Conducting Customer Due Diligence - Part II

3rd December 2025

Valeria Catalano

Agenda

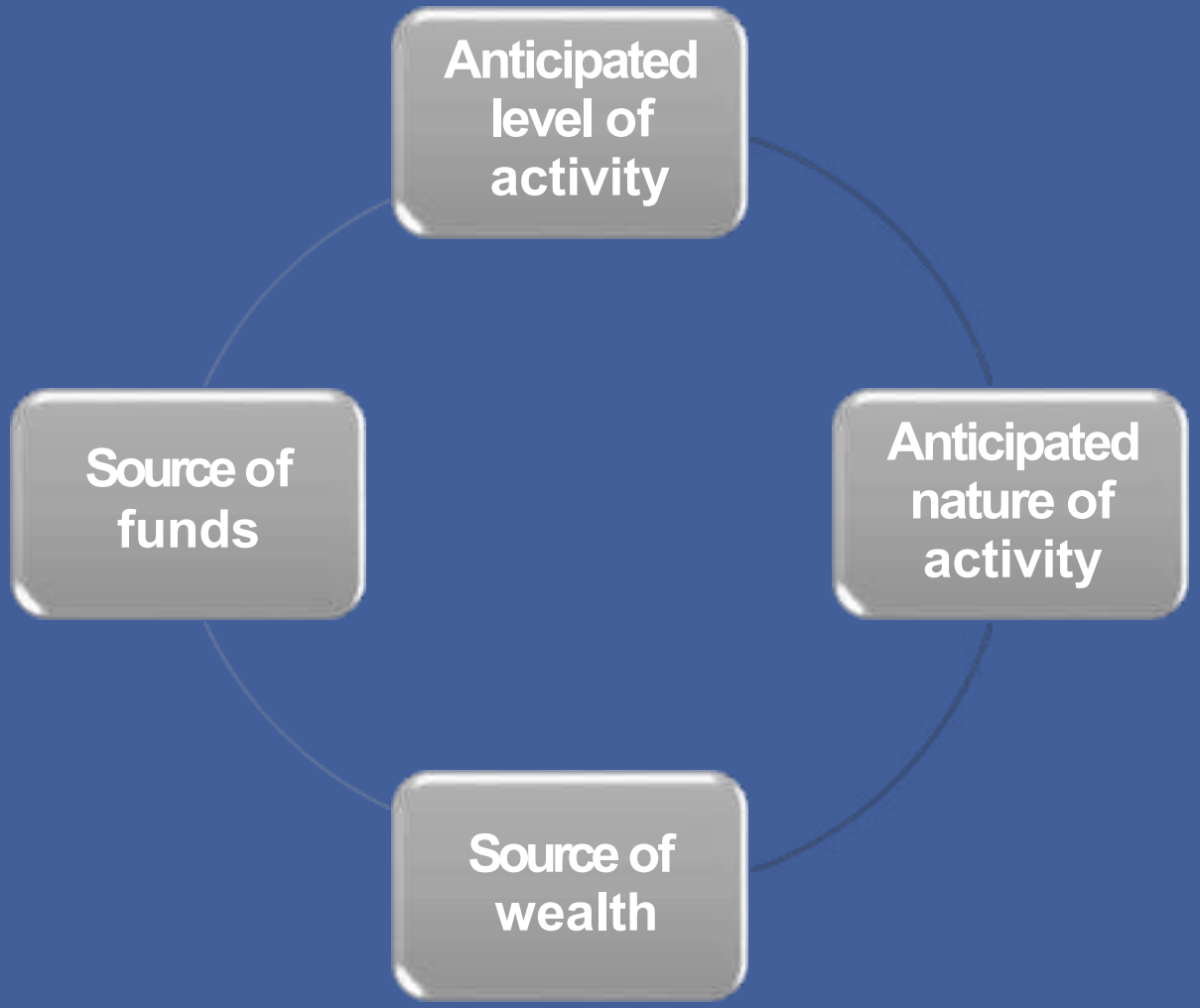
- Purpose and intended nature of business relationship & risk profile;
- Source of Wealth & Source of Funds;
- Customer business & risk profile;
- Ongoing monitoring;
- Sanctions
- Simplified Due Diligence;
- Enhanced Due Diligence;

Purpose & Intended Nature

One of the main CDD obligations is that of assessing and obtaining information on the purpose and intended nature of the business relationship

Subject Person must understand why the customer is requesting their services/products and how these services/products are expected to be used in the course of a business relationship

Purpose & Intended Nature



Purpose & Intended Nature

Subject persons are required to obtain information and/or documentation on the customer in order to:

- Determine the business rationale behind the service or product being requested vis-à-vis the customer's profile and how the service/product is going to be used.
- Use the acquired information to build the CRA
- Ensure that the customer falls within the subject person's risk appetite
- Determine the appropriate risk mitigating measures
- Undertake ongoing monitoring where applicable to ensure that the actual activity remains in line with the expected activity

Purpose & Intended Nature

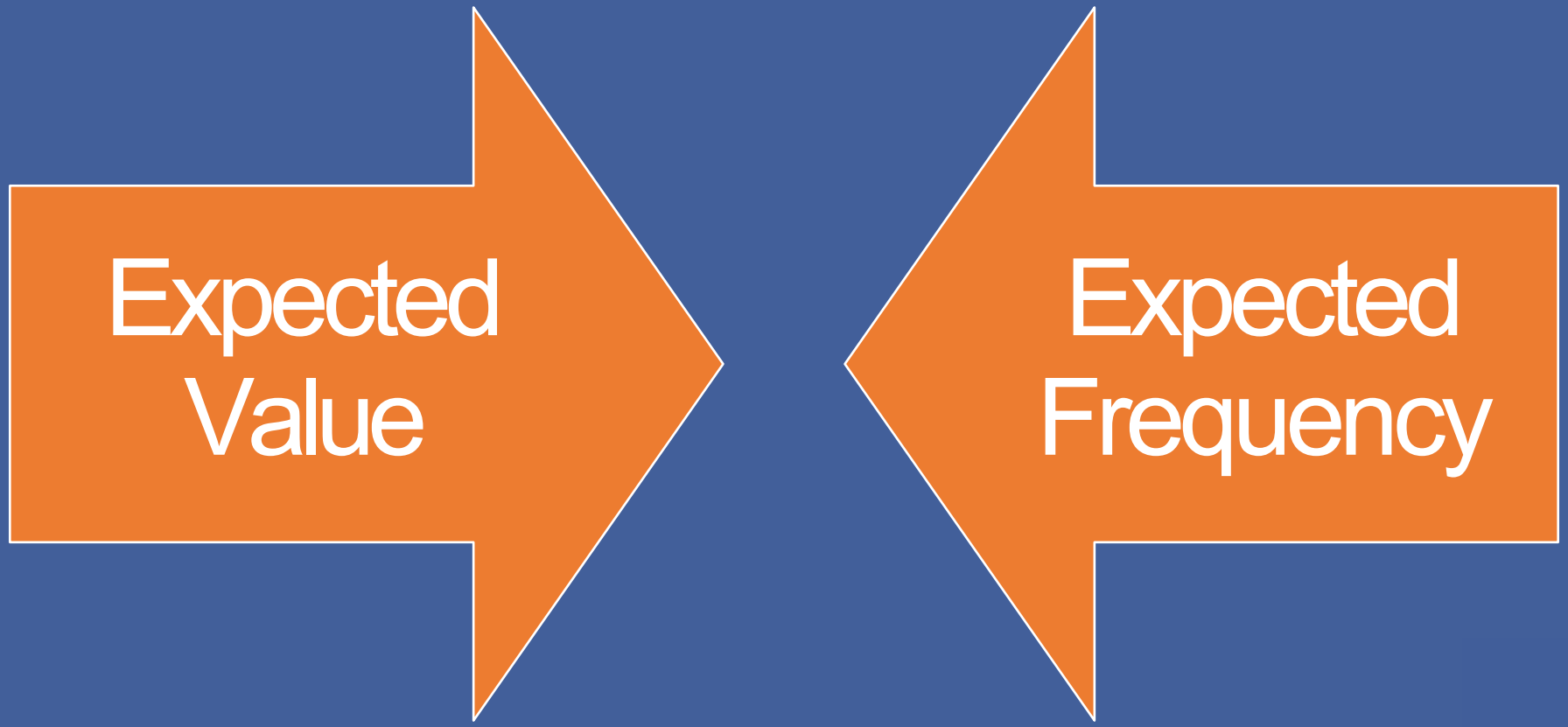
What to look out for when assessing purpose & intended nature?

Purpose and Intended Nature

Sufficient information obtained during the commencement of the business relationship also serves as a good basis to carry out appropriate monitoring, as well as to determine that the product or service requested makes sense when compared to the customer's profile.

Establishing the purpose and intended nature of the business relationship permits subject persons to adequately monitor transactions conducted during the business relationship and to assess how these correspond to transactions intended to be conducted during the relationship. In the assessment of where these differ, subject persons can better understand whether any further documentation needs to be requested or any further action taken.

Anticipated Nature & Level of Activity



Anticipated Nature & Level of Activity

An SP must obtain a clear indication of both the nature and level of activity at the start of the business relationship

This information will form the set of parameter of activity and transaction that are to be considered as 'normal' for a client

Activity falling out of the '**normal**' parameters should trigger a review by the Subject Person

Bad Practice identified by the FIAU

- Simply obtaining the Memorandum & Articles of Association is considered insufficient toward understanding the intended nature of the business relationship

- Not obtaining information on the anticipated level and nature of activity and thus not being able to build a risk profile for the customer leading to a lack of fully understanding the business relationship.

Source of Wealth (SoW)

- The economic activity generating the total net worth of the customer.
- Usually identified at the beginning of the business relationship and updated on a need-to-basis.
- Generic SOW descriptions are not enough.
- SOW may in itself be a high-risk indicator e.g. SOW derived from a high-risk industry.
- Verification and corroboration required in higher risk scenarios.
- Verification and extent of corroboration to be determined on a risk-based approach.

Source of Funds (SoF)

- The source of the particular funds which are the subject of, or which will be utilized in a transaction.
- Identification and (at times) corroboration of SOF throughout the relationship
- Needed to preserve that audit trail and make sure that the BO of the funds is always identified.
- Goes beyond the identification of the source of transfer
- Different SOF present different risks.
- Verification and corroboration on a risk-based approach.

SoW and SoF

SOW / SOF vis-à-vis Business Relationships & Occasional Transactions

- Establishing the SoW is a requirement in the case of a business relationship
- Establishing the SoF is a requirement in the case of a business relationship, when and where this is necessary
- Establishing the SoW & SoF may also be required in the context of an occasional transaction

The most effective mitigating measures is likely to be that of querying on the SOW / SOF – obtaining information on how the funds have been acquired + concluding whether this makes sense considering the customer's SOW.

What sources of information can corroborate SOW/SOF?

Customer Sourced Information

- Tax declarations
- Bank Statements
- Payslips
- Dividend warrants
- Declaration causa mortis
- Audited Financial Statements

Third-party sourced information

- Information obtained from professionals such as legal or accountancy professionals or entities/persons undertaking relevant financial business or equivalent activities in reputable jurisdictions

Open-source information

- Open-source internet searches and access to constitutive documents from companies' registries such as the MBR

SOW for Body Corporates

- Where the customer is a body corporate, subject persons must establish the source of wealth of the customer. In situations where the customer is a trading company and has developed its commercial activities, the source of wealth needs to be determined through obtaining information on the nature and extent of these commercial activities, supported by audited financial statements.

- This would be sufficient to satisfy the obligation to establish a customer's source of wealth, so long as the financial statements attest to a sound financial situation resulting from the company's turnover generated from the carrying out of its own activities.

Best Practice identified by the FIAU on SOW/SOF supporting documentation

1. The beneficial owner of the customer company indicated that the source of wealth is derived from employment and dividends received from a 50% shareholding stake in a company. The subject person requested official tax statements for consecutive years and matched this data with the information provided by the customer.

2. The beneficial owner of the customer company indicated, amongst other factors, that he is the beneficial owner of a number of entities, holds investments in several entities and was a director of numerous listed entities. To corroborate this information, the subject person collected various documents such as an overview of the customer company, financial statements and annual returns for a number of entities where the beneficial owner acts as a director.

A letter from the beneficial owner's warranted accountant from a reputable jurisdiction was also obtained and was substantiated with supporting documentation. This letter confirmed that the beneficial owner had net assets in his personal name, that he was a member of a company whereby he received a fixed priority profit share, was paid additional/bonus profit share and that he received significant carried interest and co-investment distributions. The subject person also collected additional information of investment portfolios which accounted for proceeds generated from monetary donations given by a family member of the beneficial owner.

Bad Practice identified by the FIAU relating to SOW/SOF supporting documentation

- In some instances, the information and/or documentation collected on the purpose and intended nature of the business relationships (including the source of wealth and source of funds) was considered to be too vague and generic, since the subject person only opted to obtain memoranda and articles of association, which did not delve into the level of detail expected in the IPs. There were also instances where the subject person obtained a brief description of the customer company in the early stages of the business relationship and did not update the information when the business relationship matured, leading to insufficient details which hindered the correctness of the customer's risk profile.

- In some cases, information on the source of wealth and source of funds was generic and not supported with documentation. For example, in certain instances, subject persons only had information that the funds were obtained through inheritance but did not have evidence to corroborate this further.

Customer's business & risk profile

- The kind of information/documentation gathered will **vary** depending on the risk profile of the customer and the service identified through the customer risk assessment.

- Low/medium risk – declaration (e.g. nature of employment, salary etc) from customer can suffice

- High risk – additional documentation that originates from independent and reliable source

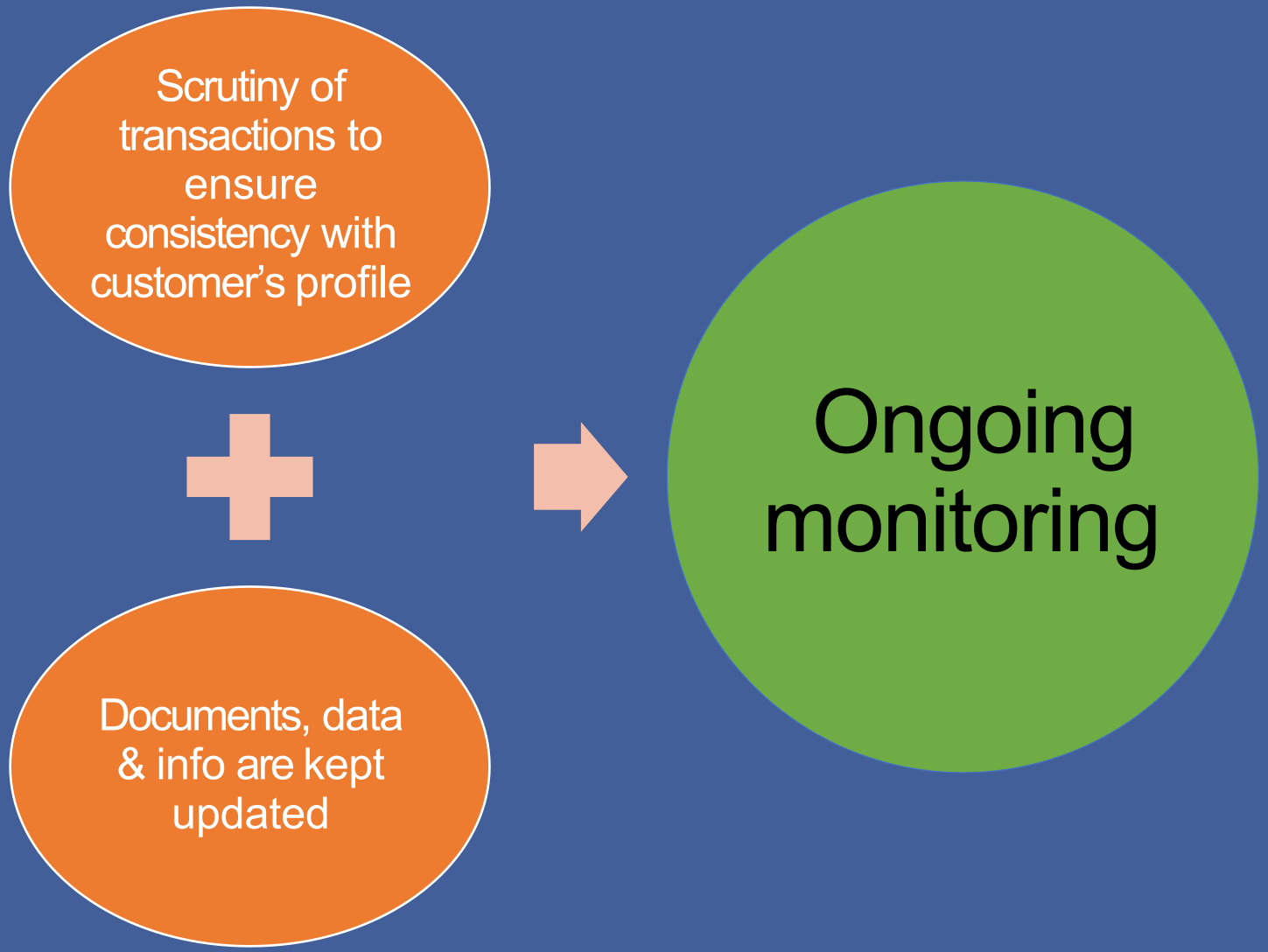
Lessons learnt from FIAU enforcement measures on purpose & intended nature

Detail to establish overall accumulation of wealth

Information on the anticipated level and nature of the activity to be undertaken

Formal documentation where necessary

Ongoing monitoring



Purpose of Ongoing Monitoring

- Business relationships are **not static**, and the circumstances surrounding them and the customers themselves are very likely to change over time. The CRA, as well as the initial CDD measures and any other mitigating measures carried out, would have all been based on the information obtained on the customer prior to the establishment of the business relationship.

- The requirement for monitoring relationships means that where the basis of a relationship **changes significantly**, firms should carry out further CDD procedures to ensure that the revised risk and basis of the relationship are fully understood

- For example, changes that **affect the risk profile** and, possibly, the CRA should lead the subject person to update its CRA accordingly.

How to keep CDD up-to-date?

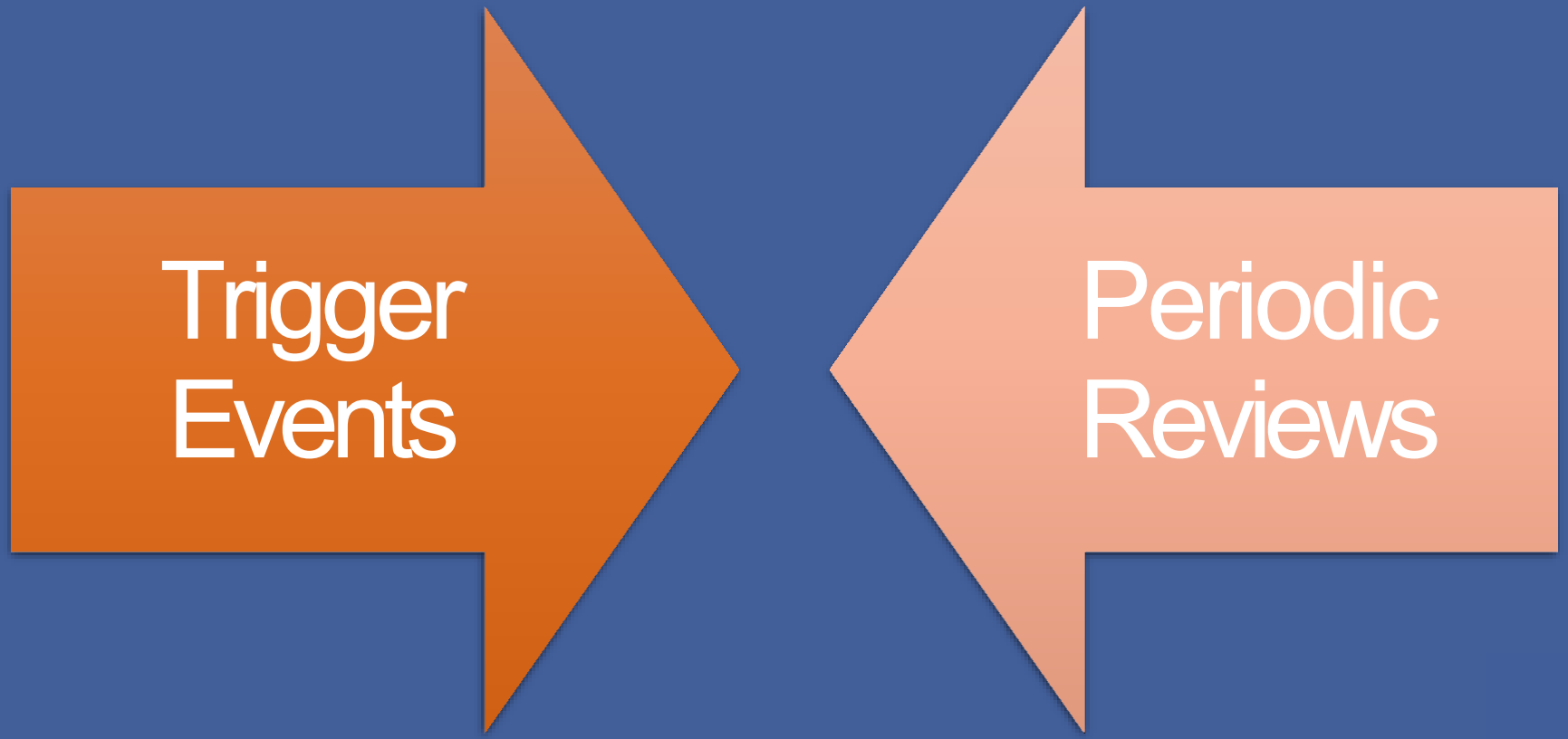
- The easiest way of keeping the CDD information up to date is through contact with the customer. Information gained through **meetings, correspondence, electronic mail or telephone conversations should be documented** with the customer's records to ensure that emerging patterns of activity and any changes in circumstances are recorded.

- Wherever possible, for ease of reference, a **summary file** of relevant information on each customer should be maintained and cross-referenced to the files containing the more detailed information.

OM – Keeping documents, information and data up-to-date

a) ID&V of Customer → b) ID&V of BO → c) Purpose and Intended Nature of Business Relationship & Risk Profile

Information Monitoring Methods



Triggers Events

- At times, updating may be prompted by certain trigger events. For instance, an assessment of an unusual transaction or pattern of transactions carried out, referred to in the previous section, may indicate that there has been a (legitimate) change in the business relationship or in the customer's relevant circumstances, and the business and risk profile may need to be adjusted to ensure that all relevant factors are being taken into account. This may entail obtaining new information or documentation to substantiate the new circumstances.

- By way of example, updating would be necessary in the light of a request for a new product or service that presents different ML/FT risks. In these cases, Subject Persons would need to consider whether the information held is sufficient or whether it would be best to request more detailed information on, for instance, the anticipated source of funds.

- A request for information received from the FIAU or the Police on a particular customer may also be a trigger for the subject person to take a closer look at how it had risk assessed and rated that customer and what it knows about him/her.

Trigger Events (cont.)

- Trigger events can also be applied in relation to the updating of documentation that has a set expiry date, such as identification documents. A customer who has been inactive for a considerable period of time is unlikely to pose any ML/FT risk and therefore even if the documentation used to verify his/her identity may have expired, requesting fresh copies would not be addressing any particular risk.
- However, if the customer attempts to make use of the subject person's services or products once more, any activity should be made subject to the customer providing copies of fresh identification documents prior to any such activity taking place.
- Trigger events can also assist the subject person in questioning whether any changes to the beneficial ownership of the customer are taking place or have already taken place. Examples would include situations where the subject person is acting as director or company secretary for a corporate customer and is requested to sign and submit to the Malta Business Registry a copy of the relative form notifying a change in shareholding. The same can be said with respect to fiduciaries holding shares in a corporate customer who are requested to transfer part of the shares to existing or new shareholders.

What Constitute a Trigger Event

- Changes in involved parties of a particular corporate customer (change in shareholders or BOs);
- Changes in business operations/activities identified through transaction monitoring;
- Customer requests the setting up of new corporate structures;
- Customer requests services that pose a higher risk;
- Unexplainable frequent changes in the name of the company;
- The filing of an STR to the FIAU, which should lead the CSP to assess whether CDD information is to be updated.
- A change in the country risk assessment of a jurisdiction to which the client is linked;
- A change in the client's ownership structure or business model (including an expansion of business particularly to new sectors or jurisdictions);
- One or more beneficial owner(s) of the client acquires PEP status;
- Client or one or more of its beneficial owners are listed on UN/EU sanctions lists

Periodic reviews

- Another method that may be applied to ensure that information is up to date is that of periodic reviews. Depending on the level of risk, subject persons may set up a schedule to review the information they hold on file at regular intervals, even in the absence of an event that may point to a change in the given business relationship.

- Periodic reviews may be particularly useful when it comes to the documentation collected for verification of identity purposes, where the subject person sets out a schedule for their review and requests updated copies when it emerges that this has expired. Periodical reviews would be equally relevant in the context of ensuring that beneficial ownership information and documentation is kept updated.

- Since this process necessarily needs to be risk based, the timeframe for the review of business relationships considered to present a high risk of ML/FT should be more frequent than those deemed to be low risk.

Periodic reviews – Frequency & Extent

Frequency

- High – every 12 months
- Medium – every 24 months
- Low – every 36 months

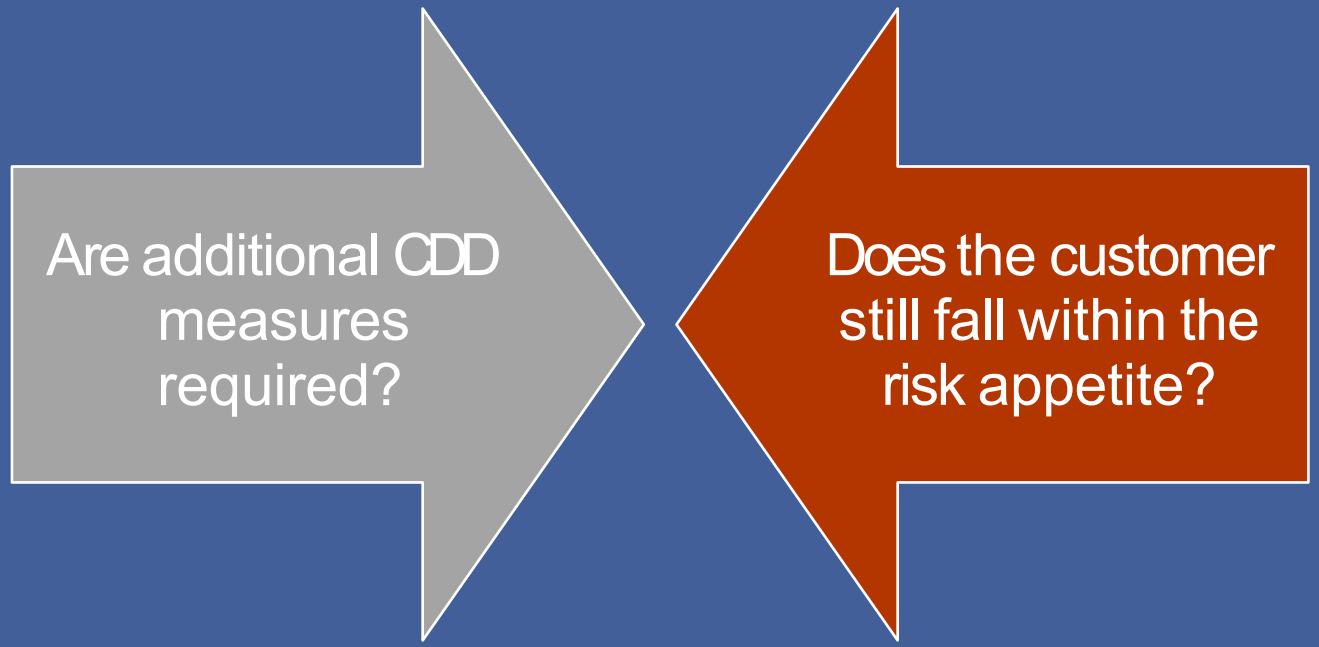
Extent

- Is dependent 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.

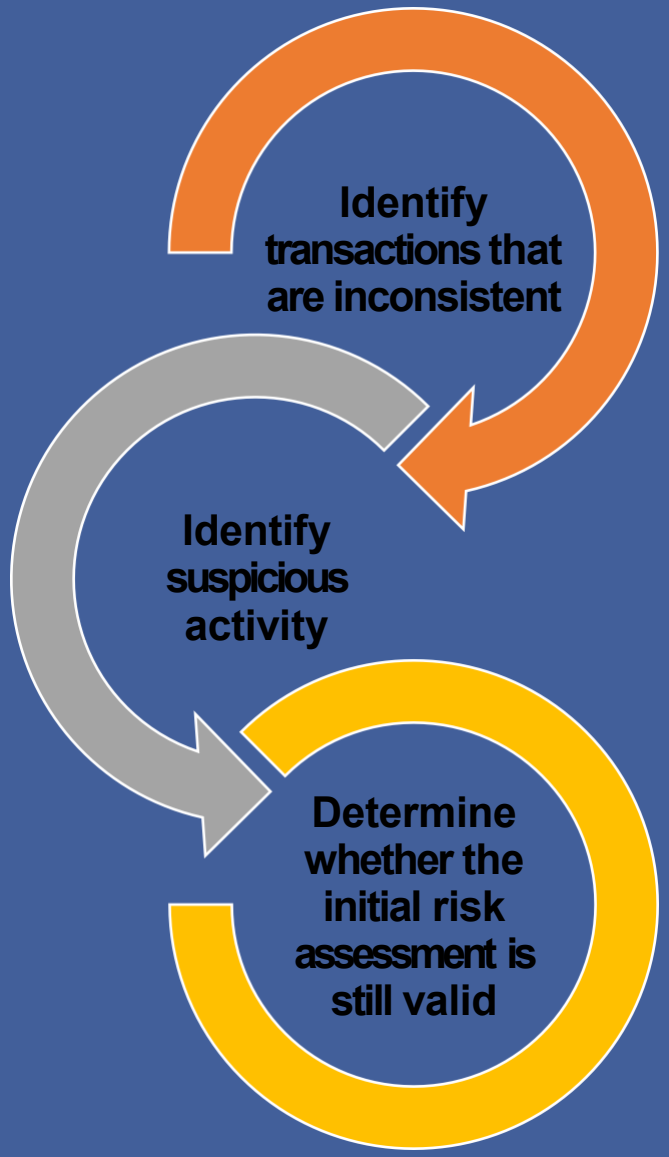
It should be noted that not all information adds value to the business and risk profile or serves to mitigate any ML/FT risks, in which case subject persons should consider whether the information is actually necessary. By way of example, requesting updated documentation evidencing the customer's change in occupation or residence may not be necessary when the customer has retained the same risk rating and transaction patterns.

Customer Risk Assessment

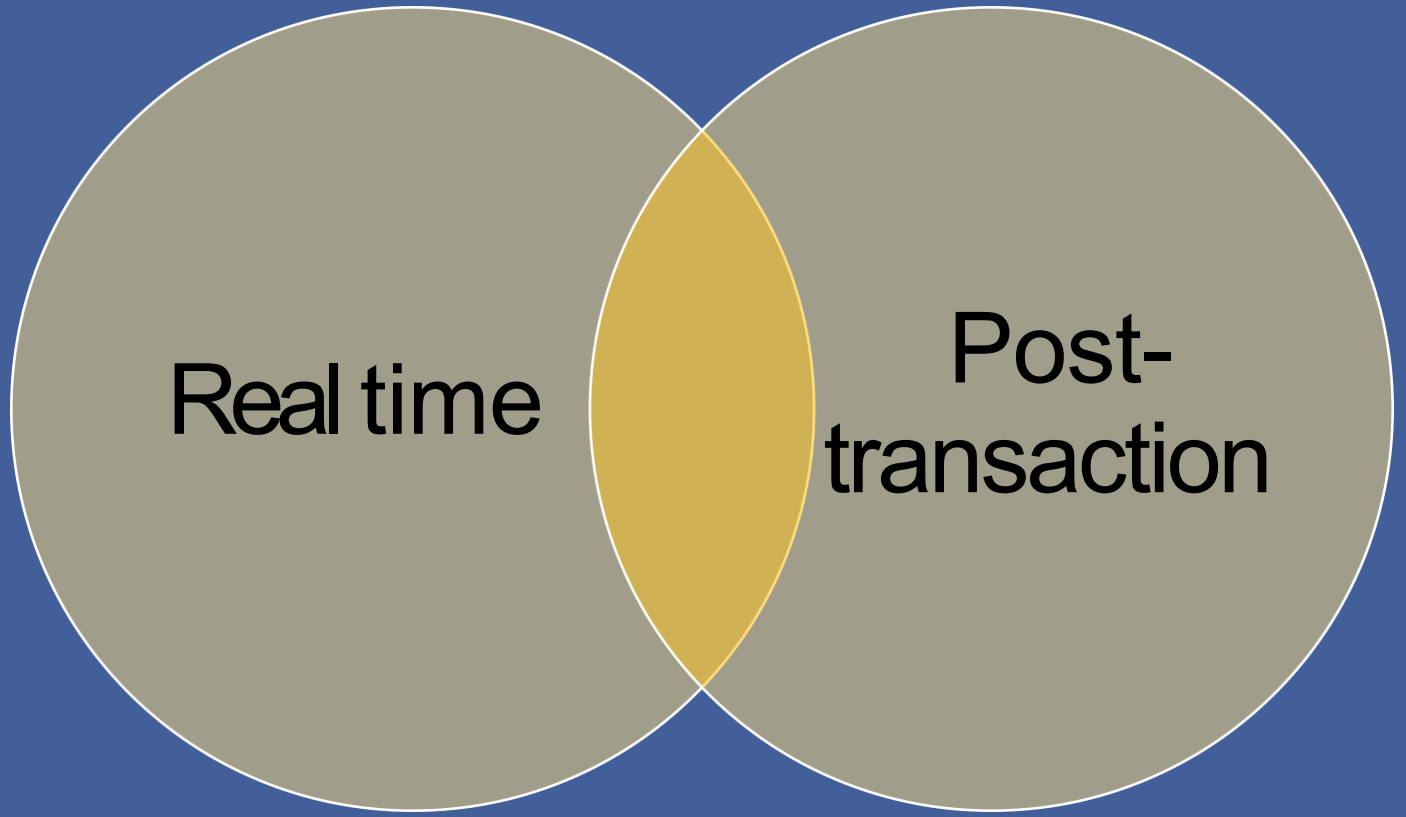
The CRA is a live document



Scrutiny of Transactions



Types of transaction monitoring

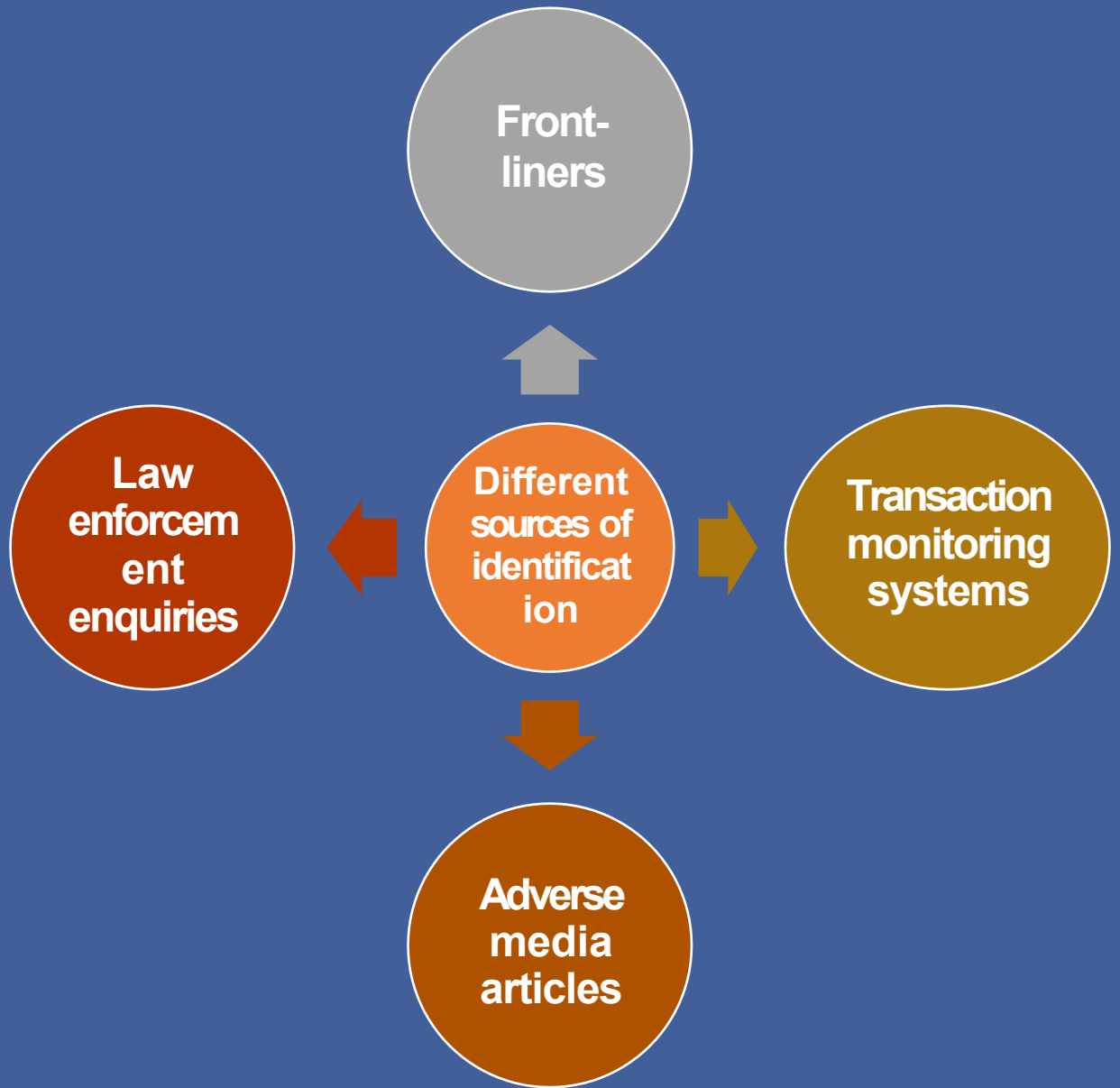


Real-Time Monitoring

- Focus on activity & transactions when information or instructions are received from customers, before or as an instruction is processed
- More effective at reducing exposure to risk
- Suitable for face-to-face scenarios
- Non-face-to-face where transactions are not executed immediately
- Requires awareness of relevant trigger events and red flags
- Requires understanding of the expected behaviour/use of the relationship
- EDD measures for high-risk customers and transactions
- Best combined with post-transaction monitoring to detect patterns

Post-Transaction Monitoring

Different Sources of Identification



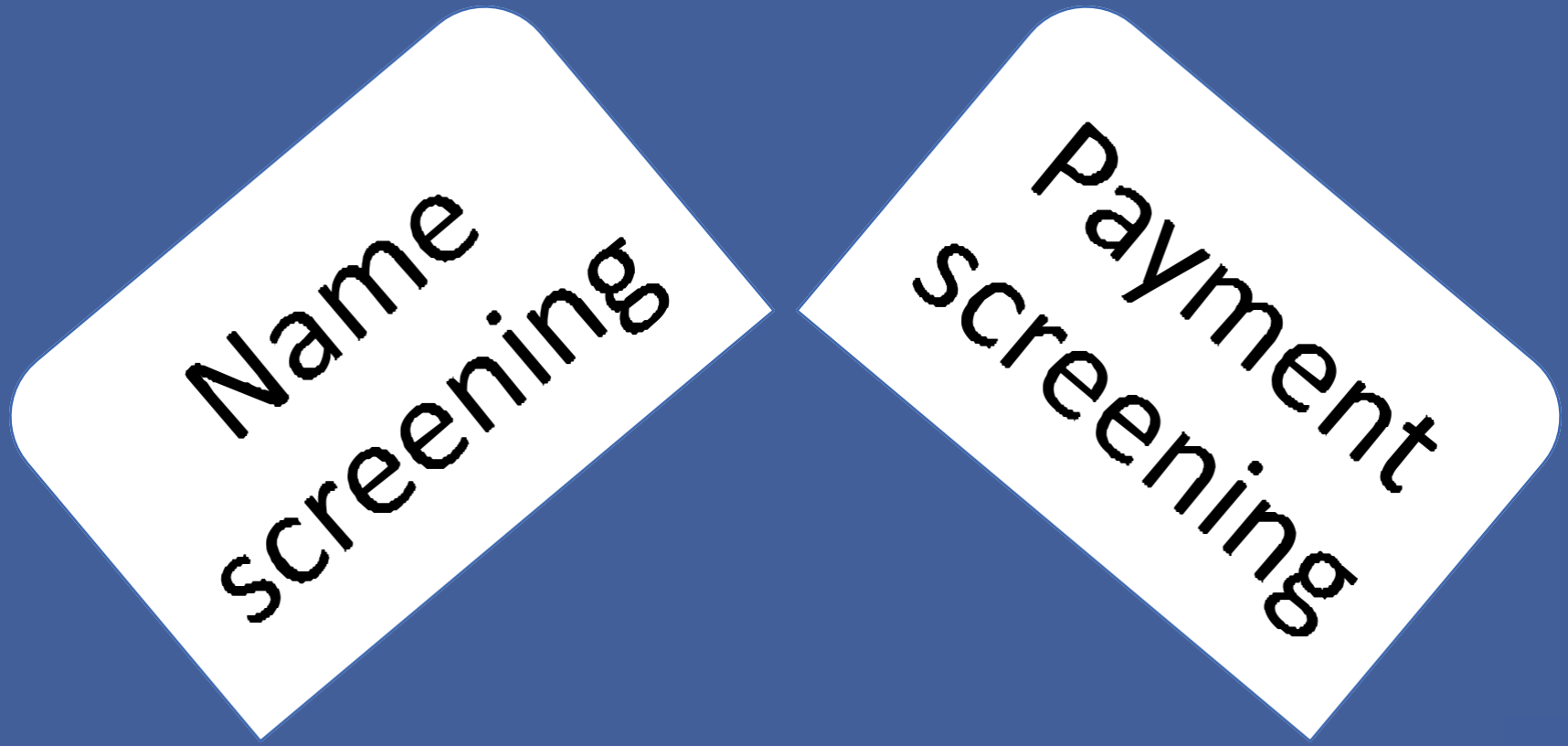
Key elements of a TM framework

Manual or Automated?

- ✓ Depends on size of SP, number of clients and transactions, level of risk
- ✓ System must yield the desired results, including relevant alerts within adequate timeframes
- ✓ Large transactions are better monitored through automated systems
- ✓ If the SP uses an automated system, does the system generate reports showing reasons, rules and parameters? Can system be easily adapted to cater for changes? Can the system learn from previous false positive? (fine-tuning)

Screening - Purpose

Types of screening



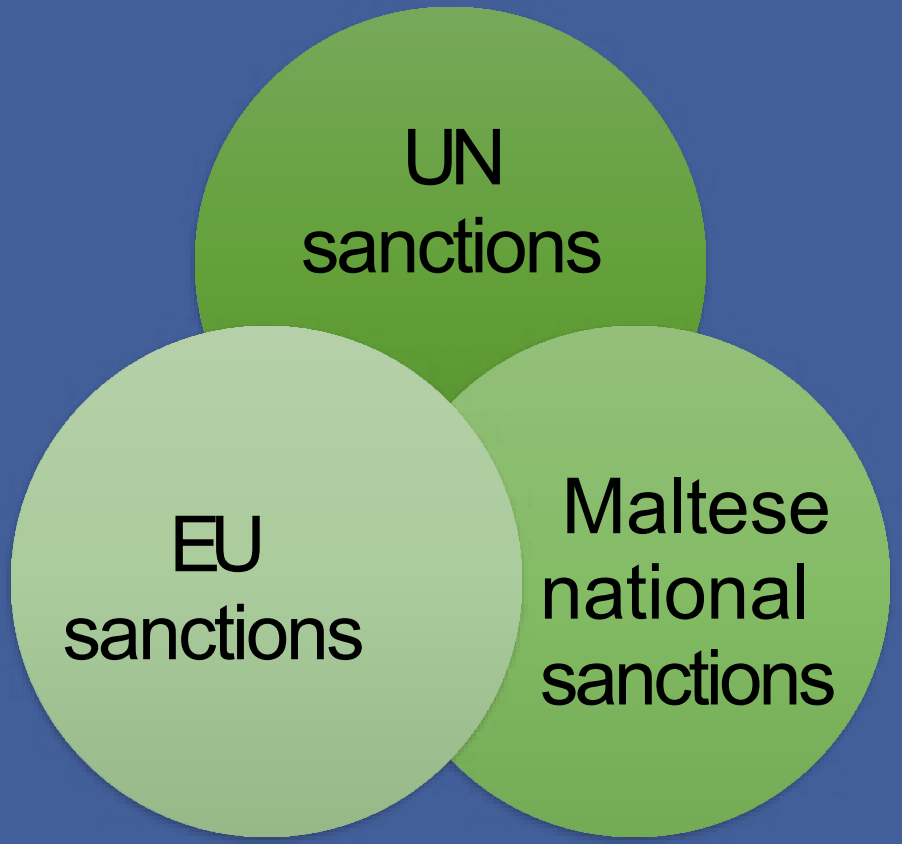
Adverse Media

- Review the article and consider if it matches your client's age, location and other circumstances
- Consider what the article is actually highlighting about your customer (e.g. investigation vs conviction)
- Consider the source and date of publication
- Looking at the customer in light of the additional information, is there anything that would now be considered suspicious?

Leave an audit trail of findings and conclusions (document searches)

Sanctions

What Sanctions are applicable to Malta?



Obligations

Subject persons are required to:

- Be able to detect whether a customer or a transaction is subject to any sanctions;
- Freeze the funds, financial assets or economic resources owned or controlled, directly or indirectly, by designated persons or entities;
- Prevent funds, financial assets or economic resources from being made available to or for the benefit of designated persons or entities;
- Report – In Malta, the competent authority for sanctions implementation is the Sanctions Monitoring Board.

Controls

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

Such system should be 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

Lessons learnt from FIAU enforcement measures on ongoing monitoring

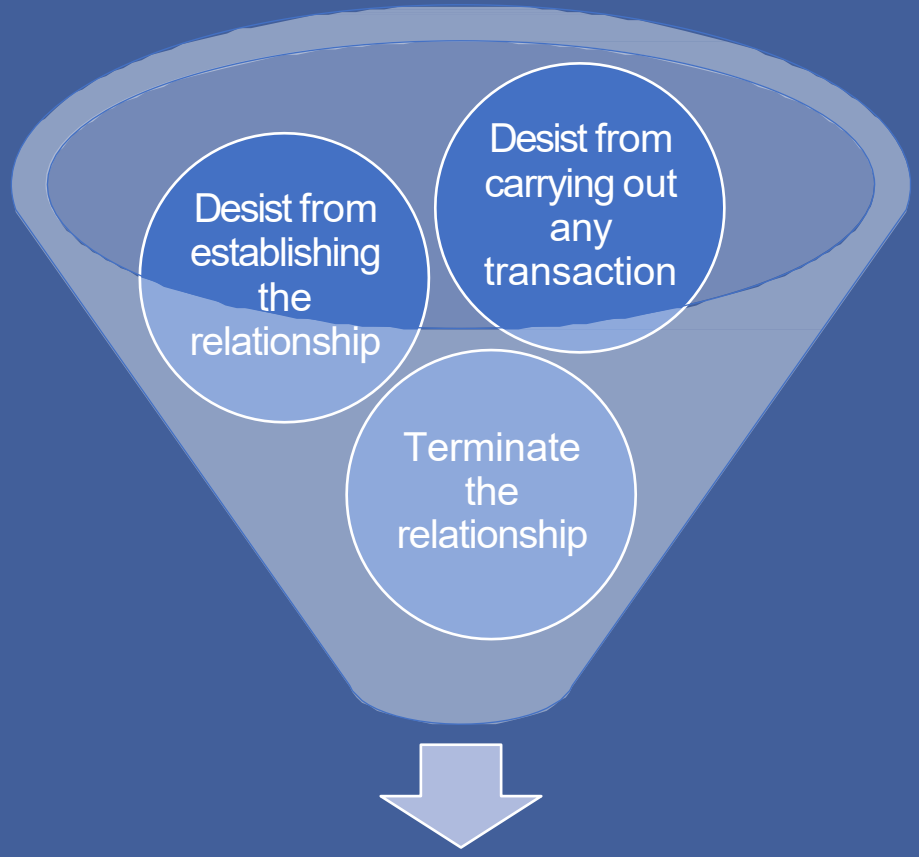
Documented procedure, including defining rules to flag suspicious activity

Documentary evidence around source of funds, especially when inconsistent with customer profile

Periodic reviews necessary & to be documented

Manual checks challenged

Failure to complete CDD



Consider filing an STR

SDD & EDD

When does SDD apply?

In relation to activities or services that are determined by the FIAU to represent a **low risk**

When, following a CRA the relationship/transaction is **low risk**

What can be adjusted for SDD?

Timing of CDD	Quantity of information	Quality of information	Frequency & intensity of ongoing monitoring
• 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	• 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	• 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	• 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

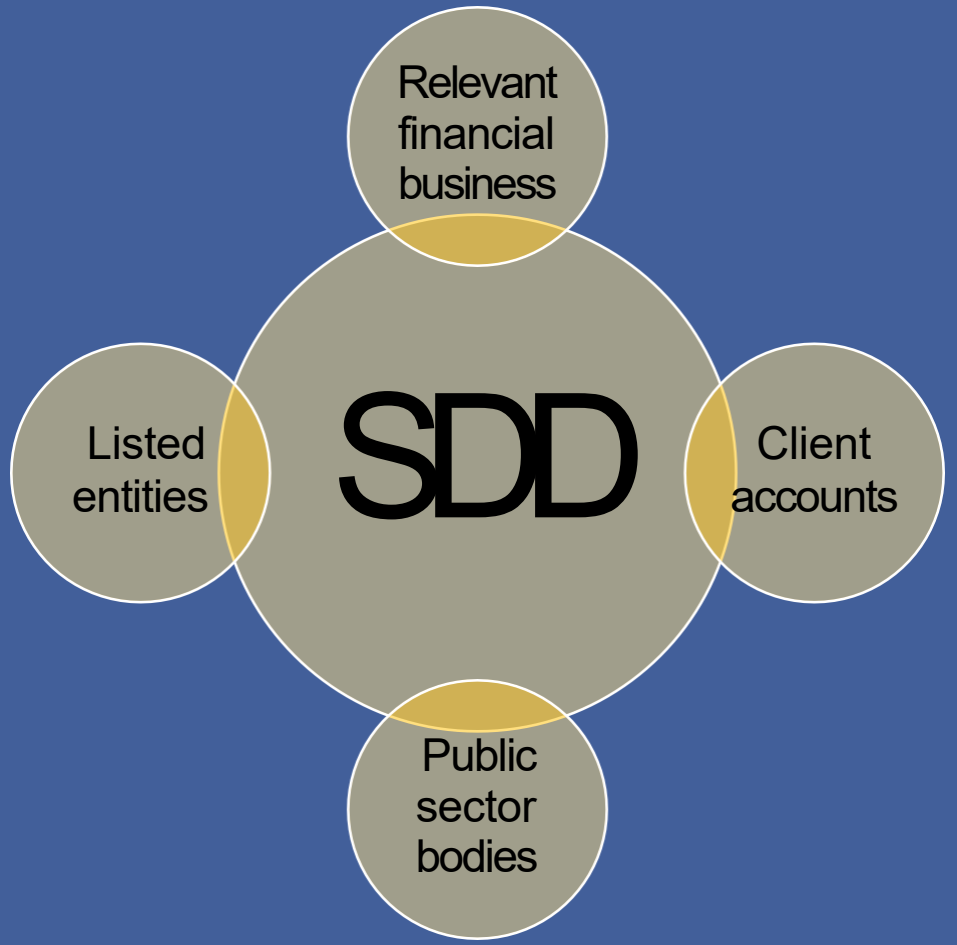
Variation in the extent and timing of CDD does not result in a de facto exemption from CDD measures

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



High-risk relationships or transactions (EDD)

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 outcome of relationship/transaction is high risk**
  - 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
- **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

Who is a PEP?

- A PEP as a natural person who is or has been entrusted with a prominent public function, other than middle ranking or more junior officials.
- Public functions which are considered as prominent public functions and would therefore render the holder thereof a PEP include:
  - Heads of State, Heads of Government, Ministers, Deputy or Assistant Ministers, and Parliamentary Secretaries;
  - Members of Parliament or similar legislative bodies;
  - Members of the governing bodies of political parties;
  - Members of the superior, supreme, and constitutional courts or of other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances;
  - Members of courts of auditors, or of the boards of central banks;
  - Ambassadors, charge d'affaires and other high ranking officers in the armed forces;
  - Members of the administrative, management or supervisory boards of state-owned enterprises;
  - Permanent secretaries within all the Government ministries;
  - Chiefs of staff within all the Government Ministries;
  - The Commissioner and Deputy Commissioners of Police;
  - Anyone exercising a function equivalent to those set out above within an institution of the European Union or any other international body.
- Both domestic and foreign PEPs are to be considered as PEPs and EDD measures on a risk sensitive basis must be applied

Who is a PEP?

- **Family members** of PEPs must also be treated as PEPs – these include:
  - the spouse, or any person considered to be equivalent to a spouse;
  - the children and their spouses, or persons considered to be equivalent to a spouse; and
  - the parents.
- Similarly, persons known to be **close associates** also classify as PEPs and include:
  - a natural person known to have: (1) joint beneficial ownership of a body corporate or any other form of legal arrangement; (2) or any other close business relations, with that PEP.; and
  - a natural person who has sole beneficial ownership of a body corporate or any other form of legal arrangement that is known to have been established for the benefit of that PEP.
- In determining whether the customer or a beneficial owner is a PEP, subject persons may:
  - rely on publicly available information; or
  - obtain such information directly from the customer or beneficial owner; or
  - use commercial databases.

Unusual transactions

- Transactions may be unusual because they are :

Any questions?

Valeria Catalano

Modern Business Solutions

valeria.catalano@modern.mt