant value depreciation within a specified period. The scenario also distinguishes between new and seasoned accounts based on the account open date.	Fortnightly
Dep/WD Same Amts.	Most deposits and withdrawals of funds into and out of an account are done for specific purposes and therefore occur in varying amounts. The occurrence of repetitive patterns, or a high percentage, of deposits or withdrawals in the same amount or similar amount, may be unusual activity for the account or customer. This type of activity may indicate attempts to structure funds into	Fortnightly

		the institution or remit funds in a structured manner to fund illicit activities. This scenario detects patterns of deposits and/or withdrawals made in the same or similar amounts that aggregate above specified thresholds. The specification of similar amounts is configurable.	
--	--	--	--

Escalation AC	Inactive	Money launderers may open accounts, deposit illicit funds, conduct a small number of transactions to test the system, and then leave the account alone for a period to avoid raising suspicions. They then remove a significant portion of the balance of the account, often leaving the remaining balance behind to avoid detection. This scenario generates an alert for accounts that are inactive for a predefined period and then have a sudden escalation in activity. It identifies accounts that may be considered to be at risk based on the number, amount, or a large portion of recent transactions in contrast to its previous dormant status. The client's risk exposure is greater for outgoing funds relative to incoming funds. The system then monitors significant withdrawal activity at more stringent thresholds than deposit activity.	Daily
Lg. Depreciation Acct. Value		A large and sudden debit, or series of debits, from an account causing a significant depreciation in the account's net worth could signal account takeover or other type of fraudulent activity. This scenario identifies accounts that experience a significant value depreciation within a specified period. The scenario also distinguishes between new and seasoned accounts based on the account open date.	Fortnightly
Dep/WD	Same Amts.	Most deposits and withdrawals of funds into and out of an account are done for specific purposes and therefore occur in varying amounts. The occurrence of repetitive patterns, or a high percentage, of deposits or withdrawals in the same amount or similar amount, may be unusual activity for the account or customer. This type of activity may indicate attempts to structure funds into the institution or remit funds in a structured manner to fund illicit activities. This scenario detects patterns of deposits and/or withdrawals made in the same or similar amounts that aggregate above specified thresholds. The specification of similar amounts is configurable.	Fortnightly

Trans - Round Amts.	Most electronic funds transfers (EFT) or monetary instruments are done for a specific purpose and, therefore, in a precise amount. The occurrence of a high percentage of transactions in round amounts may be indicative of attempts to launder funds or perpetrate fraud. This scenario detects patterns of EFT or monetary instruments in round amounts that in the aggregate satisfy specified thresholds.	Fortnightly
Structuring: Avoid Report Threshold	Money launderers seeking to place or move funds in the banking system may structure their cash or monetary instrument transactions to avoid reporting requirements, such as the filing of a currency transaction report (CTR) or other report required in a given country. The institution may wish to monitor more closely any accounts, customers, households, or external entities engaging in such activity. Oracle detects instances of cash or monetary instrument transaction(s) in amounts just below applicable reporting thresholds during a specified Lookback Period. The scenario supports the use of multiple thresholds sets to accommodate reporting requirements that may differ by country or jurisdiction, as well as to support multiple thresholds within a country or jurisdiction (that is, support of CTR and cash log thresholds can occur simultaneously).	Weekly /
Large Reportable Trans	Certain countries require that financial institutions report customer transactions that exceed a specified threshold. These requirements typically pertain to new customer relationships and transactions associated with account opening. They may also pertain to existing customer relationships. Clients may also have internal policies that require the reporting or review of transactions exceeding certain amounts. This scenario detects deposits of any type (across products and asset types), made at account opening or within a certain period after account opening, which exceed a specified threshold. The definition of new account is configurable. The scenario also detects deposits or withdrawals of any type (across products and asset types) in existing accounts that exceed a certain threshold. The scenario detects such transactions involving a single account or multiple accounts that are linked to the customer or household through the client's householding process. The scenario provides separate thresholds for each type of relationship (new or existing) that are tunable to support client and country specific regulatory requirements.	Fortnightly

Pot Structuring Cash and Equivalents	Money launderers seeking to place or move funds in the banking system may structure their cash or monetary instrument transactions to avoid reporting requirements, such as the filing of a currency transaction report (CTR) or other report required in a given country. The institution may wish to monitor more closely any customers, engaging in such activity. This scenario identifies when a customer shows a pattern of conducting significant transactions in cash and cash equivalents that aggregate above reporting thresholds. These episodes of structuring may occur on individual days or spread across multiple days. This behavior may indicate that a customer is breaking up large amounts of cash into multiple smaller transactions in order to avoid scrutiny.	
Terrorist Financing	<p>Government and international agencies have published anecdotal information on how known terrorists and terrorist organizations move funds between countries, organizations, and individuals that are part of terrorist cells. Many examples focus on the fact that accounts opened by known terrorists at U.S. institutions were titled in multiple names, and the nature of the activity involved relatively small transaction amounts. Some of these typologies or examples are detectable through other Mantas scenarios. However, this scenario focuses specifically on activity involving frequent, structured transactions in relatively small amounts achieved through funds transfers or through checks and monetary instrument activity.</p> <p>The scenario provides additional logic to support targeted detection of efforts to move funds to or from multiple individuals or organizations, including seemingly unrelated entities that share accounts or are associated with multiple accounts. This scenario considers both debits and credits for Electronic Funds Transfers (EFTs), Checks, and Monetary Instruments. Debit and credits are treated in absolute values, disregarding the sign (+/-) for the amount.</p>	

In addition to the above system inbuilt scenarios, the following two scenarios will also be deployed in FCCM system.

The above scenarios will be subject to the changes as and when required upon necessary approvals by HBL - PAKISTAN authorities.

## 5.6 Customer Segmentation

Customer Segmentation in FCCM (updated version) group customers together that have similar transactional patterns so that thresholds set per segment detect unusual activities. Currently applicable segments are provided below.

Category	Segment
CORP	This captures all customer accounts defined as corporate Public Limited Companies
EMPL	This jurisdiction covers all HBL SL Employee Accounts
FINS_GOV	This is focused on Financial Institution and Government
T HRSK	Organizations This captures certain customer types that carry an inherent risk such as DIPLOMAT, CLUB/ASSOCIATION/TRUST/ETC (NON-PRO), FOREIGN MISSION, etc....
INDV	This focuses on the individual customers
BIND	This is assigned to capture accounts that are opened under the name of individuals to conduct business transactions
PR_P	This scenario captures all non-individual entities that does not fall under the above categories of CORP, FINS_GOV, BIND and INDV

## 5.7 Alert Management

Alerts in the Alert Management might be found in the following statuses:

New	The application has generated an alert, and the analyst has not yet viewed the alert detailed information.
Open	Analyst has viewed the alert detail information.
Follow-Up	When analyst recommends alert for closure, closure with SAR, and when authorized user takes action of "With Manager
Reassigned	An authorized user has assigned the alert to another owner, and the new owner may not yet have viewed the details of the alert.
Rework	An authorized user considered the quality of work insufficient, or the conclusion met was wrong and has sent back the alert to the analyst.
Closed	Authorized User has closed the alert after proper analysis. Option is also available for requesting KYC update subsequent to closure or Alert.

**Reopened**

An authorized user has opened an alert that had previously been closed (new owner may not yet view the reopened alert).

Alerts are reviewed based on the current transaction pattern, available KYC information, historical transactions & feedback (RFIs) on earlier alerts generated against the same customer. If transactions under review are found to be consistent with customer's KYC information, such alerts may be recommended for closure by compliance analyst and closed by supervisor with appropriate remarks/comments.

However, if the available information is not sufficient/satisfactory or further information is required from the customer and or relevant branch/department, an inquiry will be sent to the business (RFI).

## 5.8 Case Management

Once an alert is promoted to a case, it will be subject to Case Management. Case Management is providing more options when it comes to a range of investigative steps to be performed on an alert. You can create a case manually, when it's not deriving from an alert.

## 5.9 Actions available

In order to act on an alert, after a proper analysis, the user has a catalogue of actions available in the system (alert and case module). Key actions are presented below.

Action	Description
Viewed by Owner	An eligible user has viewed an alert or case that has been assigned to them or to a user group to which they have access.
Recommend for closure	Alert was recommended for closure after proper analysis was carried out. These may include, analysis of transactional pattern and how it commensurate with KYC information.
Recommend for closure – SAR	Alert was recommended for closure with SAR/STR after proper analysis was carried out. These may include, but is not limited to, analysis of transactional pattern and how it commensurate with KYC information.
Recommend Promotion to Case	Alert was recommended for promotion to case after proper analysis was carried out.
With Manager	When there are doubts regarding the next steps or the alert is requiring manager's attention, it can be escalated to a manager using "with manager" action.
Reassign	An authorized user has assigned the alert to another owner. Reassign should be used when there the initial analyst is not available, or alert require specific knowledge.

Invalid Alert (Recommendation)	When an alert was generated based on incorrect tagging or any other justifiable reason, for example where the account holder is a corporate customer, but the threshold applied is for an individual customer (as per system information). Such situations should be raised with the manager/supervisor.
Duplicate Alert (Recommendation)	When an alert is a duplicate of an alert already investigated (same transaction, same scenario etc.).
Rejected	An authorized user considered the quality of work insufficient, or the conclusion met was wrong and has sent back the alert to the analyst.
Reject Promote to Case	An authorized user considered the quality of work insufficient, or the conclusion met was wrong and has sent back the alert to the analyst.
Invalid Alert	An authorized user, after a proper verification and quality control, accepts the recommendation of an analyst.
Duplicate Alert	An authorized user, after a proper verification and quality control, accepts the recommendation of an analyst.
Promote to Case	An authorized user considered the quality of work sufficient, and an alert was promoted to a case.
Close and Initiate SAR Module	An authorized user considered the quality of work sufficient and accepted recommendation for closure.
Internally (closed)	An authorized user considered the quality of work sufficient and accepted recommendation for closure.
Print Summary	Action used to print a summary of an alert.
Print Comments	Action used to print comments added to an alert.
Print Details	Action used to generate a report with alert details.
Add Comment	This action enables you to add a comment to an alert.
Add Attachment	This action enables you to add an attachment to an alert.

#### **New alert which is related to already generated alert:**

If the related alert is already promoted to a case, user may follow one of the options:

- Link the alert with the same case or recommend the alert for closure (with proper comments including Alert / Case ID).
- Recommend this alert for new case, accordingly checker will promote to case, link this new case with existing case

## 5.10 Roles & Responsibilities

### ROLE OF MAKER (COMPLIANCE ANALYST)

- After conducting investigation on alert/case, Maker (compliance Analyst) will close the alert/case if no anomalies were identified, and the account activities are in line with the declared profile of the customer.
- However, if the Maker is not satisfied with the account activities/ transactions of the customer even after conducting further investigation such as raising a RFI to branch/Relationship Manager, the Maker is required to escalate the same to Checker (Respective Supervisor).
- While reassigning the alert to checker, maker should clearly mention his/her findings and attach necessary documents, if any i.e. Branch Response, supporting documents submitted by branch, Internet searches, etc. using “Save and Attach” option.
- In case of possible suspicion, analysts will recommend alert/case for SAR with detailed findings and reason of suspicion.
- In case the alert is rejected by the checker for closure, the maker will have to review the observations made by the checker.

### ROLE OF CHECKER (SUPERVISOR)

- Checker (Team Leader) will review the alerts/cases assigned to him/her by respective analyst.
- After reviewing the Maker’s findings, Checker will either “approve” or “reject” the alert/case for closure within defined TAT.
- In case alerts/cases recommended for SAR, checker will review the reason of suspicion and if agree he/she will close the alert/case with SAR for onward reporting of STR to FIU with consultation and approval from Head of Compliance Sri Lanka.
- In case of rejecting the closure of alert/case, Checker will provide reason for rejecting alert/case and / or suggest necessary action.
- Give at least one liner reason for approving the alert/case for closure in comment box for e.g. “Analysts findings are appropriate.”

Due to segregation of duties of Maker and Checker with reference to handling FCCM alerts/cases, audit trail will be captured in FCCM under “Audit History” tab enabling system to track the record of Alert/Case for reference at later stage or in case required by regulators.

## 5.11 Request for Information (RFI) for alert management

Users of the system can request further information from the branch network in order to aid their investigation of alerts/cases. Information may include some sort of documentation / explanation / evidence from the client to support the investigation process.

- Alert is generated within FCCM for analysts to review.
- Upon review, if the analysts identify area to be questioned / additional details to be obtained the analyst will send an e-mail to the respective branch / unit requesting responses for the questions / documents
- Branch users respond via the same email keeping audit trail and provide analyst with all relevant information.
- Such e-mails are attached to the alert / alerts the query was raised in the system.



- In instances where alerts generated on staff accounts, further information may be requested from HR team if branch responses are not sufficient to review the alerts.

## 5.12 Alert Handling Process

Alerts are generated on an ongoing basis depending upon the certain frequency period of each scenario. The process for the handling of alerts is as follows:

- New alerts generated by the system are assigned by default to the Compliance Team. All the alerts will be handled after adopting a Risk Based Approach.
- Currently there is no regulatory requirement on the turnaround time (TAT) for discounting transaction monitoring alerts. However, HBL group following a prudent approach and has established an internal TAT at 60 working days for discounting TMS alerts to ensure effective internal monitoring and the timely escalations of any unresolved alerts.
- Accordingly, Alerts will be handled and closed either on "Satisfactory" comment or "Unsatisfactory" comment before 60 working days from the date of generating the alert. When handling alerts, the Compliance analyst will obtain where needed proper responses with justification from relevant business. "Unsatisfactory" comment implies that the alert was closed with insufficient justification on the account/transaction conduct where the outcome of such closures would be to raise potential STR to regulator.
- If the alerted transaction aligns with the customer information i.e. KYC profile, transaction pattern, activity within an account, jurisdiction and assessment of historical alerts, the Compliance analyst may update the alert with his/her findings and alert will be qualified for upfront closure.
- If any transaction which requires additional clarity regarding purpose of transactional activity, source of funds, etc. then the query will be referred to the branches / business for the clarification on the alert.
- World check and internet searches may be performed, on case-by-case basis, after adopting risk-based approach and considering the customer's segment.
- Appropriate audit log for closing alerts will be maintained in the system.
- Compliance Analyst may cover the following points while reviewing the alerts:
  - o Pattern of transactions/ account activities over a reasonable period
  - o Review the alerted reason against customer's declared profile.
  - o Review the Alerted transaction(s) against the profile of customer and the customer's connection with transaction(s)
  - o Parties engaged in the transaction(s) if any and their relationship with the customer
  - o Any Correspondence the alerted transaction(s) have/had with Business (if any)
  - o Conclusion
- In case of suspicion, STR will be raised by the Compliance analyst with the consent of Compliance Supervisor along with consultation and approval from Head of Compliance for onward submission to FIU.
- STR will be reported to FIU on the format provided by them and all the information/ documents related to STR must be retained as per HBL Sri Lanka AML, CFT, CPF & KYC policy.

## **5.13 Roles & Responsibilities**

### **5.13.1 Role and Responsibility of Compliance Team along with Turn Around Time of Alert Resolution**

#### **Role of Maker (Alert Management Analyst)**

- After reviewing the assigned alert, the maker (Alerts Management Analyst) will submit the same to the checker on the same day.
- While recommending the alert to the checker, the maker should clearly mention the findings.
- In case further information is required, the analyst will recommend the alert to be promoted to a case to enable the relevant supervisor to review/approval.
- In case the alert is rejected by the checker for closure, the maker will have to review the observations made by the checker.
- After assessment, the analyst will decide if further reviews/ Information from branches/business are required. However, disposal of the alerts should be completed within 60 working days.
- Analyst, along with relevant Team leader, will be responsible to review and complete their analysis and conclude the alert either on satisfactory note or Unsatisfactory note within 60 working days of alert creation,
- Analysts will be responsible for taking an action as soon as possible on the alerts checked by the respective TL/Checker.

#### **Role of Checker**

- Checker will review the alerts recommended by respective Analyst.
- After reviewing the maker's findings, checker will either "approve" or "reject" the alert for closure within defined TAT.
- In case of rejecting the closure of alert, checker will provide reason for rejecting alert and / or suggest necessary action.
- Provide brief reason for approving the alert for closure in comment box for e.g., "Analysts findings are appropriate."

#### **Roles, Responsibilities & Authorities of Stakeholders along with levels of escalation**

##### **Level 1**

Alert escalated by Compliance analyst to branches for arranging any clarification/ assistance from business and operations team(s) with Cc to their respective Line Managers/ Supervisors.

##### **Level 2**

Compliance team will share the list of "Outstanding Alerts" on monthly basis with International Compliance-HBL - PAKISTAN through CCMI.

### Level 3

Compliance team will share the “Outstanding Alerts on Quarterly basis with Compliance Committee of Management of HBL SL.

#### 5.14 Staff Accounts

Staff accounts are deemed of less risk since the source of funds for this account are usually from the bank itself. However, any remittances of unusual values or from any other party apart for the employer itself will be questioned.

For monitoring of HBL - Staff accounts, the query will be referred both / either of the Branch Manager or Branch Operations Manager.

- The branch manager or branch operations manager will be responsible to arrange the responses on the Compliance queries on the concerned staff(s). The clarification may also necessitate the requirement of presenting any documentary evidence obtained during the transactions occurrence.
- All credit transactions related to official entitlements e.g. salary, expense reimbursements, house rent /staff loan etc. will not be inquired from staff and internally reviewed by Compliance.
- Routine debits clearly arising from staff salary and other official entitlements needs to be reviewed by Compliance. The same does not require inquiry and will be closed after review by compliance. Similarly, transfer of funds by staff to own account with HBL or other banks and clearly sourced from staff salary and other official entitlements, will be reviewed by Compliance for closure.
- If the Compliance Team is not satisfied with the conduct of the transaction, the case with necessary details must be escalated as per HR policies and procedure and the action will be taken as per the procedure in compliance with the Local Regulatory framework/ Bank’s Policy and applicable procedures.

Note: Upon exit of staff member from service, HR HBL SL will intimate operations for the changing of customer type to non-staff category and such will be dealt with like any other customer of the bank.

#### 5.15 MIS Reports in FCCM

Reports	Frequency
Alert Search	Weekly
Active Alerts Per User-Organization	Fortnightly
Active Cases Per User-Organization	Fortnightly
Alert Final Disposition	Fortnightly
List of Cases	Monthly
Account Entity Search	Monthly
Customer Entity Search	Monthly

Presently, standard reports are available on FCCM with standard functionalities which authorized user can access, as and when required, through reports menu available on FCCM as part of the primary navigation bar. Authorized user can utilize available standard filters to apply conditions to the individual reports. A menu has further drill down options to be utilized for additional analysis, if needed.

## **5.16 Reporting of STRs/CTRs/EFTs/IFTs to FIU**

Compliance will report STRs to Financial Intelligent Unit (FIU) based on the assessment made on the internal STR. Where the bank,

(a) has reasonable grounds to suspect that any transaction or attempted transaction may be related to the commission of any unlawful activity or any other criminal offence; or

(b) has information that it suspects may be relevant—

(i) to an act preparatory to an offence under the provisions of the Convention on the Suppression of Financing of Terrorism Act, No. 25 of 2005;

(ii) to an investigation or prosecution of a person or persons for an act constituting an unlawful activity or may otherwise be of assistance in the enforcement of the Money Laundering Act, No. 5 of 2006 and the Convention on the Suppression of Terrorist Financing Act, No. 25 of 2005, AML/CFT red flags and suspicious indicators to identify suspicious activities are given under Annex VI. Lists of Red flags applicable to different business units/banking functions provided by the regulator are also attached in Annexure VI.

### **5.16.1 Procedures for STRs**

- Compliance will report STRs post analyzing, received from any staff member within the bank, to FIU immediately but not later than 2 Working Days once the suspicion is established keeping in view the regulatory directives.
- The basis of determination to file STR or not shall be documented and kept in record together with all internal findings and analysis done in relation to the suspicions whether transactions are reported to FIU or not.
- Suspicious transactions will be reported regardless of the amount of the transaction.
- While reporting, business teams are requested to review the background and purpose of these suspicious transactions and findings shall be documented with a view to making this information available whenever required. The minimum documents (i.e. AOF and related documents, Counterparty details, support evidence for suspicion etc.) required to be submitted along with the internal STR form.
- From October 2022, the reporting of suspicious transactions, attempted transactions, or information to the FIU (collectively referred as STR reporting process) was changed from the previous LankaFIN system to the goAML system.
- STR reporting process of the goAML system consists of two report types. They are Suspicious Transaction Report (STR) and PAE Report (Follow-up report to STR to complete suspicion reporting). STR, which is a transaction report is used to report Transactions with related PAEs, while PAE Report, which is an activity report is used to report suspected Persons, Accounts, or Entities (PAEs) relating to the suspicion.

- It is important to note that submission of both the above reports (STR & PAE Report) are mandatory for the completion of STR reporting process to the goAML system, for every suspicious transaction, attempted transactions, or information.
- Please refer the Annexure X for the process of filing STR through goAML system. (Please note that the process of reporting may subject to change by the regulator)
- Bank shall not disclose any information to any other person in line with the Section 9(1) & 10(1) of the FTRA No. 06 of 2006.
- As per Guidelines for Financial Institutions on Keeping Accounts in Suspicious Transaction Reports, Under Surveillance, No. 01 of 2022, the below process is noted and followed at HBSL:
  - FIs are required to closely monitor the reported accounts informed by FIU to be Kept Under Surveillance (KUS), for a period of three months, unless specified otherwise and submit a report to the FIU within three working days from the end of the period of three months or the end of the specified period on whether the reported suspicious transactions are continuing or not.
  - Upon the lapse of the three-month period, if the bank do not receive instructions to the contrary from the FIU or instructions to extend the period of surveillance mentioned in above guideline upon lapse of the aforementioned three-month or specific period, the bank shall treat such STRs as STRs that have exited the KUS mode.
  - Notwithstanding the above, the bank should immediately report any special circumstances of which several are listed below that occurred during these three-month period or specified period, to the FIU.
    - Customer requests to close the reported account.
    - Significant deposits/ withdrawals to/from the reported account does not line with the declared profile.
    - Change in the transaction pattern/ emergence of new trends (this does not encompass the continuity of the previously identified transaction pattern/ trend).
    - Change of ownership/ control of the reported account.
    - Significant changes in Know Your Customer/ Customer Due Diligence details.
  - In the event of an escalation of the reported suspicion, immediate action should be taken by the bank to report further suspicion.
  - Moreover, the bank may follow the instructions given by the FIU after reporting the activities of the reported account at the end of the above-mentioned three-month period.
  - In the event Branch/Relationship Manager identifies suspicious transaction/ account activity during the course of operations the same should be escalated immediately to Compliance through an Email using the recommended format (Annexure XII). Upon the receipt of the same Compliance department will perform an investigation and will take necessary steps such as either file a SAR, keep under surveillance for close monitoring or close as no action required.

### **5.16.2 Procedures for CTRs, EFTs & IFTs**

In terms of the Financial Transaction Reporting Act, all cash transactions, all electronic fund transactions and International Fund transactions of Rs. 1 million (or equivalent foreign currency) and above must be reported to FIU within 31 days of processing the transaction.

The goAML application is a fully integrated software solution developed specifically for use by Financial Intelligence Units (FIU's) and is one of UNODC's strategic responses to financial crime, including money-laundering and terrorist financing.

And as per the instructions given by FIU the Cash Transactions Reporting (CTR), Electronic Fund Transfers (EFT) and International Fund Transfers (IFT) are reported to FIU through goAML system. Currently automation of reports is taking place from manual reporting to XML report upload. Until the automation of goAML system is fully implemented a manual uploading of the reports is noted as mentioned below,

- IT department to extract all qualifying transactions (Refer Annex 1) on a weekly basis that exceeds the threshold of LKR 1 million on Rupee or equivalent in any other currency before 10.00 a.m on the first working day of the following week of the transaction that occurred on the previous week and share it with a party appointed by Head of Country Operation by keeping Compliance Sri Lanka team and Head of Country Operation in copy.
- Upon communication of the data from IT the operations department through its assigned members will start entering the data where this must be completed within the week it was received from IT after coordinating/obtaining required information from the relevant branches/department
- Upon completion of feeding of transaction data into the system but prior to generating XML report, the relevant files/transactions should be validated by the Checker to ensure all eligibility transactions/scenarios are captured and there are not any missing transactions relevant for the period. A confirmation email should be provided to the Maker while retaining records of the validations/checks performed for Audit purposes. Upon receipt of the confirmation email, the Maker will generate the XML report and coordinate with IT department for generating the Hash codes report using the validator Tool.
- Once the Hash code added reports are received back from IT, the same will be shared with the Compliance Department for uploading.
- Upon receipt of notification the Compliance Department will submit the file to the Central bank and closely follow it up for the status of the file. Irrespective of whether it is rejected / unable to be submitted or accepted by Central Bank the Compliance department will communicate to the Operations Department immediately through an e-mail The status of the upload.
- Upon communication of rejection or any other errors, the relevant operations department will do the error correction preferably within the same day and inform Compliance of the Completion.
- In order to facilitate the parties who upload the data and transaction to the FIU website and to ensure data availability at ease the branches, centralized clearing, centralized RTGS, trade department and treasury back office should maintain a tracker of all transactions above LKR 1 million.
- The Central Operations Department shall keep a proper tracker in place to monitor report (all three types-CTR, IFT and EFT) submissions, transactions/file rejections, report/transaction resubmissions to ease identification of transactions uploaded to FIU. Further, the department should ensure through random checks that all relevant transactions have been uploaded on a periodic basis.

## **6. TRADE COMPLIANCE ADVISORY**

Sri Lanka Compliance team acts upon escalations, decide and advise first line of defense on trade sanctions and trade-based money laundering concerns and guide further course of action. Trade-based money laundering is a process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimize their illicit origin.

The use of trade finance to obscure the illegal movement of funds includes methods to misrepresent the price, quality or quantity of goods. Generally, these techniques rely upon collusion between the seller and buyer, since the intended outcome from such arrangements is obtaining a benefit in

excess of what would be expected from an arm's length transaction. The collusion may arise because both parties are controlled by the same persons.

## **6.1 Main methods of TBML**

The transfer of value in TBML may be accomplished in a variety of ways some of which are described briefly below:

### **6.1.1 Over Invoicing:**

This is done by misrepresenting the price of the goods in the invoice and other documentation (stating it at above the true value) the seller gains excess value as a result of the payment.

### **6.1.2 Under Invoicing:**

This is done by misrepresenting the price of the goods in the invoice and other documentation (stating it as below the true value) the buyer gains excess value when the payment is made.

### **6.1.3 Multiple Invoicing:**

This is done by issuing more than one invoice for the same goods a seller can justify the receipt of multiple payments. This will be harder to detect if the colluding parties use more than one FI to facilitate the payments and or transactions.

### **6.1.4 Short Shipping:**

In this method, the seller ships less than the invoiced quantity or quality of goods thereby misrepresenting the true value of goods in the documents. The effect is similar to over invoicing.

### **6.1.5 Over Shipping:**

The seller ships more than the invoiced quantity or quality of goods thereby misrepresenting the true value of goods in the documents. The effect is similar to under invoicing.

### **6.1.6 Deliberate obfuscation of the Type of Goods**

In this method, parties involved may structure a transaction in a way to avoid alerting any suspicion or to other third parties, which become involved. This may simply involve omitting information from the relevant documentation or deliberately disguising or falsifying it. This activity may or may not involve a degree of collusion between the parties involved and may be for a variety of reasons or purposes.

### **6.1.7 Phantom Shipping**

The trade transaction where no goods are shipped, and all documentation is completely falsified.

## **6.2 Due Diligence Checks**

The following are due diligence checks that should be conducted by 1st line of defense role while conducting trade finance transactions:

### **6.2.1 Identification of Customer's Line of Business:**

In order to mitigate TBML risk, Business must ensure that Due Diligence with reference to trade is being conducted at the time of customer on boarding by acquiring relevant details to identify line of business, which includes the following but not limited to.

- Details of Customer Interest in Trade Product and Services of the Bank
- Detail of Local and International Counter Parties
- Detail of Counter Parties related to Customer (Related Parties)
- Nature of Goods in which Client or Counterparty is dealing with

Trade HBLSL to review updated KYC in MISYS system before processing any transaction. The compliance team shall further review cases escalated by Trade. In case of any ambiguity, the Compliance team shall initiate Request for Information (RFI).

### **6.2.2 Identification of Clients Dealing in Defense or Dual Use Goods:**

The risk associated with the clients dealing in Defense or dual use goods is part of client onboarding process. The following scenarios cover risk, where the client deals in defense or dual use goods:

- Client dealing with defense bodies or agencies
- Dealings with corporations where defense or dual use goods represent a line of business ?  
Goods description in which our client is dealing.
- Explanation of Application of goods.
- Dealing with clients who are proprietors, partners or promoters or majority shareholders in a defense business concern.
- List of counterparties with whom client shall be dealing in his relationship with HBL.

The bank shall consider transactions pertaining to defense or dual use goods strictly on a case-case basis subject to the following:

- Clear understanding of the nature of goods
- The country of manufacture of goods
- The country of import or export of goods
- Purpose of goods being imported or exported
- End Use of goods being imported or exported

Business shall ensure that all relevant details are obtained from the customer, which shall provide all necessary details to relevant stakeholders as and when required or when RFI is initiated in this regard.

Trade shall refer transactions pertaining to Defense or Dual Use Goods to TBML HBL - PAKISTAN or Compliance Team, and if required Compliance team shall escalate to Head, FCC and International Compliance Department at HBL - Pakistan.



### **6.2.3 Goods Description and Pricing Factor of Goods:**

Goods description specified on the invoice presented under the Import or Export document shall be clear and shall be in line with the Documentary Credit or Contract signed between importer and exporter. In case where pricing of goods is not listed in the Price List, Trade shall refer to search engines to conduct advanced search on relevant pricing of goods in order to mitigate the element of Over/Under invoicing of goods.

All relevant stakeholders shall escalate the transactions to Compliance for further review if there is a deviation in Pricing of Goods.

### **6.2.4 Determination of Movement of Goods:**

It is necessary to ascertain the movement of goods as per contract between customer and counterparty and to confirm whether the same has received the goods and has not called on any sanctioned port, in order to mitigate Phantom Shipment or Trade Sanctions Risk.

Movement of goods is ascertained by the following tools:

- Bill of Lading Tracking
- International Maritime Bureau (IMB) Report
- Goods Declaration Form (GDF)

In case of any concerns identified, Trade shall refer the transaction to Compliance for further review.

## **6.3 Review & Advise Related to Sanctions**

1st line of defense shall refer transactions related to prohibited countries, as per latest circular issued on "Country Risk Assessment and Guidelines" by HBL - Pakistan to Compliance team of HBL SL.

Compliance shall review the details, for any possible sanctions nexus as per the Bank's policy and advise further course of action.

1st Line of Defense must ensure that transactions are screened for any sanction's element at every stage of the trade transaction lifecycle, which may include, but not limited to name of all parties, countries, addresses of parties involved, port of loading, transshipment ports, port of discharge and all vessels involved in shipment of goods.

## **6.4 Review & Advise Related to TBML Red Flags**

Trade and Business being first line of defense shall review the transaction for the attempted or indication to attempt money-laundering, terrorist or proliferation financing and identify / detect TBML Red Flags (Annexure XIII)

Trade shall assess the risk event including all relevant assessment of customer relationship, HBL product and services being utilized and current transaction and refer the transaction to Compliance team for further review. Compliance shall further review the transaction in the light of TBML Red flags detected, assessed and referred to Trade.

## **6.5 Role of Trade Finance Team**

- Trade being first line of defense screens all trade transactions through World-check (preferably part and phonetic match) to mitigate trade sanction risk.
- Trade is the first line of defense to perform sanction screening, where designated trade officers report to Head of Trade Team at HBL SL.

- Trade shall refer the case with their proper review to the Compliance team for further review where Trade detects or identifies any potential match or match related to prohibited country while screening trade transactions. Compliance shall further review the referred risk event for any possible Sanction Nexus and applicability as per Bank's policy. If any further information is required, Request for Information (RFI) is raised to Trade.
- If no Sanctions Nexus is evident, then Compliance accords appropriate advisory via e-mail and vice versa.
- Trade to check for any TBML Red Flags when processing trade finance transactions where there is a suspicion that the transaction may contain any TBML element and may use HBL channel for financial crime purposes. In case of any TBML Red Flags identified by the Trade team, the same shall be referred to Compliance for further perusal. Compliance may direct Trade Department to obtain expertise from TBML team at HBL - Pakistan from TBML perspective.
- Trade maintains TBML Procedures at HBL SL, which extensively covers all related procedures for screening the transaction, detection/identification of TBML red flags and reporting to management.

As a part of due diligence process, Trade has been provided access to World Check application to screen names of different parties/ entities involved in the transaction and vessels against negative lists in order to ensure that HBL remains fully complied with international and local sanctions/ embargoes and internal policy in all jurisdictions.

## **6.6 Filing of STRs:**

If there are grounds to suspect that a customer is using trade finance to launder money, finance terrorism or facilitate Proliferation Financing, same should be escalated to SL Compliance Department by first line of defense. Compliance team will review transactions escalated by 1st Line of Defense and shall file STR to FIU after proper analysis.

## **Annexure I – World Check Format**



Annex v - WC  
Format - Version 2.0

## **Annexure II – CRRM Methodology**



CRRM  
Methodology HBLSL

## **Annexure III – Beneficial Ownership declaration**



Annex II - Beneficial  
Owner Declaration.

## **Annexure IV – High Risk Profile forms**



HIGH RISK PROFILE  
- ENTITY (EC).docx



HIGH RISK PROFILE  
- ENTITY (NTB).docx



HIGH RISK PROFILE  
- INDIVIDUAL (EC) -



HIGH RISK PROFILE  
- INDIVIDUAL (NTB) -

## **Annexure V – Periodic KYC SOP\*\***



Periodic Reviews -  
SOP (002).pdf

## **Annexure VI – Suspicious Indicators**



Annex vi - AML CFT  
Red flags & Suspicious

## **Annexure VII - Compliance Management Information Reports**



Compliance  
Management Inform

## **Annexure VIII - RFI**



Annex vi - SOP -  
RFI.pdf

## **Annexure IX – PEP Approval forms**



Annex I - PEP Risk  
Assessment form.pdf

## **Annexure X – STR reporting manual**



goAML\_STR\_Report  
ing\_User\_Manual\_-



Guidelines\_for\_KUS  
.pdf

## **Annexure XI – Identification of Beneficial Ownership, Drill Down process**



Guideline-04-2018.pdf

## **Annexure XII- STR Reporting Format for Branches**



STR Format  
-individual.xlsx



STR format-Entity.xlsx

## **Annexure XIII- TBML red flags**



Red Flag Indicators  
on Trade Based Money

## **\*\*Annexure V- Periodic KYC SOP**

### **Scope of Periodic KYC Reviews**

Financial regulators require banks to perform AML KYC due diligence when onboarding a new customer and on a periodic basis throughout the life of the relationship.

KYC reviews are conducted on a periodic basis to ensure that existing customer information is kept updated. The bank should also perform periodic reviews to confirm that each customer's assigned risk rating continues to reflect the appropriate AML risk rating.

In addition, conducting regular KYC reviews ensures that Bank is able to capture any material change in the customer's profile or any potentially suspicious activity that was not detected by real-time transaction monitoring platforms.

### **Objective**

The objective of this document is to provide specific guidelines to Branches and Business teams on conducting periodic KYC review.

### **Why Periodic KYC reviews?**

Stale documentation/ Information does not serve the purpose of an AML KYC program and hence requires the documents/Information to be updated on a regular time period which is why regulators stress so much on performing periodic reviews. While collecting the fresh data one might be able to capture any material change in the customer profile which might have taken place after on boarding the customer.

Periodic reviews also allow the financial institutions to keep an eye on the risk rating of the customer to make sure that the risk rating assigned to the customer continues to reflect the appropriate risk rating.

### **When to Perform**

As per Global AML/CFT/CPF and KYC policy, KYC reviews shall be performed based on below frequencies;

High Risk Customer	One Year from the account opening date/last KYC review date or earlier if required
Medium Risk Customer	Two Years from the account opening date/last KYC review date or earlier if required
Low Risk Customer	Three Years from the account opening date/last KYC review date or earlier if required

In addition to the above, the bank shall also perform trigger-based reviews / event driven reviews due to any material changes in customer circumstances. Few examples for material changes are mentioned below;

- Identification of customer as PEP during the relationship
- Any material adverse news (World-Check or from any other public sources including market news)
- Changes in principle activity / line of business
- Material changes to ownership
- Any indication / reflection of business of customer in high-risk countries
- Significant changes in customer transaction pattern from expected (changes in volume, count, mode, concentration in specific periods, origination and destination etc.)
- Any inquiry from Regulator (FIU / CBSL / CID and other law enforcement agencies)

- Required by Country Manager / Compliance / PSU/ICU
- Reactivation of inactive / dormant account
- Customer profile mismatch with the customer KYC.

### Responsibility of Branch Operations Manager (BOM)

- Centralized Operations Department will have to generate a report (with the assistance of IT team) on all accounts maintained at the respective branches on a monthly basis (As at month end date) and share with the respective branch managers on or before the 7<sup>th</sup> day of the month. This report should consist of the following data along with any additional data as required by BOM with relevant to respective customers/Accounts.

Account Opened date	Branch	Account No.	CIF no.	Account Status	Last KYC review Date	Customer Risk Rating	Next KYC review Date

- A Branch official/ Relationship Manager must contact the customer and inform the requirement to update KYC information before the due date. A separate log to be maintained to record such customer contact with date, time and officer involved with Signoff.

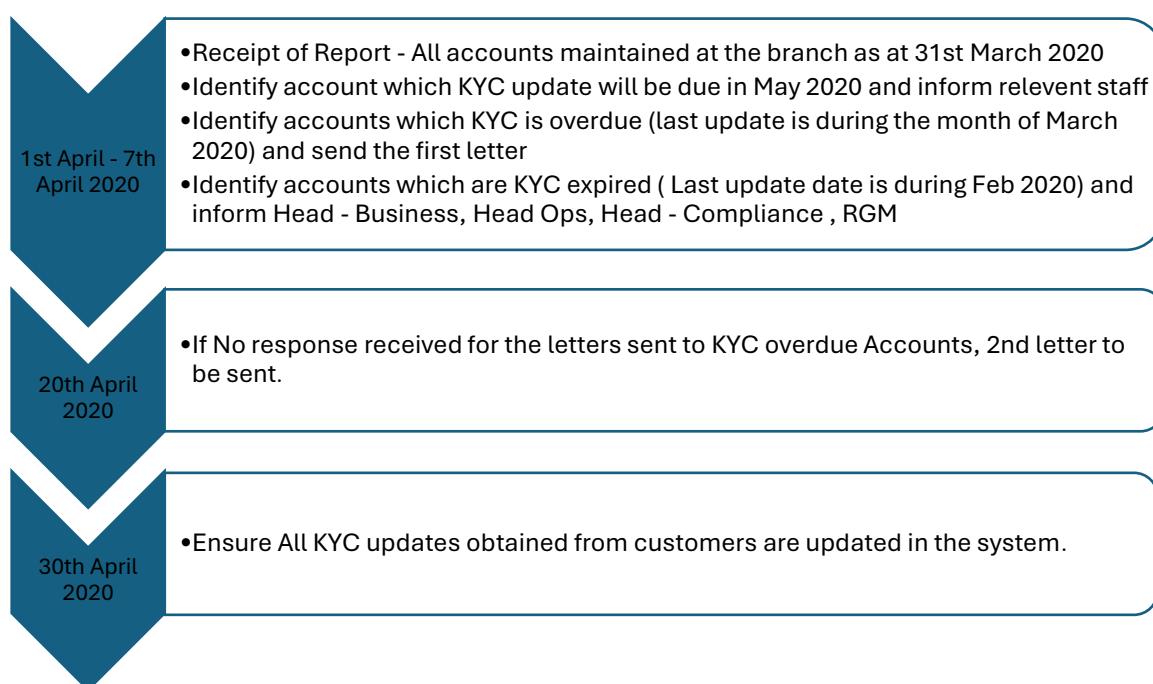
Example – Report generated as of 31<sup>st</sup> March 2020 should be circulated among the team by 7<sup>th</sup> April 2020. In this report, KYCs which are going to be due in May 2020 will be informed for their necessary action.

- An account shall be treated as “KYC overdue” if branch is unable to complete the review before end of the month. Example, an account which becomes KYC due on 15<sup>th</sup> May 2020 (This account would have circulated by BOM on or before 7<sup>th</sup> April 2020) can be completed / approved before 31<sup>st</sup> May 2020 and would become overdue on 1st June 2020.
- BOM should identify the KYC Overdue accounts by using the above-mentioned Report generated as of the month end date.  
Ex – in the report generated as of 31<sup>st</sup> March 2020, if there are accounts which “last KYC updated date” is captured as March 2020, all such accounts need to be classified as KYC overdue.
- BOM shall send a letter/ email to the registered email address / SMS to the registered mobile number (preferred communication method of the customer) to all such KYC overdue account holders requesting to update the KYC asap. This letter must be sent before the 7<sup>th</sup> day of the month and a copy of such a letter or copy of the email to be retained with the account opening mandate. Further BOM may consider to debit freeze the account subject to business / operational decision.
- If the Branch does not receive any response until the 20<sup>th</sup> day of the month, another letter/ email/ SMS to be sent as a reminder, requesting to update the KYC by 30<sup>th</sup> day of the month, copy of the letter/Email to be retain in account opening mandate.
- An Account will be considered as “KYC expired” on the last day of the following month since the KYC became overdue.

Example - an account which becomes KYC due on 15<sup>th</sup> May can be completed / approved before 31<sup>st</sup> May 2020 and if not updated, would become overdue on 1st June 2020. Further, if a customer is not responding to the 1<sup>st</sup> letter sent by the branch before 7<sup>th</sup> June 2020 and second letter sent by 20<sup>th</sup> June 2020, such account will be considered as KYC Expired on 1<sup>st</sup> July 2020.

- BOM is required to identify the KYC Expired account using the above-mentioned Report and such accounts needs to be informed to Head – Business & Head Centralized Operations with a copy to Head – Compliance & Country Manager on or before 7<sup>th</sup> day of the month. Head – Business shall take a decision on such accounts and inform Compliance on the outcome.

Periodic KYC review Process of a BOM (during the month) is as follows. Example – April 2020



\*This process needs to be continued every month.

In addition, BOM/BM will be responsible for following.

- Sufficient awareness/knowledge of the customer (for entity: this would refer to ultimate beneficial owner (UBO's) up to 10%, shareholding, management (effective control), organization structure, business, counterparties i.e. buyer and supplier, geographies and expected transaction profile to assess the various risks associated to the customer; and to ensure that the customer is compliant with HBL policies specifically Global AML/CFT/CPF and KYC policy and relevant local regulations;
- An assessment whether maintaining the relationship with respective customer is appropriate, in respect of bank's target market, reputation and the money laundering/ terrorist financing risks.
- Customer Due Diligence has been completed and is kept up to date as per guidelines, policies, and procedures. All related forms as specified in annexure I shall be duly completed.



- In case of mandated account and joint account, KYC of mandate / joint account holder will also be revised along with the customer KYC & will be attached, reviewed & signed like KYC of primary customer.
- KYC review shall be conducted before due date and approved by respective Branch manager or their designate through sign-off on Periodic KYC review check list (Annexure II. Annexure III) and CDD form / EDD form (if applicable)
- During the review of customer KYC, any upgrading to Risk rating of the customer (as per CRRM methodology) should be approved by Head of Compliance and Head of Business. (Annexure IV). However, any downgrading to the Risk rating of the customer should require only the approval of the Business Head while keeping the same informed to Senior Management (Head of Operations, Head of Compliance and Country Manager).
- To update MISYS promptly (during the day) and accurately for all new / changed customers related information.
- Maintain physical custody of customer files / documents including CDD forms, KYC review check list and supporting documents etc.
- Completion / updating of documents is the responsibility of Branch/Business and shall ensure appropriate scrutiny of documents and identify any incomplete documents / expired documents and follow-up with Customers.
- In case where BM/BOM believes that it would no longer be satisfied with the true identity of the account holder or any other suspicion, a Suspicious Transaction Report (STR) should be filed with the Compliance department.
- All periodic KYC records shall be maintained for a period of 10 years from date of account closure like account opening form.

### **Responsibility of HBSL Compliance Team**

- All KYC overdue accounts will be circulated to Head of business, Head of Operations and Head of Finance while keeping the Country Manager in copy through CCMI (Country Compliance Management Information) report on a Monthly Basis. Upon circulation and in the absence of any concerns (unless received within TAT of 2 days) from the Country Management the information will be submitted to International Compliance HBL Pakistan through CCMI.
- All KYC Expired Accounts and decision made by Business on such accounts will be escalated in Compliance Committee Meeting (CCM)
- All KYC Expired accounts will be monitored closely and if any suspicious nature is observed, the Compliance team will consider raising an STR on such customers.

### **Periodic KYC Review Process**

- Take a print of existing CDD form (expiring CDD Form) from MISYS before initiating updating process. This will ensure a physical audit trail of previous KYC information/ form for maintaining in customer file.
- Review KYC information including line of business, changes in occupation, counterparties and geographies if applicable and update where necessary.

- Obtain valid Company/Business registration, Passport, Visa, National Identity Card, and other documents in case they are expired. Changes in Permanent / correspondent address to be supported by appropriate documentary evidence.
- Changes in source of income/funds including income levels, expected turnovers and etc. shall be updated and supported by appropriate documentary evidence.
- Review customer ownership structure for any changes and update if required along with obtaining of related supporting documents.
- Perform Adverse Media Check of customers, UBOs, Authorized Signatories, Shareholders, Directors, Parent's companies, Subsidiaries and Affiliates if any. All matched results shall be duly reviewed and discounted with proper remarks as per Bank policies and procedures. All possible/ uncertain matches to be referred to Compliance for discounting as per the Global AML/CFT/CPF and KYC policy.
- Perform the Customer Risk Rating accordingly and conduct extra due diligence based on the risk rating of the customer.
- Duly signed CDD forms (previous and revised), Annexure II/ III (KYC check list) along with supporting KYC checks e.g., Negative News Check needs to be maintained by Branches as part of account mandate file. All updated documents e.g. NIC, passport, address proof, Source of income etc., also need to be maintained by Branch in the account mandate file.
- EDD form shall be completed for all high-risk individual customers alongside the file notes which shall be duly approved and signed as per the approval matrix. The approved EDD form shall be retained with Branches along with Account mandate file.
- PEP Risk Assessment & high-risk assessment shall be completed for all PEP & PEP exposed customers which shall be duly approved as per section 5.4 on approval matrix for High-Risk Customers in the CRRM methodology. The approved PEP Risk & High-Risk Assessment shall be retained with Branches along with the Account mandate file.
- In case if account periodic review concluded with unsatisfactory status/suspicion on customer/ transaction e.g. true match on world check, incomplete documents/ CDD or in case of suspicion the same shall be reported to Compliance for necessary course of action.

### **Maintaining updated records of Resident Visa / Permit – Non-Nationals**

- The branch must ensure that a valid residence visa is always held by the customers, during the continuation of the account.
- On the expiry of the visa, the account shall be operated with a debit freeze. Upon the customer leaving the country, the account shall either be considered in compliance with the Rule 35 (b) of the CDD Rules No 01 of 2016 or be converted into a non-resident account as per prevailing Foreign Exchange Regulations.
- The branch must generate a report on Passport and Visa expiry with the assistance of IT team on a monthly basis. Branch needs to follow up with the customers to collect renewed Visa/ Passport copy. Copy of the valid resident visa, verified against the original, should be obtained and certified by the branch.
- In case when a customer is not contactable, a formal communication should be sent mentioning the visa expiry date and requesting the customer to forward a certified copy of the renewed residence visa alongside first page of the current passport.
- A separate log to be maintained to track the collection of a new visa/ passport. all customer communications and the details of the accounts where the debit freeze has been placed and lifted should be kept at the Branch.

- As and when the customer submits renewed certified visa copies, the debit freeze shall be lifted and the “expiry date” field should be updated with the new visa expiry date.
- In case of no action has been taken by the customer after one month of the expiry of the residence visa a letter shall be sent to the customer stating that the account shall cease to operate until further instructions are received.
- The branch should make a total freeze or terminate the account as per internal process and also may consider raising a suspicious transaction report (STR).

## Annexures

Annexure I – Documentary requirements based on account type

Annexure II – KYC Review Check list – Entity

Annexure III – KYC review check list – Individual

Annexure IV – Approval form for change in Risk Rating



Annexure I.docx



Annexure II - KYC  
review check list - Enti



Annexure III - KYC  
review check list - Indi



Annexure IV-  
Approval form for cha

~End~

# AML CFT Procedure SL 2025 - (Clean Version)










## 16-Jun-25 (003) -Final-signed-signed-signed

Final Audit Report

2025-06-24

Created:	2025-06-24
By:	Sara Sheraz (sara.sheraz@hbl.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAAbedhQh9nCd41Kxp4oKFFzyHKUbrpxb5H

## "AML CFT Procedure SL 2025 - (Clean Version) 16-Jun-25 (003) -Final-signed-signed-signed" History

-  Document created by Sara Sheraz (sara.sheraz@hbl.com)  
2025-06-24 - 6:37:05 AM GMT
-  Document emailed to majid.aziz@hbl.com for signature  
2025-06-24 - 6:37:15 AM GMT
-  Email viewed by majid.aziz@hbl.com  
2025-06-24 - 6:44:48 AM GMT
-  Signer majid.aziz@hbl.com entered name at signing as majid aziz  
2025-06-24 - 6:45:32 AM GMT
-  Document e-signed by majid aziz (majid.aziz@hbl.com)  
Signature Date: 2025-06-24 - 6:45:34 AM GMT - Time Source: server
-  Document emailed to Syed Saad Uddin Ahmed (saad.ahmed@hbl.com) for signature  
2025-06-24 - 6:45:36 AM GMT
-  Email viewed by Syed Saad Uddin Ahmed (saad.ahmed@hbl.com)  
2025-06-24 - 6:46:49 AM GMT
-  Document e-signed by Syed Saad Uddin Ahmed (saad.ahmed@hbl.com)  
Signature Date: 2025-06-24 - 6:47:08 AM GMT - Time Source: server
-  Agreement completed.  
2025-06-24 - 6:47:08 AM GMT