



www.21Academy.education

FIAU Implementing Procedures

3 November 2020

Diane Bugeja

CAMILLERI PREZIOSI
— ADVOCATES —

Agenda

- Introduction
- Case Study
- Subject Persons
- Implementing Procedures
- Key Obligations
- Simplified and Enhanced DD
- Record-keeping
- Suspicious Transaction Reporting
- Reliance
- Outsourcing
- Training and Awareness
- Screening for financial sanctions
- Concluding remarks
- Questions

Introduction

Case Study

A Brazilian judge established a trust in the Caribbean Islands, and the actual settlor of trust was a shell company in another Caribbean Island. Both the trust and the company had a nominal value of 1 dollar but were able to purchase a million-dollar apartment in Miami.

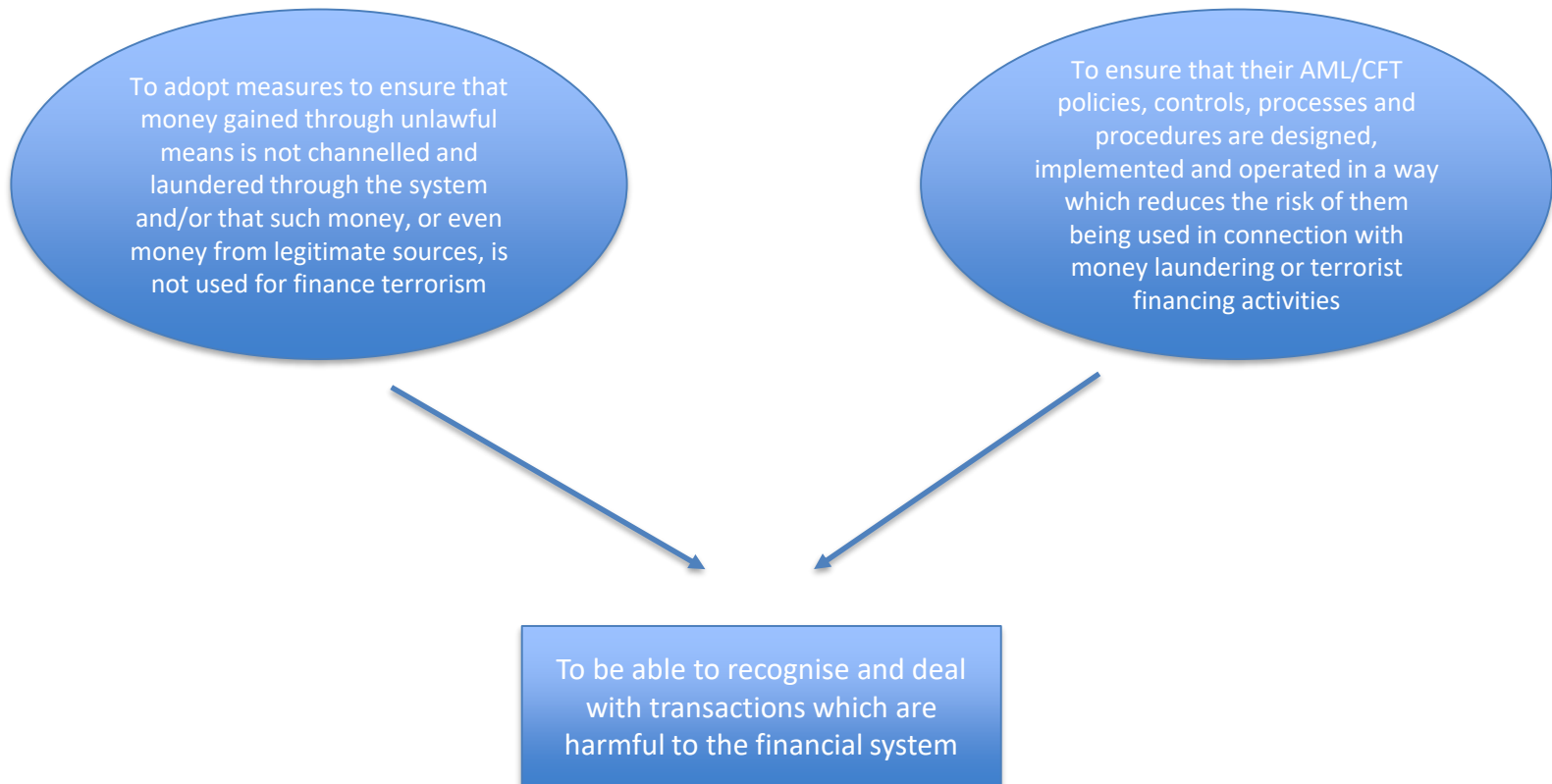
SUBJECT PERSONS

RECAP

The FIAU is responsible for imposing AML/CFT requirements on all ‘subject persons’, which are defined in Regulation 2 PMLFTR as **“any legal or natural person carrying out either relevant financial business or relevant activity”**.

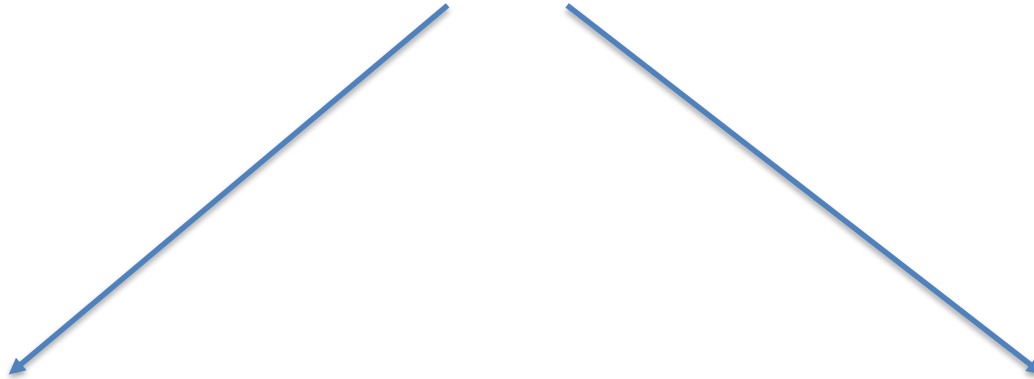
RELEVANT ACTIVITY	RELEVANT FINANCIAL BUSINESS
<p>This includes subject persons when acting in the exercise of their professional activities, such as:</p> <ul style="list-style-type: none">- Auditors- External accountants- Tax advisors- Real estate agents <p>As well as, acting in the context of certain transactions, such as:</p> <ul style="list-style-type: none">- 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. <p>In light of recent amendments Regulation 2 PMLFTR also includes the provision of intermediation services in relation to property letting by real estate agents where the monthly rent amounts to €10,000 or more, within the relevant activity category.</p>	<p>This includes activities carried out by the credit institutions, such as:</p> <ul style="list-style-type: none">- 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?



THE IMPLEMENTING PROCEDURES

The Aim of Implementing Procedures



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

Why?

- To avoid the misuse of the financial system to channel illicit gains or even lawful gains destined for unlawful purposes (terrorism)
- To reduce risk to the **integrity, proper functioning, reputation and stability** of the financial system.
- To uphold legal and professional standards for the integrity of financial markets.

Purpose for Implementing Procedures

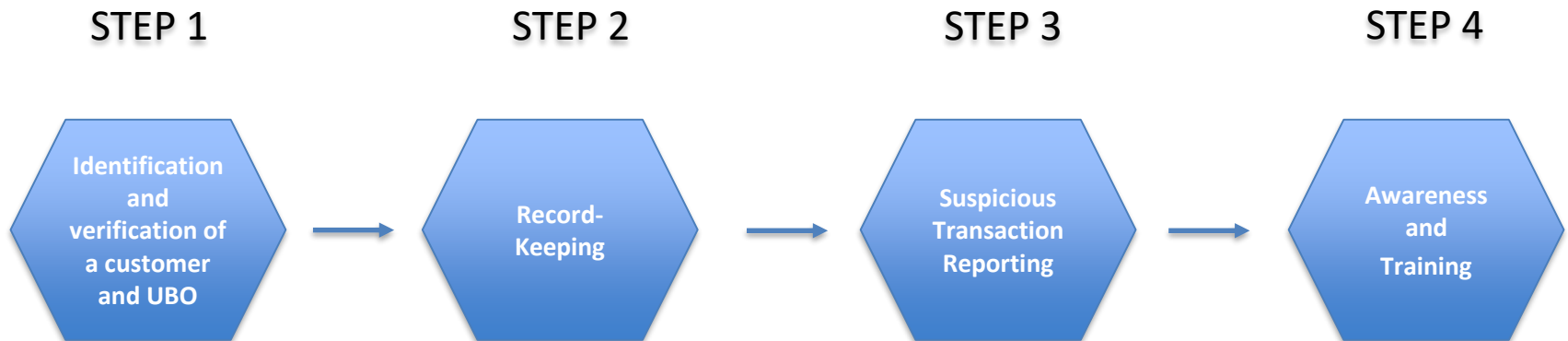
To assist subject persons to understand and fulfil their obligations and effectively implement the provisions under the PMLFTR.

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

Key obligations

Overview of Key Obligations



STEP 1: Identification and 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

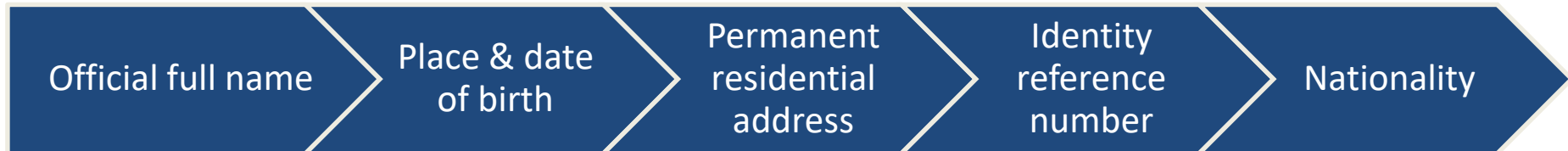
Establish purpose and intended nature of the business relationship & business & risk profile of customer

In the case of a business relationship, monitor the same on an ongoing basis

Who is the customer?

- _ A person (whether legal or natural)
- _ 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.

Natural person: *Identification*



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

Legal person: *Identification of BOs*

Body corporate or body of persons	<ul style="list-style-type: none">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 informationii. After having exhausted all possible means and provided there are no grounds of suspicion, no beneficial owner has been identified, subject persons shall consider the natural person or persons who hold the position of senior managing official or officials to be the beneficial owners, and shall keep a record of the actions taken to identify the beneficial owner
Trusts, foundations, and other similar legal entities or arrangements	<ul style="list-style-type: none">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
Long-term insurance business	<ul style="list-style-type: none">i. Beneficiaries if specifically named personsii. Class of beneficiaries if not determined – to identify and verify at time of pay-out or at the time the beneficiary intends to assign any rights vested under the policy

Senior managing officials

Those who are responsible for taking strategic decisions that fundamentally effect the business operations or general direction of that entity

- All directors, including NEDs

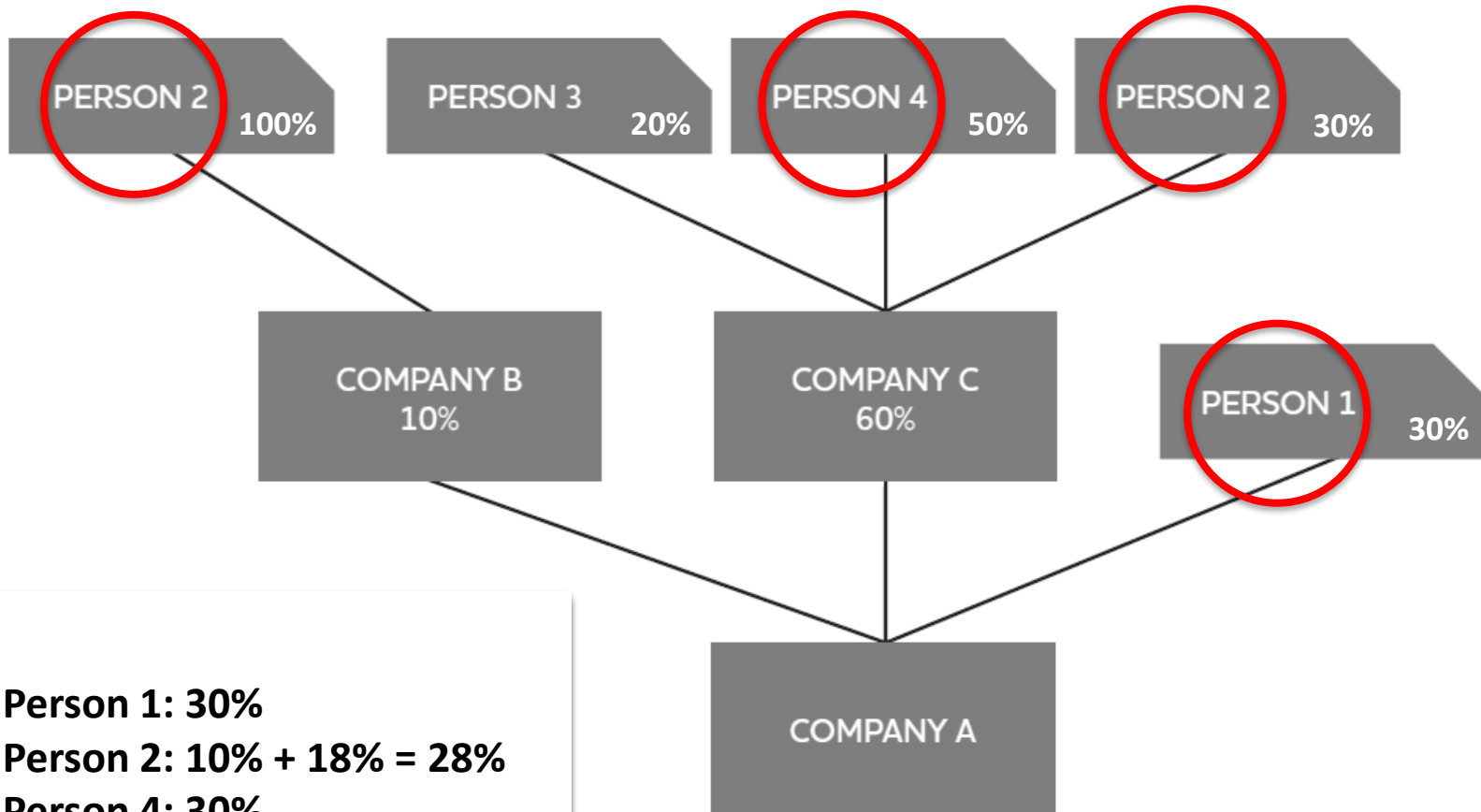
Those who exercise executive control over the daily or regular affairs of the entity through a senior management position

- Executive management, including CEO, CFO

Persons exercising control

- Disposing / advancing / lending / investing the assets of the entity
- Vary or terminating material agreements, e.g. trust deed
- Adding or removing beneficiaries
- Appointing or removing trustees
- Appointing or removing the majority of board members (or administration) of an entity, or to appoint or remove the CEO of that entity
- Directing, withholding consent to the exercise of certain powers
- Rights through formal arrangements (such as shareholders' agreements or through rights attached to shares) by means of which that person(s) can exert dominant influence or veto the decision-making of that legal person (e.g., having absolute discretion or veto rights over the entity's business plan, borrowing options or business model)
- Individuals who, though not being owners of a sufficient percentage of shares or voting rights (i.e., less than the 25% threshold explained previously), collectively exceed the 25% threshold and are subject to an arrangement to exercise their rights collectively in the same way (acting on concert)
- Individuals who through family connections exert influence over the decision-making body of that entity (e.g., a family business in which a family member, even though not being formally involved in that entity, is routinely referred to for direction about company decisions).

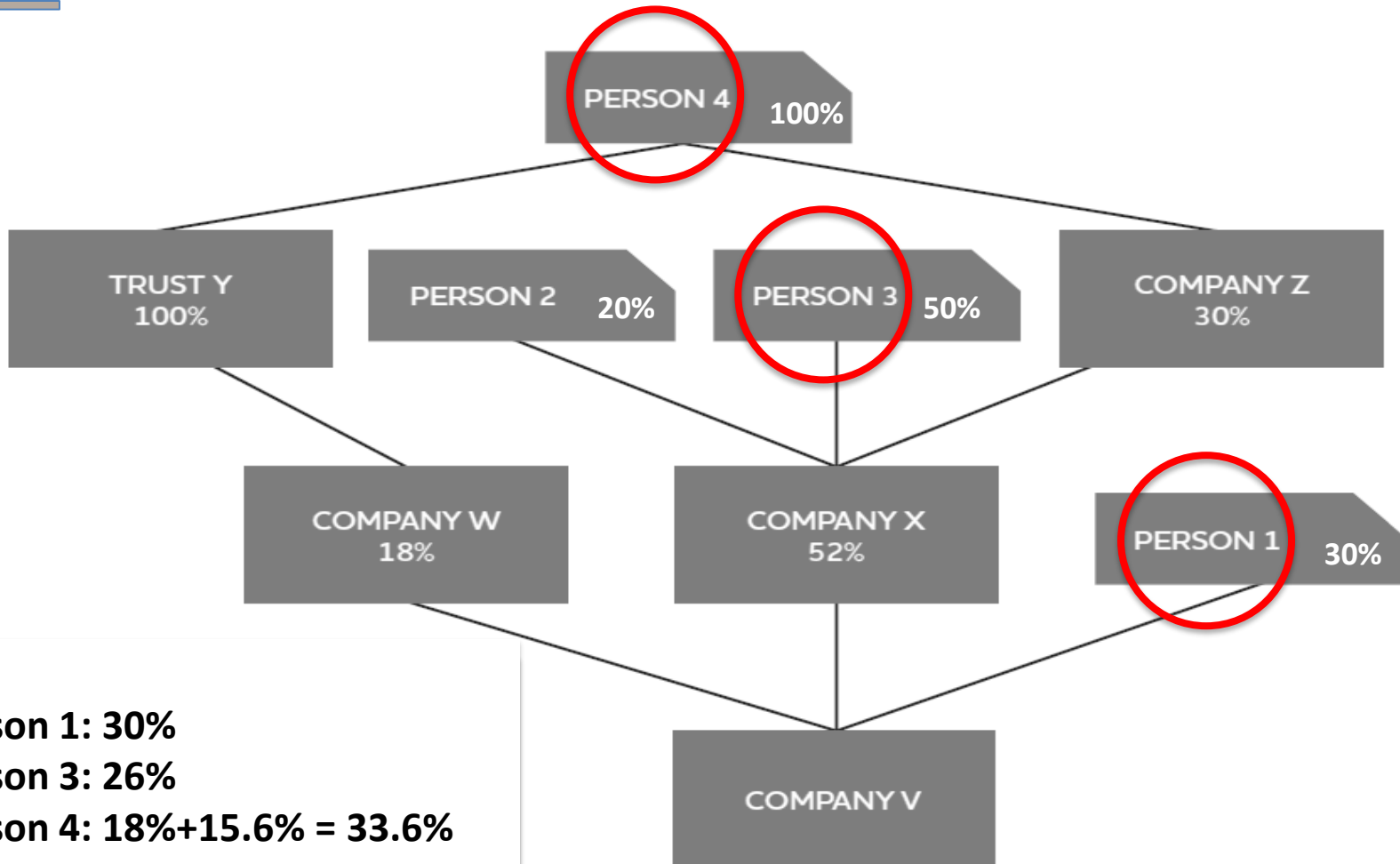
BO examples – Example 1



BO examples – Example 1

Key take away: It is important to establish and figure out the customer's entire corporate structure to be in a position to understand whether an individual features within an ownership structure through more than 1 entity. In such cases, all holdings of that same individual are to be assessed since, through the different holdings within the structure he may hold a sufficient % of shareholding that would make him a BO.

BO examples – Example 2

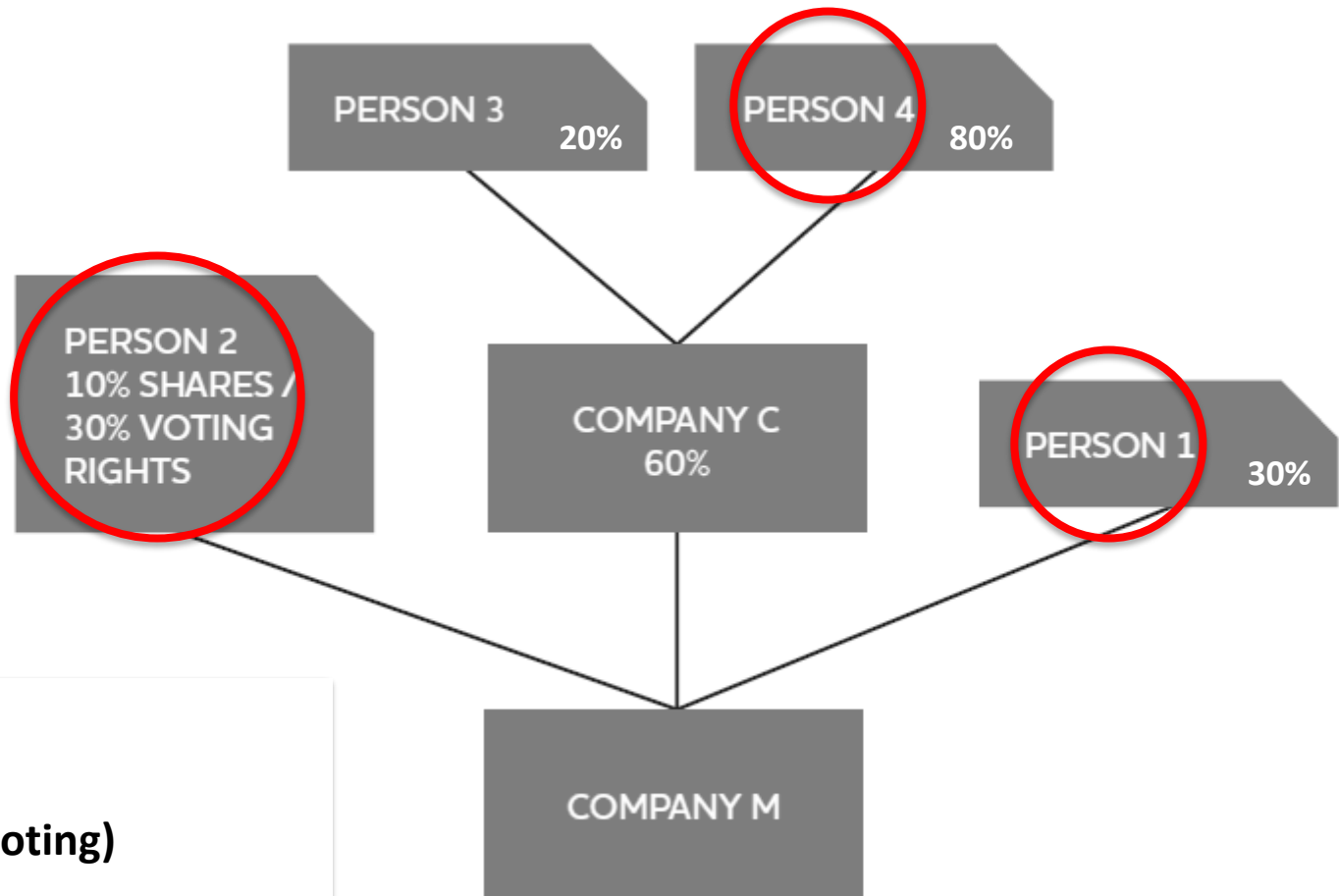


Person 1: 30%
Person 3: 26%
Person 4: 18%+15.6% = 33.6%

BO examples – Example 2

Key take away: Whenever the shares of a body corporate (the customer) are held in trust, and that trust is administered by a corporate trustee, subject persons are not expected to identify and verify the BO(s) of that corporate trustee. The requirement is to identify and verify the identity of the BO of the customer's entity, i.e. the body corporate, and not the trustee administering the trust which holds the shares in that body corporate.

BO examples – Example 3



Person 1: 30%
Person 2: 30% (voting)
Person 4: 48%

Natural persons: *Verification*

- Verification of the customer's identity must happen on the basis of documents, data or information that is obtained from a reliable and independent source.
- The customer's identity and address may be verified by referring to documents (e.g. valid & unexpired passports, ID cards, driving licences, recent utility bills, lease contracts, bank reference letters, and bank statements) or by making use of electronic sources (e.g. e-IDs, Bank-IDs and electronic commercial databases).
- Databases maintained by public authorities (e.g. electoral roll) or third-party service providers can also be used to verify residential address provided that the database is reliable and independent, and that verification of identity is carried out in advance

Verification in exceptional scenarios

- 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;
- 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;
- when the customer is residing in a nursing home or similar residential care institution, the subject person may verify the customer's residential address by obtaining a letter from the director or manager of the home/institution confirming the customer's residential address;
- when the customer is homeless or a member of the travelling community, subject persons must gather sufficient information and, where available, documentation on the customer's situation and frequent whereabouts;
- 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;
- when the customer is a minor (and therefore might not have identification documents or cannot present documents issued by recognised credit institutions or other financial service providers), subject persons may rely on a birth certificate to verify the minor's identity. The subject person must additionally proceed to identify and verify the parent(s) or legal guardian(s) and obtain reasonable evidence of parenthood or legal guardianship. With respect to the residential address, verifying the residential address of the parents or guardians with whom the minor resides would suffice.

Legal persons: *Verification*

Nature of principal	Identification & verification procedures
Public / Private company Commercial partnership	<ul style="list-style-type: none">• 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&As (or partnership agreement), recent certificate of good standing (not older than 3 months), or other 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	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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

Verification records

Face-to-face

- _ Keep original itself or true copy of original document on file (wet ink dated and certified by an officer or employee of the subject person) or scanned in electronic format (provided system requirements are met).
- _ Where exceptional verification measures are used, the subject person must also appropriately document the reasons for recurring to such exceptional measures and the reasons for considering such means as reasonably re-assuring to verify the customer's identity.

Verification records

Non face-to-face

- Subject persons may receive documentation in copy or scanned format and should avoid accepting documents that are more susceptible to being tampered with (e.g. in Word version).
- Information should be clearly visible and legible and in a language understood by the subject person.
- Copies sent via email addresses that do not seem to tally with the name or other details of the customer sending the documentation should raise concern.
- Use of video conferencing tools and verification software is also acceptable provided that certain system capabilities and requirements are satisfied.

Additional measures for non face-to-face

Subject persons should determine whether they are confident in having adequately verified the customer or whether additional measures should be taken on the basis of a risk assessment. Such additional measures may include:

- Requesting additional identification documents;
- Requiring certified documentation and checking the certifier;
- Ensure that the first payment/transaction into the account is done through another account in the name of the same customer with a bank/financial institution authorised in the EU/EEA/reputable jurisdiction;
- Requesting the customer to confirm automatically generated codes/PINs before accessing the service;
- Holding a ‘welcome call’ and confirming certain information;
- Using information that can be retrieved from a customer’s device (e.g. IP address or geo location);
- Sending a small transfer of funds to a bank account held by the customer asking him to return the funds or indicate the value;
- Requiring the customer to send a photo clearly showing his face and image on the ID document being held in the same picture.

Authenticity checks

- Particular care should be taken to ensure that the documents obtained are authentic and have not been forged or tampered with. Possible checks include:
 - examining the optical security features and confirming that these can be seen;
 - examining the lamination;
 - checking for uneven document colours and non-uniformity;
 - verifying or decoding the MRZ code contained on the identification document.

Customer vs Agent

- Where the customer is represented by another person acting as agent, the subject person is required to carry out additional measures over and above identifying and verifying the identity of the customer and the BO:
 - ensure that the agent is duly authorised in writing to act obo the customer; and
 - identify and verify the identity of the agent – if the agent is a natural person, then full ID&V needs to take place; if it is a legal entity, then subject persons do not have to establish its ownership and control structure, identify who its BOs are, and identify and verify the entity of its officers and/or employees who provide instructions to the subject persons.
 - seek to understand the rationale behind such arrangement and why the customer did not seek to contact the subject person directly.
- Circumstances which the subject person must have regard to when determining whether the customer is acting obo another person include:
 - from where the subject person is receiving instructions;
 - the source of the funds;
 - the destination of the funds;
 - payment references or rationale;
 - unusual delay in answering questions.

Purpose and intended nature of the business relationship & profile

Subject persons are required to gather and analyse information to determine whether a service being provided to a customer makes sense in the customer's situation and profile. For this purpose, subject persons must:

- _ assess the customer's intention in acquiring a particular service and/or product;
- _ contribute to its customer risk assessment and ensure that the customer falls within the subject person's risk appetite;
- _ determine the appropriate risk mitigating measures to be adopted; and
- _ carry out meaningful ongoing monitoring as it will be able to understand and identify the expected behaviour, including the expected nature of transactions or activities, of the customer throughout the business relationship.

Purpose and intended nature of the business relationship & profile

- At times, the purpose of the establishment of the relationship is quite self-evident (e.g. opening of a gaming account, setting up a company, etc), and, limitedly to this aspect, it is not required that subject persons obtain any additional information from their customers.
- However, this does not exonerate the subject person from the development of a customer business and risk profile, the key element being to have sufficient information available so as to allow a proper appreciation of the risks involved and the detection of unusual activity.
- To this end, subject persons have to collect sufficient information and, where necessary, documentation to establish a prospective customer's **source of wealth** as well as the **source of the funds** to be used for his expected outlays.

Source of wealth and source of funds

	Source of wealth	Source of funds
Definition	The economic activity which generates the total net worth of the customer	The activity, event, business, occupation or employment from which the funds used in a particular transaction are generated
Timing of checks	Usually identified at the beginning of the business relationship; updated from time to time in case of material developments	Identified for each individual transaction
Evidence	The subject person should not be satisfied with a generic description when questioning the customer about the origin of the funds used in the context of a business relationship. For instance, an explanation by the customer stating that the funds consist of the proceeds generated by a business would not be sufficient and the subject person is required to request the customer to provide more detailed information on the business concerned as well as producing documents, such as copies of invoices or contracts, to substantiate such explanation.	

Customer's business and risk profile

- The kind of information gathered will vary depending on the risk profile of the customer and the service identified through the customer risk assessment.
- Where the risk is medium or lower, a declaration from the customer with some details (e.g. nature of employment/business, usual annual salary etc.) can suffice. Where the risk of ML/FT is higher, or subject persons have doubts as to the veracity of the information collected, the information obtained would need to be supplemented by means of independent and reliable information and documentation.
- Hence, information gathered may vary from declaration obtained directly from the customer to the collection of documentation to verify the same or information derived from reliable and independent third parties.
- Subject persons should take a risk-sensitive approach which considers data protection principles and hence requests should not be disproportionate, excessive or irrelevant.

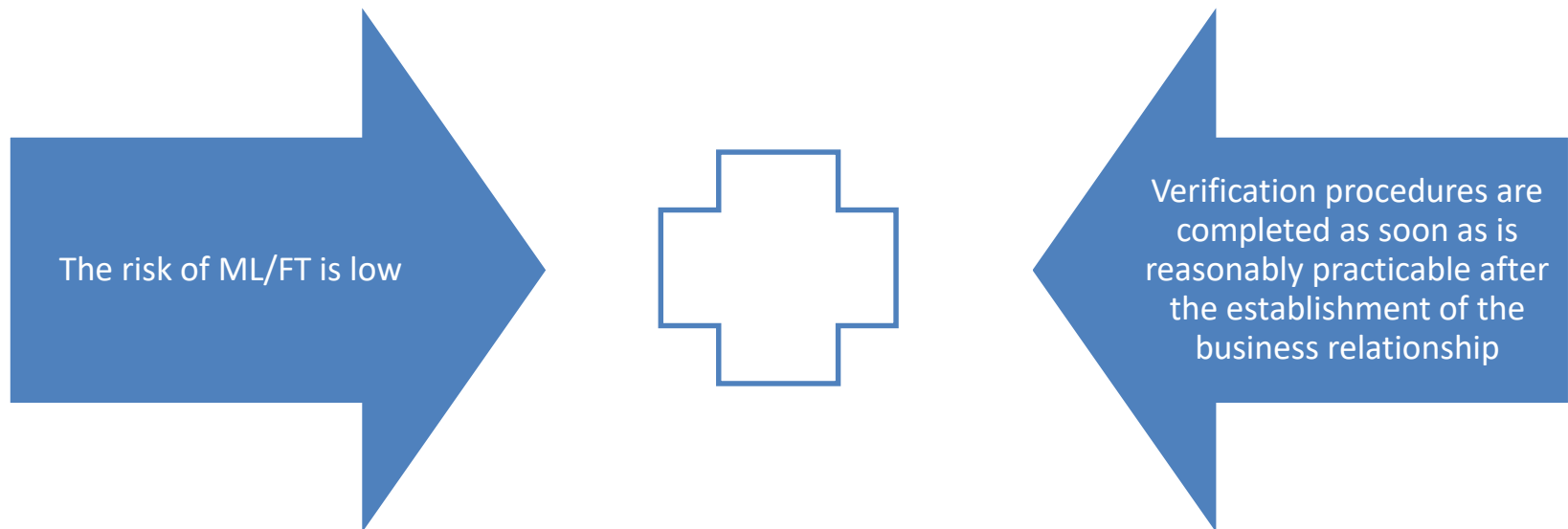
Timing of CDD

- Subject persons are to verify the customer's identity and, where applicable, the beneficial owner's identity when establishing a business relationship.
- In practice, requiring the customer to provide documentation for the purposes of verification in the context of a preliminary meeting or when initial enquiries are still being made, may not always be realistic and reasonable.
- However, when the same person takes active steps that show that there is an intention to establish a business relationship, with the exception of circumstances that justify a delay in the carrying out of CDD measures, the subject person is required to complete these CDD measures.

Exceptions: when CDD can be delayed

Business relationships

Notwithstanding the obligation to complete verification procedures prior to the establishment of a business relationship, verification procedures may be completed **after** the establishment of a business relationship when it is necessary so as not to interrupt the normal conduct of business. However, this exception is subject to the following two conditions being met:



Exceptions: when CDD can be delayed

Business relationships

- The low risk of ML/FT does not here refer to the overall risk of the business relationship that would result following the carrying out of the CRA.
- Rather, it is the risk within the initial phase of the business relationship that must be assessed.
 - By way of example, the use of some products within the initial phase of a business relationship may be so limited in value, or the type of product itself or its level of activity may appear to pose such a low risk of ML/FT, that the business relationship at that point in time will present a low risk of ML/FT independently of any other factors.
- In the event that CDD measures are applied after the establishment of a business relationship, subject persons should record the reasons for deferring their application.

Exceptions: when CDD can be delayed

Occasional transactions

- When a customer seeks to carry out an occasional transaction, subject persons are required to apply CDD measures when the prospective customer takes active steps to benefit from a service or a product provided by the subject person and at all times prior to any product or service being provided to the customer.
- On the other hand, when a customer merely seeks to obtain information from the subject person, such as, for instance, the general conditions under which a subject person would be ready to provide its services or products, the subject person would not be required to carry out any CDD measures. Such an obligation would only arise once the customer takes active steps to engage the subject person to provide its services or products to carry out the occasional transaction.
- Occasional transactions may vary in nature and therefore, depending on the case at hand, subject persons are to apply suitable CDD measures. For instance, in the case of a company incorporation, CDD measures have to be applied, and documentation collected, prior to carrying out the incorporation.

Exceptions: when CDD can be delayed

Legal arrangements

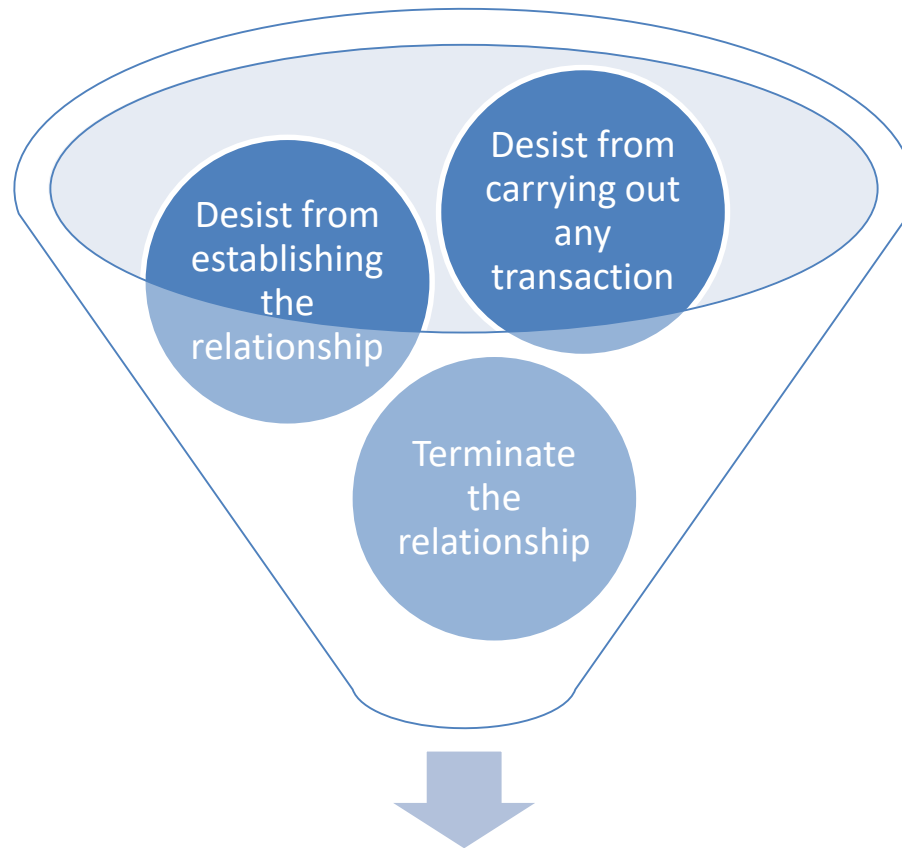
- Where it is not possible to identify and verify the identity of the beneficiary at the time of the establishment of the business relationship, e.g. where the beneficiaries are simply designated by particular characteristics or class and not (specifically) named as beneficiaries, at the establishment of the business relationship (such as the setting up of the trust), the subject person is only required to gather sufficient information concerning the class or characteristics of beneficiaries (which information one would expect to be contained in the trust instrument) to be able to establish if the beneficiaries, once they are determined, are entitled to receive the distribution.
- Having established as much, subject persons are to carry out identification and verification of the beneficiaries. The verification of their identity may be delayed until the time of pay-out (i.e., prior to the funds being transferred to the beneficiary) or at the time the beneficiaries seek to exercise their vested rights.
- Furthermore, if the beneficiary assigns any of its rights, the assignee has to be identified as soon as the subject person becomes aware of this assignment. Here again, the verification of the assignee's identity may, however, be delayed until pay-out.

Exceptions: when CDD can be delayed

Legal arrangements

- _ Where the beneficiaries are not aware that they have been designated as beneficiaries, identification can still be carried out on the basis of the personal details contained in the trust instrument and/or obtained from the settlor/trustee. However, verification of identity can then be delayed until pay-out.
- _ The same reasoning can be applied to beneficiaries who have not yet received any distribution under the trust or when the distribution is subject to one or more conditions being met or to the trustee's discretion, and the risk of ML/FT is considered to be low. Even in these cases, it is possible for verification of identity to be delayed until pay-out.

Failure to complete CDD

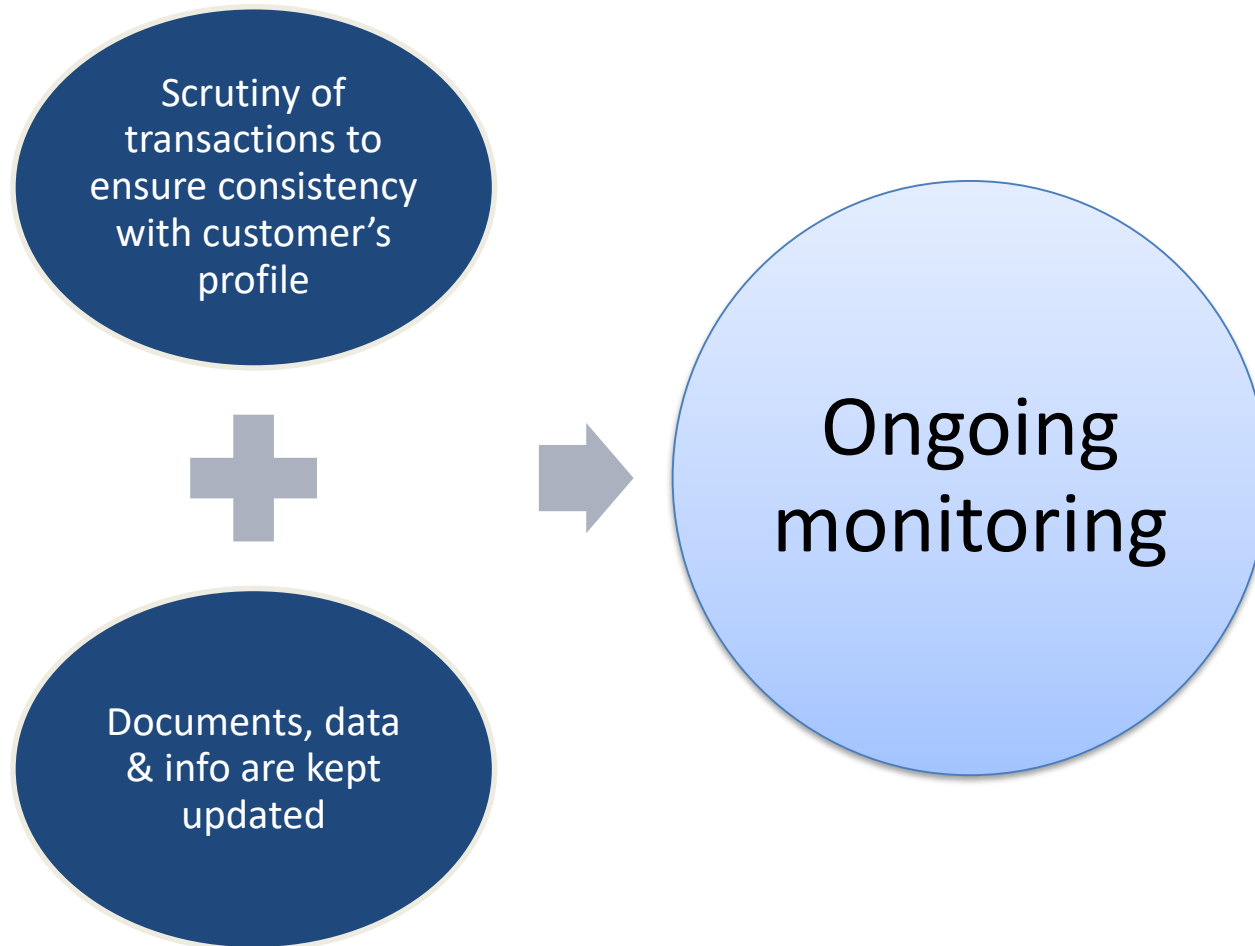


Consider filing an STR

Remitting back the funds

- _ When remitting funds back to the customer, you must:
 - _ remit the funds to the original source using the same channels used to receive the funds; and
 - _ to the extent that this may be possible, indicate in the script/instructions accompanying the funds that these are being remitted due to its inability to complete CDD.
- _ In the event that you are unable to remit the funds to the source using the same channels, you will inevitably have to request fresh instructions from the customer. If these instructions give rise to a suspicion, an STR should be submitted and remittance should be suspended in line with the applicable timeframes.

Ongoing monitoring



Updating of documents

- Trigger events, e.g. adverse media concerning a customer, customer is now doing business with high-risk jurisdictions
- Periodic reviews
 - **Frequency** will depend on the customer's risk rating, the kind of information to be updated, and whether there are any risks that can be mitigated through updating;
 - **Extent** will depend on the above factors as well as the relevance of information with respect to CDD and AML/CFT and the necessity of the information to be updated.

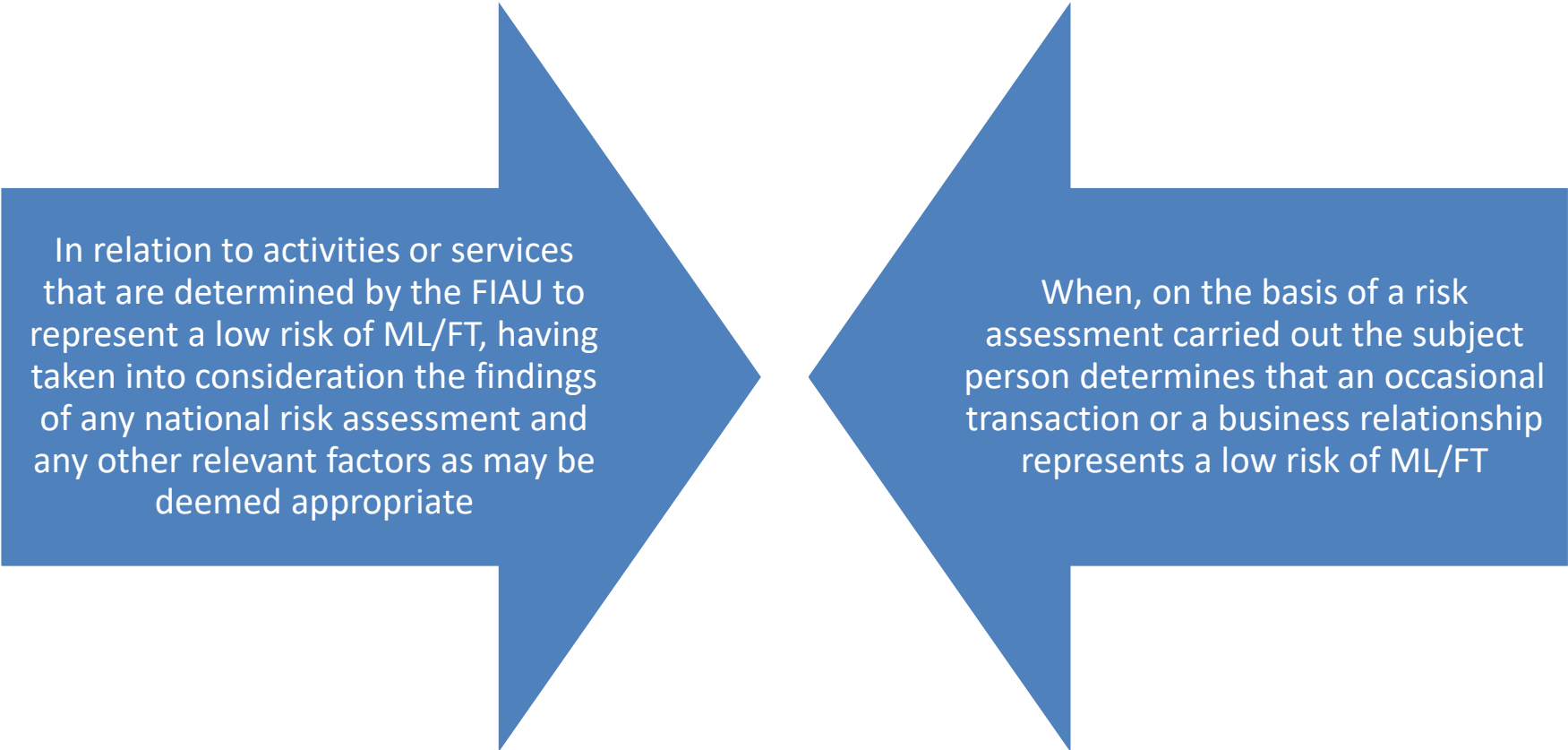
Ongoing monitoring

More specifically, you should consider the following on-going monitoring measures for the activities listed below:

<i>All services</i>	keep documentation up-to-date (by ensuring that identification data is not expired, confirming with the client that other data held on file is still relevant on a regular basis depending on the risk classification); carrying out real-time (or at least daily) sanctions checks; review of financial statements; carrying out adverse media searches on an ongoing basis with the frequency being dependent on the risk classification of the client determined in accordance with the risk assessment
<i>Registered office</i>	making sure that the correspondence being received is in line with your understanding of the activities being carried out by the client
<i>Directorship</i>	ensuring minutes of discussions and decisions at board level are taken and that they are in line with the expected activities of the client; requesting supporting documents when approving a payment or a transaction
<i>Company secretarial</i>	ensuring that updated and comprehensive board minutes are maintained and that the necessary statutory forms are filed on time registry forms; ensuring that discussions at board level are in line with your understanding of the client's business activities
<i>Nominee services</i>	Ensuring changes in the beneficial owners are captured
<i>Trustee services</i>	DD on each settlement and use of the trust assets

Simplified and Enhanced Due Diligence

When does SDD apply?



In relation to activities or services that are determined by the FIAU to represent a low risk of ML/FT, having taken into consideration the findings of any national risk assessment and any other relevant factors as may be deemed appropriate

When, on the basis of a risk assessment carried out the subject person determines that an occasional transaction or a business relationship represents a low risk of ML/FT

What can be adjusted for SDD?

Timing of CDD

- When the product, service or transaction sought has features that limit the possibility of its use for ML/FT purposes, subject persons can decide to postpone the verification of identity or other CDD measures until a pre-determined threshold or other triggering event is reached

Quantity of information

- When the product sought is limited in use and transaction values, the subject person can opt to obtain less information the customer's source of wealth or funds

Quality of information

- When the product, service or transaction sought has features that limit the possibility of its use for ML/FT purposes, subject persons can adjust the source of information obtained for CDD purposes, such as by accepting information obtained from the customer rather than an independent source to establish the customer's business and risk profile
- This would not be acceptable to verify the customer's own identity

Frequency & intensity of ongoing monitoring

- monitoring only transactions that meet or exceed a given threshold;
- the frequency of CDD updates and reviews of the business relationship is adjusted, for example, to take place only when trigger events occur, such as the customer looking to take out a new product or service or when a certain transaction threshold is reached – this should not result in a de facto exemption from keeping CDD information and documentation up to date.

Conditions for SDD

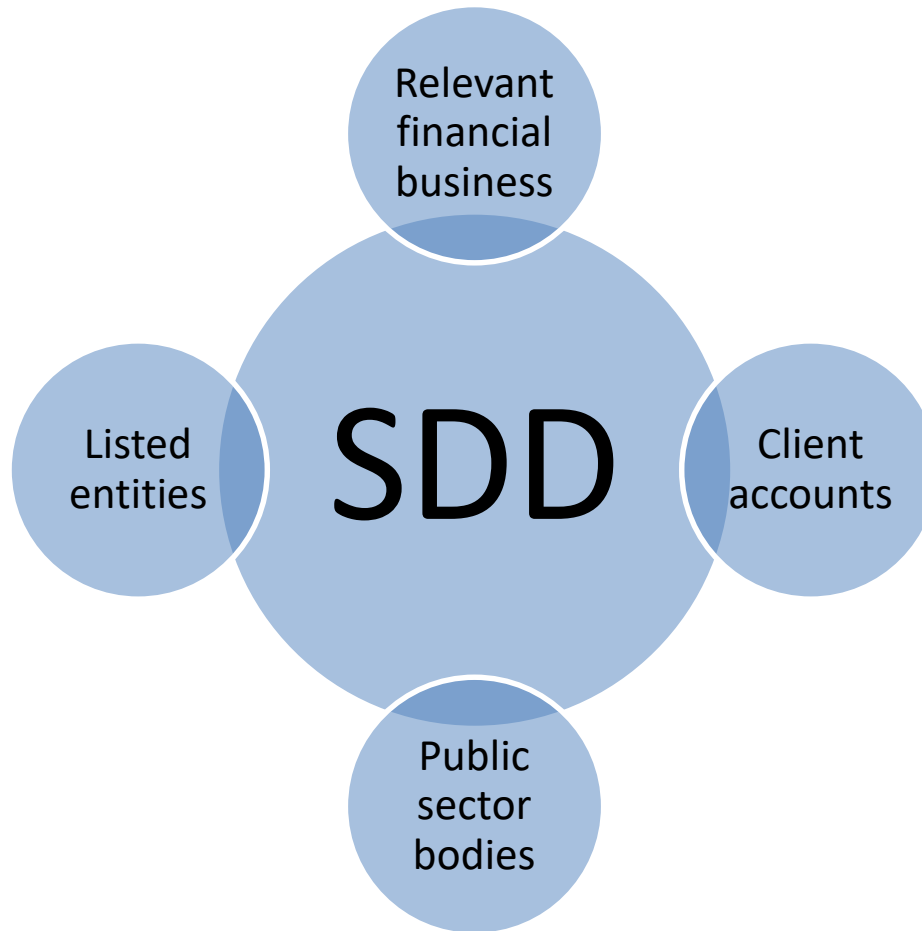
Variation in the extent and timing of CDD does not result in a de facto exemption from CDD measures

Any threshold or event set to trigger CDD measures is set at a reasonably low level

Systems are in place to (i) detect when the threshold has been reached or/and an event has materialised and (ii) prevent bypassing any restrictions, limitations or characteristics applicable to the product or service

Subject persons do not vary, defer or delay any CDD measures they cannot vary, defer or delay under any EU Regulations, the PMLFTR, the Implementing Procedures or any other binding instrument, order or directive

Typical SDD circumstances



Customers carrying out relevant financial business

SDD can be applied to customers who are subject persons carrying out relevant financial business or third parties established in an EU Member State or in a reputable jurisdiction carrying out an equivalent activity and subject to equivalent AML/CFT requirements and supervision as those required by the EU. For this purpose, the following measures should be taken:

- checking for any publicly available adverse regulatory or supervisory information;
- obtaining evidence that the customer institution is licensed or authorised to conduct financial and/or banking business;
- have an understanding of the activities that customer is undertaking as well as the customer base;
- carry out checks with respect to omnibus accounts.

Client accounts

Persons who hold client money or other assets in pooled accounts (whether in a bank account or through a securities holding) may themselves be subject to AML/CFT measures. Hence, subject persons carrying out a relevant financial business, with whom these client accounts are held, can consider applying SDD measures, provided that all of the following conditions are met:

- the business relationship with the holder of the pooled account presents a low risk of ML/FT, considering among others the account holder's business, the type of underlying customers serviced by the holder and the jurisdictions the holder's business is exposed to;
- the holder of the account is a subject person or is otherwise a third party established in the EEA or in a reputable jurisdiction that is subject to equivalent AML/CFT requirements and supervision as those required by the EU;
- it is determined that the holder of the pooled account applies robust and risk-sensitive CDD measures to its own customers and, where applicable, to their beneficial owners;
- an undertaking is obtained from the customer that CDD information and documentation on the identity of the persons on whose behalf monies are held in the pooled account will be made immediately available to the subject person upon the subject person's request, with any such undertaking being tested from time to time; and
- there is no adverse information on the account holder.

In these cases, the subject person may decide not to ask for any information and documentation on the identity of the assets' beneficial owner/s and limit itself to applying CDD measures to the account holder and carrying out a sufficient level of ongoing monitoring to ensure that there is no change in the level of risk to which the subject person is being exposed to.

Public sector bodies

- In respect of customers who are local or overseas governments (or their representatives), supranational organisations, government departments, state-owned companies or local authorities, the approach to identification and verification may be tailored to the customer's circumstances, reflecting the subject person's determination of the level of ML/FT risk presented. When the subject person determines that the business relationship presents a low risk of ML/FT, SDD measures may be applied. Public sector bodies include state supported schools, colleges and universities.
- For the avoidance of doubt, subject persons must make a distinction between state-owned entities and bodies engaged in public administration. Bodies engaged in public administration may involve different revenue/payment streams from those of most businesses and are typically funded from government sources, or from some other form of public revenues.
- State-owned businesses, on the other hand, may engage in a wide range of activities, some of which might involve higher risk factors, leading to a different level of CDD being appropriate. These entities may be partly publicly funded or may derive some or all their revenues from trading activities.
- Furthermore, in determining the level of ML/FT risk presented, subject persons are required to assess the jurisdictional risk.
 - By way of example, a government department of a jurisdiction listed by FATF as a high-risk and non-co-operative jurisdiction should not be considered to represent a low degree of ML/FT risk and hence should not be subject to SDD. The same may apply to other jurisdictions that may not necessarily be listed by FATF but, for instance, are characterised by corruption, political instability or civil unrest.

Listed entities

- When the customer is a listed company, i.e., it has its securities admitted to trading on a regulated market, subject persons may limit themselves to identifying and verifying the company, and refrain from identifying the directors, obtaining an understanding of the ownership and control structure, and identifying and verifying the identity of the beneficial owners.
- In order for this to apply, the subject person has to establish whether:
 - the company's securities are traded either on an EEA regulated market within the meaning of MiFID or on a non-EEA regulated market. If the regulated market is located within the EEA, the subject persons has to document how it has ascertained the status of the regulated market. If the market is outside the EEA, the subject person has to ascertain that the jurisdiction where this market is located is a reputable one and then establish that the market is subject to regulation in a manner similar to that provided for within the EEA.
 - the company is subject to disclosure requirements, which ensure adequate transparency of ownership information. This can be assumed to be the case when the company's securities are traded on an EEA regulated market. When the trading is taking place on a non-EEA regulated market, the subject person has to determine whether the company is subject to disclosure obligations that are contained in international standards and are equivalent to the specified disclosure obligations in the EU. The subject person should ensure that, as a minimum, the company is subject to specified disclosure obligations that are consistent with the specified articles of (i) the Prospectus Directive, (ii) the Transparency Obligations Directive, and (iii) the Market Abuse Directive and with EU legislation made under the specified articles.

Listed entities (cont.)

- Subject persons are to note that, prior to exercising this discretion, they are to consider whether any regulatory action has been taken either by the relevant supervisory authority or by the regulated market against the listed company for breaches of its disclosure requirements. Should this prove to be the case, the grounds for the application of this exemption would be questionable and the subject person would have to assess the relevance of these breaches and determine whether the grounds for the application of this exception still subsist.
- Subject persons must retain on file records of the assessment they carried out and of the conclusions reached. Moreover, they should ensure that they review the position as part of the ongoing monitoring process to ensure that there were no changes that would no longer allow the subject person to apply SDD (e.g. delisting of the company).
- With respect to companies that are themselves owned in whole or in part by a listed company, a distinction has to be drawn between situations when the customer is wholly owned, directly or indirectly, by the listed company and situations when that ownership is only partial. In the former situation, the above would still apply since the beneficial ownership would be subject to disclosure requirements due to the parent company's listing. On the other hand, in the latter case, the subject person would have to determine what percentage of shares or voting rights are held or controlled by the non-listed entity (this entails establishing the ownership and control structure) and, when it is determined that there may be additional beneficial owners behind these entities, the beneficial owners would still need to be identified and verified.

When is EDD applied?

In addition to the default CDD measures, enhanced due diligence (EDD) measures must be applied in the following situations:

- _ In relation to activities determined by the FIAU to represent a high risk of ML/FT;
- _ Where, on the basis of a CRA, the subject person determines that a business relationship or transaction represents a high risk of ML/FT
 - _ verify identity of customer/BO on the basis of more than one reliable and independent source; identify & verify identity of other shareholders; obtain more information about the customer and the nature and purpose of the relationship; review and update documentation more frequently
- _ Complex and unusually large transactions
 - _ Same as above with an emphasis on the importance of making enquiries to test reasonableness
- _ When dealing with persons established in a non-reputable jurisdiction
 - _ Same as above plus inform the FIAU if you intend to proceed in the case of a jurisdiction against which counter-measures have been applied
- _ When dealing with a PEP
 - _ Obtain senior management approval; verify source of wealth and funds; and conduct enhanced ongoing monitoring, on a risk-sensitive basis

Record-keeping

Record-keeping

Category	Detail	Retention period
Actions taken to adopt and implement the RBA	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• Training• Employee screening• Reliance agreement• Outsourcing agreement• Other reports which may be useful for FIAU, e.g. internal audit reports	<ul style="list-style-type: none">• 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

To facilitate the retrieval of records and to assist in any compliance monitoring activity conducted by the FIAU or other relevant supervisory authorities, 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.

Suspicious Transaction Reporting

Red Flag Indicators

- ❖ Complex transactions in which multiple properties are bought, re-sold or exchanged
- ❖ Customer buys multiple properties in a short period of time
- ❖ Customer uses cash to settle transactions which are usually not cash-based
- ❖ Deposits made to a legal practitioner's account to fund transactions (e.g. real estate purchases) which do not take place
- ❖ International funds transfer instruction to or from legal firm's account to or from high-risk jurisdictions
- ❖ Legal entity structures are used in transactions for no apparent commercial or other reason
- ❖ Multiple unexplained funds transfers to foreign beneficiaries
- ❖ Significant or structured cash deposits to and withdrawals from a legal practitioner's account
- ❖ Structured cash deposits into an account and then funds withdrawn via transfer or bank cheque to a payee that is a legal firm's account
- ❖ Transactions involving politically exposed persons (PEPs)

Highlighting Suspicious Activity

- Provide trust deeds
- CDD documentation and KYC
 - Copy of I.D.
 - Passports
 - Company details
 - M&A
 - Details of UBO
- Determining source of funds and wealth
 - Obtain supporting documentation
 - Sufficient evidence and documentation
- Adverse media articles
 - Provided to substantiate the suspicion
 - A simple link or particular website may suffice

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

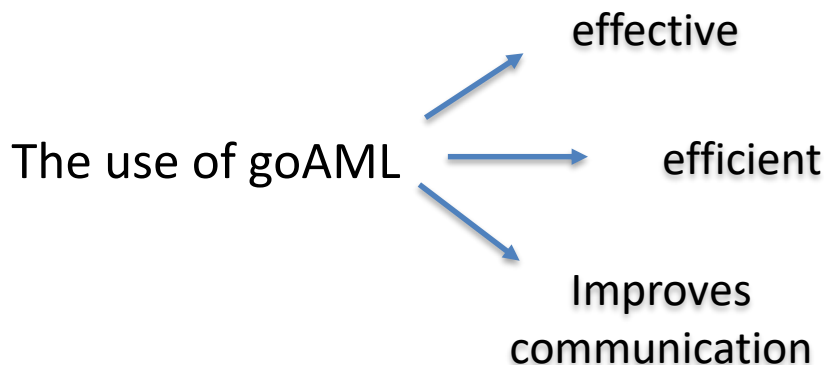
- Provide details of the review/investigation carried out by the reporting entity.
- State the facts in a clear and concise manner
 - Rationale must be clearly identified
 - State who the person is (individual or group of persons)
- Details of activity/transaction and accounts
 - How did the transaction take place?
 - Values and amounts involved

3. Conclusion

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

New System: goAML

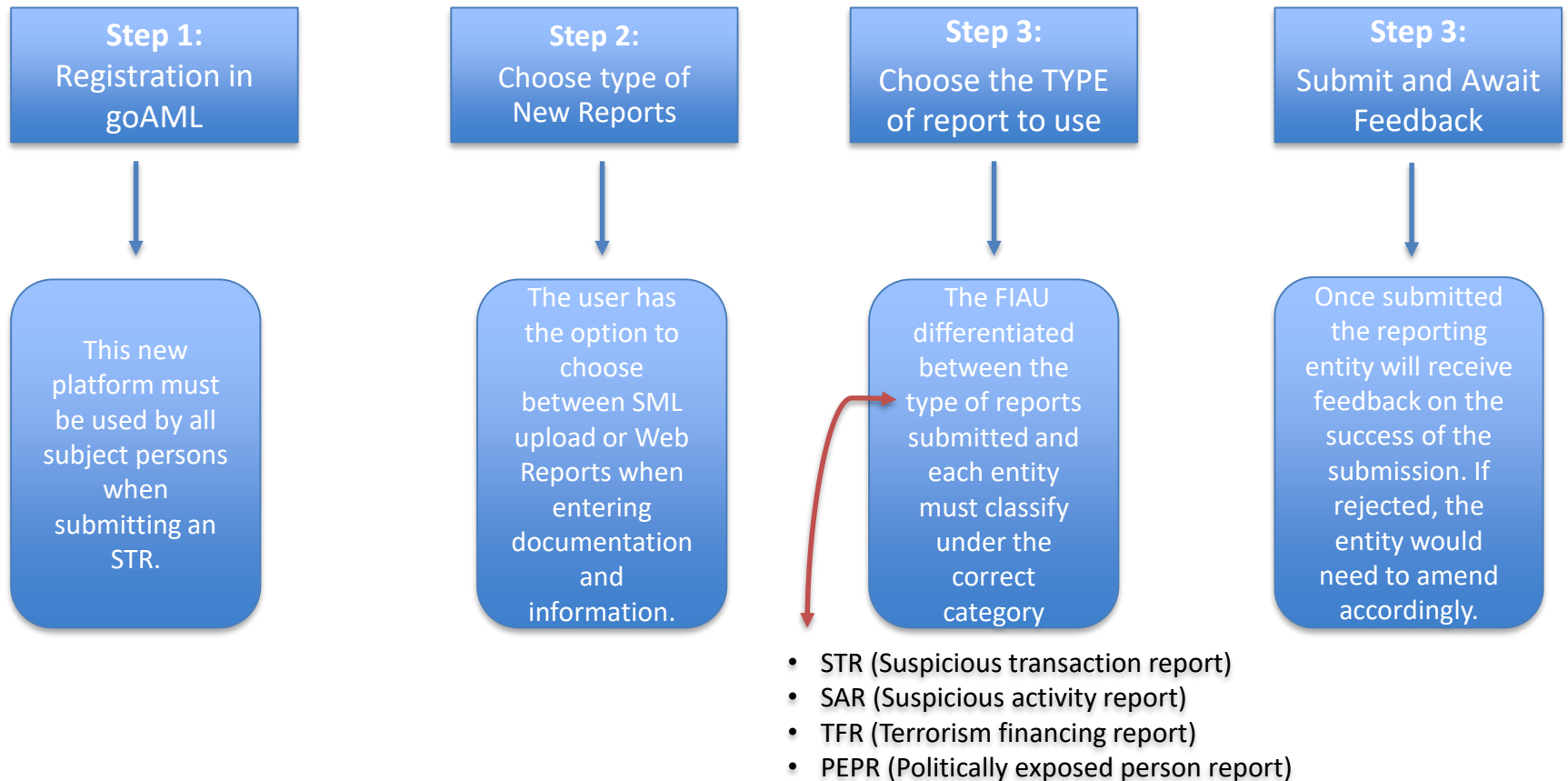
The FIAU has replaced the STR submission system and implemented the goAML software solution which has been developed by the United Nations Office on Drugs and Crime.



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?



Reliance

Scope

- Subject persons may only rely on the CDD measures undertaken by other subject persons or third parties in relation to:
 - the identification and verification of a customer;
 - the identification and verification of beneficial owner(s), where applicable; and
 - information on the purpose and intended nature of the business relationship and on the business and risk profile
- The obligation to carry out ongoing monitoring of the business relationship continues to rest with the subject person.
- Subject persons always remain ultimately responsible for compliance with their CDD requirements.
- Subject persons must understand whether the measures carried out by the other entity to counter the risks of ML/FT are equivalent to those that the subject person deems sufficient. Prior to entering into a reliance arrangement, the subject person should thus ensure that it understands the type of CDD measures which the entity undertakes on its customers.
 - Such assessments should be put down in writing and documented accordingly.
- Moreover, subject persons may only rely on CDD measures actually carried out by the entity relied on. Thus, it cannot rely on information, data or documentation obtained by that entity or to which it has access through other reliance arrangements; **having a chain of reliance arrangements is not permissible.**

Entities that can be relied upon

Subject persons may rely on the CDD measures carried out by:

1. Persons falling within the definition of 'subject person' under the PMLFTR; and
2. Third parties being:
 - Persons or institutions undertaking activities equivalent to 'relevant financial business' or 'relevant activity';
 - Member organisations or representative bodies of such persons; or
 - Other institutions or persons in an EU Member State or other third country

As long as the persons listed under (2) above also:

- apply CDD requirements and record keeping requirements that are consistent with those laid down under the PMLFTR; and
- have their compliance with AML/CFT obligations monitored in a manner which is consistent with the 4th AML Directive.

Reliance agreement

- Written and signed formal agreement regulating the procedures and conditions concerning such requests, in order to ensure that the data is made available immediately.
- Consider carrying out occasional tests to ensure that the entity being relied upon is in a position to provide the requested information and documentation and, moreover, to ensure, from time to time, that the CDD measures undertaken by the entity are satisfactory.
- Provide for situations where the entity terminates its business relationship with the customer, or ceases to operate altogether, in order to ensure that the subject person is still in a position to fulfil its obligations at law, even where the reliance agreement ceases to be in force.
- Must be retained by the subject person as part of its record keeping obligations, together with any copies of the documentation forwarded by the entity being relied upon.

Outsourcing

Extent of outsourcing

- The obligations which may be outsourced, whether in whole or in part, relate to:
 - the implementation of risk assessments procedures;
 - the implementation of CDD procedures; and
 - the implementation of record keeping obligations
- The MLRO and monitoring functions cannot be outsourced – therefore, the determination as to whether a STR is to be filed with the FIAU or otherwise cannot be outsourced either and is to remain within the discretion of the MLRO.
 - Still, a subject person may still outsource a third party to flag unusual transactions that may become the subject of an internal report to the MLRO or engage consultants to assist in the determination of whether a STR is to be filed or otherwise.

Conditions to which outsourcing is subject

- Prior to outsourcing to a third party, the subject person should: (i) make an assessment of any potential ML/FT risk due to the proposed outsourcing, (ii) maintain a written record of the assessment, and (iii) monitor the perceived risk.
- The subject person shall also ensure that all of the following conditions are met:
 - The outsourcing does not negatively prejudice the ability of the subject person to comply with its obligations at law and the effectiveness of its compliance and audit functions, nor will the outsourcing impede the effective supervision of the subject person by the FIAU or the compliance by the subject person with any obligation related to the analytical function of the FIAU;
 - The third party has the necessary resources, qualifications, skills and authorisations (if required) at its disposal to effectively carry out the measures and procedures it is to perform on behalf of the subject person;
 - The manner in which the third party proposes to implement the outsourced activities is in line with all applicable legal requirements and the subject person's own policies and procedures;
 - The third party is in good standing, there being no adverse information in its regard, and it is located and operating from Malta, an EU Member State or another reputable jurisdiction; and
 - The third party is not subject to any obligation which would lead to a breach of any data protection, professional secrecy, confidentiality or non-disclosure obligation to which the subject person has to adhere.
- The subject person shall maintain a copy of the assessment undertaken prior to entering into an outsourcing arrangement and shall make it available to the FIAU upon request.

Outsourcing agreement

- the exact parameters of the measure or procedure being outsourced to the third party;
- the precise requirements concerning the performance of the measure or procedure, taking account of the intended objective of the measure or procedure to be outsourced;
- the respective rights and obligations of the parties to the agreement;
- the circumstances under which the agreement can be terminated and the terms that would become applicable;
- the ownership of any data, information, reports or other documentation that may be produced, collated or collected in the course of carrying out the measure or procedure being outsourced, taking into consideration the record-keeping obligations of the subject person;
- that any processing of personal data has to take place in accordance with applicable data protection laws and any data, information, reports or other documentation are kept confidential and will not be disclosed to anyone other than in those circumstances where the law permits such disclosure;
- the communication lines to be followed, especially with regard to the transmission of data, information, documentation, reports or findings to the subject person by the third party related to the measures or procedures outsourced;

Outsourcing agreement (cont.)

- that the third party is to allow the FIAU, including anyone duly authorised to act on its behalf, direct access to its premises and to any data, information, documentation reports or finding relative to the outsourced measures or procedures as may be required by the FIAU;
- the fact that sub-contracting by the third party is not to be allowed without the prior agreement of the subject person, which consent can only be granted once the subject person has ascertained that the sub-contractor meets the conditions for outsourcing and that the sub-contracting will not impact negatively the arrangement entered into between the subject person and the third party;
- the subject person must regularly evaluate the performance of the third party using mechanisms such as service delivery reports, self-certification, independent reviews or the subject person's own audit function.

Responsibilities

- The subject person must effectively monitor how the service provider is carrying out the outsourced AML/CFT measures and procedures to ensure that these are being carried out as required by law and in accordance with the subject person's own policies and procedures.
 - This can be done through periodical reports provided by the person to whom a function has been outsourced to the subject person, spot checks, and requests for CDD information on particular clients.
- The subject person must ensure that it has a contingency plan in the eventuality of a sudden termination of the outsourcing arrangement which would ensure that it can resume without undue delay the implementation of the outsourced AML/CFT obligations.
- The FIAU will at all times consider the subject person as responsible for compliance with its AML/CFT obligation

Training and Awareness

Training and employee screening

- 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 data protection requirements, as well as of the subject person's AML/CFT measures, policies, controls and procedures; 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.
- Broadly speaking, training should cover: (1) a refresher of AML/CFT laws; (2) any new developments in the AML/CFT framework; and (3) the ML/FT risks which the particular subject person is exposed to.
- Subject person 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, with this documentation being refreshed on an ongoing basis.

Screening for financial sanctions

Purpose

Subject persons are required to know who their customers are in order to comply with sanctions obligations. Various UN Security Council Resolutions and EU Regulations impose financial sanctions upon individuals or entities known to be involved or linked to terrorism or the financing of proliferation of weapons of mass destruction (“designated persons or entities”).

Financial sanctions typically impose a requirement on any person and entity to:

- _ Freeze the funds, financial assets or economic resources owned or controlled, directly or indirectly by designated persons or entities; and
- _ Ensure that any funds, financial assets or economic resources are not made available to or for the benefit of designated persons or entities.

Controls

```
graph LR; A[Establish a system to detect whether clients & UBOs are subject to any financial sanctions] --> B[Such system should be sufficiently adequate to consider all financial sanctions issued and updated from time to time]; B --> C[Screen clients & UBOs to determine whether they are designated persons or entities at the inception of the relationship and whenever there are changes in UBOs or new / updated sanctions];
```

Establish a system to detect whether clients & UBOs are subject to any financial sanctions

Such system should be sufficiently adequate to consider all financial sanctions issued and updated from time to time

Screen clients & UBOs to determine whether they are designated persons or entities at the inception of the relationship and whenever there are changes in UBOs or new / updated sanctions

Concluding remarks...

Be prepared...



Train staff



Think about updating
policies & procedures

Plan any
remediation
work



Any questions?



Thank you



Diane Bugeja

Senior Associate, Corporate & Finance

D (+356) 25678132

E diane.bugeja@camilleripreziosi.com

Technical Excellence, Practical Solutions



www.21Academy.education