

# AML/CFT COMPLIANCE OBLIGATIONS

Practical Session for Compliance Officers

DNFBP Supervision Division



ශ්‍රී ලංකා මහ බැංකුව  
இலங்கை மத்திய வங்கி  
CENTRAL BANK OF SRI LANKA



Financial Intelligence Unit  
இலா உத்டி லீகை  
நிதியியல் உளவறிதல் பிரிவு

# APPOINTMENT OF A COMPLIANCE OFFICER



# Why do You Need to Appoint a Compliance Officer?

- DNFBPs are obliged to appoint a compliance officer under the requirements of AML/CFT laws and regulations in Sri Lanka.
- Accordingly, Section 14 of the **Financial Transactions Reporting Act No, 06 of 2006 (FTRA)** specifies the legal requirement to appoint a compliance officer.

# Who is a Compliance Officer?

- **Compliance Officer** is the person who is responsible for ensuring the institution's compliance with the **AML/CFT** requirements.
- Compliance Officer should be a **senior management level** officer.

# Duties of the Compliance Officer

Compliance officer is responsible to ensure the Institution's compliance with the AML/CFT obligations by carrying out following tasks,

- Assess and periodically update overall ML/TF risk of the Institution.
- Prepare the **AML/CFT Compliance Policy** and procedures and obtain the approval of the top management.
- Implement customer identification requirements.
- Implement procedures for record keeping requirements.
- Make officers aware of laws relating to ML/TF and, train officers, employees and agents to recognize suspicious transactions.
- Screen all persons before hiring them as employees.
- Establish an audit function to test its procedures and systems for the provisions of the Act.

# How to Appoint a Compliance Officer?

Download the “Compliance Officer Declaration Form” from [www.fiusrilanka.gov.lk](http://www.fiusrilanka.gov.lk)



Owner/Managing Director/Chief Executive Officer of the institution should make the appointment of the compliance officer



Appointment of the Compliance Officer should be notified to the Director FIU



Hard copy of the declaration form should be posted or hand delivered to:

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




Send the soft copy of the duly filled declaration form to [fiudnfbp@cbsl.lk](mailto:fiudnfbp@cbsl.lk)





# Compliance Officer Declaration Form


 <b>Financial Intelligence Unit</b> இலங்கை மத்திய வங்கி நிதியியல் உளவறிதல் பிரிவு		<b>Declaration of the Compliance Officer appointed under Section 14 (1) (a) of the Financial Transactions Reporting Act, No. 6 of 2006</b>		<i>for office use only</i> <div style="border: 1px solid black; width: 30px; height: 20px; margin: 0 auto;"></div>
This form should be filled by the owner/Managing Director/Chief Executive Officer of the institution				
<b>Type of declaration</b> A <input type="checkbox"/> Initial Registration B <input type="checkbox"/> Alteration of existing information		<b>Sector</b> A <input type="checkbox"/> Real Estate      D <input type="checkbox"/> Lawyer/Notary B <input type="checkbox"/> Gem and Jewellery      E <input type="checkbox"/> Accountant C <input type="checkbox"/> Casino      F <input type="checkbox"/> Trust/Company Service Provider		
We wish to inform you that Mr/Mrs /Miss .....(name) .....(Designation) has been appointed as the Compliance Officer of .....(Reporting Institution) under Section 14 (1) (a) of the Financial Transactions Reporting Act, No. 6 of 2006, to ensure the institution's compliance with the Act.				
<b>The details of the Compliance Officer are as follows:</b> NIC/Passport Number: ..... Official Address : ..... Telephone number : Office ..... Mobile..... Email Address : ..... Fax ..... Specimen Signature : .....  Yours faithfully ..... Signature of the owner/MD/CEO with Official Stamp ..... Date .....  Name of the owner/MD/CEO : Mr/Mrs/Ms/Dr ..... NIC/Passport Number : ..... Official Address : ..... Telephone number : Office ..... Mobile ..... Email Address : ..... Fax .....  Copy to : ..... (name of the compliance officer)				



**ශ්‍රී ලංකා මහ බැංකුව**  
**இலங்கை மத்திய வங்கி**  
**CENTRAL BANK OF SRI LANKA**



**Financial Intelligence Unit**  
**இலங்கை நிதியியல் உளவறிதல் பிரிவு**

 <b>Financial Intelligence Unit</b> இலங்கை மத்திய வங்கி நிதியியல் உளவறிதல் பிரிவு		<b>Declaration of the Compliance Officer appointed under Section 14 (1) (a) of the Financial Transactions Reporting Act, No. 6 of 2006</b>		<i>for office use only</i> <input type="text"/>
This form should be filled by the owner/Managing Director/Chief Executive Officer of the institution				
<b>Type of declaration</b> A <input type="checkbox"/> Initial Registration B <input type="checkbox"/> Alteration of existing information		<b>Sector</b> A <input type="checkbox"/> Real Estate B <input type="checkbox"/> Gem and Jewellery C <input type="checkbox"/> Casino D <input type="checkbox"/> Lawyer/Notary E <input type="checkbox"/> Accountant F <input type="checkbox"/> Trust/Company Service Provider		
We wish to inform you that Mr/Mrs /Miss .....(name) .....(Designation) has been appointed as the Compliance Officer of .....(Reporting Institution) under Section 14 (1) (a) of the Financial Transactions Reporting Act, No. 6 of 2006, to ensure the institution's compliance with the Act.				

- 1) Clearly mention whether it is a initial registration or alteration of the existing information under the **Type of declaration**
- 2) Clearly mention the relevant **Sector** in which they conduct business
- 3) **Full name** of the Compliance Officer and his/ her **Designation** should be written clearly in the form
- 4) Name of the company should be clearly mentioned in the blank of “**Reporting Institution**”



The details of the Compliance Officer are as follows:

NIC/Passport Number: .....

Official Address : .....

Telephone number : Office ..... Mobile.....

Email Address : ..... Fax .....

Specimen Signature : .....

Yours faithfully

.....

Signature of the owner/MD/CEO with Official Stamp

Date

Name of the owner/MD/CEO : Mr/Mrs/Ms/Dr .....

NIC/Passport Number : .....

Official Address : .....

Telephone number : Office ..... Mobile .....

Email Address : ..... Fax .....

Copy to : ..... (name of the compliance officer)

5

Official telephone numbers and the mobile number of the compliance officer, the official e-mail address for which the compliance officer has access and the official fax number should be clearly written under the contact details.

6

The appointment must be certified by the **CEO/ Senior Official** of the company with the official stamp.

7

Details of the chief executive officer or the sole practitioner or the sole proprietor should be clearly mentioned and **certified form** should be copied to the appointed Compliance Officer for his/her knowledge and reference.



ශ්‍රී ලංකා මහ බැංකුව  
இலங்கை மத்திய வங்கி  
CENTRAL BANK OF SRI LANKA



Financial Intelligence Unit  
இலா உத்டி ஸீகைக  
நிதியியல் உளவறிதல் பிரிவு

# After the Appointment...

- Compliance Officer must **participate in Training Sessions** conducted by the FIU, on AML/CFT obligations.
- Compliance Officer should **be knowledgeable** on relevant Money Laundering and Terrorist Financing risk of the sector.
- Compliance Officer should be **contactable**.
- If the Compliance Officer resigns from his institution, he/she should inform it to the Chief Executive Officer/Managing Director or Owner and the CEO/Managing Director/Owner should **immediately appoint a new person** as the Compliance Officer.
- **New appointment** of the Compliance Officer should be informed to the Director/FIU using the same procedure.

# ML/TF Risk Assessment Questionnaire

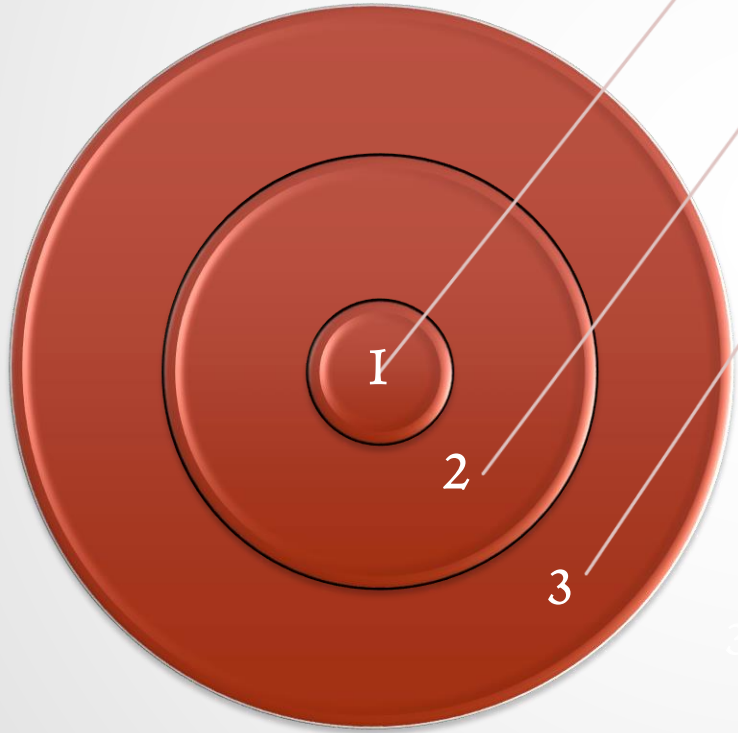
- The FIU sends you a questionnaire annually.
- Purpose is to assess your ML/TF Risk for offsite supervision.
- You are required to fill the questionnaire properly.

## ML/TF Risk Assessment Questionnaire

# ML/TF RISK ASSESSMENT



# ML/TF Risk Assessment



1. **Institutions** identify, assess and understand **institutional ML/TF risk**
2. **Supervisory authorities** identify, assess and understand **sector wise ML/TF risk**
3. **Countries** identify, assess and understand **national level ML/TF risk**





# Why ML/TF Risk Assessment is Important?

It provides foundation for:

- entire risk-based AML/CFT programme.
- efficient allocation of resources across AML/CFT functions in most effective way.
- developing appropriate risk mitigation or controlling measures according to identified risk levels.



Risk Assessment is the base of entire AML/CFT Programme



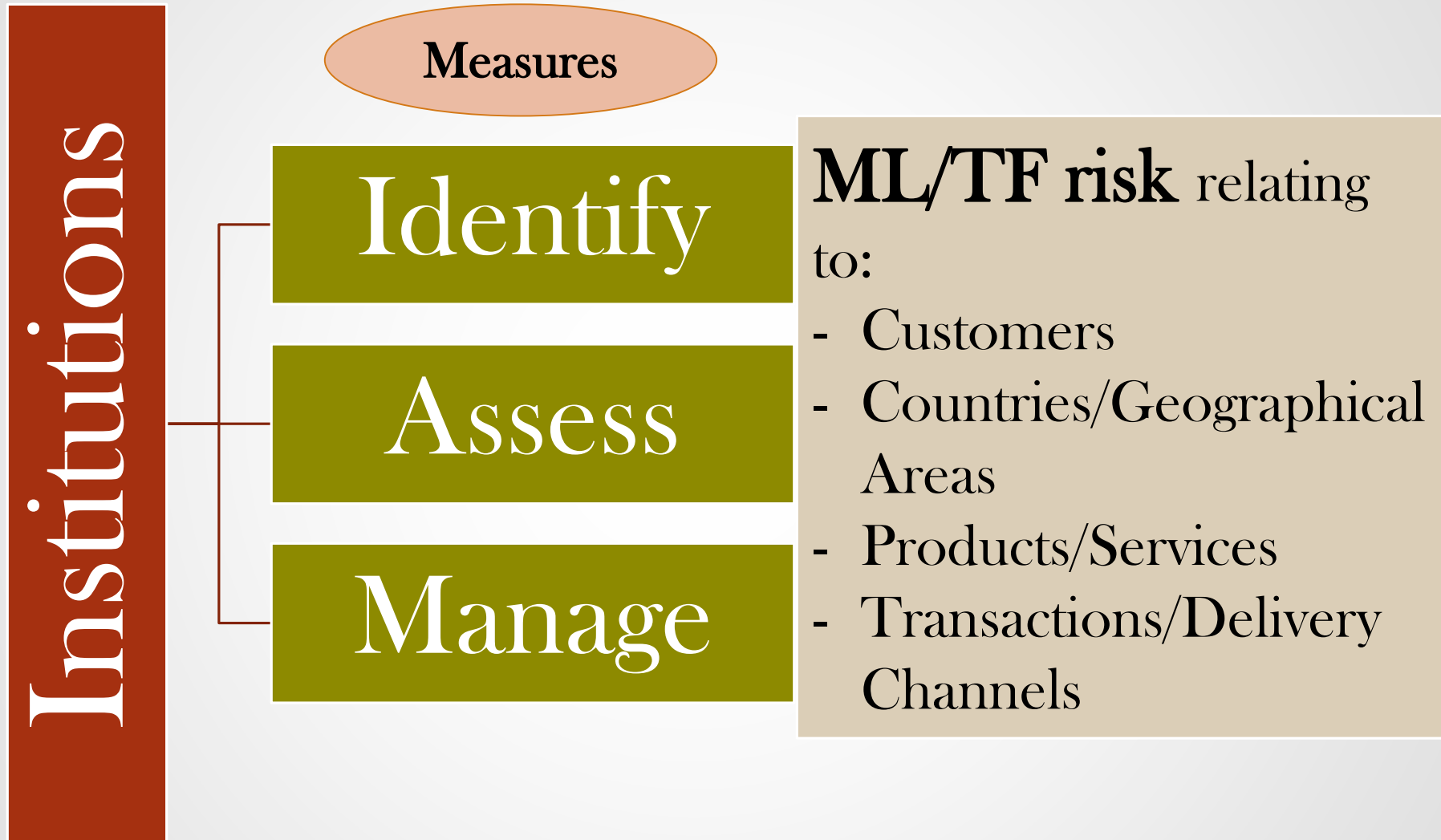
ශ්‍රී ලංකා මහ බැංකුව  
இலங்கை மத்திய வங்கி  
CENTRAL BANK OF SRI LANKA



Financial Intelligence Unit  
இலங்கை நிதியுதவிப்  
நிதியியல் உளவறிதல் பிரிவு



# ML/TF Risk Management Concept



# Identifying ML/TF Risk

- You are the one who knows your business well.
- Identify 'inherent risk' (**threats** + **vulnerabilities**) that your business faces during the normal course of business.
- Generally, threats include external factors that can make attractive your business for money launderers and terrorist financiers.
- When identifying vulnerability of your business to ML/TF, the following can be considered:
  - nature, size, complexity of the business.
  - nature of products and services.
  - nature of delivery methods/delivery channels.
  - types of customers (individual or corporate).
  - countries that your business deals with/geographic location of clients.



## ❑ Nature, Size and Complexity of the Business

Factor	Vulnerability to ML/TF	
	High	Low
Scale of the business	Medium to large scale businesses (due to large customer base)	Small to medium scale businesses
Conduction of transactions	across international boundaries (can be easily exploited by money launderers)	Domestic transactions only
Complexity of business activities/structure	Complex in nature (Money launderers can hide themselves)	Simple in nature

## ❑ Nature of Products and Services

Factor	Vulnerability to ML/TF	
	High	Low
Product type	allows payments to third parties (Eg. repayments in cancelling real estate bookings)	Does not allow third party payments
Receipt and payments	Involve cash	Bank transfers
channeling of funds	across borders	domestic



## ❑ Nature of Delivery Methods/Delivery Channels

Factor	Vulnerability to ML/TF	
	High	Low
Customers relationship	Non-face-to-face (relationships through internet, telephone or intermediaries)	Face-to-face
Offering of products	via internet	Over the counter
Involvement of intermediaries	Allowed	Not allowed
Cash payments	Involved	Not involved
Destination of final delivery	Foreign jurisdiction	Within the country



## ❑ Types of Customers

Factor	Vulnerability to ML/TF	
	High	Low
Nature of the customers	Corporate clients (because difficult to identify the beneficial owner)	Individuals
Residency	Outside Sri Lanka/from high risk countries	In Sri Lanka
PEPs/NPOs	Yes	No
Carry on transaction through gatekeepers	Yes	No
Source of funds	Clear	Not clear

## ❑ Geographical Location of Clients/Countries you Deal with

Factor	Vulnerability to ML/TF	
	High	Low
AML/CFT measures of the country of the client	ineffective	effective
Exposure to criminal activities	High level of organized crimes	Peaceful countries
Exposure to terrorism	Presence of terrorist activities/groups	Not associated with terrorist activities
Country's location in the world map	In conflict zones or their border countries	In peaceful continents
Exposure to drug trafficking	Yes (eg. Colombia)	no

❑ Further, you should identify any other aspects that are susceptible for ML/TF activities.

e.g. : new technologies, new product and new delivery channels



# Assessing ML/TF Risk

- There is no standardized format to assess the identified risk.
- Use your professional judgement to assess or determine the **level of risk**.
- To determine the level of risk, you can consider:
  - each element of risk you have identified.
  - your business experience.
  - publicly available information.
- You can simply focus on ‘how likely an ML/TF event is?’
- Considering above as a combination, you can determine whether the ML/TF exposure of a particular risk factor is ‘**high**’ or ‘**low**’.

# A Sample Risk Assessment Matrix

Money Laundering and Terrorist Financing (ML/TF) Risk Assessment					
Risk Category	Risk Factors	Risk Elements	Yes/No	Special Remarks	ML/TF Risk (Yes/No)
Customer Risk					
Product/Service Risk					
Delivery Channels Risk					
Geographical Risk					



# Managing Risk

- Risk Assessment of your institution will enable you to develop proper policies, procedures and controls to **manage** and **mitigate** ML/TF Risk.
- You can allocate more resources for high risk areas.
- Proper risk mitigation measures are required at instances where you can effectively mitigate risks.
- Some risks may be inevitably inherent in nature and therefore cannot be mitigated or eliminated. In such instances, you have to develop proper risk controlling methods.
- Further, you can take simplified measures where lower risks are identified.



# Points to Ponder...

- You should periodically evaluate and review the Risk Assessment so as to identify the implications of new and emerging risks.
- Further, when there is any material change in your business, such as introducing new products, exploring new markets, expanding customer base, new delivery methods etc., you have to repeat your ML/TF risk Assessment.
- Do not forget to properly document your risk assessment and communicate to the management and all relevant employees.
- Maintain appropriate mechanisms to provide risk assessment information to relevant authorities, if required.



# AML/CFT COMPLIANCE POLICY AND PROCEDURES





# What is the legal requirement of an AML/CFT Compliance Policy?

- The Section 14 (1) (b) of the Financial Transactions Reporting Act, No. 06 of 2006.
- Rules 6 (f) and (g) of the Designated Non-Finance Business (Customer Due Diligence) Rules, No. 1 of 2018.

Accordingly, it is required to formulate an internal policy approved by the Board of Directors (BOD) or Senior Management subject to any written law in force for the time being on AML/CFT to manage the identified ML/TF risks.





# Importance of an AML/CFT Compliance Policy for your Institution

- To endorse regulator's presumption that your institution acts within a defined AML/CFT framework.
- To have a proper and fixed guidance within the company on AML/CFT compliance.



# AML/CFT Compliance Policy and Procedures Should be:

- I. Written.
- II. Well Documented.
- III. Obtained the approval of BOD/ Senior Management.
- IV. Well Communicated among all employees and staff.
- V. Periodically reviewed.

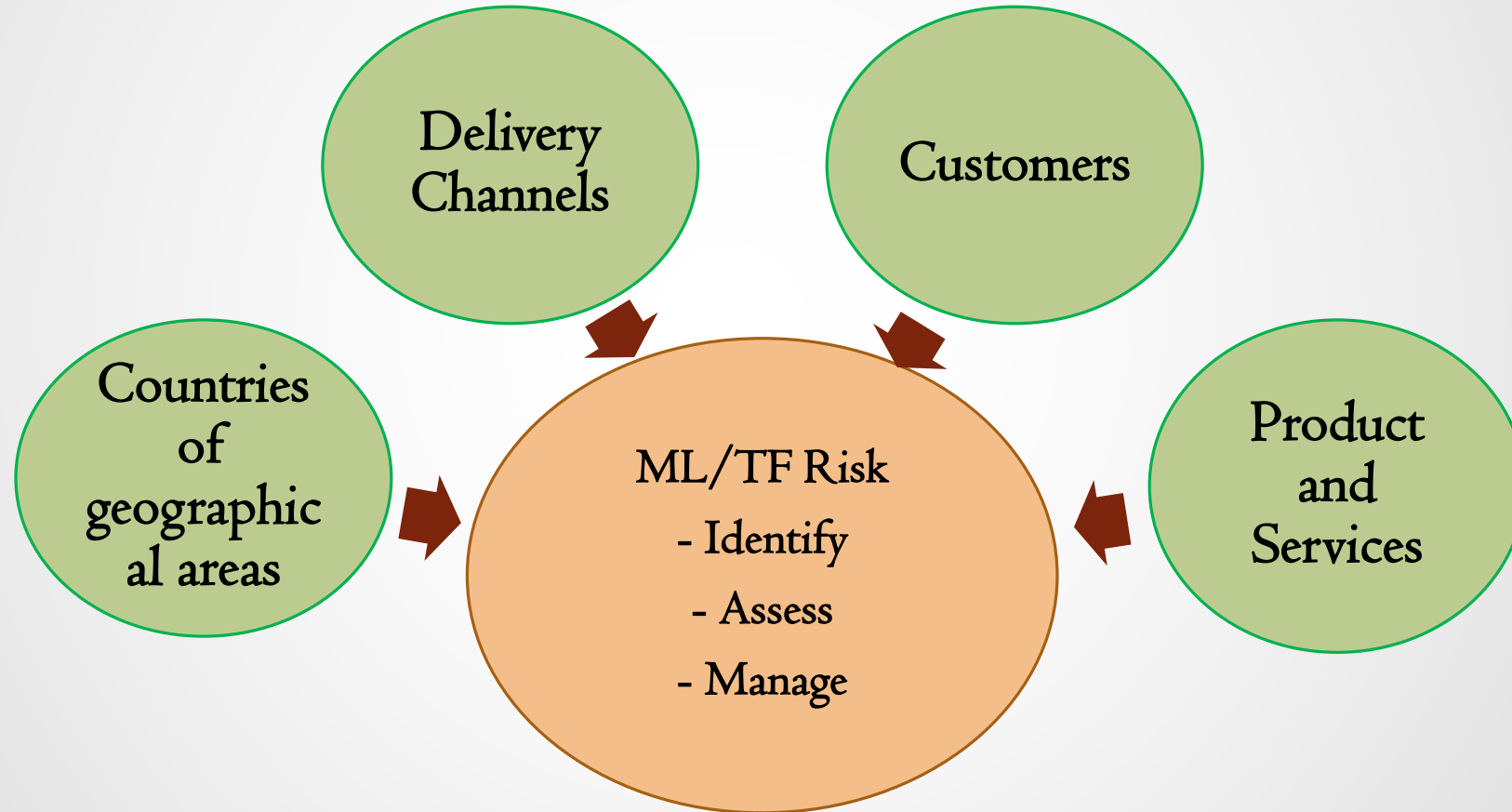


# What Should be Included in the AML/CFT Policy?

- The procedure of:
  - conducting Institutional ML/TF Risk Assessment.
  - conducting Customer Due Diligence (CDD) measures.
  - identifying and verifying the identity of the beneficial owners when establishing business relationships with legal persons and legal arrangements.
  - risk profiling of customers and beneficial owners.
  - conducting enhanced CDD.
  - screening customers against designated lists by United Nations Security Council.
  - keeping records.
  - submitting Suspicious Transaction Reports.
  - providing training programmes for employees.
  - screening employees.
  - maintaining an independent audit function.

# What Should be Included in the AML/CFT Policy?

- The procedure of conducting Institutional Risk Assessment
  - Format should be attached to the AML/ CFT Policy



# What Should be Included in the AML/CFT Policy?

- The Procedure of conducting Customer Due Diligence (CDD) measures against customers/beneficial owners.
  - The company can design their own procedure to identify and verify customers/beneficial owners according to the CDD Rule (Include the CDD form).

## Identify

- the full name;
- permanent residential or mailing address;
- occupation, name of employer, business or principal activity;
- 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;
- date of birth;
- nationality;
- source of funds;
- purpose of transaction;
- telephone numbers (residence, office or mobile)

## Verify

- obtain original documents and make copies



# What Should be Included in the AML/CFT Policy?

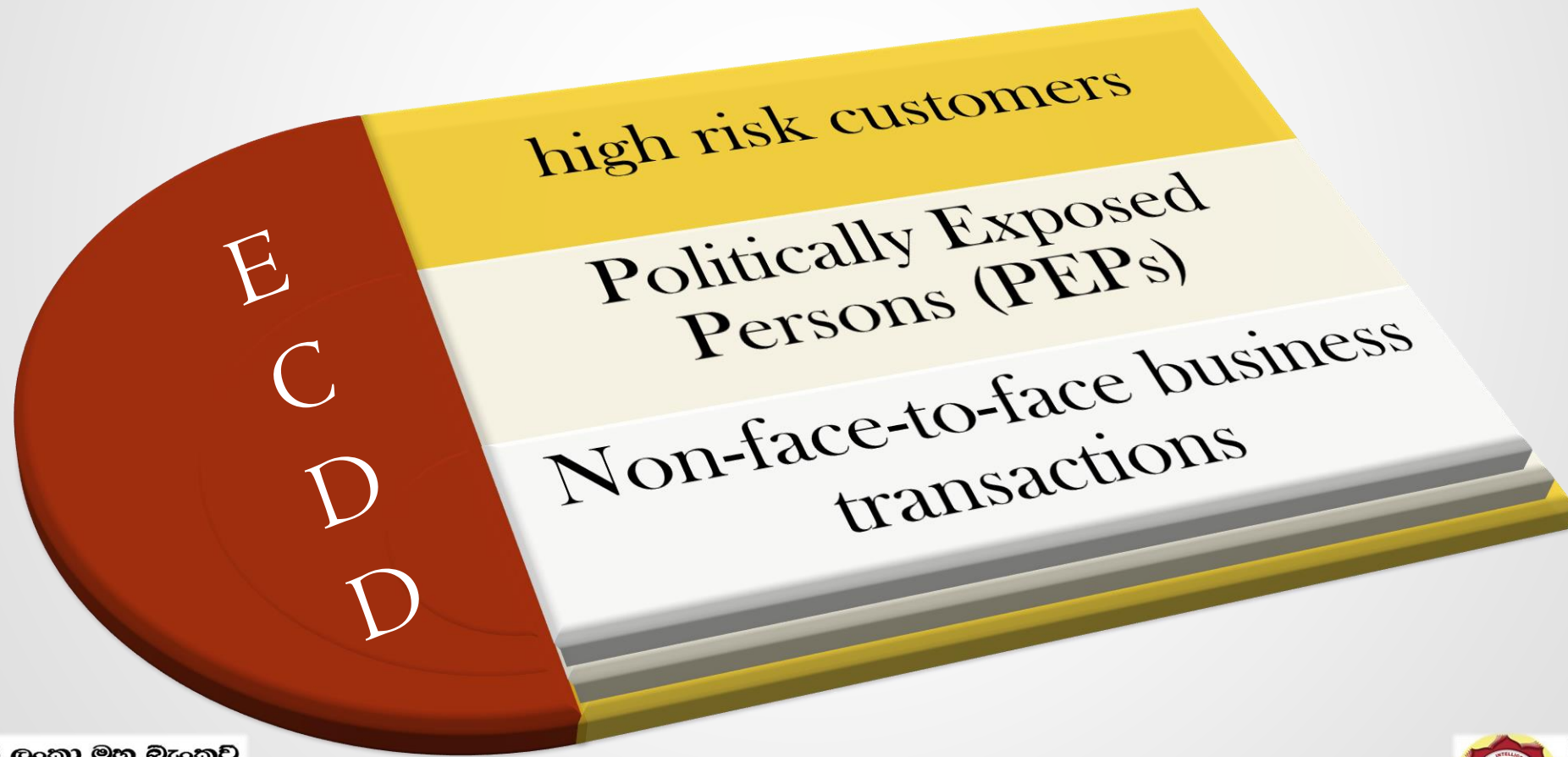
- The procedure of identifying and verifying the identity of the beneficial owners when establishing business relationships with legal persons and legal arrangements.
- The procedure of risk profiling of customers and beneficial owners.
  - Annex the format designed for customer risk profiling in the AML/CFT Policy.





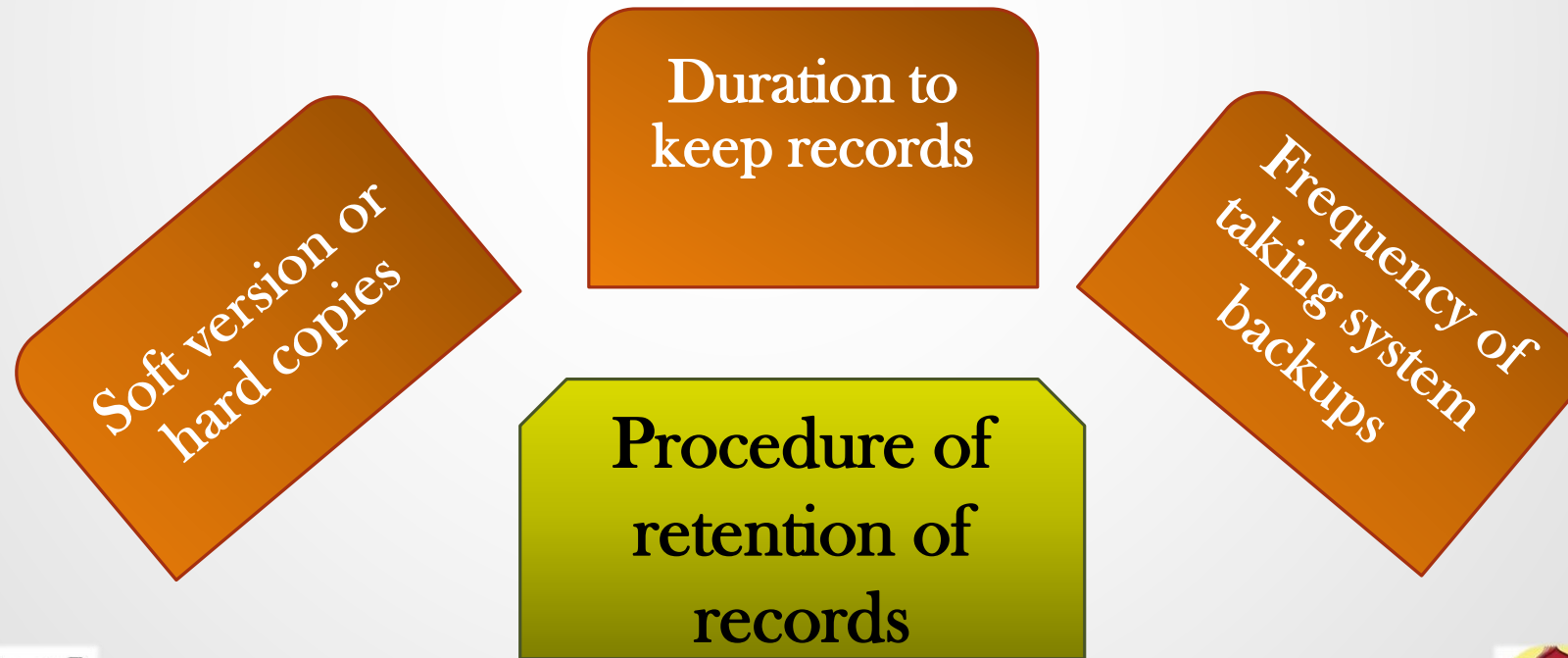
# What Should be Included in the AML/CFT Policy?

- The procedure of conducting enhanced CDD and the information the company should obtain from customers, should be specified.



# What Should be Included in the AML/CFT Policy?

- The procedure of screening customers against individuals and entities designated by the United Nations Security Council Resolutions (UNSCR) relating to targeted financial sanctions.
- The procedure of retention of records.



# What Should be Included in the AML/CFT Policy?

- Detection and internal reporting procedure of unusual or suspicious transactions.
- A procedure for reporting suspicious transactions to the Financial Intelligence Unit.
- Procedure of providing training programmes for relevant employees on identification of suspicious transactions, effectively managing the risk of money laundering and terrorist financing.
- A comprehensive employee due diligence and screening procedures at the time of appointing or hiring employees on permanent basis or any other basis.
  - Specify the documents which should get from the employees (eg: police report, Gramasewaka Certificate, Character Certificate, copy of National Identity Card, etc.).
- Procedure to maintain an independent audit function subject to relevant written laws.

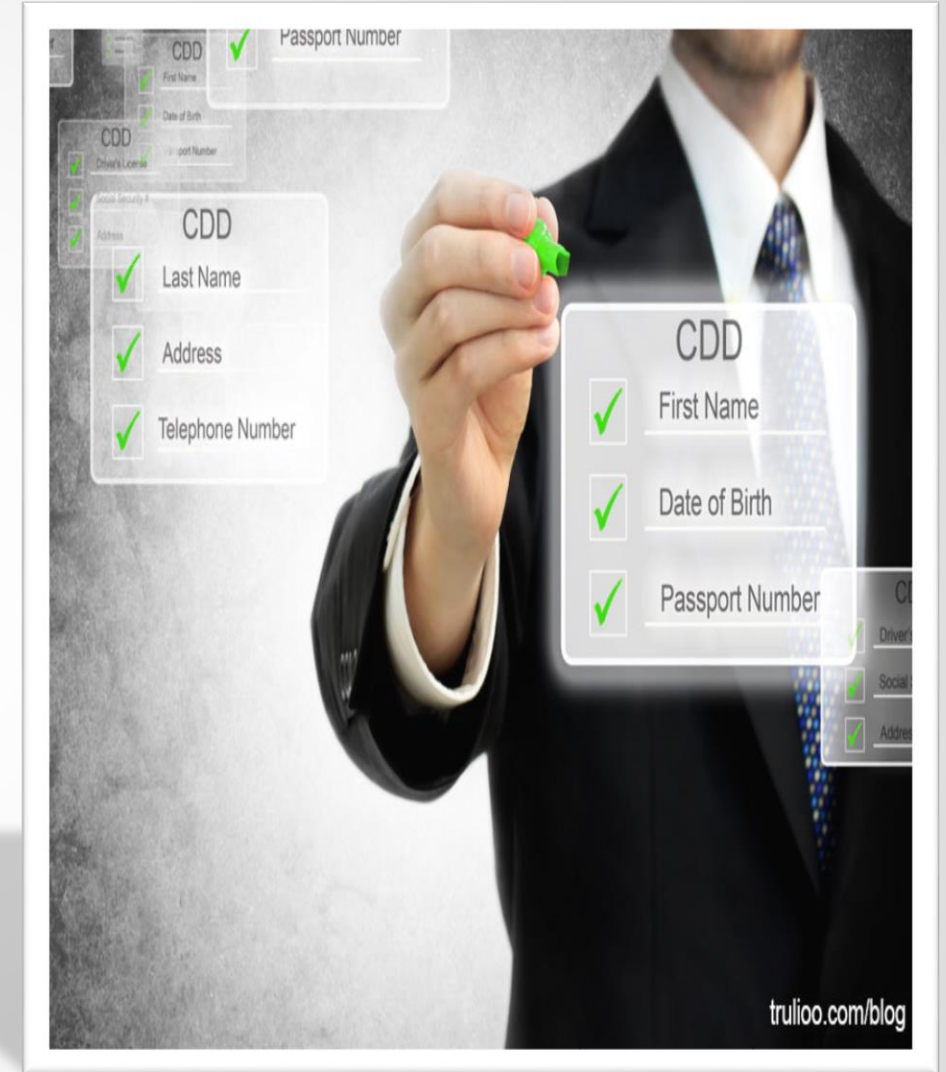
# References to formulate a Company AML/CFT Policy

- Financial Transactions Reporting Act No. 6 of 2006
- Designated Non-Finance Business (Customer Due Diligence Rules) No. 1 of 2018
- Guidelines on AML/CFT Compliance Obligations for Dealers in Real Estate, Precious Metals, Precious and Semi-Precious Stones
- Suspicious transactions (Format) Regulations of 2017

(The FIU has published a Guidance Note on preparation of the AML/CFT Policy)



# CONDUCTING CUSTOMER DUE DILIGENCE (CDD)





# What is CDD?

- Identify the customer and, verify customer's identity using reliable source documents, data or information.
- Verify whether any person purporting to act on behalf of the customer is authorized, and identify and verify the identity of such person.
- Identify the beneficial owner and take reasonable measures to verify the identity of the beneficial owner, using relevant information or data obtained from a reliable source, to the satisfaction of the non-finance business.

*Source: CDD Rules for DNFBPs*





# Do You Need to Conduct CDD for Each Customer?

Gem & Jewellery Dealers and the Casinos are ***not required*** to conduct CDD for each and every customer, as they have specific thresholds to conduct CDD.

**BUT**

Real Estate Agents are required to conduct CDD for every customer with whom they are carrying out transactions.



# Thresholds for Conducting CDD

## Real Estate Agents

- Conduct CDD for every customer

## Gem & Jewellery Dealers

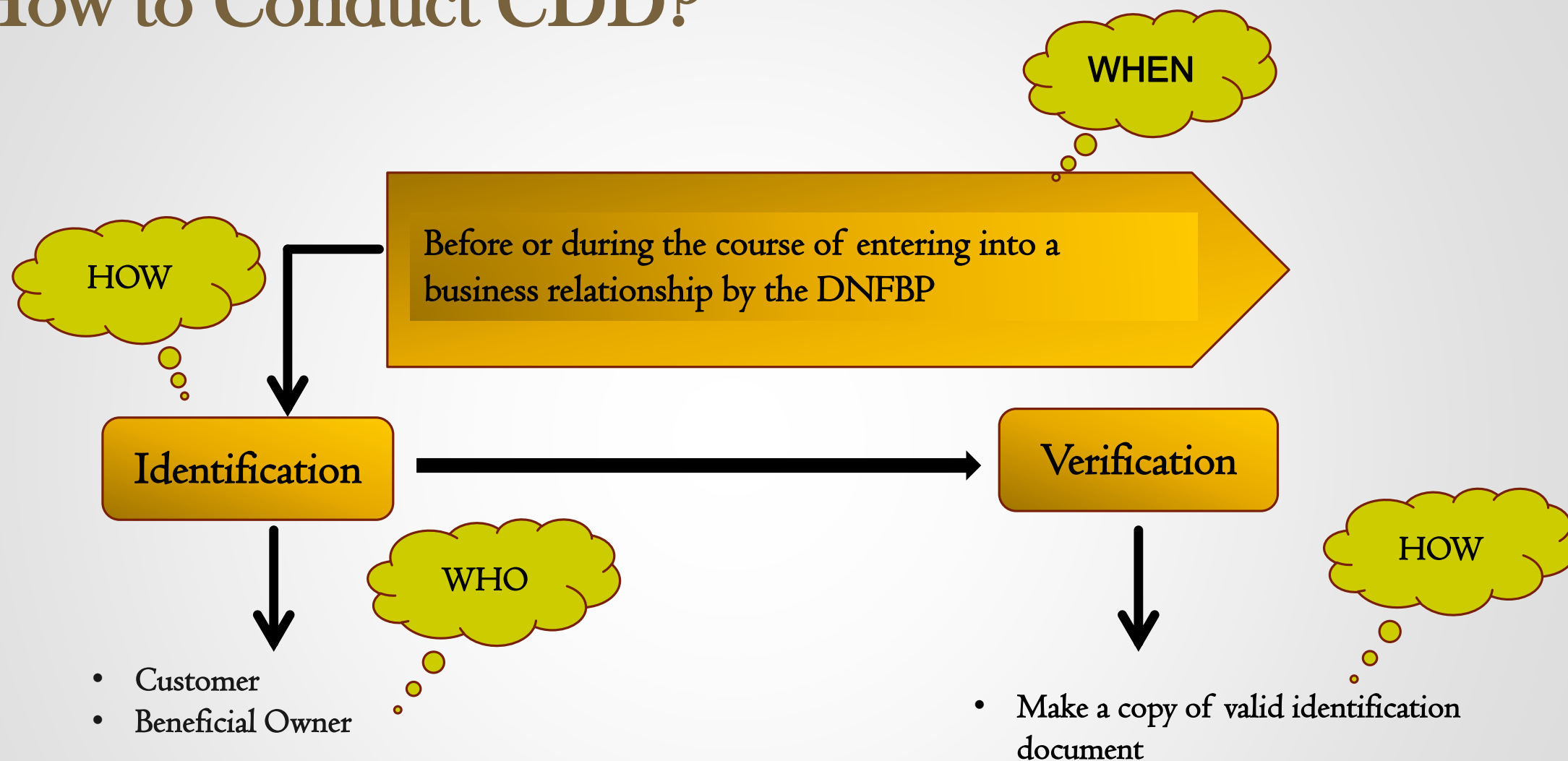
- Conduct CDD for customers engaging in **cash transactions** in Sri Lankan rupees or in any foreign currency equivalent to or above **USD 15,000**

## Casinos

- Conduct CDD for customers engaging in **financial transactions** in Sri Lankan rupees or in any foreign currency equivalent to or above **USD 3,000**



# How to Conduct CDD?



# Minimum Information you Should Obtain to Identify the Customer/Beneficial Owner

- (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)

# How to Obtain Minimum Identification Information?

Corporate world example  
for a CDD form

- Individual Customers
- Corporate Customers



# How to Verify the Individual Customer/Beneficial Owner?

For Customers-  
Using reliable,  
independent source  
document

NIC

Passport

Driving  
License

For any person  
purporting to act on  
behalf of the  
customer

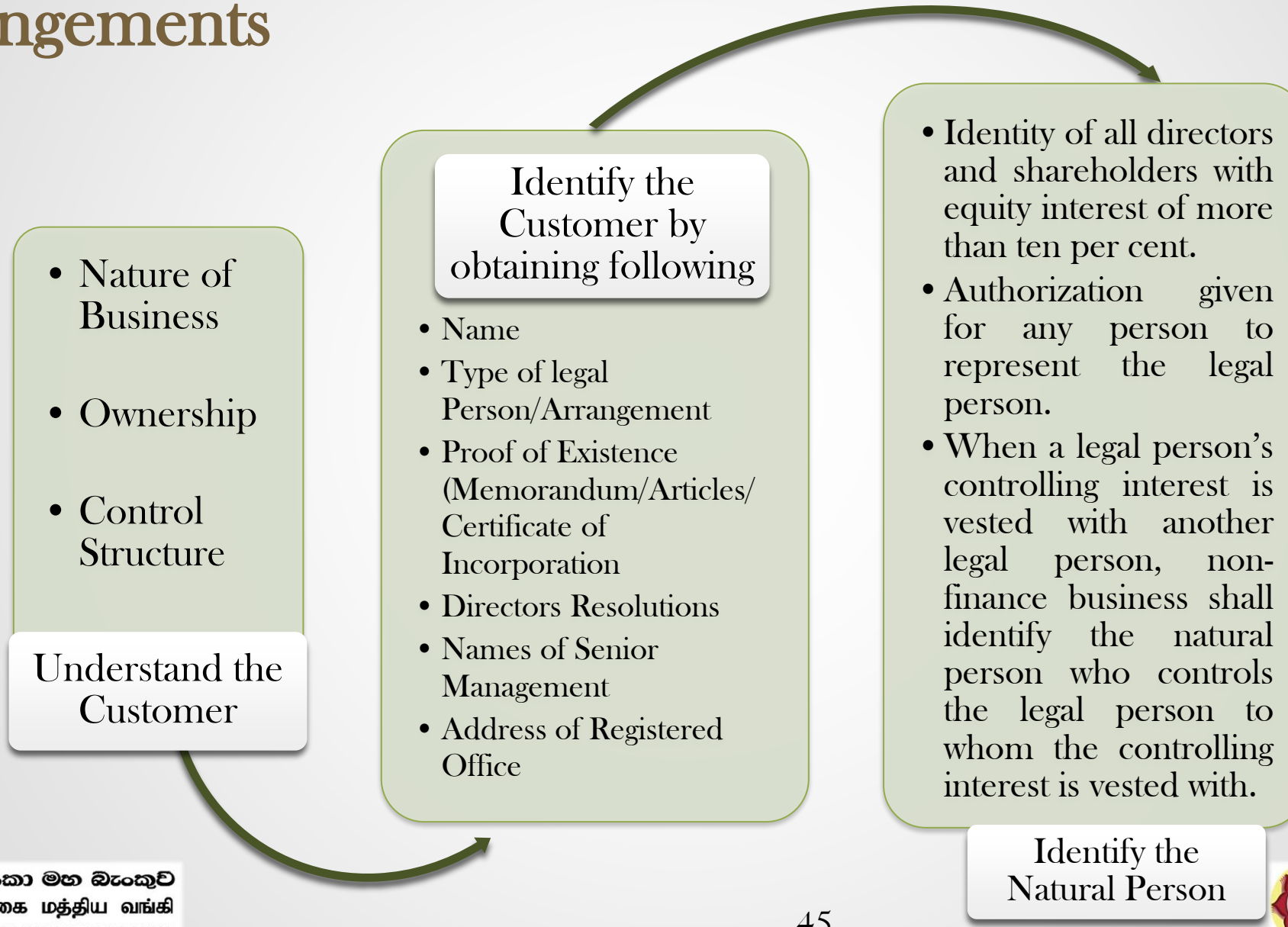
Verify the Identity

Verify the Authority  
to act on behalf of  
Customer





# CDD for Customers that are Legal Persons or Legal Arrangements



# What is Customer Risk Profiling?

Customer Risk Profiling is the formal process of rating the customers as high or low based on their ML/TF risk exposure which is conducted using the CDD information obtained.



# What are the Areas to be Concentrated for Customer Risk Profiling?



Customers Category



Geographic Location of Business /Country of Origin/Country of Residence



Products/Services/Transactions/ Delivery Channels



Others Important Areas

# What are the Areas to be concentrated for Customer Risk Profiling?

Area	Example
Customers Category	<input type="checkbox"/> Whether the customer is <ul style="list-style-type: none"> <li>• an individual, company or legal arrangement</li> <li>• local, foreign or non-resident</li> </ul>
Geographic Location of Business /Country of Origin/Country of Residence	<input type="checkbox"/> conduct transactions with customers from countries with AML/CFT deficiencies <input type="checkbox"/> locations that have designated terrorist organizations operating within their country
Products/Services/Transactions/Delivery Channels	<input type="checkbox"/> cash intensive businesses and cross border transactions
Others Important Areas	<input type="checkbox"/> Whether the customer or business operates in sectors that are inherently vulnerable to ML/TF risk



# Customer Risk Profiling Process

Identify the ML/TF Risk

Rate the Customer

Document the Risk Rating

ECDD for High Risk  
Customers



# Examples for Customer Risk Profiling of a Real Estate Agent

Mr. Y, a foreign customer visits your real estate company for the purpose of buying an apartment. In responding the questions raised by the sales personnel of your company to identify the customer, it was observed that the customer is a resident person of Pakistan. Since, Pakistan is a country with AML/CFT deficiencies as categorized by the FATF, the customer has to be rated as 'high risk' under the risk profiling.

XYZ corporate visits a land sales company to buy a land for their new branch. XYZ is owned by Sri Lankan citizens and the beneficial ownership of the company can be easily identified. In view of these, the land sales company can rank XYZ as a 'low risk' customer under the risk profiling.





# Examples for Customer Risk Profiling of a Gem & Jewellery Dealers

A foreign corporate entity orders a bulk of gems worth of around USD 25,000/- from a gem dealer on Sri Lanka via the gem dealer's web-site. Further, he does not visit the gem dealer to finalize the transaction and the payment is done via wire transfer. As the transaction is both non-face-to-face and cross-border the corporate entity has to be ranked as a 'high risk' customer in the risk profiling.

A customer visits a gem dealer for the purchase of a gem worth of around USD 15,000/- and he claims that he is a Chief Executive Officer of a highly reputed Bank of Sri Lanka. Further, his source of income is justifiable by his occupation details. In such a scenario the gem dealer can rank the customer as 'low risk' and obtain only the minimum CDD information specified by the CDD Rules.



# Sample Risk Profiling Outcome of an Institution

## Customer Risk Profiling of the XYZ Company

S/N	Full Name	NIC/ Passport	Address	Contact No.	Occupation	Country	Source of Income	Risk Categoriza tion
01	Mr. Mohammad Abdullah	1111111	425, Lahore Pakistan	22-22222	Business	Pakistan	Business	High
02	Mr. Anil Perera	233333V	65, Dewala Rd, Kesbewa	33-233333	Chairman - State Corporation	Sri Lanka	Salary	High
03	Mrs. Namali Fernando	652222V	87, 1 <sup>st</sup> Lane, Rajagiriya	44-255555	Teacher	Sri Lanka	Salary	Low



# How to Conduct Risk Profiling?

A specimen Customer Risk Profiling Matrix has been developed by the FTU for Real Estate and Gem and Jewellery Sectors



ශ්‍රී ලංකා මහ බැංකුව  
இலங்கை மத்திய வங்கி  
CENTRAL BANK OF SRI LANKA



Financial Intelligence Unit  
இலா உத்டி லீகை  
நிதியியல் உளவறிதல் பிரிவு

# What is Enhanced Customer Due Diligence (ECDD)?

Enhanced CDD is conducting following procedure with respect to a customer been rated as a high risk for ML/TF risk, in addition to minimum CDD information specified by the CDD Rule 11.

- obtain additional information on the customer and beneficial owner (e.g. volume of assets and other information from public database.
- obtain approval from the Senior Management , if any, before establishing or in the case of an existing customer for continuing such business relationship with the customer.
- obtain additional information on the intended nature of the business relationship.
- regularly update the identification data of the customer and the beneficial owner.
- enquire and record the reasons for prospective or performed transactions.



# ECDD Should be Conducted for following Customers;



- Customers rated as High Risk.
- Politically Exposed Persons.
- Non-face-to-face customers.
- NGOs and NPOs.
- Customers from High Risk Countries.

# Practical Example for ECDD

Mr. X a customer of a DNFBP has been identified as a 'Politically Exposed Person' (PEP) since he is a Chairman of a state-owned co-operation and the following procedure should be followed in conducting ECDD for the PEP;

- Obtain additional information on Mr. X (Title and details on the position the PEP holds).
- Obtain approval from Senior Management for the proceeding of the transaction.
- Obtain additional information on intended nature of relationship with Mr. X.
- Regularly update identification data of Mr. X on a specified time interval.





# IDENTIFYING AND REPORTING SUSPICIOUS TRANSACTIONS



# Pre Requisites for Identifying and Reporting STRs for DNFBPs

Establishing  
Procedures

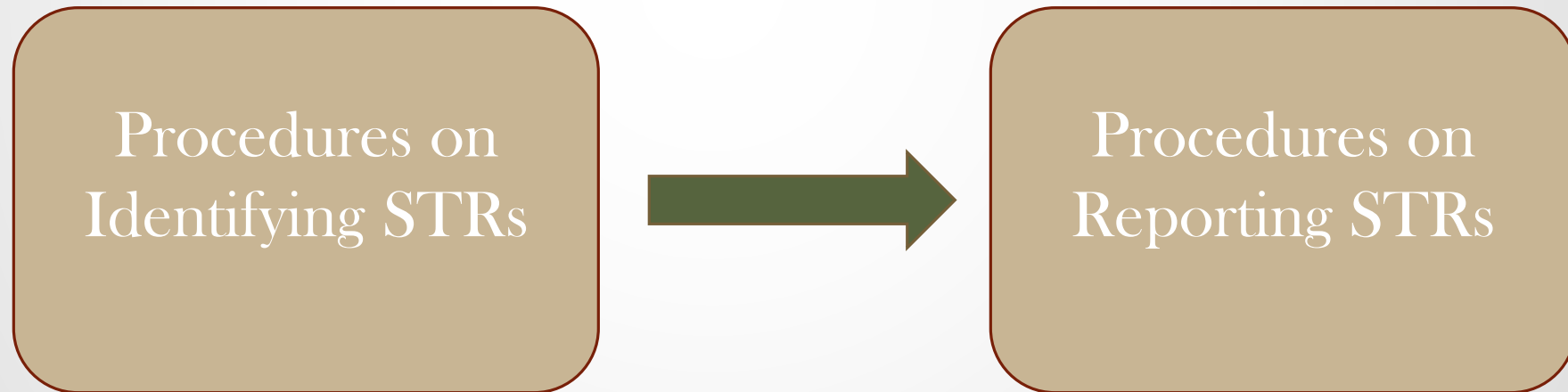
Communicating  
Procedures to  
relevant employees

Providing Adequate  
Training to relevant  
employees



# Establishing Procedures

- DNFBPs must develop procedures on how they should identify and report suspicious transactions.
- Must be included in the AML/CFT Policy.
- The procedures are two folded;



# Procedures for Identifying STRs

“Whenever a suspicious nature of transaction is identified by the **front desk sales employees**, the details of the transaction with the reasons for suspicion should be **informed immediately** to the **Sales Manager** of Company X.

The Sales Manager is then required to **immediately** report the suspicion to the **Compliance Officer** of Company X with all the information”.

# Procedures for Reporting STRs

“After a suspicion is generated by the front desk employees it is **immediately reported to the Compliance Officer** by the **Sales Manager**.

Thereafter, The Compliance Officer immediately submit an STR to the FIU and records the details of the suspicion in the **STR Registry** of Company X. The submission of the STR **should be within two working days** of forming the suspicion.”

# Communicating Procedures to Relevant Employees

- Procedures won't be effective without proper communication.
- Relevant employees must be made aware of the company procedures.

## Examples:

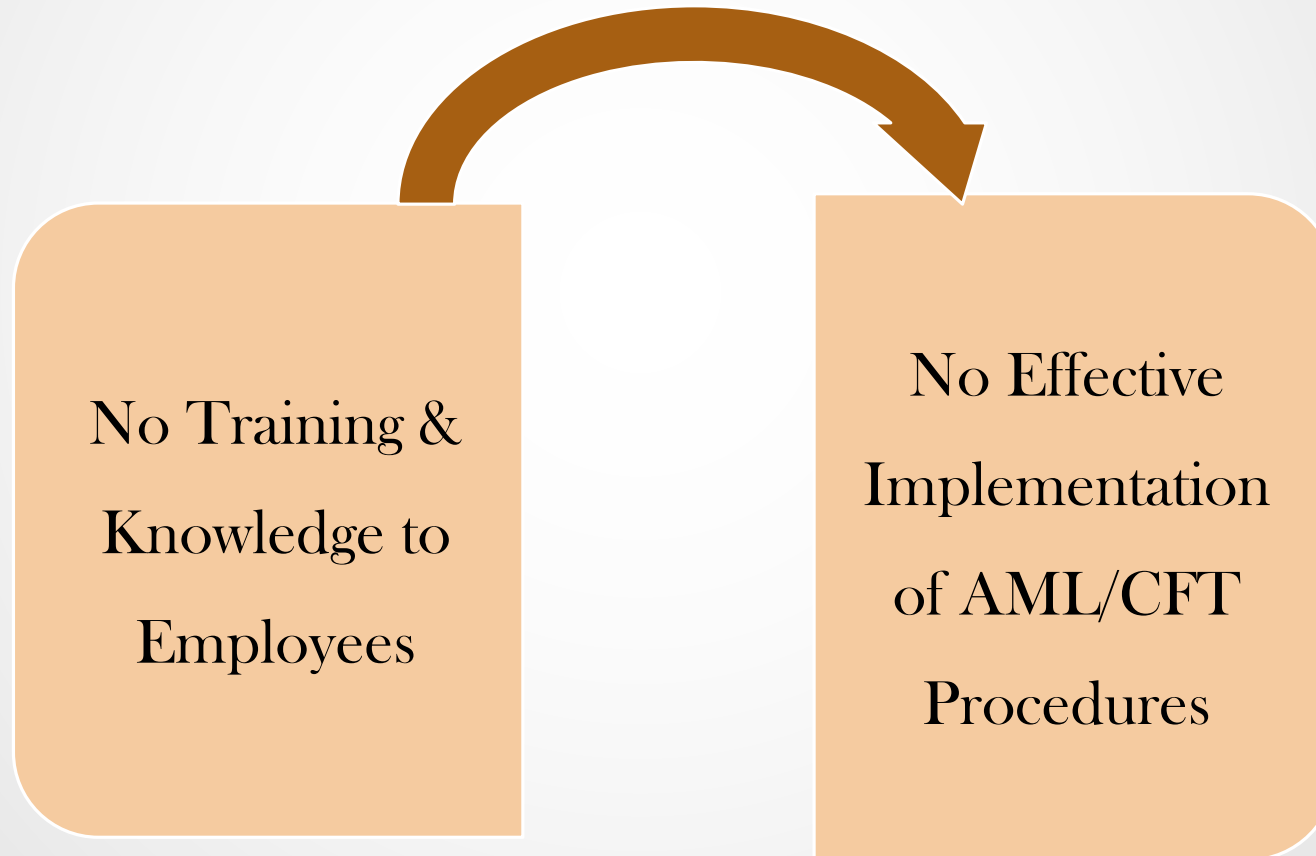
- Distributing the AML/CFT Policy at the Induction Programmes.
- Inform and update about STR Procedures at regular meetings.
- Review the implementation of the procedures at performance evaluations.





# Providing Training to Relevant Employees

Training is the most important aspect in identifying and reporting suspicious transactions.



# Important Facts to Know in STR Reporting

- The STR must be submitted to the FIU within 2 working days of forming the suspicion.
- The STR must be submitted in Written form.
- The CO can inform about the suspicion through telephone.
- However, should be followed by a written STR within 24 hours of informing the suspicion.
- There is a prescribed form to submit STRs.

The Format is prescribed in “**Suspicious transactions (Format) Regulations of 2017**”

DNFBPs must submit STRs using Schedule V



# Important Facts to Know in STR Reporting

- The CO must maintain an STR Registry.

What is an STR Registry?

**A database with all details on STRs submitted to the FIU**

What should be included in the STR Registry?

- Who reported the STR to the CO.
- When was the STR reported to the CO.
- Details of the suspicion (name, ID numbers, nature of suspicion etc..).
- When the STR was reported to the FIU.

# After Reporting an STR ?

- The FIU has a separate division for analyzing STRs.
- Confidentiality of reports are highly protected.
- Details of Institutions/persons who reported STRs are not revealed for any outside party.
- You are Protected under the FTTRA.



# Protection for Reporting STRs

Under Section 12 of the FTRA, no civil, criminal or disciplinary proceedings shall lie;

- in relation to any action carried out in good faith or
- in compliance with regulations made under the FTRA or any other rule issued under the Act.

Protection of persons reporting suspicious transactions.

12. (1) No civil, criminal or disciplinary proceedings shall lie against —

- (a) a such Institution, an auditor or supervisory authority of an Institution ; or
- (b) a director, partner, an officer, employee or agent acting in the course of that person's employment or agency of an Institution, firm of Auditors or of a supervisory authority,

in relation to any action by the Institution, the firm of auditors or the supervisory authority or a director, partner, officer, employee or agent of such Institution, firm or authority, carried out in terms of this Act in good faith or in compliance with regulations made under this Act or rules or directions given by the Financial Intelligence Unit in terms of this Act.

(2) The provisions of subsection (1) shall not apply in respect of any proceedings for an offence described in section 8 of this Act.

(3) If an Institution, firm of auditors or supervisory authority or any director, partner, officer, employee or agent, of any Institution, firm or authority or makes a report under



# What are Red Flags ?

Usually it's an **Indicator** or a **Sign of Danger**.

Therefore, learning about **Red Flags** on ML/TF is useful to detect suspicious transactions or customers.



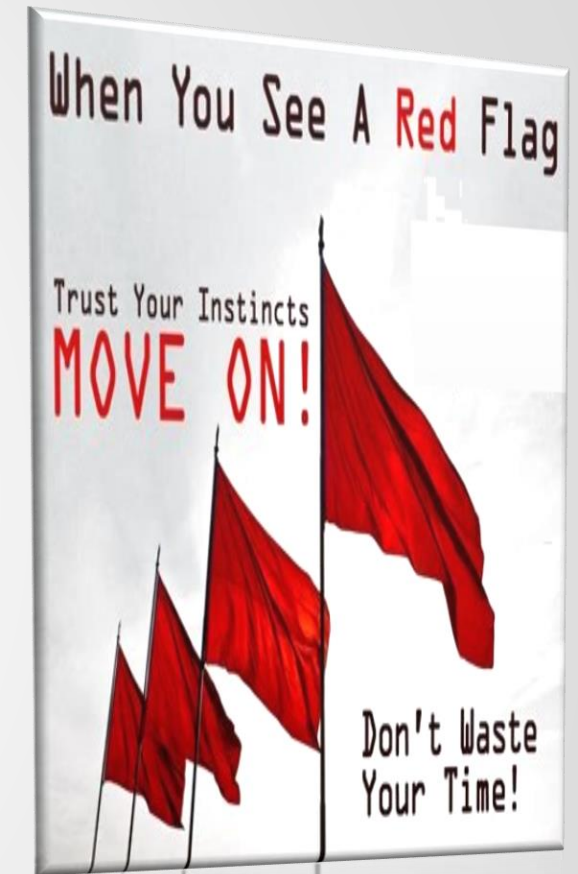


# Red Flags – Real Estate Sector

- Use of Nominees/Minors in purchasing real estate

The customer Frequently buys lands or apartments under the names of nominees or minors.

Cannot identify the relationship between the nominated person and the funding person.



# Red Flags – Real Estate Sector

- Address given by the customer is suspicious.

*Ex:*

- Address seems unknown.
- Address is simply a correspondence address.
- Letters sending to the given address get returns.



# Red Flags – Real Estate Sector

- Customer purchases the property without inspecting anything.

Ex:

- Customer not worrying about the price.
- Customer is not interested in site visits.
- Not concerned about other features of the land or apartment.



# Red Flags – Real Estate Sector

- Transaction does not match with the business activity known to be carried out by the customer.

Ex:

A customer approaching to buy a luxury apartment. Occupation is mentioned as a teacher and source of funds is salary.





# Red Flags – Real Estate Sector

- Customer suddenly cancels / aborts transaction and requests refund

Refund may be back to himself /herself / itself or to a third party.

Ex:

A customer visited a real estate agent and payed an advance in cash to buy an apartment. A month later, customer visited the office and asked to cancel the reservation as he cannot afford to buy the apartment. He agreed to the penalty of 5% from the initial advance for cancelling the reservations. The customer also requested to provide the refund through a company cheque.

# Red Flags – Gem and Jewellery Sector

- Customer executes transaction/transactions which is/are not consistent with his profile.

Asking ‘Occupation’ and ‘Source of Funds’ is extremely important.

Ex:

A customer walk in to the showroom and buys jewellerys of large values. The occupation mentioned in the CDD form is a teacher of a government school. The source of funds mention is salary.

The sales person must get the initial suspicion as to how a teacher of a government school affords to buy this value of jewellerys from his salary.



ශ්‍රී ලංකා මහ බැංකුව  
இலங்கை மத்திய வங்கி  
CENTRAL BANK OF SRI LANKA



Financial Intelligence Unit  
இலா உத்டி ஸீகை  
நிதியியல் உளவறிதல் பிரிவு



# Red Flags – Gem and Jewellery Sector

- Customer does not appear properly concerned about the value, size, quality and/or colour of the precious stone/metal or jewellery product.

Ex :

A customer walked in to the showroom to buy a gem. However, he did not care about the type of the gem or its colour. He asked about prices of the gemstones and purchased a gemstone for very high price.

\*usually gem buyers are very much concerned about type, colour and quality of the gemstone. Therefore, if a customer of above nature comes to your place, you should be cautious in dealing.

# Red Flags – Gem and Jewellery Sector

- Customer pays the value of the precious stone/metal or jewellery producing an unusual payment method.

Ex:

A customer pays for a gem stone with cash notes bundled with small denominations.

A customer in Sri Lanka buys the gemstone or jewellery, but payment comes from a unknown account from a foreign jurisdiction.

A customer walks in to the showroom with a third party (not a relative). Gemstone is purchased by the customer while the payment is done in cash by that third party.

# Red Flags – Gem and Jewellery Sector

- Frequent transactions by a customer especially over a short period of time below the regulatory threshold for customer due diligence, however the total of such transactions is substantial.

Need to be cautious if a customer frequently purchase jewelleries or gems under the threshold limit. It may be to avoid conducting CDD for his transactions.

Ex: a customer buys 3 gems for values below Rs. 2.0 mn within a week. However, the total value of his transactions within a week is extremely large.

# COMPLYING WITH UNSCR

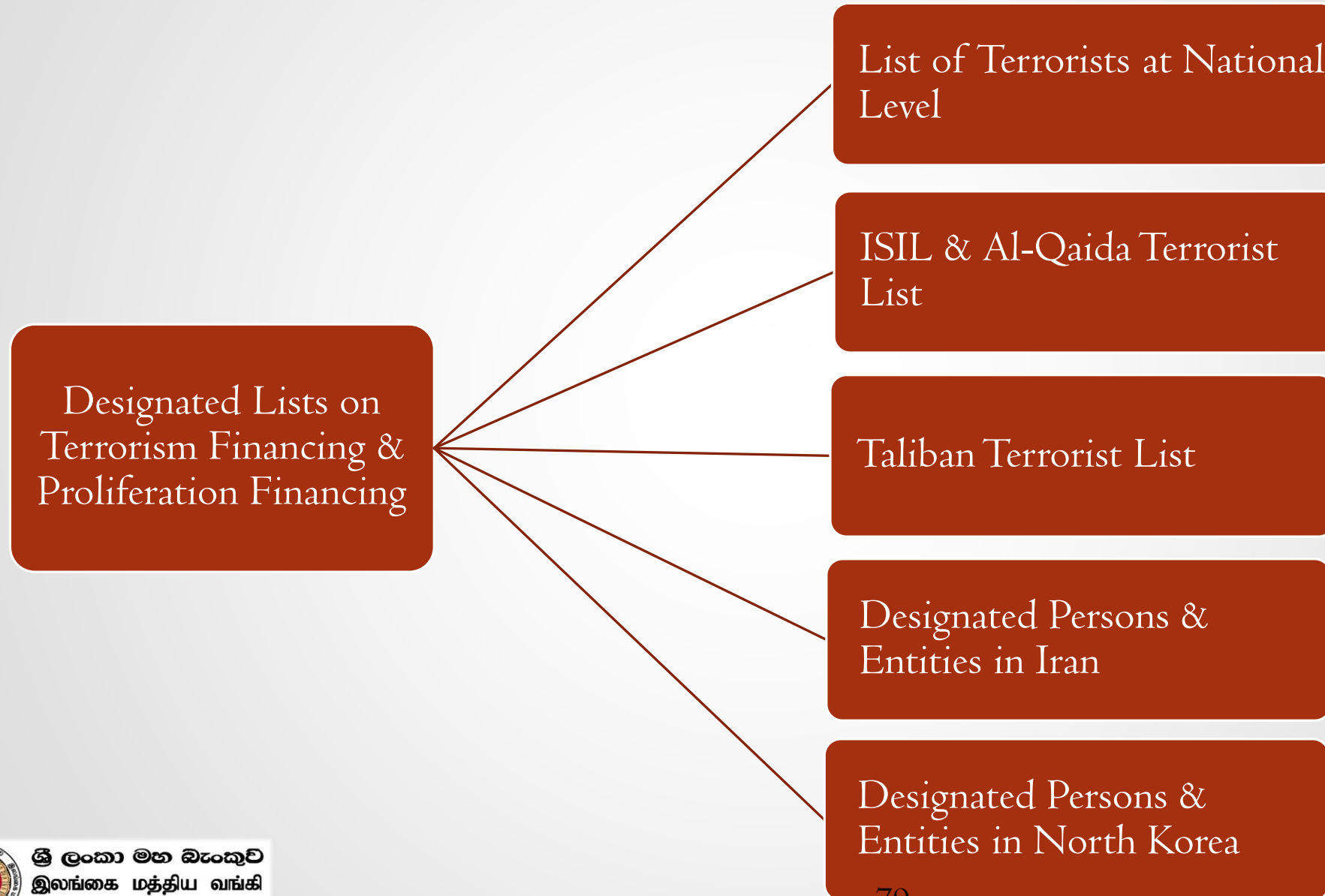


ශ්‍රී ලංකා මහ බැංකුව  
இலங்கை மத்திய வங்கி  
CENTRAL BANK OF SRI LANKA



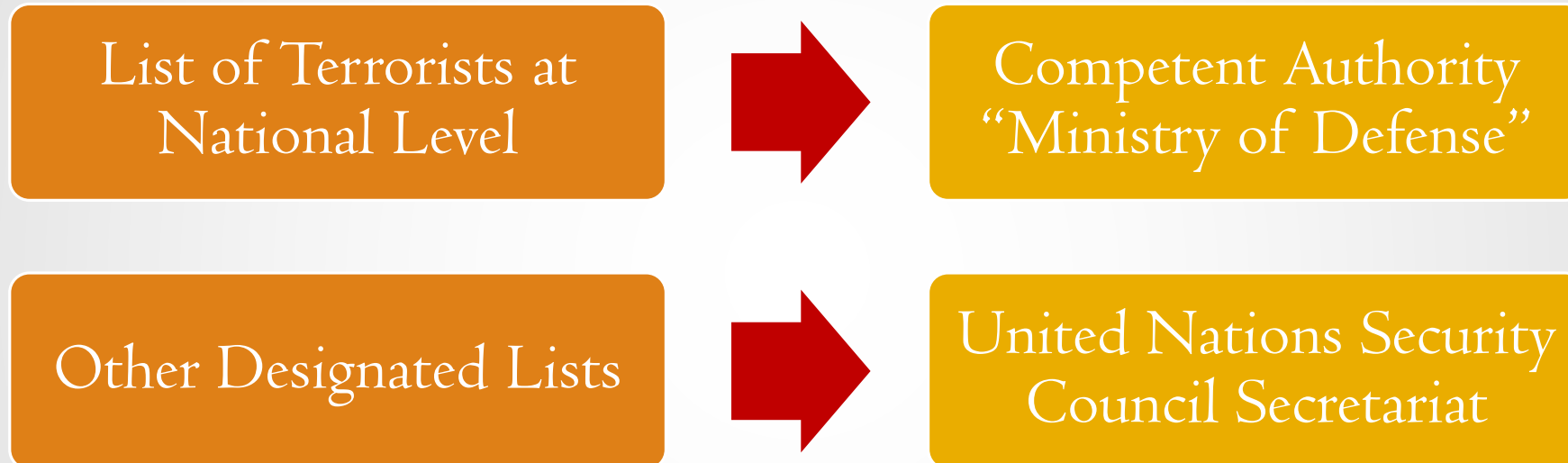
Financial Intelligence Unit  
இலா உத்டி லீகை  
நிதியியல் உளவறிதல் பிரிவு

# Overview of the Designated Lists



# How the COs Receive Updates to Designated Lists

- The FIU receives updates of the designated lists from following Institutions;



- Once the FIU receives the notification on update, immediately shared with Reporting Institutions.



# Responsibilities of the Compliance Officers (COs) in Screening Customers against Designated Lists

- Procedures must be established

AML/CFT Policy must be included with procedures on how to screen customers against designated lists on UNSCR.

Ex:

It is the responsibility of the CO to keep the designated lists received from the FIU, in **MS Excel format** and duly update the same whenever an update is forwarded by the FIU.

The CO must share the updates with the employees **involving in sales**, enabling them to cross check whether a customer appears in any list.



# How to Screen Customers Against Designated Lists

- All lists must be make available with relevant officers.

How to download lists ?

Lists are available at [www.fiusrilanka.gov.lk](http://www.fiusrilanka.gov.lk)



ශ්‍රී ලංකා මහ බැංකුව  
இலங்கை மத்திய வங்கி  
CENTRAL BANK OF SRI LANKA



Financial Intelligence Unit  
இலா உத்டி ஸீகைட  
நிதியியல் உளவறிதல் பிரிவு

# How to Screen Customers Against Designated Lists

Go to [www.fiusrilanka.gov.lk](http://www.fiusrilanka.gov.lk)

1. Click on “UN Sanctions”

Click on  
“Sanctions on  
TF”

The screenshot shows the website of the Financial Intelligence Unit of Sri Lanka, which is part of the Central Bank of Sri Lanka. The page is titled "UN Sanctions >> Sanctions on TF". It lists "SANCTIONS RELATED TO TERRORISM AND TERRORISM FINANCING" with two main items: "1. THE UNITED NATIONS REGULATIONS NO. 02 OF 2012 (1267)" and "2. THE UNITED NATIONS REGULATIONS NO. 01 OF 2012 (1373)". Under item 1, there are two red links: "Link to Updated List - Al-Qaida & ISIL" and "Link to Updated List - Taliban". A green arrow points from the text "Click on 'link to updated Lists'" to the "Link to Updated List - Taliban" link. Another green arrow points from the text "Click on 'Sanctions on TF'" to the "Sanctions on TF" link in the left sidebar. The left sidebar contains a menu with items like Home, About FIU Sri Lanka, Legislations, Reporting Institutions, Press Releases, Publications, Training Material, Download, UN Sanctions (highlighted), MOUs, Gallery, International, FATF Public Statement, Related Sites, and Compliance Officer Declaration. The main content area also has a sub-menu for "UN Sanctions" with options for Overview, Sanctions on TF, and Sanctions on Proliferation.

2. Click on “link to updated Lists”



ශ්‍රී ලංකා මහ බැංකුව  
இலங்கை மத்திய வங்கி  
CENTRAL BANK OF SRI LANKA



Financial Intelligence Unit  
இலா இல்டி ஸீகை  
நிதியியல் உளவறிதல் பிரிவு

# How to Screen Customers Against Designated Lists

3. Click on the PDF or XML or HTML to download the Sanctions List

Welcome to the United Nations

UNITED NATIONS SECURITY COUNCIL

Search the UN

About the Council | Sanctions | Members | Meetings | Documents | News

Sanctions List Materials

Home » Sanctions » ISIL (Da'esh) & Al-Qaida Sanctions Committee » Sanctions List Materials

### Sanctions List Materials

#### ISIL (Da'esh) & Al-Qaida Sanctions List

List in alphabetical order

[PDF](#) [XML](#) [HTML](#)

List by Permanent Reference Number

[PDF](#) [XML](#) [HTML](#)

By [resolution 2368\(2017\)](#), the Security Council imposes individual targeted sanctions (an assets freeze, travel ban, and arms embargo) upon individuals, groups, undertakings and entities designated on the ISIL (Da'esh) & Al-Qaida Sanctions List.

The Sanctions List currently contains the names of 260 individuals and 84 entities and was last updated on **21 May 2019**, and supersedes all previous versions. The name of the List changed on 17 December 2015 with the adoption of [resolution 2253 \(2015\)](#). Further changes will be made to the ISIL (Da'esh) & Al-Qaida Sanctions List immediately following the relevant decision of the Committee. A press release documenting such changes will also be issued and posted in the "[Press releases](#)" section. The List is available in the PDF, XML and HTML formats.

In accordance with paragraph 55 of resolution 2368 (2017), the Committee makes accessible a [narrative summary of reasons for the listing](#) for individuals, groups, undertakings and entities included on the ISIL (Da'esh) & Al-Qaida Sanctions List.

The Committee works with INTERPOL to produce [INTERPOL-United Nations Security Council Special Notices](#) for listed individuals, groups, undertakings and entities. These notices promote information sharing and implementation of the measures among Member States.

#### Procedures for Listing

##### I. Relevant Security Council resolutions / Committee Guidelines



# How to Screen Customers Against Designated Lists

- List updates must be immediately communicated to relevant officers.

List updates are **immediately** informed to COs by the FIU through  
E-mail [fiudnfbp@cbsl.lk](mailto:fiudnfbp@cbsl.lk).

The CO must forward the updates to relevant officers **immediately** to screen customers against the lists.



# How to Screen Customers Against Designated Lists

Res. 1267/1989/2253 List

**Find (1/1)**  
ziad  
Previous Next

**QDi.167 Name:** 1: KAMEL 2: DJERMANE 3: na 4: na  
**Name (original script):** كمال جرمان  
**Title:** na **Designation:** na **DOB:** 12 Oct. 1965 **POB:** Oum el Bouaghi, Algeria **Good quality a.k.a.:** a) Bilal b) Adel c) Fodhil d) Abou Abdeljalil **Low quality a.k.a.:** na **Nationality:** Algeria **Passport no:** na **National identification no:** na **Address:** Algeria **Listed on:** 3 May 2004 (amended on 7 Apr. 2008, 13 Dec. 2011) **Other information:** In detention in Algeria as at April 2010. Arrest warrant issued by the German authorities on 9 Oct. 2003 for involvement in kidnapping. Former member of the Katibat Tarek Ibn Ziad of The Organization of Al-Qaida in the Islamic Maghreb (QDe.014). Review pursuant to Security Council resolution 1822 (2008) was concluded on 27 Jul. 2010. INTERPOL-UN Security Council Special Notice web link: <https://www.interpol.int/en/How-we-work/Notices/View-UN-Notices-Individuals> [click here](#)

**QDi.249 Name:** 1: YAHIA 2: DJOUADI 3: na 4: na  
**Name (original script):** يحيى جوادى  
**Title:** na **Designation:** na **DOB:** 1 Jan. 1967 **POB:** M'Hamid, Wilaya (province) of Sidi Bel Abbes, Algeria **Good quality a.k.a.:** a) Yahia Abou Ammar b) Abou Ala **Low quality a.k.a.:** na **Nationality:** Algeria **Passport no:** na **National identification no:** na **Address:** na **Listed on:** 3 Jul. 2008 (amended on 15 Nov. 2012) **Other information:** Belongs to the leadership of the Organization of Al-Qaida in the Islamic Maghreb (listed under permanent reference number QDe.014). Located in Northern Mali as of Jun. 2008. Mother's name is Zohra Fares. Father's name is Mohamed. INTERPOL-UN Security Council Special Notice web link: <https://www.interpol.int/en/How-we-work/Notices/View-UN-Notices-Individuals>

32 (32 of 72)

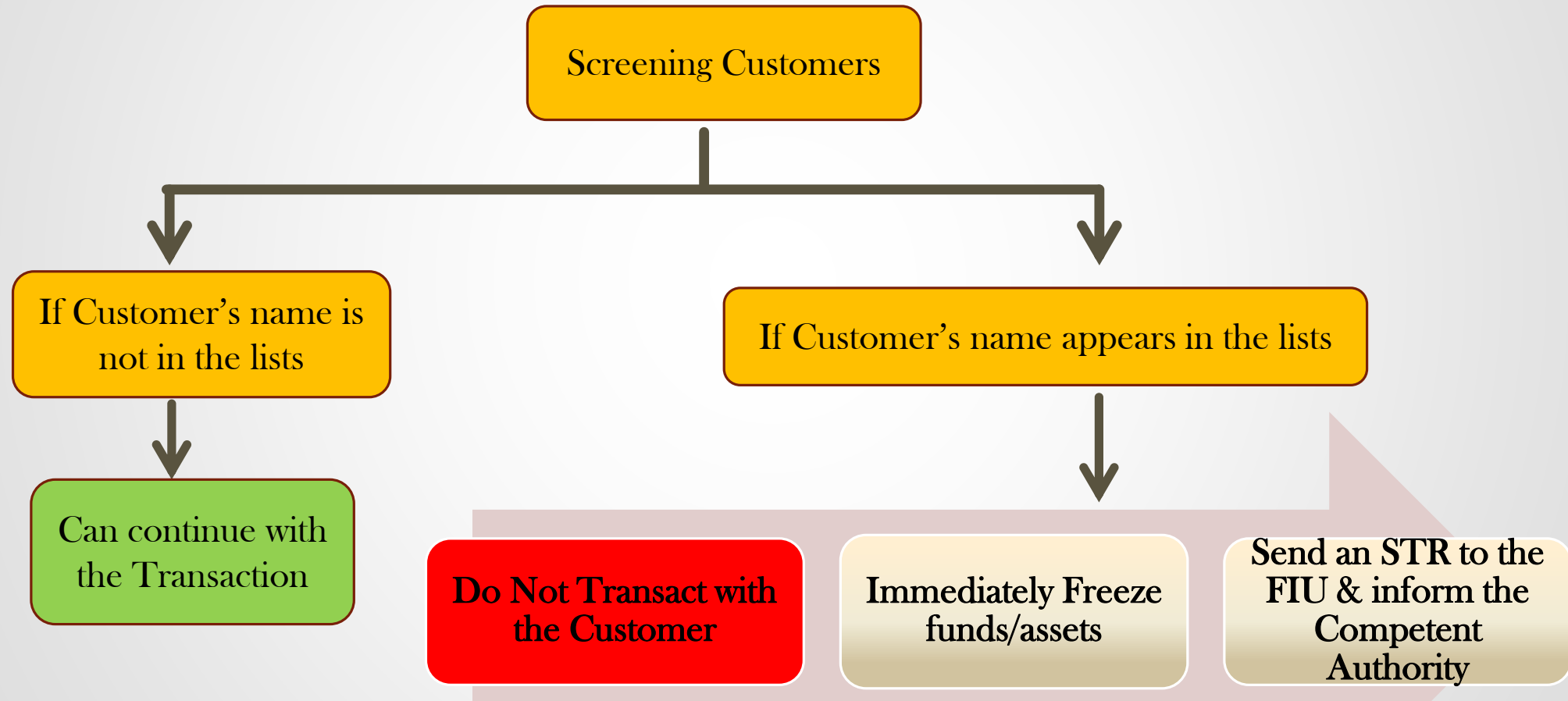
Ctrl + F





# How to Screen Customers Against Designated Lists

- Make sure that your institution does not conduct transactions with any designated person or entity.



# OTHER AML/CFT COMPLIANCE OBLIGATIONS



# Other AML/CFT Compliance Obligations

- Record Keeping
  - Section 4 of the FTRA
- Screening Employees before Hiring
  - Section 14(a) (vi) of the FTRA
- Training on AML/CFT Measures
  - Section 14(1) (d) of the FTRA
- Auditing of AML/CFT Measures
  - Section 14(1) (c) of the FTRA



# What are the Records to be maintained?

## 1. Customer Due Diligence information

- Copies of National Identity Card /Passport/ Driving License
- If the customer is a legal person or legal arrangement
  - Certified true copies or notarially executed copies of Memorandum, Articles, Certificate of Incorporation or Registration document

## 2. Transaction Records

- Bill Books
- Invoices
- Consignment Letters

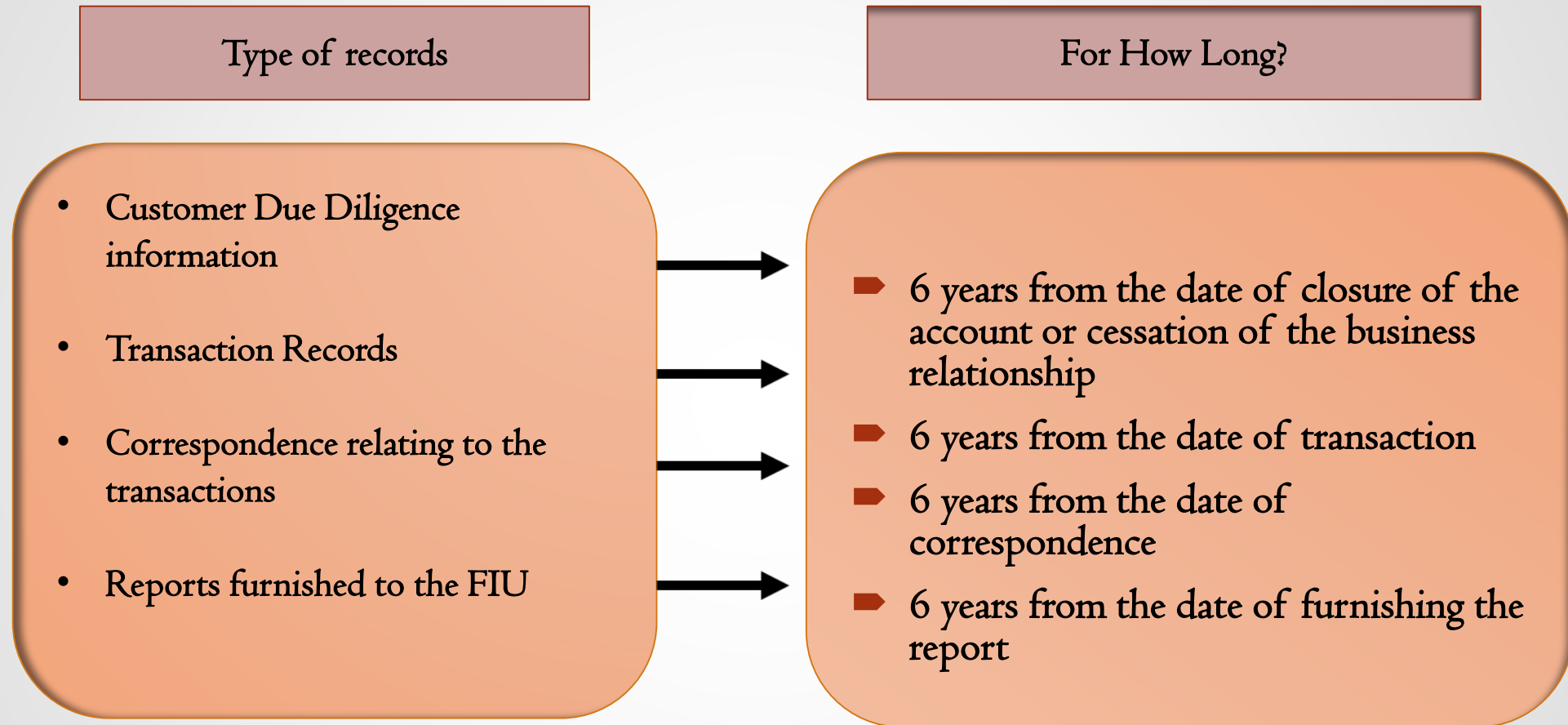
## 3. Correspondence relating to the transactions

## 4. Reports furnished to the FIU

- Copies of Suspicious Transaction Reports (STRs)
- Correspondence relating to the FIU



# For how long, the Records Should be Kept ?



HOWEVER; records must be retained for more than 6 years if, FIU directs to keep any information/record of transaction/report for such longer period.



# Screening Employees before Hiring

**Why?**

CDD Rules for DNFBPs requires to establish screening procedures to ensure that the institution's ML/TF risk is at a minimal with respect to the employees

**When?**

Before appointing or hiring employees on permanent basis or any other basis

**How?**

By obtaining a Police Report, Gramaseva Certificate, Non-relative referrals or any other valid references





# Training on AML/CFT Measures

**Why?**



CDD Rules for DNFBPs requires to provide training programmes for relevant employees to ensure they have adequate knowledge on AML/CFT measures

**On What?**



On identification of suspicious transactions, effectively managing the risk of money laundering and terrorist financing

**To Whom?**



Employees/agents/any individual authorized to act on behalf of the institution's AML/CFT Compliance Policy

**Frequency?**



Decide based on the level of ML/TF Risk, Capacity of the institution and the level of knowledge on ML/TF



# Auditing of AML/CFT Measures

Requirement

Independent Audit Function to  
audit AML/CFT function

Internal Division/ Employee

External Audit Function



ශ්‍රී ලංකා මහ බැංකුව  
இலங்கை மத்திய வங்கி  
CENTRAL BANK OF SRI LANKA



Financial Intelligence Unit  
இலங்கை நிதி அறிவு  
நிதியியல் உளவறிதல் பிரிவு

# Thank You



ශ්‍රී ලංකා මහ බැංකුව  
இலங்கை மத்திய வங்கி  
CENTRAL BANK OF SRI LANKA



Financial Intelligence Unit  
இலா உத்டி லீகை  
நிதியியல் உளவறிதல் பிரிவு