FIAU Implementing Procedures

19th November 2025

Valeria Catalano

Agenda

- Introduction
- Who are the Subject Persons?
- Implementing Procedures
- Key Obligations
- Risk Assessments
- Record-keeping
- Suspicious Transaction Reporting
- Training and Awareness
- Sector-Specific IPs

Who are the Subject Persons?

The PMLFTR define subject persons as those persons, legal or natural, carrying out "**relevant activity**" or "**relevant financial business**".

These persons are considered subject persons **exclusively** when carrying out those activities listed under the definitions of "**relevant activity**" and "**relevant financial business**".

In scope

RELEVANT ACTIVITY	RELEVANT FINANCIAL BUSINESS

This includes subject persons when acting in the exercise of their professional activities, such as:
• Auditors
• External accountants
• Tax advisors
• Real estate agents where the monthly rent amounts to €10,000 or more
• As well as, acting in the context of certain transactions, such as:
  • Assisting clients with opening bank accounts or the creation of companies
  • Independent legal professionals (lawyers, fiduciary/company service providers)
  • Licensed gaming operators
  • Where the transaction involves a payment in cash of €10,000 or more
  • Persons engaged in trading of goods.
	This includes activities carried out by the credit institutions, such as:
	• Payment institutions
	• Electronic money institutions
	• Insurance undertakings and intermediaries
	• Recognised, licensed or notified collective investment schemes and fund administrators
	• Service providers licensed under the Investment Services Act
	• Service providers licensed under the Retirement Pension Act
	• Safe custody service providers
	• Regulated markets
	• Virtual financial assets agents and licence holders within the meaning of the Virtual Financial Assets Act + issuers of virtual financial assets

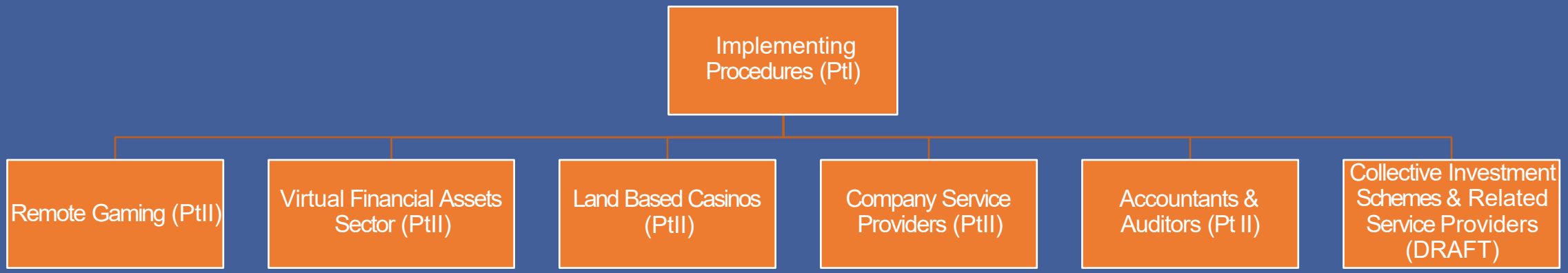
Why are they important?

To adopt measures to ensure that money gained through unlawful means is not channelled and laundered through the system and/or that such money, or even money from legitimate sources, is not used for finance terrorism

To ensure that their AML/CFT policies, controls, processes and procedures are designed, implemented and operated in a way
which reduces the risk of them being used in connection with money laundering or terrorist financing activities

To be able to recognised and deal with transactions which are harmful to the financial system

The Implementing Procedures - Part I & Part II



Aim

To assist persons who meet the requirements of subject persons to understand and fulfil their obligations under the law

+

To provide guidance to implement effective AML/CFT policies and measures to detect and flag suspicious transactions

=

Proper implementation of the RBA

Why?

To avoid the misuse of the financial system to channel illicit gains or even lawful gains destined for unlawful purposes (terrorism);

To reduce the risk to the **integrity, proper functioning, reputation and stability** of the financial system; and

To uphold legal and professional standards for the integrity of financial markets.

Purpose of IPs

To assist subject persons to understand and fulfil their obligation and effectively implement the provisions under the PMLFTR.

To achieve the following objectives:

(a) To outline the requirements set out in the PMLFTR and other obligations emanating from the PMLA;

(b) To interpret the requirements of the PMLFTR and PMLA and to provide measures on how these should be effectively implemented in practice, promoting the use of a proportionate risk-based approach;

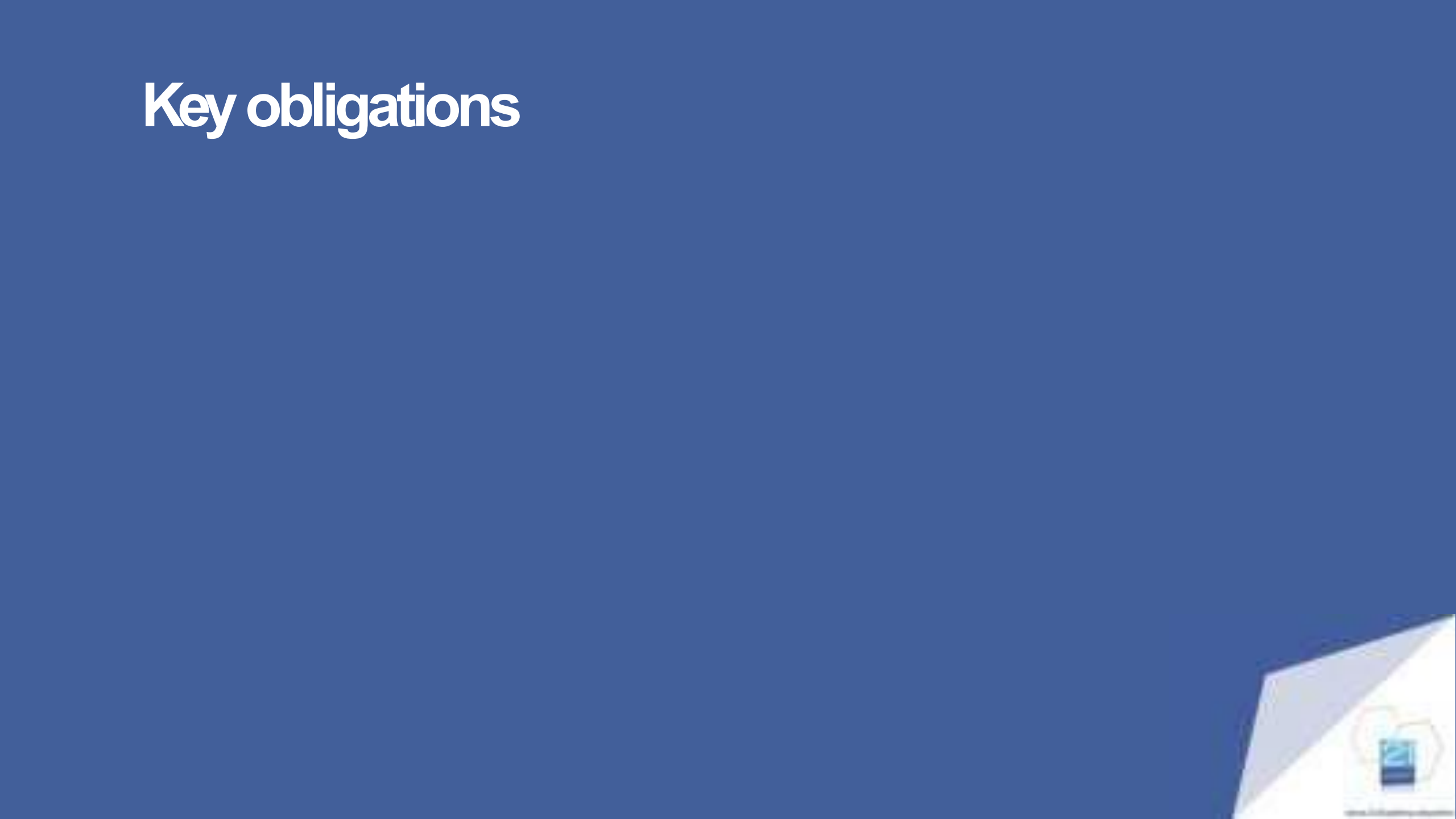
(c) To provide industry-specific good practice guidance and direction on AML/CFT procedures; and

(d) To assist subject persons in designing and implementing system and controls for the prevention and detection of ML/FT.

Status and Application

- These Implementing Procedures are **legally binding** on all subject persons (from the date on which they are issued) and are not merely consultative.
- The Implementing Procedures set out what is **expected** of subject persons and their staff in relation to the prevention of ML/FT by providing an interpretation on how the PMLFTR is to be **effectively implemented in practice** and by indicating what the FIAU expects from subject persons when implementing their obligations at law. In view of this, subject persons should be aware that **failure to comply with these procedures may render them liable to the imposition of administrative sanctions.**
- From time to time, the Implementing Procedures **may be amended** to ensure that they remain harmonised with amendments to legislation and other material developments originating from changes in international standards, especially those emanating from the FATF and EU AML Directives and Regulations.
- Subject persons should therefore ensure that they adhere and refer to the **most recent version** of the Implementing Procedures.
- A reading of the Implementing Procedures should **not be a substitute for a reading of the PMLFTR and the PMLA themselves**, besides the relevant provisions of the Criminal Code dealing with terrorist financing and related offences.

Key obligations

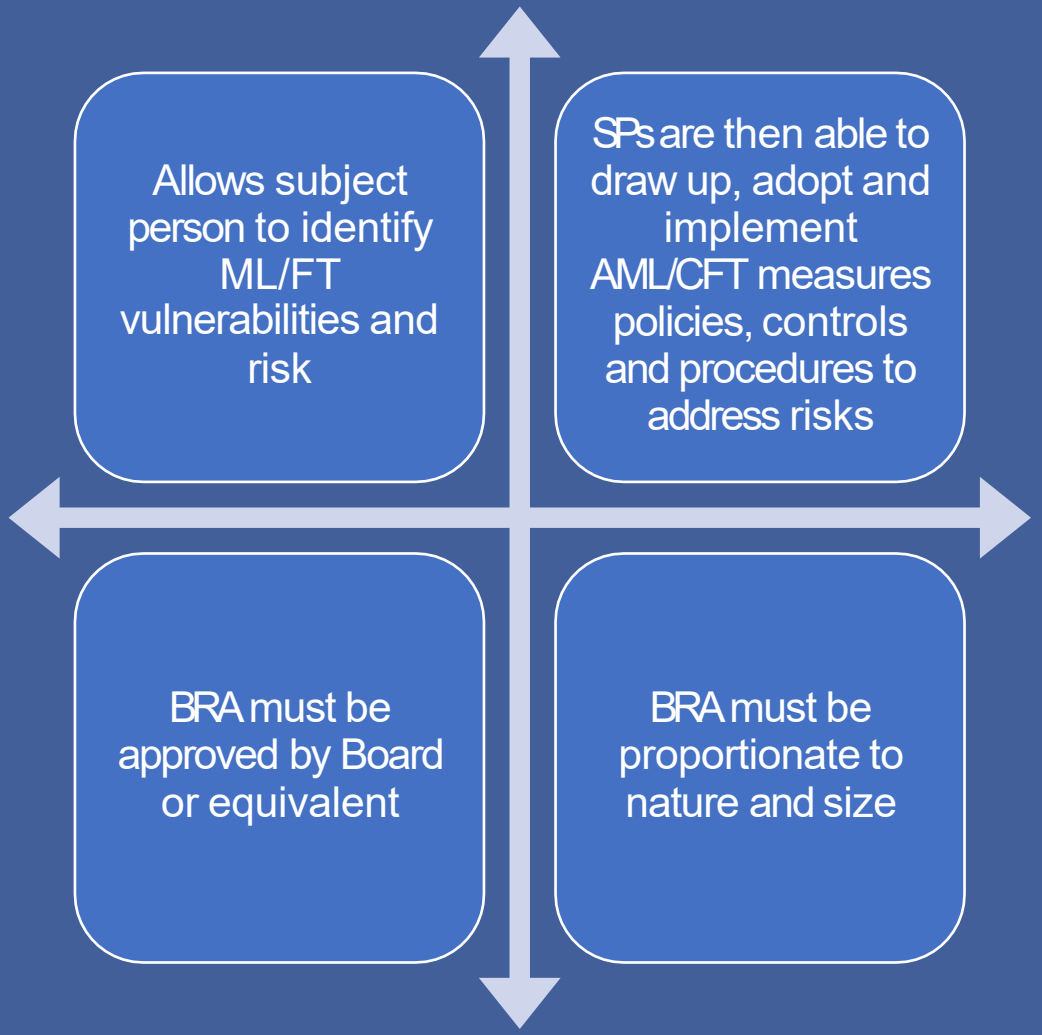


Overview of key obligations

Risk assessments

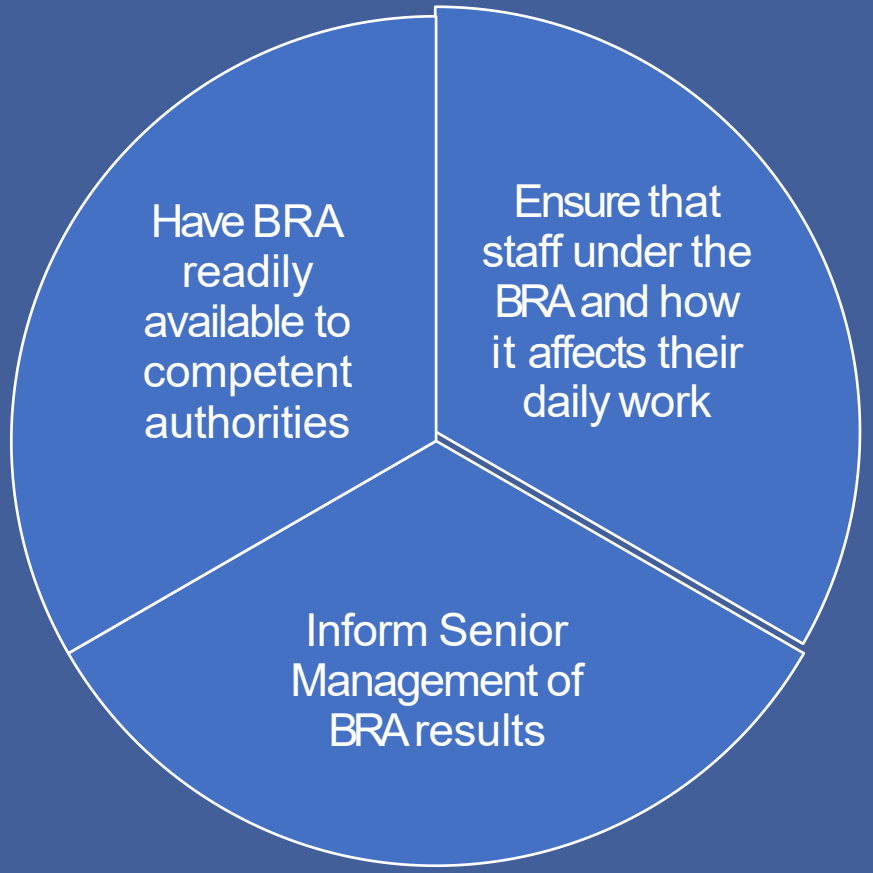
Entity-level risk assessment

Business risk assessment



Implementation of BRA

Firms should:



Business risk assessment

1. Risk identification

- Identify the main ML/FT risks associated with customers, products & services, business practices/delivery channels, & geographical locations

2. Risk assessment / measurement

- Measure the size & importance of ML/FT risks including the likelihood of them materialising and their impact on the subject person

3. Risk management

- Manage the identified ML/FT risks by applying measures, policies, controls & procedures which minimise as much as possible the identified risks

4. Risk monitoring & review

- Monitor, review and keep updated the BRA
- Document the assessment process & any updates to the BRA & the corresponding AML/CFT measures, policies, procedures & controls

Lessons learnt on the BRA from FIAU enforcement measures

Consider threats and vulnerabilities	Consider likelihood of risks materialising (i.e. scenarios) & their impact	Assess the mitigating effect of control measures to determine level of residual risk
Prepare jurisdictional risk assessments	Be as detailed as possible in the documentation	Evidence of discussion & approval at board level

Customer risk assessment

- This assessment allows the subject person to identify potential risks upon entering a **business relationship** with, or carrying out **an occasional transaction** for, a customer.
- It allows the subject person to develop a risk profile for the customer and to categorise the ML/FT risk posed by each customer as low, medium or high.
- The level of detail of a CRA is to reflect the complexity of the business relationship or occasional transaction to be entered into.

Adverse Media

- The nature of the adverse news will also have an impact on its actual relevance for risk assessment purposes.

- Ideally, the subject person should develop guidelines to allow officers and employees to discern what is to be considered as reliable media reports and what impact these can have on one's risk understanding.

- The impact of adverse media can at times also depend on how remote in time it is.

Non-exhaustive list of high-risk factors

Customer risk	Geographical risk	Product / service / transaction risk	Delivery channel risk
• Overly secretive or evasive • False documentation • Criminal connections • SoF/SoW information not commensurate with customers' profile • PEP links • Sanctions • Employment status and industry • Complex structure • Has benefitted from or applied for residency schemes	• Transfers to a high-risk jurisdictions with no apparent connections • Links to high-risk jurisdictions	• Large financial transactions with no apparent economic rationale • Transactions involve recently-created companies • No justification for the transactions being proposed • ML/FT risk presented by the product/service itself	• Multiple intermediaries without good reasons • Use of third parties without good reasons • Non-face-to-face without sufficient controls

Non-exhaustive list of low-risk factors

Customer risk	Geographical risk	Product / service / transaction risk	Delivery channel risk
• Listed entity • Entity operating in the regulated financial business • Client accounts • Government-owned entities	• EU/EEA Member States • Links to jurisdictions which are considered to be reputable and have an equivalent AML/CFT regime	• Use of product/service has been tested • Product does not allow anonymity • There are controls around the product, e.g. capping	• Face-to-face • Use of regulated intermediaries

Weighting and rating of risk factors

- Taken together, the scores assigned to the individual risk factors should allow the subject person to generate an overall risk score and lead it to understand whether the business relationship or occasional transaction falls within its risk appetite
- The method used to weight risk factors is left to the subject person, provided that the following principles are followed:
  - **Weighting is not to be unduly influenced by just one factor;**
  - **Monetary considerations are not to influence the risk rating;**
  - **PMLFTR default high risk situations are not to be over-ruled (e.g PEPs);**
  - **Weighting does not lead to a situation where it is impossible for any relationship or transaction to be classified as high risk.**

Lessons learnt on the CRA from FIAU enforcement measures

- Requirement for a comprehensive methodology
- Importance of understanding the risk even in the case of reliance
- Documented methodology and scoring system
- Timing of CRA
- CRA must include all risk factors

Jurisdictional Risk Assessment

- Subject Persons are required to carry a JRA with respect to the countries it may be exposed to ML/FT risk;
- The assessment should highlight the main risks connected with the specific jurisdiction;
- Similar to the BRA, the detail included should be proportionate to the nature and size of the business and its exposure;
- There is no one size fits all approach expected for EU member states
- To take into consideration the customer activity, including business activities, SOW and SOF to determine the SP's geographical risk exposure

Step 1: Identification & Verification of a Customer and BO

Determine who the customer is	Determine who the BO is, where applicable	Verify customer & BO (where applicable)
Determine whether such person is acting on behalf of another person	Establish purpose and intended nature of the business relationship & business & risk profile of customer	In the case of a business relationship, monitor the same on an ongoing basis

Application of CDD measures

Subject persons are to apply CDD measures in the following circumstances:

- **When establishing or entering a business relationship;**
- **When carrying out an occasional transaction that amounts to €15,000 or more, whether that transaction is carried out in a single operation or in several operations which appear to be linked;**
- **When there is a suspicion of money laundering or terrorist financing, irrespective of any derogation, exemption or threshold;**
- **When there are doubts about the truth or adequacy of previously obtained customer identification data**

Application of CDD measures (existing customers

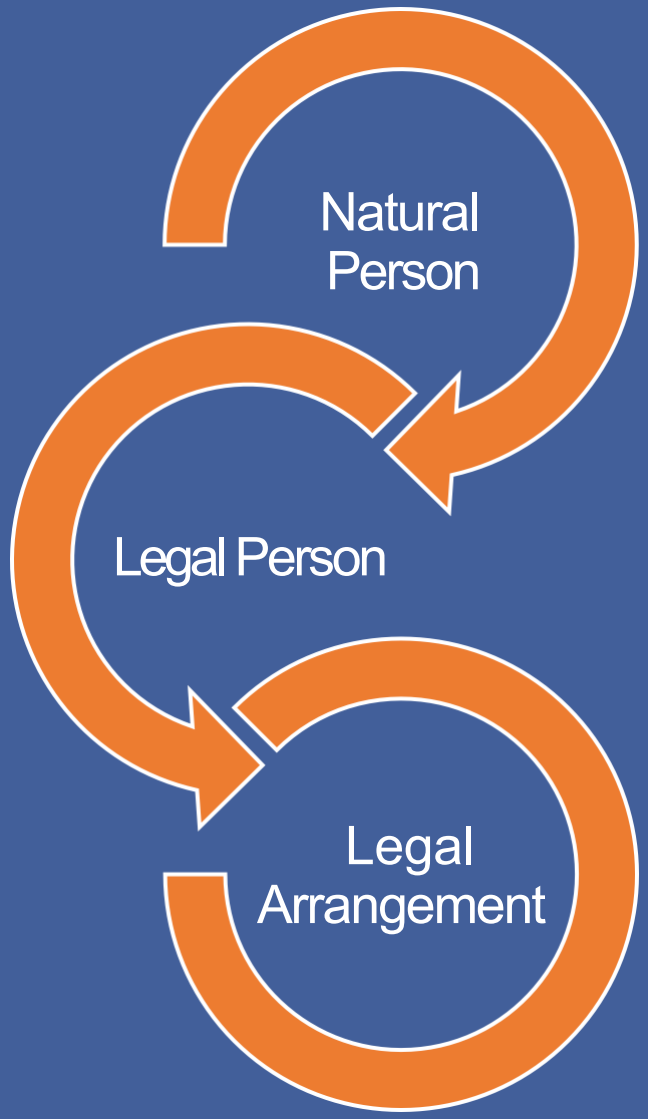
At appropriate times and on a risk-sensitive basis, including at times when the subject person becomes aware that the relevant circumstances surrounding a business relationship have changed

Whenever doubts arise about the veracity or adequacy of the previously obtained customer identification information, data or documentation.

Who is the customer?

- A person (whether natural or legal entity or arrangement)
- Who seeks to form a business relationship (i.e. a prospective customer); or
- With whom a business relationship is formed (i.e. existing customer); or
- For whom an occasional transaction is carried out.

Types of Customers



Natural person: *Identification*

- Official full name
- Place & date of birth
- Permanent residential address
- Identity reference number
- Nationality

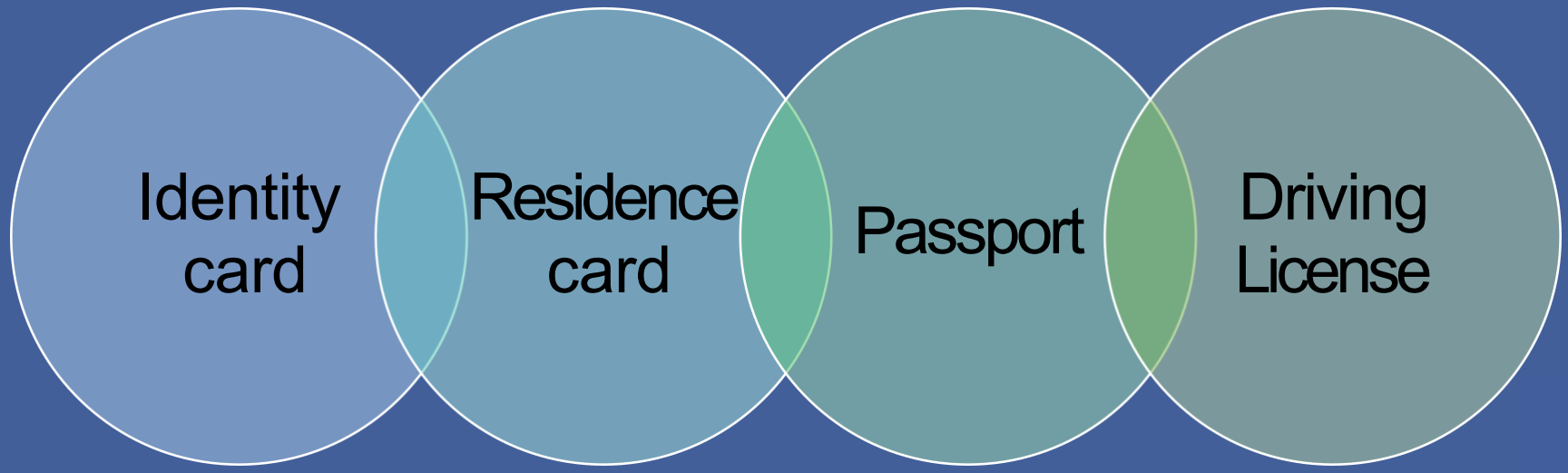
- Verification of the customer's identity must happen based on documents, data or information that is obtained from a reliable and independent source.

- The customer's identity may be verified by referring to documents (e.g. passports, ID cards, driving licences, utility bills, and bank statements) or by making use of electronic sources (e.g. e-IDs, Bank-IDs and electronic commercial databases).

This procedure should apply in the same manner with respect to both a resident and non-resident applicant for business

Natural Persons: Verification of Identity

A valid unexpired government issued document that contains photographic evidence:



Authenticity Checks

1. Examining security features present on a document and confirming that these can be seen
2. Examining the lamination of an ID card document to check for any suspicious signs
3. Ensuring that the document does not have any uneven colours and text which is non-uniform or the use of irregular fonts or typefaces
4. Verifying or decoding the Machine Readable Zone (MRZ) code contained on the ID card document or the alternative code reproduced on the ID document
5. Checking open-source information that may be of assistance in carrying out authenticity checks
6. Being aware of receiving documentation that could easily be tampered with such as Microsoft Word documents

Natural Persons: Verification of Permanent Residential Address

- Bank statement or reference letter
- Utility bill (not older than 6 months)
- Correspondence from a central or local government authority, department or agency
- Any government-issued or recognised document to verify identity, where a clear indication of residential address is provided
- An official conduct certificate
- Lease contract or agreement (the 6-month rule does not apply for lease agreements, however, subject persons must ensure the contract is still in force)
- Any other document as may be specified in sectoral implementing procedures

Natural Persons: Verification in Exceptional Scenarios

a) when a customer only has a temporary address and has no permanent residential address elsewhere, such as seasonal workers, a letter from a director or manager of the employer confirming the residence at a stated address and indicating the expected duration of employment would be sufficient;

b) when a customer resides on a yacht, the customer's residential address may be verified by obtaining documentation relating to the chartering of the yacht and berthing agreements;

c) when the customer is a student or part of the academic staff, and is residing in a university, college or any other institutional residence, the subject person may verify the customer's residential address by obtaining a letter from the director or senior official of the university, college or institution confirming the customer's residential address;

Legal persons: *Verification*

Nature of principal	Identification & verification procedures
Public / Private company **Commercial partnership**	• Identification: official full name; registration number; date of incorporation or registration; and registered address or principal place of business • Verification: certificate of incorporation; company registry search; most recent version of M&A (or partnership agreement), recent certificate of good standing (not older than 3 months), or another statutory document • Identify all directors (or partners) (natural and corporate) and in the case of corporate directors obtain: official full name, registration number and registered address or principal place of business • Establish ownership and control structure of the company (or partnership) • Identify and verify all beneficial owners • Other documentation as applicable to be obtained on a risk-sensitive basis: copy of Shareholders' Register; information from independent sources; copy of latest audited financial statements; bank statements (not older than 6 months)

Legal persons: *Verification*

Nature of principal	Identification & verification procedures
Foundation or Association	• Identification: official full name; registration number; date of incorporation or registration; and registered address • Verification: certificate of registration; most recent version of the constitutive document • Identify all persons vested with administration and representation • Establish ownership and control structure • Foundations: identify the founder, any person who has endowed the foundation and any person who has been assigned rights in respect of the foundation
Trust/Trustee	• Identify the trust: full name of the trust, nature of the trust (e.g., discretionary trust, testamentary trust, bare trust) as well as its object and purpose (e.g., wealth management, estate planning), country of administration and applicable law, and registration number if applicable • Verify the existence of the trust by requesting a copy of the trust deed or an extract of same showing the above information • Identify all beneficial owners • Obtain copy of the authorisation of the trustee if regulated

Legal person: *Identification of BOs*

Body corporate or body of persons	i. Any natural person or persons who ultimately own or control that body corporate or body of persons through direct or indirect ownership of more than 25% of the shares or more than 25% of the voting rights or ownership interests in that body corporate or body of persons, including through bearer share holdings, or through control via other means, other than a company that is listed on a regulated market which is subject to disclosure requirements consistent with EU law or equivalent international standards which ensure adequate transparency of ownership information
Trusts, foundations, and other similar legal entities or arrangements	i. Settlor(s) ii. Trustee(s) iii. Protector(s) iv. Determined beneficiaries (or, if not yet determined, class of persons in whose main interest the trust is set up or operates) v. Other natural person(s) exercising ultimate control over the trust

Step 2: Record-keeping

Record-keeping

Category	Detail	Retention period
Actions taken to adopt and implement the RBA	• Copy of BRA, changes thereto, decisions taken with respect to the BRA • Copy of most recent controls, policies, measures and procedures	5 years
CDD information & documents obtained for ID&V	• Copy of each CRA • ID&V documents • Results of commercial electronic database searches • Video conferencing records • Document ensuring that an agent is duly authorised in writing to act obo the principal	5 years from termination of relationship or transaction is completed (last transaction)
Records containing details relating to business relationship or transaction	• Information on purpose and intended nature of relationship • All business correspondence • Details on transactions	5 years from termination of relationship or transaction is completed (last transaction)

Record-keeping (cont.)

Category	Detail	Retention period
Reporting	• Internal reports • External reports • Justification why no STR was made	5 years from later date when STR was submitted or date when business relationship end or transaction is carried out
Other	• Training • Employee screening • Reliance agreement • Outsourcing agreement • Other reports which may be useful for FIAU, e.g. internal audit reports	• 5 years from when training took place • 5 years from when employment relationship ends • 5 years from when outsourcing and reliance agreements end • Other: 5 years from when adopted or the subject person ceases relevant activity

Organisation and categorisation of records

Subject persons are to maintain a list of their current business relationships setting out:

- The name of the customer and/or customer reference number;
- The risk categorization of the business relationship (risk rating or risk score);
- The type of service being provided or product being offered;
- Whether the customer is a natural person, legal person, a trust or other legal arrangements;
- The date of commencement of the business relationship and, where applicable, the date on which it ceased;
- A list of all the jurisdictions that the customer deals with;
- Whether the customer or ultimate beneficial owner is a PEP, or an immediate family member or a close associate of a PEP; and
- Whether reliance has been exercised with respect to the particular business relationship.

Step 3: Suspicious Transaction Reporting

Examples of common patterns

- unusual financial nexuses and transactions occurring among certain business types (e.g., food importer dealing with an auto parts exporter);
- transactions that are not commensurate with the stated business type and/or that are unusual and unexpected
- unusually large numbers and/or volumes of wire transfers and/or repetitive wire transfer patterns;
- unusually complex series of transactions indicative of layering activity involving multiple accounts, banks, parties, jurisdictions;
- transactions being conducted in bursts of activities within a short period of time, especially in previously dormant accounts;
- transactions and/or volumes of aggregate activity inconsistent with the expected purpose of the account and expected levels and types of account activity provided at onboarding;
- parties and businesses that do not meet the standards of routinely initiated due diligence and anti-money laundering oversight programs (e.g., unregistered/unlicensed businesses);
- transactions seemingly designed to, or attempting to avoid reporting and recordkeeping requirements

Highlighting Suspicious Activity

- CDD documentation and KYC;
  - Copy of ID/Passports
  - Company details
  - M&A
  - Details of UBO

- Determining source of funds and wealth;
  - Obtain supporting documentation
  - Sufficient evidence and documentation

Media Articles

- The way you form your suspicion should not solely be based on the publicity of a person. **HOWEVER,** having negative media information on a customer may be seen as an indicator to conduct an internal assessment of such client.

- This should be considered as a red flag to conduct internal analysis
  - Carry out an internal analysis in relation to your customers to prove suspicion
  - This analysis can result in being satisfied that customer is not high risk or conclusion that you could not prove my doubts so therefore you file an STR

Suspicion sometimes is enough to file for an STR

Preparing an STR

1. Introduction:

- Explain the suspicion
- Make reference to any previous STRs
- Summary of the suspected violations

2. Body:

- Provide details of the review/investigation carried out by the reporting entity;
- State the facts in a clear and concise manner
- Rationale must be clearly identified
- State who the person is (individual or group of persons)

3. Conclusion

- Provide a summary of the suspicion, location/s, as well as identification and any follow up the reporting institution is taking.

Example 1: Incomplete STR

- Mr X was the originator of five transfers totalling EUR175,000. All of the wires were remitted to a Qatar based company/ During the same period, Mr X deposited large sums of cash and cheques into his account.

- This STR fails to provide specific details on the application of the suspect funds (the name, bank, and account number of the beneficiary, if identifiable). The financial institution fails to provide any information concerning the relationship, if any, between the FI and the customer. Also, no specific transaction data is provided that identifies the dates and amounts of each wire transfer.

Example 2: Insufficient STR

- Account was opened in 2002. Assets were transferred in by wire. 50 checks for $250 were deposited, securities were liquidated and money was paid out in May 2003.

- This narrative provides no information to support the reason the broker-dealer submitted the STR. Although some general transaction information is included, it fails to provide dates or amounts of the incoming credits to the account, i.e., the dates, amounts, originator, and source of the wire transfers, the issuer or issuers of the 50 checks, and the beneficiary of the funds closing the account in May. Also, no information is given concerning the owner of the account.

Example 3: Sufficient STR

- This STR is being filed to summarize suspicious cash deposits and wire transfer activity conducted by John Doe, account #12345678910. John Doe has been a bank customer since April 2000. Mr. Doe is a college student and employed part-time at Quickie Car Wash.
- Cash deposits to Mr. Doe's personal checking account are structured to possibly circumvent federal reporting requirements. The deposits are followed by immediate wire transfers to Aussie Bank in Sydney, Australia to a single beneficiary, Jennifer Doe, account #981012345, with an address located in Australia. Specifically the following activity has been observed: cash deposits (dates followed by amounts): 03/15/02 $9,950.00; 03/17/02 $9,700.00; 03/18/02 $10,000; total: $29,650. Wire transfers out (dates followed by amounts): 03/16/02 $9,900.00, 03/18/02 $9,700.00, 03/19/02 $9,900.00.
- The volume and frequency of the deposits is not consistent with previous banking transactions conducted by Mr. Doe. The amounts of currency do not appear consistent with the customer's stated employment. Also, the relationship between the customer and Jennifer Doe and the purpose for the wire activity is unknown.
- Therefore, due to the structured cash deposits by the customer on almost consecutive days into the account, and the immediate wire transfer of the funds out of the account to Jennifer Doe, Aussie bank, account #891012345, Sydney Australia, this STR is being filed.

Example 4: Complete STR

- On June 27, 2003, Jane Smith came up to the third main cage and cashed out $5,000 in chips. She proceeded to hold purple chips (looked to be about $5,200) stating that she was going to keep those chips until later. While waiting in line, Ms. Smith was talking to another patron about the currency transaction reporting (CTR) process and basically telling him how to avoid a CTR. She was explaining how the cage, table games, and slots compare their amounts and fill out a CTR when someone gets over $10,000. Ms. Smith told the other patron that's why she pulls some of her chips back so she will not have to pay taxes. She and the other gentleman then walked out together.
- Ms. Smith has visited our casino over the last month, usually once a week. Her winnings were minimal until last week when on June 20, 2003 she cashed out $5,000 in chips one day. She returned the following day and cashed out an additional $5,000 in chips. We have maintained a copy of Ms. Smith's winnings over the last month and also a copy of her driver's license.
- Today, Ms. Smith was informed that she was barred from our casino after she was overheard instructing another patron on how to avoid a CTR

goAML System

The FIAU has replaced the STR submission system and implemented the goAML software solution which has been developed by the United Nations Office on Drugs and Crime.

The use of goAML

- effective
- efficient
- Improves communication

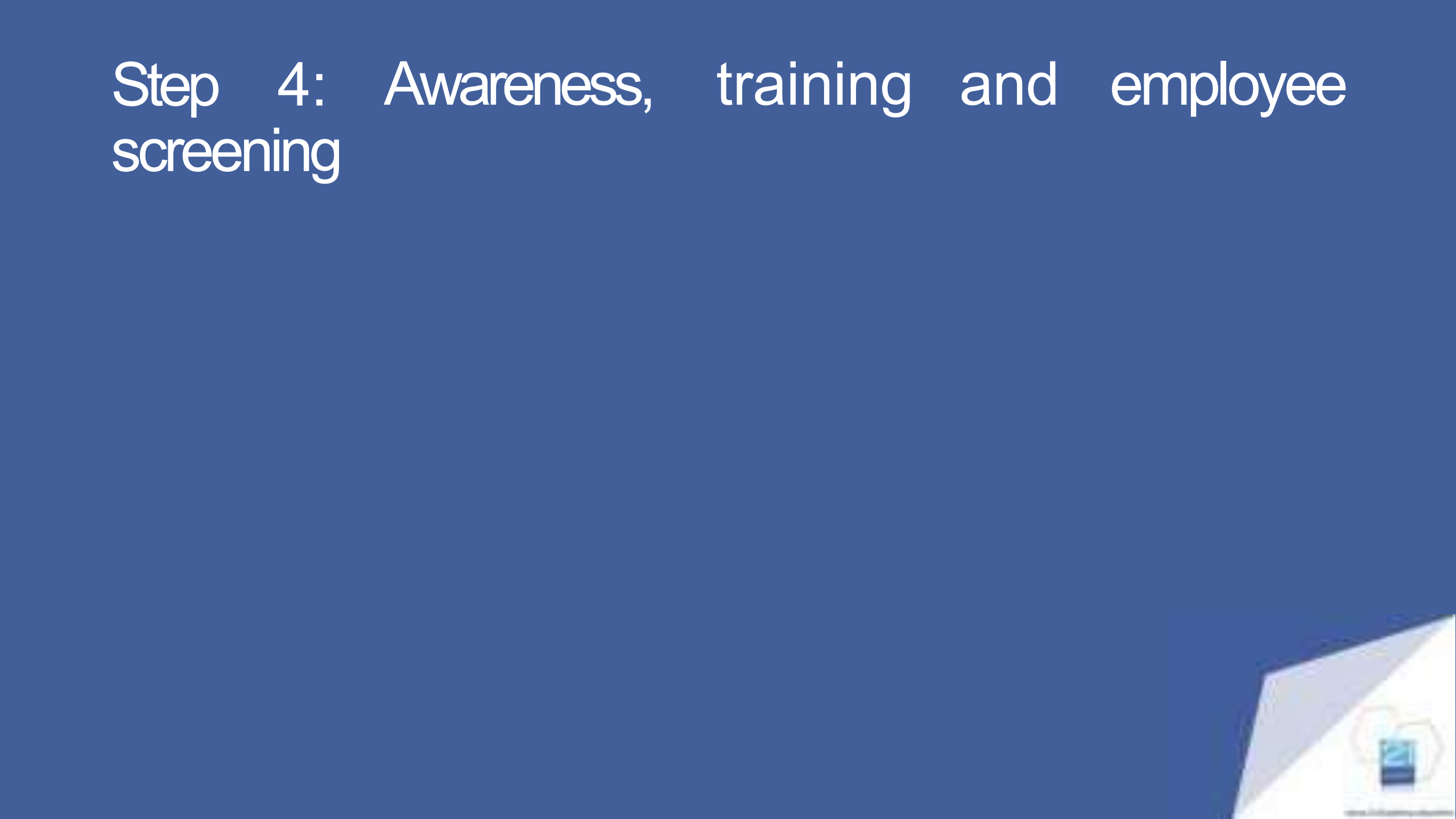
About goAML

- Built system made for FIUs by UNODC
- Consists of online report data entry forms
- Possibility to upload reports in the form of XML
- Helps subject persons improve report data quality
- Notification and messaging system to inform about report status and feedback
- Supports submitting bank account history electronically
- History of reporting and statistics

How it works?

Step 1:
Registration in goAML
Step 2:
Choose type of New Reports
Step 3:
Choose the TYPE of report to use
Step 4:
Submit and Await Feedback
STR (Suspicious transaction report)
SAR (Suspicious activity report)
TFR (Terrorism financing report)
PEPR (Politically exposed person report)

Step 4: Awareness, training and employee screening



Training

A subject person is required to take appropriate and proportionate measures from time to time to:

- ensure that employees are aware of relevant AML/CFT legislation (and any updates) and data protection requirements, as well as of the subject person's AML/CFT measures, policies, controls and procedures and any ML/FT risks particular to subject person; and

- provide training in relation to the recognition and handling of operations and transactions which may be related to proceeds of criminal activity, money laundering or the funding of terrorism.

Training

Tailored Training	The Unit must tailor training for employees that fulfil roles with higher financial crime risk exposure – those being staff that are client facing.
Practical Dimension	Training carried out should have a strong practical dimension to it and includes case studies and the regular testing of staff, in order to ensure that the staff understand their responsibilities. The training must not unduly dwell on legislation and regulations, as this may prove to be monotonous for the staff and lead to disinterest and not give the staff necessary tools in real life scenarios. Thus, for example, if computerised training is used, this should conclude with a test at the end.
Training Follow-Ups	Completion of training must be documented and monitored through appropriate management information metrics, and non-completion of training must be taken seriously through appropriate consequence management.
External Training	External training carried out by third parties as well as relevant conferences/seminars should also be recommended for employees.

Employee screening

Subject persons shall also have in place appropriate employee screening policies and procedures when hiring employees, which may include;

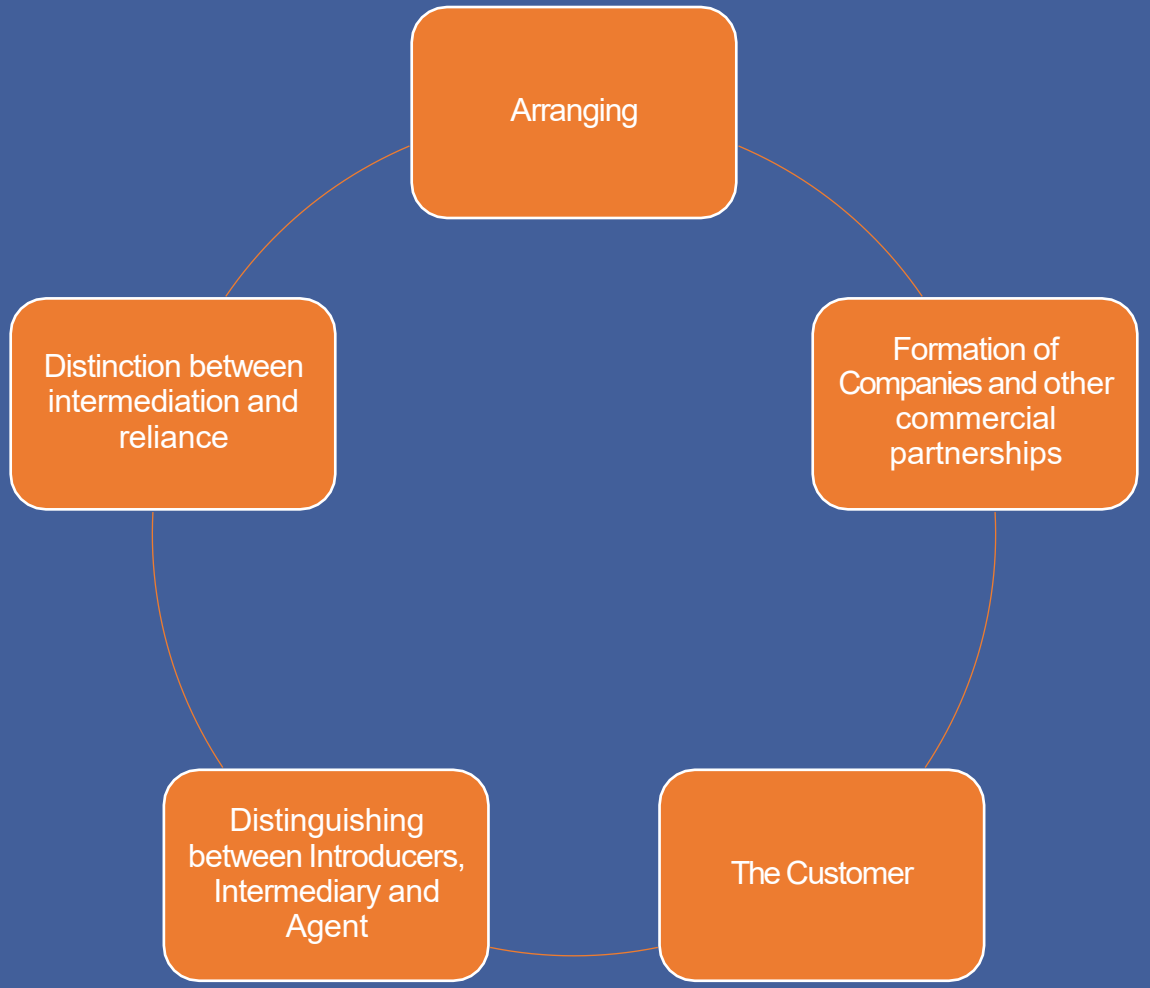
- obtaining a Police conduct certificate or equivalent documentation;
- documentation being refreshed on an ongoing basis.

Sector Specific Implementing Procedures

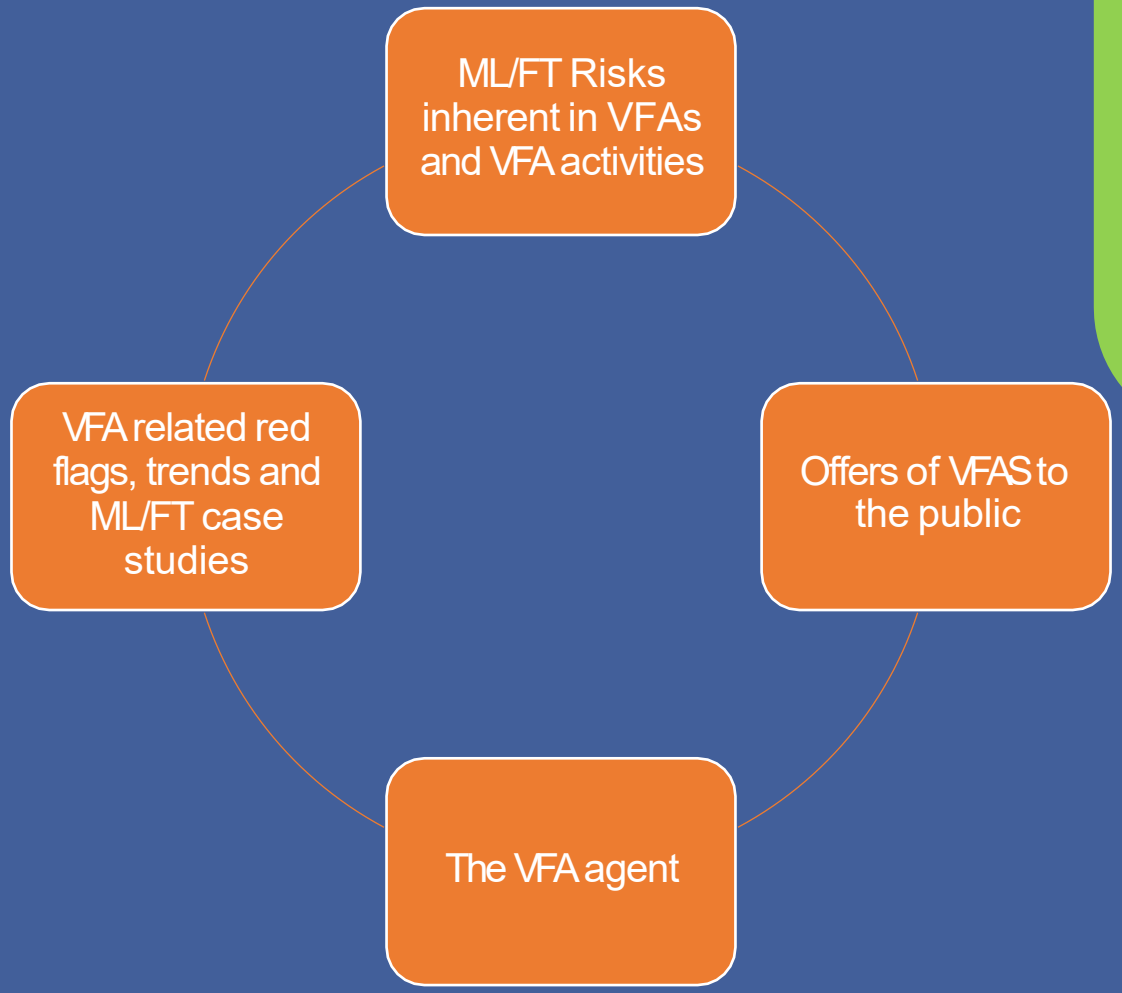
Remote Gaming

Land-Based Casinos

Company Service Providers (CSPs)



Virtual Financial Assets (VFAs)

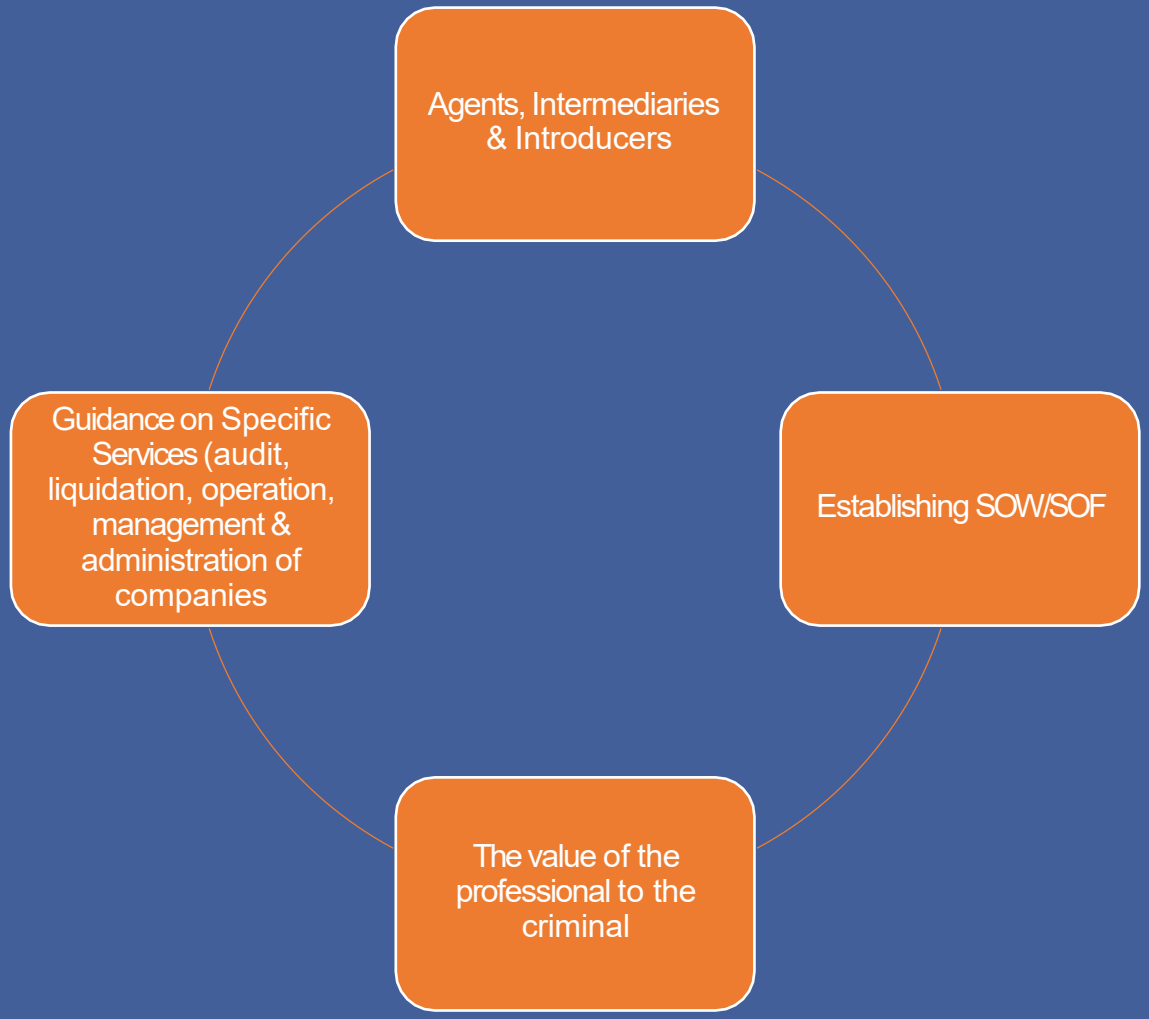


Consultation Exercise on the revision of the Implementing Procedures – Part II addressed to the Virtual Financial Assets Sector

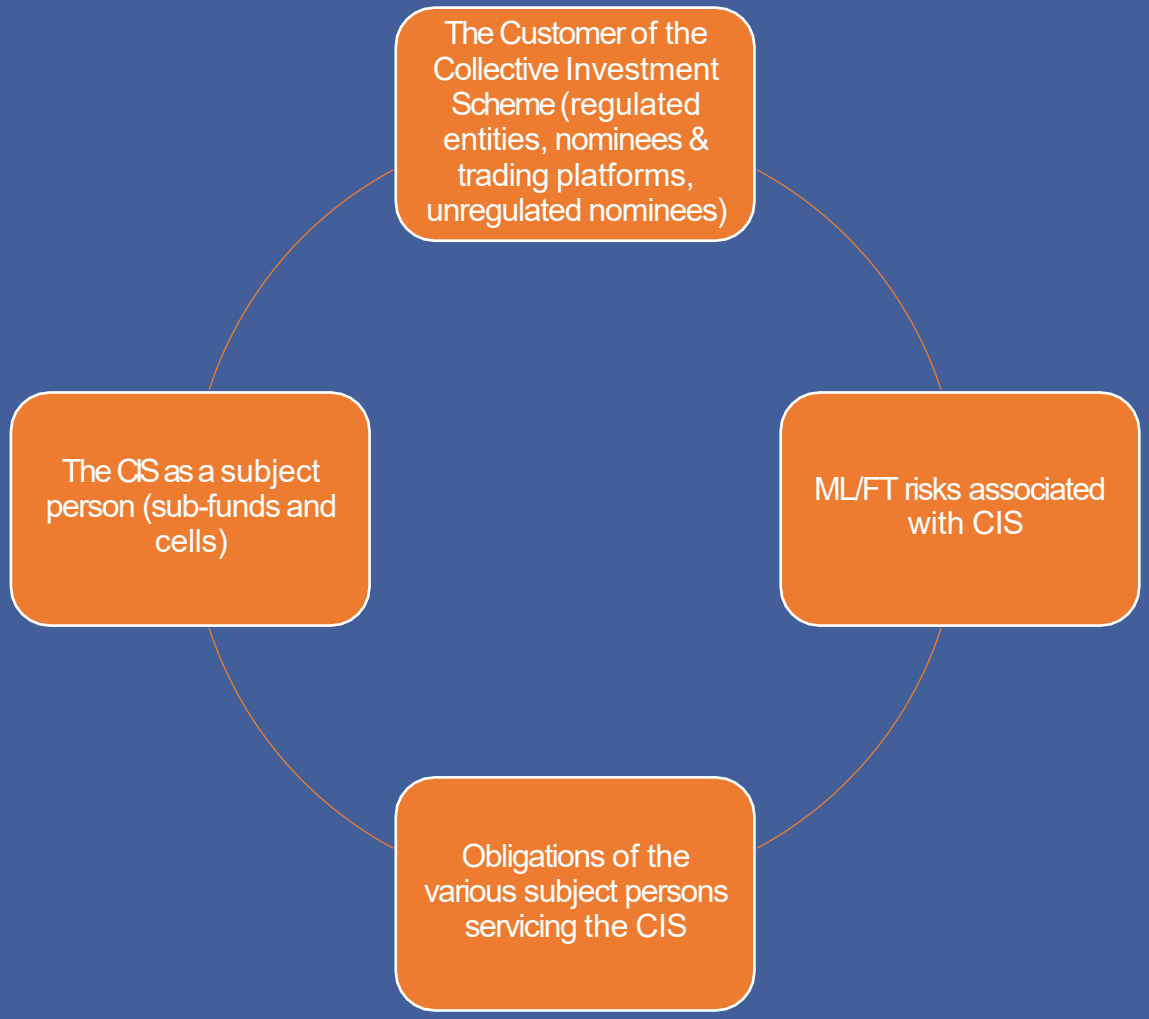
On the 7th of November 2024, the FIAU launched a consultation exercise on the revision of the Implementing Procedures – Part II addressed to the Virtual Financial Assets Sector.

These efforts seek to align the domestic AML/CFT framework with recent EU and local legislative developments in the crypto-assets sector, namely the MiCA Regulation, the recast of the Transfer of Funds Regulation, the amendments to the 4AMLD and the recent amendments to the Virtual Financial Assets Sector. The revisions also reflect the revised EBA ML/FT Risk Factor Guidelines that were published on 16 January 2024.

Accountants & Auditors



Collective Investment Schemes & Related Service Providers – Consultation Document



Concluding Remarks

Any questions?

Thank you