Adapting Risk-based Approach in Casinos to Combat Money Laundering & Terrorist Financing

Presentation by the Financial Intelligence Unit of

Central Bank of Sri Lanka

(Publicly available information on case studies of ML/TF and indicators of suspicious transaction are used in this presentation to educate the casino sector on possible money laundering threats)

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

What is Money Laundering?

Money Laundering is the process of hiding the origin of illegally earned money

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

Money Laundering is illegal in Sri Lanka

- Money Laundering Offence:

  Unlawful Activities: Predicates Offences for Money Laundering

  - Drug Trafficking
  - Arms Dealing
  - Human Trafficking
  - Violation of Bribery Act (Chapter 26)
  - Violation of Foreign Exchange Act
  - Conduct of prohibited schemes such as Pyramid Schemes
  - Violation of the Customs Ordinance
  - Violation of the Excise Ordinance
  - Violation under the Payment Devices Frauds Act, No. 30 of 2006
  - Violation under the National Environment Act, No. 47 of 1980
  - Transnational organized crimes such as; credit card frauds, computer and Internet related crimes,
  - Offences committed against children
  - An offence under any other law, punishable by death or with imprisonment for a term of five years or more

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

What is Terrorist Financing?

Providing financial support to terrorism through legally or illegally earned money

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

Global efforts on combating Money Laundering & Terrorist Financing

- Financial Actions Task Force (FATF)
- Asia Pacific Group on Money Laundering (APG)
- Egmont Group of Financial Intelligence Units
- World Bank
- International Monetary Fund (IMF)

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

Institutions to report against Money Laundering & Terrorist Financing

- **Financial Institutions-**
  - Banks
  - Finance Companies
  - Stock Brokers
  - Primary dealers, etc..
- **Designated Non-Financial Institutions (DNFBPs)-**
  - **Casinos**
  - Real Estate Agents
  - Gem & Jewellery Dealers
  - Accountants, Lawyers,
  - Notaries
  - Company Secretaries

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

FATF Recommendations against Money Laundering & Terrorist Financing

FATF International Recommendations For DNFBPs:

- 22: Customer Due Diligence: (LC)
  - R. 10 (Customer Due Diligence)
  - R. 11 (Record Keeping)
  - R. 12 (Politically Exposed Persons)
  - R. 15 (New Technologies)
  - R. 17 (Reliance on Third Parties)
- 23: Reporting Suspicious Transactions: (C)
  - R. 18 (Internal Controls, Foreign Branches and Subsidiaries)
  - R. 19 (High Risk Countries)
  - R. 20 (Reporting of Suspicious Transaction)
  - R. 21 (Tipping-off and Confidentiality)
- 28: Supervision and Monitoring (NC)
  - R. 35 (Sanctions)

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

FATF Recommendations against Money Laundering & Terrorist Financing

1. Technical Compliance:

- This measures implementation of FATF requirements (International Standards)
    - C- Compliant
    - LC- Largely Compliant
    - PC- Partially Compliant
    - NC- Non-Compliant

2. Effectiveness Under Immediate Outcome (IO) 3:

- This is to assure that proceeds of crime and funds in support of terrorism are prevented from entering the financial and other sectors or are detected and reported by these sectors.
- Supervisors appropriately supervise, monitor and regulate financial institutions and DNFBPs for compliance with AML/CFT requirements.

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

The Financial Intelligence Unit (FIU)

- The FIU is the apex institution in Sri Lanka to monitor AML/CTF requirement of the country.
- The FIU examines AML/CFT compliance of reporting Institutions including casinos under Designated Non-Financial Business and Professions category.

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

National Risk Assessment

- FIU conducted National Risk Assessment in 2014.
- Casinos, real estate agents and gem and jewellery dealers were Found as High Risk sectors for ML/TF in Sri Lanka.
- This is mainly due to their high cash intensiveness in operations.
- And there were no AML/CFT measures in casino operations.

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

Casinos were found as High-Risk for ML/TF compared to other DNFB sectors

- Although casinos are generally classified as entertainment institutions, casinos are by nature cash-intensive businesses undertaking various financial activities such as;
  - Cash in/Cash out
  - Wire transfers
  - Exchanging Currencies
  - Credit facilities
  - Use of credit/debit cards

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

AML/CFT Threshold for conducting CDD in Casino operations

Casinos in Sri Lanka are required to conduct CDD on customers when they are engage in inward and outward financial transactions that aggregate in either direction to the equivalent of **USD 3,000** or more, regardless of the actual currency of the transaction(S) in a single business day.

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

Factors impact on ML/TF risks:

- Types of gambling offered
- Location
- Speed and volume of business
- Types of payment/payment methods accepted from customers
- Size of premises
- Customers (regular customers with membership rules or passing trade such as casual tourists or organized casino tours, junket operations)

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

Control measures that Casinos already in place

Casinos are generally subject to a range of regulatory requirements, commercial considerations, and security measures, which can complement AML and CFT measures:

- Age verification
- Financial crime controls
- Social responsibility provisions
- Security controls
- Gaming surveillance, e.g. to deal with problem gambling

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

Case Studies

Possible methods of Money Laundering using Casino operations:

- Use of casino value instruments such as chips, tokens, credits, casino cheques, etc.
- Structuring, rearranging or smurfing of transactions
- Refining of currency notes
- Use of individual customer accounts and safe deposit boxes
- Use of false or forged documents and means of payments
- Collusion in fixed games
- Other methods

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

Use of casino value instruments such as chips, token or cheques to launder money

1. Purchasing of casino chips or gaming credits with the intention of subsequent redemption of value of the instrument by way of payment documents such as cash, casino cheques or transferring back to bank or individual accounts.

- Money launderers who pretends as customers of casinos will purchase casino chips with cash or bank transfers.
- Then they will make repayment requests in the form of cash, to a given bank account or by a casino cheque.

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

Use of casino Value Instruments such as chips, token or credits to launder money

2. Money launderers who pretend as customers may purchase of chips or winnings from clean/genuine players at an attractive higher price:

- Money launderers may purchase of chips or winnings from customers with clean background who use the casino for gaming.
- They will make very attractive proposals to purchase at a higher price than the face value of the chip.
- This will make the arrangement favorable for both the seller and the buyer.

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

Use of casino value instruments such as chips, token or credits to launder money

3. Casino chips are used as currency in illegal transactions:

- Criminals may use casino chips, gift certificates and casino reward cards as currency to pay for illegal transactions such as purchasing of drugs, arms or payment for human trafficking.
- The party who received the casino value instruments as the payment for such transactions can exchange them later at the casino businesses with least gaming or sometimes without gambling.

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

Structuring, rearranging or smurfing of transactions to launder money

1. Purchasing of casino chips regularly using cash:

- Money launderers make regular cash payments with value below the threshold CDD limit which is UDS 3,000 or equivalent in any other currency.
- This is mainly to avoid the monitoring procedures of any financial transaction which is above the threshold CDD limit.

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

Structuring, rearranging or smurfing of transactions to launder money

2. Money launderers may use third parties to undertake transactions:

- Money launderers are sometimes organized groups.
- They use one customers account to transfer money to the casino in purchasing of chips.
- Also, they make these payments which are just below the amount of CDD threshold reporting to avoid monitoring and possible questioning by the casino businesses.

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

Structuring, rearranging or smurfing of transactions to launder money

3. Money launderers may be on alert of casino staffs' work schedules to launder money without making any suspicion.

- Money launderers may utilize staff movements and their work shift changes to conduct transactions.
- They may trace the work schedules of casino staff specially at cash desks and conduct transactions little below the customer identification threshold to avoid any monitoring or questioning.
- Ex. Money launderers pretend as customers of casinos and will conduct transactions at the beginning of one work shift and at the end of another work shift of the cash desk employees.

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

Structuring, rearranging or smurfing of transactions to launder money

4. Money launderers will regularly change the place of gaming to avoid possible suspicion on their behavior:

- Money launderers may attempt to regularly switch or exchange among gaming tables, gaming machines or gaming rooms when their wagering amounts closely approach the customer identification threshold.

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

Structuring, rearranging or smurfing of transactions to launder money

5. Customers with the purpose of laundering money may request division of casino winnings:

- Money launderers may prefer the amount of casino winnings, which exceeds the identification threshold, to be divided into cash or cheques below the threshold limit.
- This is mainly to avoid the requirement of customer dude diligence of cash outs which exceed the customer identification threshold.

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

Refining of currency notes

1. **Exchanging currency notes at the cash desks/cashiers:**

- Members of the money laundering groups may individually approach the cash desk of the casino, introduce themselves as customers for gaming.
- They may ask to exchange low denomination bills for higher denomination ones.
- In illegal businesses such as drug dealing, people get low denomination currency notes.
- It is hard to handle large number of low denomination currency notes.
- Therefore, people involve in such illegal activities may use businesses like casinos to exchange their sale proceeds to high value currency notes by pretending as they are regular customers of the casino.

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

Refining of currency notes

2. Money launderers can use gaming machines or currency note acceptors to refine currency:

- Modern casinos have advanced gaming machines which consist note acceptors.
- These machines provide facilities to customers in adding credits to their individual casino accounts/ to the casino's bank account.
- These technologies could be used by money launderers to feed low denomination currency notes into the machine.
- This will provide accumulation of credit to the customer's individual account or to the casino's bank account.
- Then, money launderers will redeem these accumulated credits with little or no gaming for high denomination banknotes.

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

Use of wire transfers and safe deposit boxes

1. Money launders may deposit cash into casino accounts by making wire transfer:

- Funds are deposited into the customer's individual account/ casino account by a wire transfer from a local or foreign financial institution.
- This enables the customer to freely make use of those funds, for gaming activities or any other service provided at the casino.
- Money launderers may use such wire transfers to deposit money and with minimal or no gambling activity, request cash out from such balances of the casino account.

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

Use of wire transfers and safe deposit boxes

2. Money launderers may use the foreign individual holding accounts to launder money in another jurisdiction:

- There are casinos which have their chain of casino operations in other jurisdictions.
- Those chain of casinos offer customers to hold individual accounts in one country for an example jurisdiction "A", but the funds can be used to purchase casino value instruments, as well as to be cashed out in jurisdiction "B" at a casino within the same chain.
- In this case the money held in jurisdiction A's account does not leave the country physically or through electronic wire transfer.
- This prevent that the transaction been monitored under the requirements of cash or wire transfer reporting requirements.
- Also, if transactions are little below the CDD threshold limit, then the identification threshold can also be avoided.

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

Use of individual accounts and safe deposit boxes

3. Potentials of money laundering using safety deposit boxes:

- Casinos offer special services such as safety deposit boxes to their VIP or high stakes players specially who spend many hours at gaming centers.
- This service presents a money laundering risk due to lack of transparency with the use of such boxes.
- Also, there is possibility of providing access of these safety deposit boxes to third parties via a password or key.

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

Use of false/ forge documents and means of payments

1. Potential of money laundering using false identification data:

- Customer identification and verification of information is a legal requirement under the casino operations.
- Money launderers may present false identification documents and made up personal data (e.g. address, phone number, occupation etc.) to conceal their real identity from these procedures.
- Providing forge identities to customer may help money launderers to misuse casino value instruments to launder money without any suspicion.

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

Use of false/ forge documents and means of payments

2. Use of forged means of payment:

- Counterfeit currency notes or cheques can be used to purchase casino value instruments.
- Also, non-cash means of payments such as forged credit cards or gift cards by means of identity theft e.g. bank account details, passwords can be used to purchase casino value instruments with the intension of later converting them to cash outs with minimal gaming.

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

Collusion in fixed games

1. **Making bets on fixed game with another customer:**
   - There are well organized money laundering groups who gets involved in relatively low odds, low risk games such as roulette, blackjack.
   - This would involve two or more pairs of players placing opposite equivalent bets on even money wagers in the same game.
   - Ex. Person "A" bets Rs. 100,000 on black, while Person "B" bets Rs.100,000 on red in a game of roulette.
   - Every loss for person "A' is a win for person "B", and vice versa.
   - This gaming method is also called as the "intentional losses" method, when the loss of a player is factually reimbursed by the win of the associate player.

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

Collusion in fixed games

2. Making bets on fixed games with a casino employee:

- Money launderers may collude with casino staffs to enable laundering of criminal proceeds without being detected.
- Money launderers are willing to get the support of the casino staff in such activities (sometimes on paid basis) as they would support them avoiding of filing reports on over-threshold or reporting suspicious transactions.
- Also, they would support in destroying documents related to customer due diligence or records on conducted transaction, falsifying gambling records on such customers, arranging the game in a manner favorable for such customers.
- Further, they will support such customers in fixed games with another players.

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

Indicators of money laundering in casino operations

Red Flags/Indicators of money laundering suspicions:

- Use of casino value instruments such as chips, tokens, credits, casino cheques, etc.
- Structuring, rearranging or smurfing of transactions
- Refining of currency notes
- Use of individual customer accounts and safe deposit boxes
- Use of false or forged documents and means of payments
- Collusion in fixed games
- Other methods

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

Indicators of money laundering suspicions related to the use of casino value instruments such as chips, tokens, gaming credits, casino cheques, etc.

- Customers who purchase casino value instruments and cash outs using them with little or no gaming activities.
- Customer exchanges cash for chips and vice versa multiple times during the same day.
- Customer purchases and cash outs chips similar or equal amount
- Customer purchases chips and leaves casino shortly after
- Customers purchase of chips through third parties
- Detection of chips brought by customers into the casino from outside
- Customer requests to add cash to casino winnings, and then exchanges the combined amount for a single cheque or bank draft

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

Indicators of money laundering suspicions related to the use of casino value instruments such as chips, tokens, credits, casino cheques, etc.

- Customer purchases chips by depositing multiple cheques or bank drafts into individual account, or requests the winnings to be paid out in form of multiple cheques or bank drafts.
- Customer inserts funds into gaming machines and claims those funds as credits on individual account/ cash with little or no gaming activity.
- Customer claims gaming machine credit payouts with no jackpot.
- Customer frequently inserts substantial amounts of cash in gaming machines that have high payout percentages and does not play "max bet" to limit chances of significant losses or wins, thereby accumulating gaming credits with minimal play.
- Customer requests transfer of credits to individual account with another casino.
- Abrupt changes in wagering or betting pattern.
- Customer's intention to win is absent or secondary.

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

Indicators of Money Laundering suspicions related to the Structuring, rearranging or smurfing of transactions

- Customers regular purchases of casino value instruments and frequent wagers in cash just below the identification threshold.
- A third party is present for all transactions of the customer.
- Customer allows third parties to use his/her individual account.
- Cash received from third party for purchasing chips.
- Cash handed to third party after exchanging chips.
- Transfer of funds from one individual account to multiple individual accounts.

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

Indicators of Money Laundering suspicions related to the refining of currency notes

- Customer in possession of large amounts of currency.
- Customers attempt to exchange low denomination notes for high denomination ones for various reasoning.
- Customers insert low denomination currency notes into note acceptors or gaming machines with little or no gaming activity before redeeming the credits for high denomination currency notes.
- Customers frequently deposit amounts in low denomination currency notes on individual account with little or no play before redeeming the balance of account for high denomination currency notes.

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

Indicators of Money Laundering Suspicions related to the use of individual accounts and safe deposit boxes

- Customer's deposits of cash, cheques, and wire transfers into individual account/ casino account inconsistent with customer profile.
- Customer withdraw funds from casino account shortly after being deposited (May request to transfer back to a given account number or to the same account number).
- Customers with significant movement of funds through the casino account with little or no gambling activity.
- Customer credits funds into an casino account from banks or other individual accounts in high-risk countries or from unknown sources.
- Customer may use intermediaries (authorized representatives) to undertake transactions.
- Funds are transferred to casino account from a corporate accounts.
- Customer regularly allows third parties to use the customer's individual safe deposit box.

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

Indicators of Money Laundering suspicions related to the use of false/ forged documents and means of payment

- Customers introducing themselves under a fictitious name or different names.
- Customer may use identification document with altered or missing entries.
- Inconsistent and contradictory identity information presented.
- Customer may refuse to present any identification document or personal data.
- Customers may use counterfeit currency notes or cheques for purchasing value instruments or replenishing individual accounts.
- Customer may use forged non-cash means of payment (e.g. debit, credit or gift cards) for purchasing value instruments.

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

Indicators of Money Laundering suspicions related to collusion in fixed games

- Even-money wagering when conducted by a pair of betters covering both sides of an even bet (e.g., in roulette, baccarat/mini-baccarat).
- Two or more pairs of customers frequently playing at the same table.
- Two or more pairs of players frequently wagering against one another (the win of one player is "accompanied" by the loss of the other).
- Customer attempting to be friend with casino employees/staff.
- Customer prefers to play at the table serviced by a certain dealer/dealers.
- Contacts or connections between customers and casino employees/staff outside of the casino.

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

Other indicators of Money Laundering in Casino operations

Other Red Flags/Indicators of money laundering suspicions:

- Transactions inconsistency with customer profile .
- High volume of transactions within a short period.
- Sudden increase in the volume of transactions.
- Customers pertaining to high-risk groups such as drug dealing, contacts with PEPs.
- Negative information on customers (Ex. Criminal Records).

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

How to Combat ML/TF at Casinos?

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

How to Combat ML/TF Risk?

Assessing
ML/TF Risk

1. Assessing Institution's ML/TF Risk

- Countries risk
- Geographic area
- Product/Service
- Transaction/ Delivery Channels

2. Conducting Risk Profiling on Customers

- Geographical Location
- Customer Category
- Product, services, transactions or delivery channels of the customer

Implementing
Internal Risk Mitigating Controls

(Following Should be implemented)

- AML/CFT Policy & Reviewing it periodically
- Appointing a Compliance Officer
- Conduct CDD/Enhanced CDD
- Record Keeping
- Paying attention to complex, unusual, large transaction
- Screening against designated list of UNSCR
- Other measures;
  - Assess ML/TF risk before introducing New Technologies (Products, Services and Business Practices)
  - Employee Screening
  - AML/CFT Training for Employees
  - Auditing of AML/CFT measures

Reporting
Transactions to the FIU

(Reporting on suspicions & mandatory)

- Reporting Suspicious Transactions
- Cash Transaction/Electronic Fund Transfers

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

Conducting ML/TF Risk Assessment by Casinos

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

Risk Assessment

- Identify, asses and understand the ML/TF risk under these steps
    - Customers
    - Countries
    - Geographic Areas
    - Product/Services
    - Transactions/Delivery Channels
- Document the risk assessment
- Keep the assessment up-to-date
- Provide risk assessment information to the FIU through the Compliance questionnaire

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

An example of a checklist for Institutions' ML/TF Risk Assessment

Customer Risk	YES	NO	MITIGATION MEASURES
Do you have clients that:			
operate in a cash intensive business?			
reside outside Sri Lanka?			
are intermediaries or "gatekeepers" such as professionals that hold accounts for clients where the identity of the underlying client is not disclosed to you?			
are located in a known high crime rate area? the nature of their business makes it difficult to identify the true owners or controllers?			
are politically exposed persons?			
do not have an address or who have several addresses without justified reason?			
have a criminal record? have links to organized crime?			

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

An example of a checklist for Institutions' ML/TF Risk Assessment

	YES	NO	N/A
Product/Service Risk Do you offer products or services that:			
make it difficult to fully identify clients?			
assist in the establishment of a company?			
Do you:			
perform tasks for the purpose of concealing the client's beneficial owner?			
perform tasks of real estate transfer between clients in an unusually short time period without visible legal, economic or other justified reason?			
provide services linked with establishing, operating or managing of a shell company, company in nominal ownership?			

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

Delivery Channels/Business Relationships Risk Do you:	**YES**	**NO**	**N/A**
conduct non-face-to-face transactions? Do you have business relationships that:			
involve complicated financial transactions?			
involve payments towards/from third persons and cross-border payments?			
involve high risk real estate transactions? involve cash payments?			

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

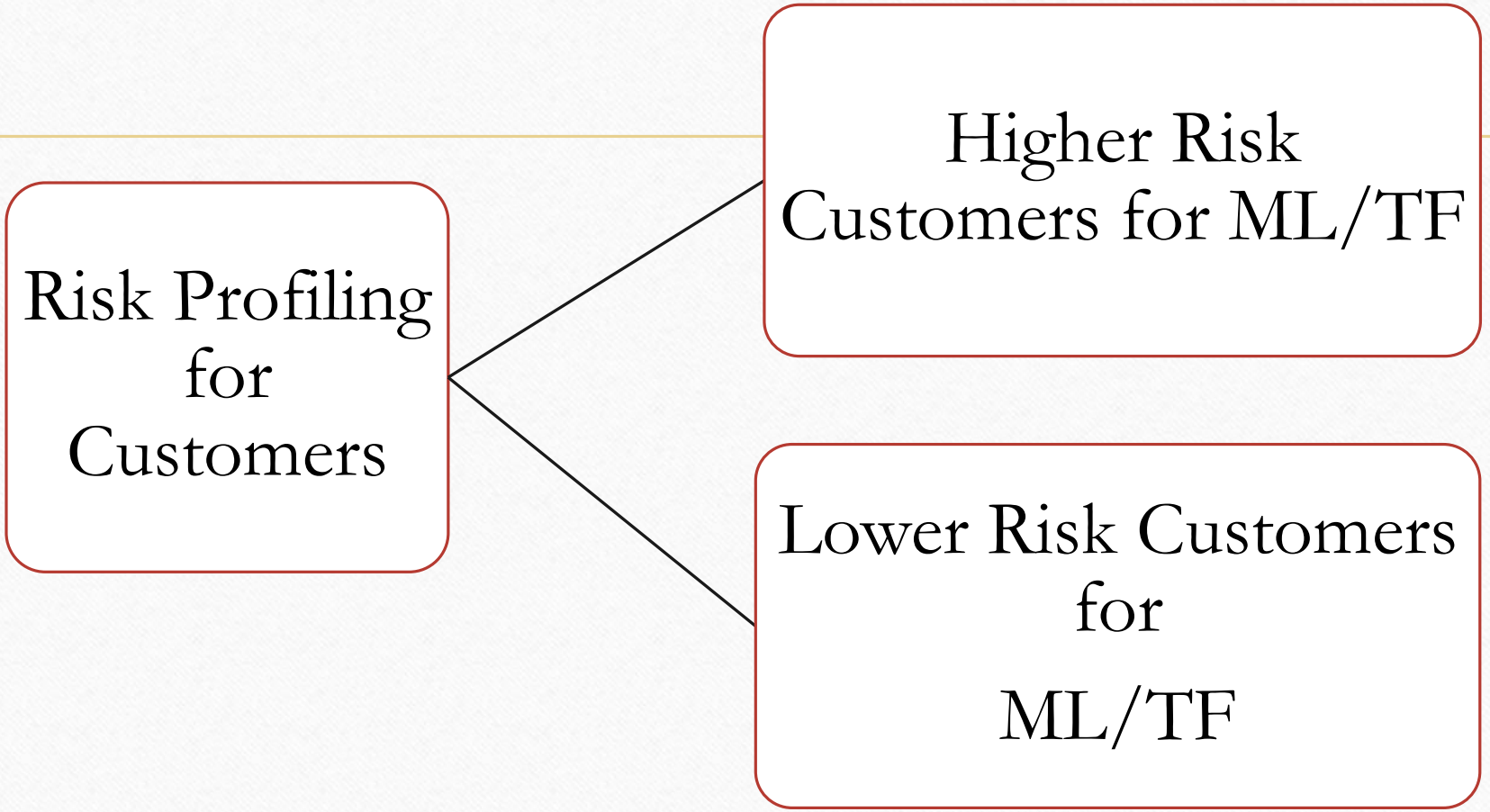
Geographical Risk	YES	NO	N/A
Do you or your clients operate or undertake activities in the following countries:			
Any country subject to sanctions, embargoes or similar measures issued by the United Nations (UNSCR)?			
Any country identified as a financial secrecy haven or jurisdiction?			
Any country identified by the Financial Action Task Force (FATF) as non-cooperative in the fight against money laundering or terrorist financing or subject to a FATF statement?			
Any country identified by credible sources as lacking appropriate money laundering or terrorist financing laws and regulations or as providing funding or support for terrorist activities?			
Any country that is known to have significant levels of corruption, or other criminal activity?			

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

Conducting Risk Profiling on Customers

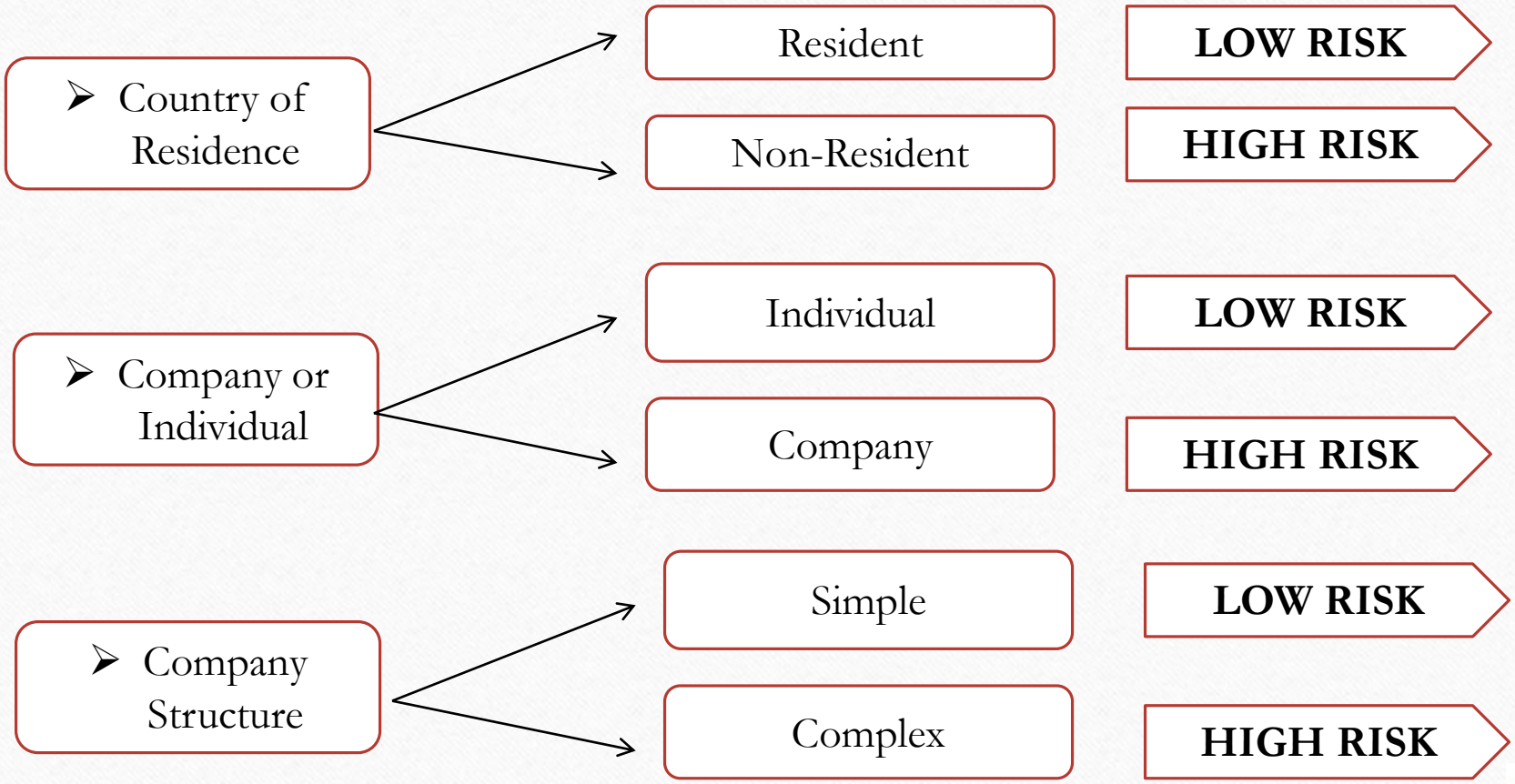
Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

Risk profiling for customers on collected data



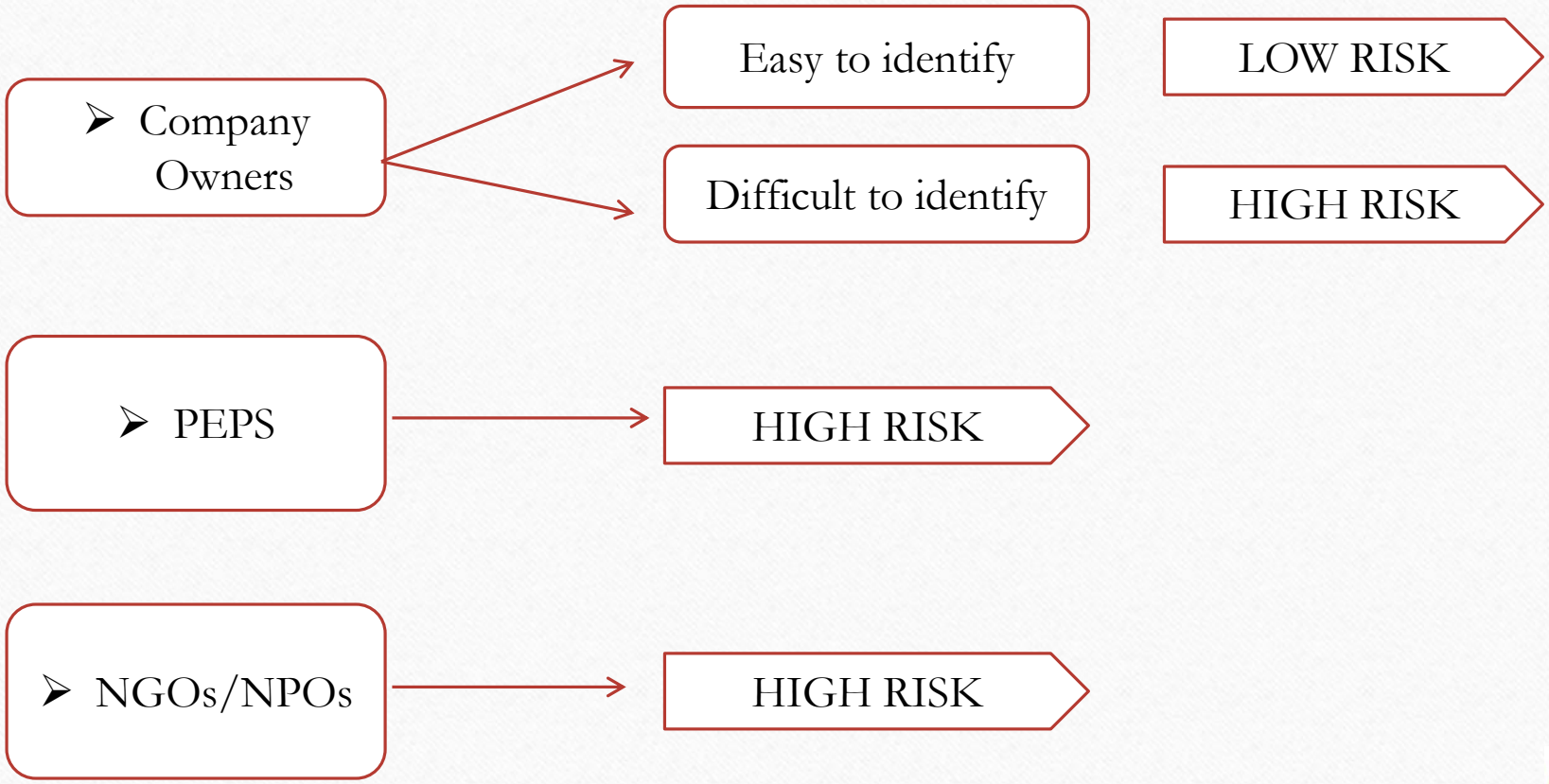
Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

Ex. How to profile customers on ML/TF risks?



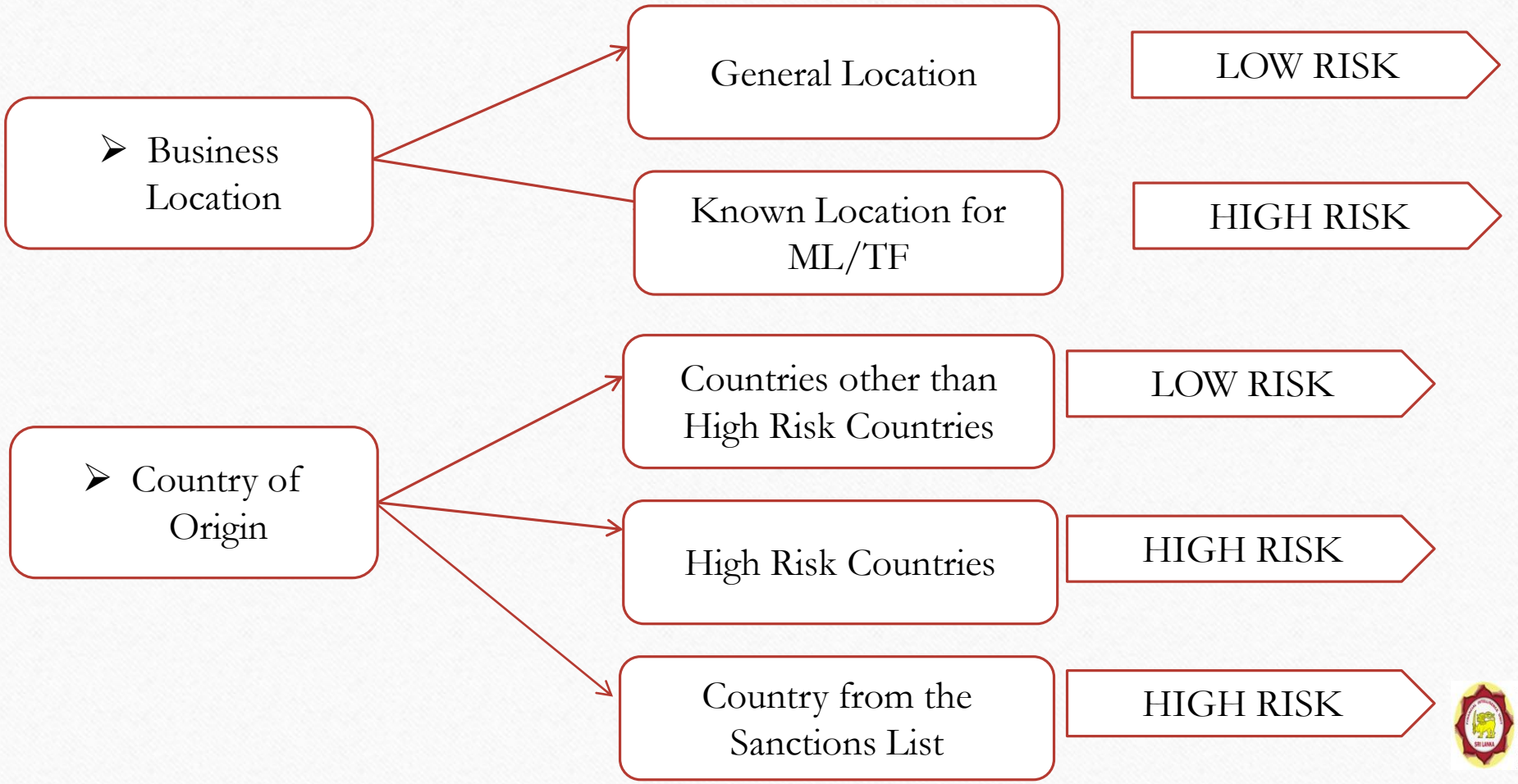
Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

Ex. Customer risk profiling Cntd…



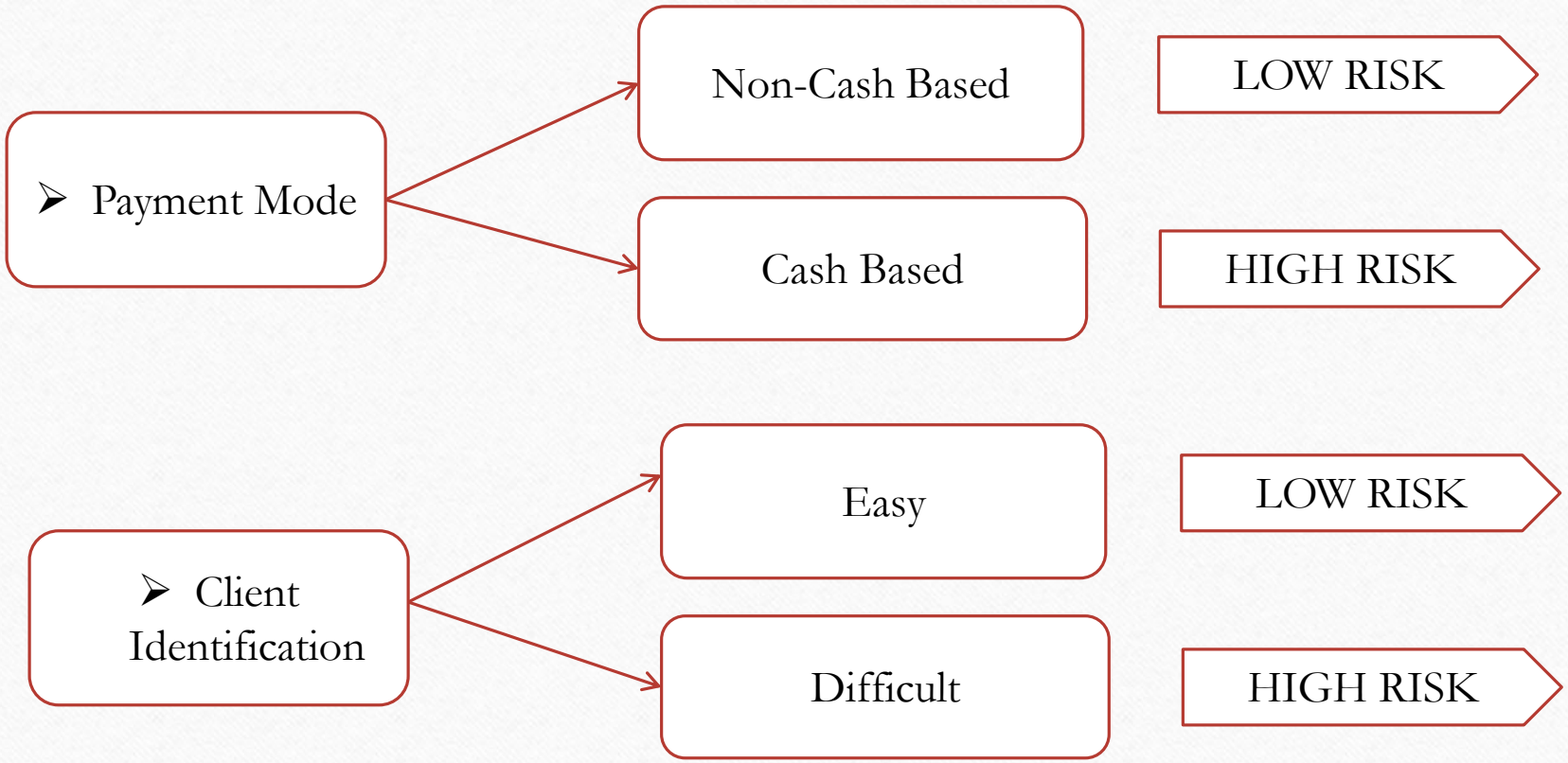
Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

Ex. Geographical risk



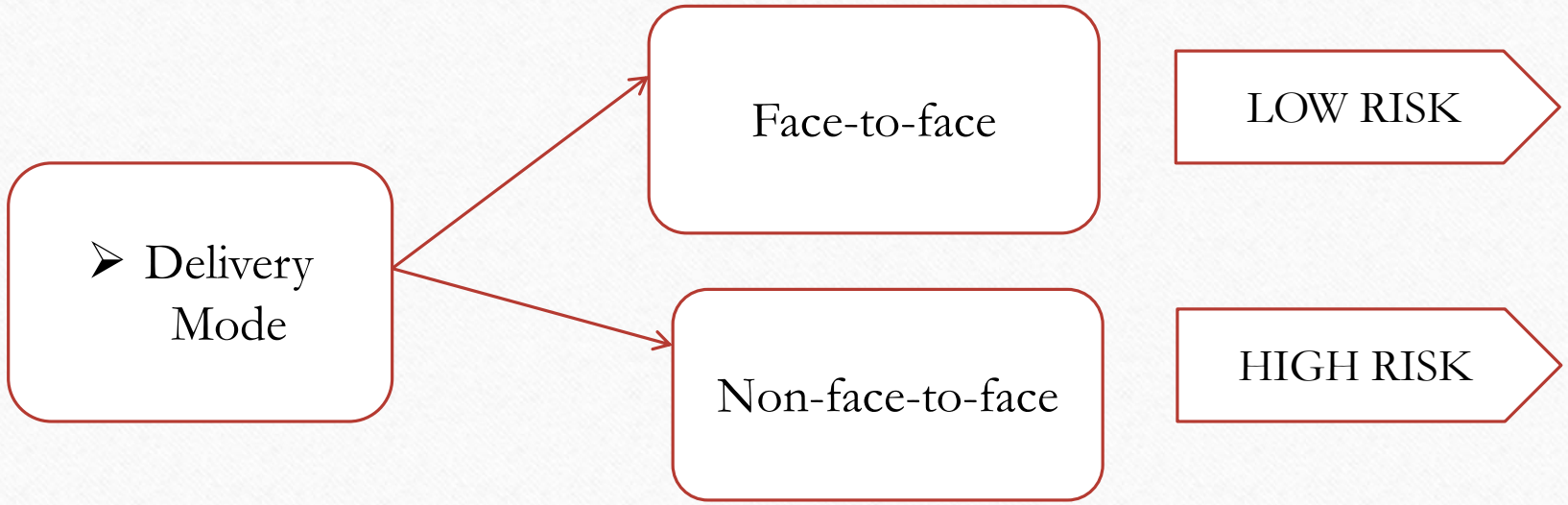
Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

Ex. Products/Services risk



Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

Ex. Delivery channel risk



Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

Risk mitigation

- Have an AML/CFT Policy, Procedures and controls approved by the senior management to manage and mitigate identified risks.
- Monitor the implementation of policies, procedures and controls.
- Take enhanced measures to mitigate the risks where higher risks are identified.
- Simplified measure can be taken where risk is found low.
- Simplified measures should not be applied when there is a suspicion of ML/TF.

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

AML/CFT internal controls for Casinos

- Casinos should have an internal AML/CFT Policy and Procedures (Compliance Programme)
- Casinos should reviewing their compliance programme periodically
- Casinos should conduct Customer Due Diligence (CDD) and Enhanced CDD
- Casinos should a have proper Record Keeping system
- Casinos should have a system to Screening Customers and Beneficial Owners against UNSCR designated lists
- Casinos need to have procedures to comply with other AML/CFT Requirements such as
    - Assessing ML/TF risk arising from New Technologies
    - Employee screening
    - AML/CFT training for employees
    - Auditing applications of AML/CFT obligations

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

AML/CFT Policy for Casinos

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

AML/CFT requirements that should be in the Non-financial Institution's AML/CFT Policy

- Risk based approach to AML/CFT
- Conducting AML/CFT Risk Assessment
- Appointing a Compliance Officer
- Conducting of CDD and Enhanced CDD Procedures
- Assessing and Managing ML/TF risks of New Technologies
- Compliance with UNSCR Resolutions
- Reporting of STRs to the FIU
- Procedures for Record Keeping
- Conducting AML/CFT Training for employees
- Conducting employee screening when recruiting new employees
- Auditing of AML/CFT Procedures

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

FIU provides a Guidance Note on Preparing AML/CFT Policy

Guidance Note on Preparing Company-wise AML/CFT Policy Document

This guidance note is provided by the FIU to the designated non-financial Institutions (herein after referred to as "Institutions"), to use as a direction on preparing AML/CFT Policy of the Institution. Therefore, this should not be used as the AML/CFT Policy of the Institutions.

Introduction:

The introduction to the AML/CFT Policy of the Institution may include;

- Brief description on what is Money Laundering/Terrorist Financing (ML/TF)
- Description on prevailing AML/CFT Laws and Regulations in Sri Lanka in relation to DNFBs:
  - Financial Transactions Reporting Act No. 6 of 2006 (FTRA)

AML/CFT Policies

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

To effectively maintain the Institution's AML/CFT Policy

How ? → Review & Monitor AML/CFT Policies and Procedures

How often? → Periodically based on the Institution's Policy

What to do? → Document the scope of the Review & Results

↓

Report Deficiencies to the Board of Directors / Top Management / Owner

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

Conducting Customer Due Diligence

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

Customer/Beneficial Owner Identification

What to collect?

As per the CDD Rules for DNFBPs;

(a) the full name;

(*b*) permanent, residential or mailing address;

(*c*) occupation, name of employer, business or principal activity;

(*d*) an official personal identification number or any other identification document that bears a photograph of the customer or beneficial owner such as the National Identity Card, passport or driving license;

(*e*) date of birth;

(*f*) nationality;

(*g*) source of funds;

(*h*) purpose of transaction;

(*i*) telephone numbers (residence, office or mobile).

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

Identity verification of Customer and beneficial owner

Verify the documents specified in (d) above, by requiring the customer or beneficial owner to furnish the original document & make a copy of that document

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

How to conduct Enhanced Customer Due Diligence ?

For customers rated as High-Risk

If a customer is
Politically Exposed Persons (PEPs)

For Customers from
High Risk Countries

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

How to conduct Enhanced Customer Due Diligence?

What to do?

Obtain Additional Information on Customer/Beneficial Owner

Obtain Approval from Senior Management to Process Business Transactions

Obtain Additional Information on Intended Nature of Relationship

Regularly Update Identification Data

Enquire and Record Reasons for Transactions

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

Record Keeping by Casinos

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

How to keep records?

What are the records?	For how long?
▪ CDD Information ▪ Copies of ID/Passport/ Driving License, etc.	6 years from the date of closure of business relationship
▪ Transaction Records	6 years from the date of transaction
▪ Any other Report Furnished to the FIU	6 years from the date of furnishing the report

However;

Must retain for more than 6 years if,

FIU directs to keep any information/record of transaction/report for such longer period

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

Screening for UNSCR's Designated lists of Sanctions

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

Screen customers against Sanction lists published under **"United Nations Security Council Resolutions (UNSCR)"**

To screen against UNSCR you need to refer

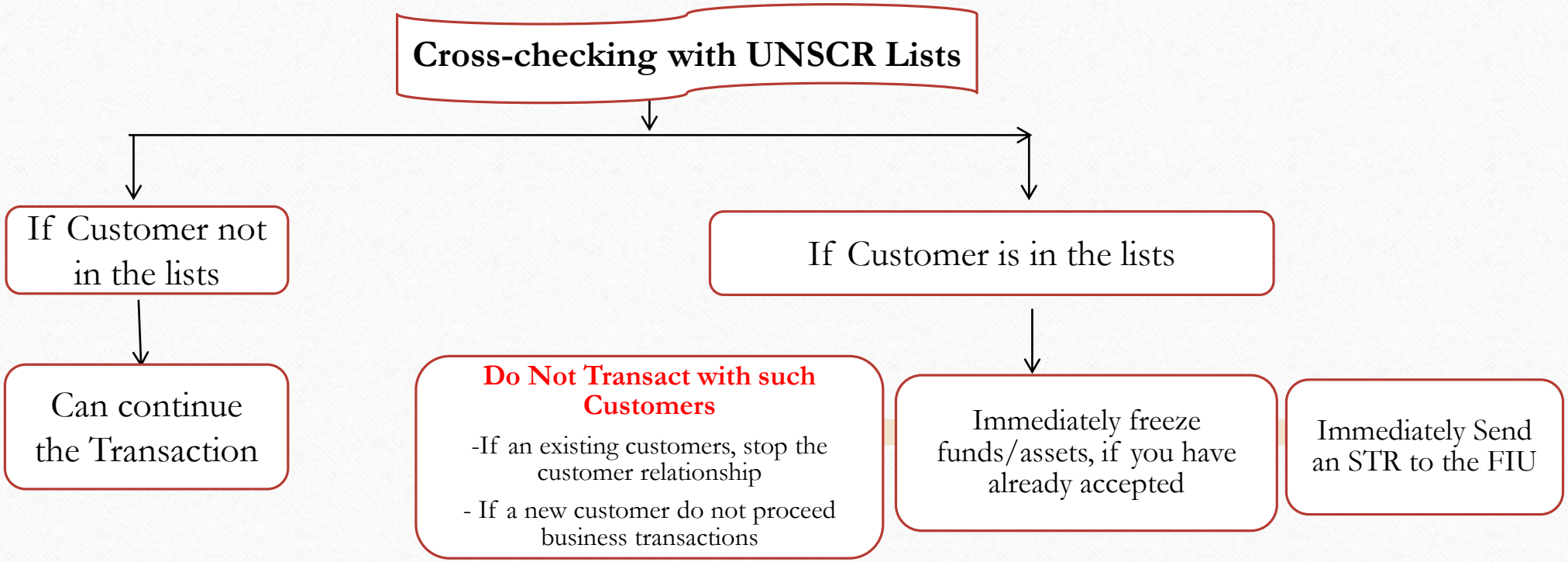
Refer www.fiusrilanka.gov.lk/UNSanctions

- Institution should screen their customers against UNSCR designated lists using the data collected at the CDD process.
- If a name matches with a name in such list that is the institution found that there are similar name/s to the customer's name in the UNSCR list, then it should be immediately communicated to the FIU while holding the funds if the institution has already accepted the fund.

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

What you should do?

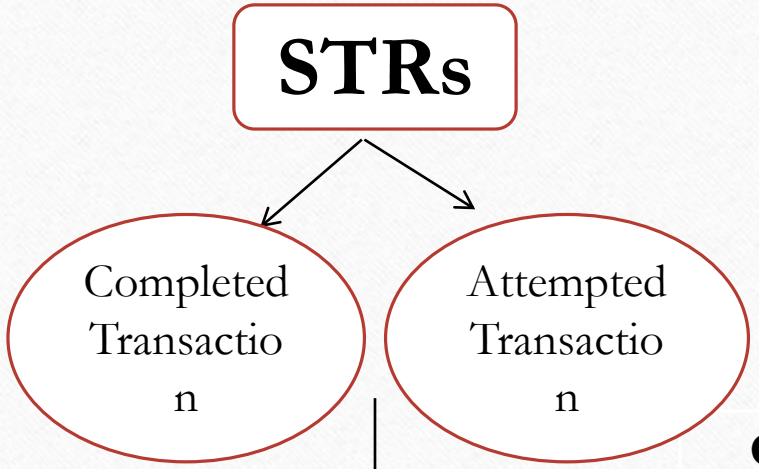
Should cross-check whether any customer/beneficiary appears on such designated lists



Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

Reporting Suspicious Transactions (STRs) by Casinos

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு



On What?

- Related to commission of any "unlawful activity or any other criminal offense"-Section 33 of the FTRA
- Has information that suspect may be relevant to an act preparatory to an offense under provisions of Convention of the Suppression of Financing of Terrorism Act No. 25 of 2005 (CSFTA)
- Has information that suspect may be relevant to an investigation/prosecution for an act of any unlawful activity or offense under CSFTA or PMLA

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

On what form?

In Writing

May be by mail or telephone;
BUT
Should be followed up in writing within 24 hours

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

How soon shall report Suspicious Transaction?

As soon as practicable after forming the suspicion

BUT!!!

Not later than two working days therefrom…

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

How to send STRs ?

Schedule V of the Suspicious Transactions (Format) Regulations of 2017

(This schedule is available at http://www.fiusrilanka.gov.lk/docs/Regulations)

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

Schedule V

CONFIDENTIAL

Province :
District :

SUSPICIOUS TRANSACTION REPORT					
a. This report is made pursuant to the requirement to report suspicious transactions under the Financial Transaction Reporting Act, No. 6 of 2006 b. Under Section 12 of the Act, no civil, criminal or disciplinary proceedings shall be brought against a person who makes such report in good faith.					
PART A - DETAILS OF REPORT					
1	Date of Sending Report				
2	Is this replacement to an earlier report ?	Yes		No	
PART B - INFORMATION ON SUSPICION					
3	Name in Full (if organization, provide registered business/organization name)				
4	Residential/ Registered Address				
5	NIC No. / Passport No./ Business Registration No.				
6	Gender	Male		Female	

7	Country of Residence and Nationality (if an individual)	
8	Business/ Employment Type	
9	Occupation (where appropriate, principal activity of the person conducting the transaction)	
10	Name of Employer (where applicable)	
11	Contact Details	
	PART C - DESCRIPTION OF SUSPICION	
12	Details of Transaction / Activity	
13	Ground / Reasons for Suspicion	

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

PART D - DETAILS OF REPORTING PERSON		
14	Date of Reporting	
15	Signature	
16	Name of Reporting Person/Agency	
17	NIC Number	
18	Designation / Occupation	
19	Address	
20	Contact Details	

Other AML/CFT requirements for Casinos

- Assessing the ML/TF risk before introducing New Technologies
- Screening of employees when recruiting
- Conducting of periodic AML/CFT Training for employees
- Auditing of AML/CFT applications

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

Reporting Requirements to the FIU

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

Main reporting requirement is

- Reporting of Suspicious Transactions (STRs): (Already discussed)

Other reporting requirements are

- Reporting of Cash Transactions and Electronic Fund Transfers:

  (A mechanism will be introduced in future to report over Rs. 1 mn transactions to the FIU)

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

Responsibilities of the Compliance Officer

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

Compliance officer of the Casino is responsible for;

- Training staff on AML/CFT measures
- Making sure whether the CDD/Enhanced CDD is conducted properly by front line officers/staff
- Making sure whether the relevant staff/employees/departments assess ML/TF risk when introducing New technologies.
- Appointing Assistant Compliance Officers if required (Ex. For branches and subsidiaries)
- Making sure whether employees are properly screened at hiring
- Reviewing the AML/CFT Policy periodically
- Arranging an internal Audit Function
- Reporting STRs and maintaining a registry for STRs
- Having a proper record keeping system

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

“Be Comply to Avoid Penalties”

For non-compliance:

- Severe financial penalties
- Suspension/cancellation of license
- Imprisonment

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

Contact details of the FIU Sri Lanka

Mail: Director,
Financial Intelligence Unit of Sri Lanka,
Central Bank of Sri Lanka,
No. 30, Janadhipathi Mawatha,
Colombo 01.

Telephone: +94112477125/509

Fax: +94112477692

E-mail: fiu@cbsl.lk/fiudnfbp@cbsl.lk

Web: www.fiusrilanka.gov.lk

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு

THANK YOU

Financial Intelligence Unit
මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதல் பிரிவு