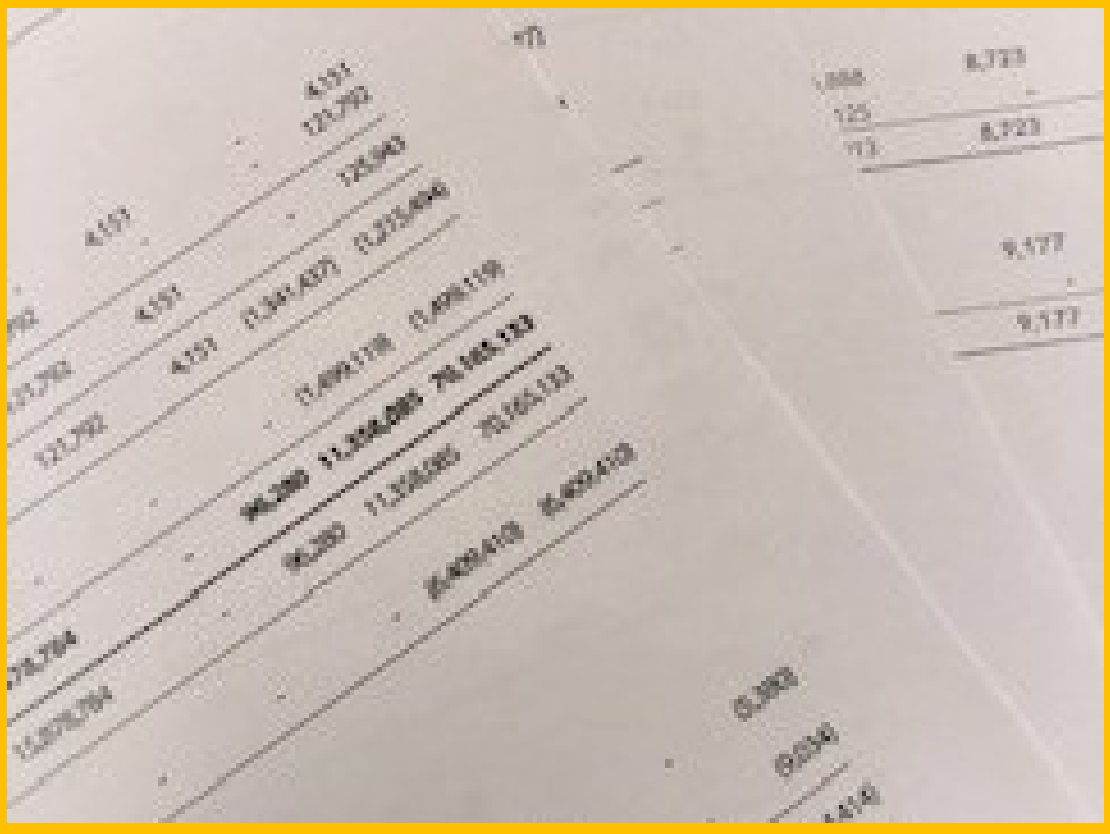
FIAU

Implementing Procedures

Issued by the Financial Intelligence Analysis Unit in terms of the provisions of the Prevention of Money Laundering and Funding of Terrorism Regulations

Part II

Accountants and Auditors



Issued: December 2022

Contents

Abbreviations

4AMLD: Directive (EU) 2015/849

AML/CFT: Anti-Money Laundering and Counter-Financing of Terrorism

BRA: Business Risk Assessment

CASPAR: Compliance and Supervision Platform for Assessing Risk

CDD: Customer Due Diligence

CRA: Customer Risk Assessment

CSP: Company Service Provider

DNFBPs: Designated Non-Financial Businesses and Professions

MIA: Malta Institute of Accountants

ML/FT: Money Laundering and Funding of Terrorism

NRA: National Risk Assessment

PEPs: Politically Exposed Persons

PMLA: Prevention of Money Laundering Act[1]

PMLFTR: Prevention of Money Laundering and Funding of Terrorism Regulations[2]

RBA: Risk-Based Approach

SNRA: Supranational Risk Assessment

STR: Suspicious Transaction Report

VFA: Virtual Financial Asset

[1] Cap. 373 of the Laws of Malta.
[2] S.L. 373.01 of the Laws of Malta.

1. Introduction

1.1 The Purpose of these Implementing Procedures

The FIAU is publishing these Implementing Procedures Part II to interpret and provide guidance on the implementation of specific AML/CFT obligations which warrant further elaboration at a sector-specific level, to ensure that they are understood, interpreted, and implemented consistently by accountants and auditors (hereinafter collectively referred to as 'practitioners').

These Implementing Procedures also provide information on the ML/FT risks faced by practitioners. This guidance will assist them in formulating a better understanding of these risks, ensure that they are better equipped to limit the possibility of abuse for ML/FT, and to detect and report suspicious activity.

These Implementing Procedures are being issued in terms of Regulation 17 of the PMLFTR. Unless otherwise stated, their provisions are applicable and legally binding with respect to all individuals or firms exercising the accountancy and/or auditing profession in terms of Maltese law, insofar as these constitute relevant activity in terms of the PMLFTR (refer to Chapter 2 below).

This document does not constitute a complete set of procedures for practitioners, and must be read in conjunction with the FIAU's Implementing Procedures Part I, which are legally binding and applicable across all sectors. Together, these documents provide a holistic understanding of the applicable AML/CFT obligations arising from the PMLA and the PMLFTR. Therefore, the absence of any reference, in this document, to other AML/CFT obligations, is not to be understood as meaning that those obligations do not apply to the practitioners.

1.2 The Provision of Company Services and/or Tax Advice

The FIAU acknowledges that the provision of company services in terms of the Company Service Providers Act[3] is central to the operations of many accountants and auditors. This document does not contain comprehensive guidance on the ML/FT risks and the application of AML/CFT laws vis-à-vis company services. Any subject person providing company services is required to comply with any applicable rules and regulations, including any sector-specific guidance and implementing procedures issued by the FIAU applicable to CSPs.

Moreover, where practitioners provide tax advice[4], reference is to be made to any specific guidance and/or interpretative notes issued by the FIAU in this regard.

[3] Cap. 529 of the Laws of Malta.
[4] This also includes *'any person that undertakes to provide, directly or through other persons to whom he is related, material aid, assistance or advice on tax matters'.*

1.3 Regulation of Designated Non-Financial Businesses and Professionals

The earliest global efforts towards preventing ML/FT were initially more focused on banks and financial services providers. These institutions were typically the first port of call for criminals and money launderers to place their illicitly obtained funds, layer them and obscure their connection with the activity that generated them in the first place. As banking systems became subject to and compliant with AML/CFT regulations, and developed systems to detect and report suspicious transactions, it became riskier for criminals and money launderers to use their services in the same way. There was therefore no longer any assurance that they could do so without attracting unwanted attention.

Criminals naturally adapted and sought lesser regulated avenues to inject illicit funds into the financial system and disguise transactions, such as through:

- the misuse of legal entities and arrangements
- the purchase of real estate
- false loan agreements
- the setting up and operating cash intensive business
- soliciting professionals to assist them with ensuring that transactions appear legitimate.

In other words, criminals and money launderers sought the services of professionals to help them launder their money, whether the professionals were aware of this or not. Over time, governments and international bodies sought to regulate these sectors and professionals that had become more vulnerable to abuse. As a result, DNFBPs are likewise required to comply with the same regulations and obligations as those imposed on credit and financial institutions. This ensures that all the sectors and services that are vulnerable to abuse by criminals, including gatekeepers to the financial system, are protected through targeted preventive measures.

1.4 The Value of the Professional to the Criminal

Why would criminals and money launderers seek the services of professionals such as accountants and auditors? This is because, whether knowingly (such as in the case of professional money launderers or even when opting to remain willfully blind to the circumstances) or unknowingly, professionals may play a role in ML/FT. Primarily, they have specialised knowledge to assist and/or advise their customers on financial matters, and/or provide assurance services. In view of the respect and trust that is associated with their profession, the services of accountants and auditors can be invoked to provide a veil of legitimacy. The following examples show how the services provided by practitioners are of value to criminals:

Incorporating Companies and Legal Arrangements

There are many legitimate uses for companies and structures such as trusts, foundations and associations. These same companies and structures are unfortunately also useful for layering and moving illicitly generated funds. Companies can be set up to carry out trading activities, with criminals creating fictitious transactions or inflating the value of specific goods or services. Illegally generated funds can then be transferred through accounts held in the name of these companies, under the guise of payments for regular activity[5]. Legal entities and arrangements are attractive vehicles because they can be used to conceal, or make it harder to identify, the identity of the individuals controlling and benefiting from them or the underlying structures. If a customer

[5] Refer to the FATF/Egmont Trade-Based Money Laundering: Trends and Developments report (December 2020) for more information on this typology:
https://www.fatf-gafi.org/publications/methodsandtrends/documents/trade-based-money-laundering-trends-and-developments.html

seeks assistance to set up or service a structure with multiple entities in different countries, all known for their confidentiality and lack of transparency, a professional has to understand the purpose and rationale behind this.

Introducing Customers to Financial Service Providers

Professionals have historically enjoyed the trust and respect of financial institutions and society at large; a recommendation from an accountant or a lawyer may provide a bridge to open a bank account in a country where the customer has no connection. This is another form of added value that can be derived when engaging practitioners.

1.5 Application of AML/CFT Obligations

The above are examples but one can consider other forms of assistance that professionals provide to their customers, even by supporting seemingly legitimate companies through the day-to-day services provided.

As gatekeepers to the Maltese financial sector and economy, practitioners, like other DNFBPs, have an important role to play in preventing and detecting ML/FT, by ensuring that their services are not misused. This takes place by conducting due diligence prior to onboarding customers when providing services which fall under the definition of 'relevant activity' in terms of Regulation 2(1) of the PMLFTR, to avoid providing services intended for ill-intentioned purposes. Practitioners are also well-placed to detect suspicious activity or transactions, be it when the transaction is being planned, or after its execution, depending on the service being provided. It is for these reasons that they are considered to be 'subject persons' and are required by law to implement controls, policies, measures and procedures compliant with the AML/CFT obligations emanating from the PMLFTR, PMLA and FIAU's Implementing Procedures.

2. Subject Persons

2.1 Practitioners as Subject Persons

The term 'subject persons' is used to refer to those persons and entities that fall within the scope of the PMLFTR, and within the FIAU's AML/CFT supervisory remit. Subject persons are categorised into two types: those conducting 'relevant financial business' (which includes credit and financial institutions, investment service providers, and insurance companies, among others) and those conducting 'relevant activity'. The latter term comprises a set of DNFBPs which includes accountants and auditors, as well as legal professionals, trust and company service providers, casinos and gaming licensees. The full definition of the terms 'relevant activity' and 'relevant financial business' may be found in Regulation 2(1) of the PMLFTR.

When it comes to **accountants and auditors**, Regulation 2(1) of the PMLFTR provides that:

> *"relevant activity" means the activity of the following legal or natural persons when acting in the exercise of their professional activities:*
>
> *(a) **auditors, external accountants** and tax advisors, including when acting as provided for in paragraph (c) and any other person that undertakes to provide, directly, or through other persons to whom he is related, material aid, assistance or advice on tax matters;*
> *[…]*

As stated above, this also includes the activities captured below, when conducted by accountants and auditors:

> *(c) notaries and other independent legal professionals when they participate, whether by acting on behalf of and for their client in any financial or real estate transaction or by assisting in the planning or carrying out of transactions for their clients concerning the –*
>
> *(i) buying and selling of real property or business entities;*
> *(ii) managing of client money, securities or other assets, unless the activity is undertaken under a licence issued under the provisions of the Investment Services Act;*
> *(iii) opening or management of bank, savings or securities accounts;*
> *(iv) organisation of contributions necessary for the creation, operation or management of companies;*
> *(v) creation, operation or management of companies, trusts, foundations or similar structures, or when acting as a trust or company service provider;*

2.1.1 The Accountant

The reference to accountants, under paragraph (a) of the definition of 'relevant activity' in Regulation 2(1) of the PMLFTR, is understood to capture those professionals who are:

(a) warranted to practice the accountancy profession in terms of the Accountancy Profession Act[6]; and
(b) who perform the work or render the services referred to in Regulation 3(2) of the Accountancy Profession Regulations[7].

However, the PMLFTR further qualifies the term, as it refers to '**external** accountants'. Thus, accountants would only be considered as subject persons when they provide services to their customers that require a warrant to do so, on their own behalf and in their own name. Any accountant who is in employment and is therefore providing accountancy services either in-house or is otherwise servicing customers on behalf and in the name of an employer, would not be considered as an external accountants.

With respect to accountancy firms, it is to be noted that any firm so registered with the Accountancy Board is equally considered to be a subject person as its registration is intended to allow it to provide accountancy services in terms of the law. However, the individuals who are part of the said firm would not be deemed to be subject persons in their own name. In this regard, reference should be made to the Interpretative Note issued by the FIAU on the AML/CFT Obligations of Professionals and Professional Firms[8].

Accountants are to note that, apart from the provision of services under paragraph (c) of the definition of 'relevant activity', it is only those activities and services that require a warrant in terms of the rules and regulations applicable to the accountancy profession that are considered as 'relevant activity' for the purposes of the PMLFTR. Also included is acting as a liquidator in terms of the Companies Act[9] (this document provides further guidance on this service).

[6] Cap. 281 of the Laws of Malta.
[7] S.L. 281.01 of the Laws of Malta.
[8] https://fiaumalta.org/wp-content/uploads/2020/05/Guidance-Interpretative_Note.pdf.
[9] Cap. 386 of the Laws of Malta.

3. Risk and the Risk Based Approach

To be read in conjunction with Chapter 3 of the Implementing Procedures Part I, which explains the RBA and the assessment of risks in more detail. Accountants may also refer to the Financial Action Task Force's Guidance for a Risk-Based Approach for Accountants, for more guidance[10].

3.1 The Risk-based Approach

The AML/CFT framework applicable to subject persons adopts a RBA. This means that practitioners are required to adopt measures, policies, controls, and procedures that are commensurate to the specific ML/FT risks which they are exposed to, so as to prevent or mitigate the effect of these risks.

The RBA acknowledges that the ML/FT risks that subject persons face vary according to the sector and according to the individual subject person, and in turn allows for resources to be invested and applied where they are needed the most. The opposite of the RBA is a prescriptive, tick-box method, which does not allow subject persons sufficient discretion in the application of AML/CFT measures.

A RBA envisages and permits the application of checks and controls that are proportionate to the risks identified by practitioners. As a fundamental principle, high-risk areas should be subjected to enhanced procedures, such as enhanced due diligence measures, while lower areas of risk can be addressed through simplified or reduced controls.

An effective RBA relies on two essential elements:

1. an understanding of the risks that a subject person is exposed to; and
2. based on this understanding, the variation of one's controls, policies, measures, and procedures to achieve the strongest mitigating effect possible, and in a way that prioritizes resources.

The successful application of the RBA requires an assessment of the risks that a practitioner's business is exposed to, through a **business risk assessment**, as well as a specific assessment of the risk that practitioners will be exposing themselves to when establishing a specific business relationship or carrying out a given occasional transaction, through **customer risk assessments**.

[10] https://www.fatf-gafi.org/media/fatf/documents/reports/RBA-Accounting-Profession.pdf.

3.2 Risk Assessments

3.2.1 The Business Risk Assessment

Regulation 5(1) of the PMLFTR requires subject persons to take steps to "*…identify and assess the risks of money laundering and funding of terrorism that arise out of its activities or business…*"

Section 3.3 of the Implementing Procedures Part I sets out in detail how a business risk assessment is to be conducted, with guidance on the various steps of the process, including the methodologies that can be applied, the risk factors to consider, and when and how often it is to be reviewed. This section is to be considered and applied in full, with the below being some of the key principles in relation to the BRA:

- The BRA is a critical tool for subject persons to identify the risks that they are exposed to, and to ensure that the measures, policies, controls and procedures adopted are sufficiently robust to prevent and mitigate such risks.

- Conducting a BRA is a legal obligation and a copy of the BRA is to be submitted to the FIAU whenever requested to do so (including as part of the information that must be kept up to date on the CASPAR Subject Person module[11]).

- As a minimum, the BRA must assess the risks arising from the four main risk factor categories, namely the customer, geographical, product/service/transaction, and delivery channel risk factors. Section 3.3 of this document provides additional risk factors that are of specific relevance to practitioners.

- The BRA must be documented in writing. The BRA and any updates thereto must be approved by the Board of Directors or equivalent management body. In the context of a partnership this would usually be done by the partners entrusted with its management. Naturally this does not apply with respect to sole practitioners, who must sign off the BRA themselves.

- Risk is dynamic and may be affected by external changes as well as changes in the activities, services and operations of the subject person. Consequently, the BRA is to be regularly reviewed and kept up to date.[12] Section 3.3.4 of this FIAU's Implementing Procedures Part I sets out the situations which would warrant a review and possible update of the BRA. In any case, the BRA must be reviewed at least on an annual basis.

- The level of detail and complexity of the BRA is to be proportionate to the nature and size of the practitioner's business. By way of example, a firm with several employees, operating across various jurisdictions, and offering multiple types of services to a large client base is exposed to a broader spectrum of risks, and would therefore be expected to have a BRA that appropriately reflects the size and nature of its activities and operations. On the other hand, a sole practitioner or a small firm servicing a limited number of customers will not require a complex assessment, and this can continue to be built upon as needed to reflect any substantial growth in the size and nature of the operations.

In addition to the relevant chapter in the Implementing Procedures Part I, practitioners may refer to the FIAU's publication entitled 'The Business Risk Assessment' for best practices to be adopted when conducting a BRA. This document is the result of an analysis of a sample of BRAs carried out across all regulated sectors.

[11] https://caspar.fiaumalta.org/.
[12] Regulation 5(4) of the PMLFTR.

3.2.2 The Customer Risk Assessment

In addition to conducting a BRA, subject persons must also assess the risks that they are exposed to when providing their services to a specific customer. The requirement under Regulation 5(5) of the PMLFTR to adopt and implement customer risk assessment procedures arises in view of the risks posed by a given customer, the service being provided to them, the risks associated with the jurisdictions they and their business are connected to, and the channels through which services are being provided to them.

A CRA allows practitioners to determine the appropriate level of CDD that would need to be carried out in order to mitigate the risks identified. A high-risk business relationship would require the application of enhanced due diligence measures set out in Regulation 11 of the PMLFTR, while the simplified customer due diligence measures envisaged under Regulation 10 can only be applied if the CRA results in a low risk of ML/FT.

Section 3.5 of the Implementing Procedures Part I provides detailed guidance on how to conduct a CRA, including aspects relating to timing, revisions, and the weighting and categorization of risk factors. The below are some key principles that are to be kept in mind when conducting CRAs, and must be read in conjunction with the respective sections of the Implementing Procedures Part I:

- A CRA must be carried out before entering a business relationship or carrying out an occasional transaction.

- As with the BRA, the CRA must include an assessment of the risks relating to main risk factors, namely customer risk, product/service/transactional risk, geographical risk and delivery channel risk. Section 3.3 below, titled 'Sector-Specific Risk Factors' provides additional risk factors that are of specific relevance to practitioners.

- The risk posed by a relationship is dynamic, which means that the CRA is to be reviewed and updated from time-to-time to ensure that it continues to reflect the risk profile of the customer. When reviewing the data, information and documentation obtained as part of one's ongoing monitoring obligations, any change in circumstances that may be noticed should trigger a review and if necessary, an update of the customer's CRA. In addition, certain events or developments that result in a material change in the nature of the relationship should equally trigger a review of the CRA.

- Events and developments that would trigger the need for a review include the detection of unusual activity, a request for new services, or changes in the structure or beneficial ownership of the customer.

- Risks relating to the beneficial owner(s) of the customer must also be factored into the CRA.

When conducting a CRA, practitioners are to assess all known risk factors, including those referred to in the previous section relating to the customer, geography, product/service/transaction, and delivery channels.

In addition to the four main risk factor categories indicated above, there are other factors relating to certain attributes of the customer that only arise in the context of a CRA, and so must be assessed and addressed when conducting it. These factors are set out in detail under Section 3.5.1(a) of the Implementing Procedures Part I and relate to the reputation, the nature and the behaviour of the customer and its beneficial owner(s). Key principles on these risk factors are highlighted below.

Reputation

- Practitioners must assess whether there is publicly available information that links the customer or its beneficial owners to criminality or terrorism. Any such information must be factored in when assessing prospective customers and should also lead to a review of the CRA of existing customers.

- Supervisory or regulatory action taken against the customer also needs to be factored in when assessing the ML/FT risk posed by the relationship. Such information is relevant if it increases the likelihood that the customer is, has been, or may be involved in activity that generates illicit proceeds.

- Existing customers that have been subject to an STR are considered to pose a higher ML/FT risk, and so any STRs filed by the practitioner should lead to a revision of the CRA.

Behaviour and Nature

The behaviour of individuals seeking a practitioner's services, as well as the structure of the entity requesting the services, can impact the ML/FT risk thereof. The following elements are considered to increase the ML/FT risk of a relationship:

- Reluctance by the customer to provide information and/or documents that are required for CDD purposes.

- Where doubts or concerns arise on the veracity or authenticity of any information and documents provided.

- Where the customer has little or no connection to Malta and there is no sound economic and lawful reason for seeking the practitioner's services in Malta.

- Where the ownership and control structure involve bearer shares or nominee/fiduciary shareholders.

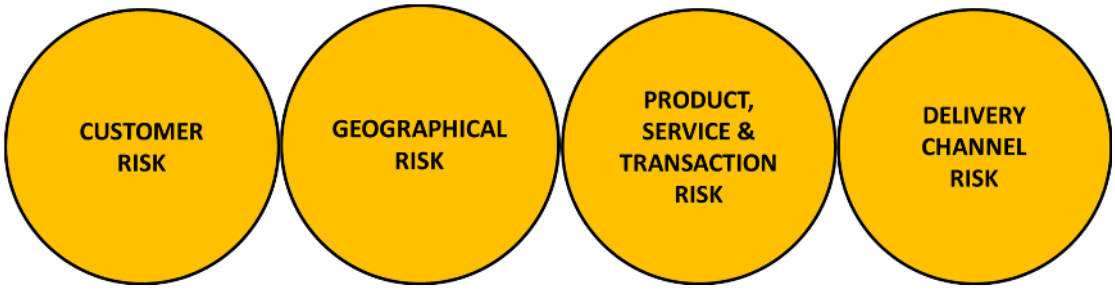
- Whenever there are material changes to the customer's ownership and control structure for which there does not seem to be a legitimate rationale.

The following sections provide guidance on sector-specific risk factors applicable to practitioners, which are to be taken into consideration when conducting and updating the BRA and CRAs. These complement the generally applicable risk factors set out in the Implementing Procedures Part I.

3.3 Sector-specific Risk Factors

To conduct risk assessments, practitioners need to identify the threats and vulnerabilities which they are exposed to. This is done by considering those areas from which risk may manifest itself – these areas are known as **risk factors**. Regulation 5(1) of the PMLFTR requires subject persons to assess at least four main categories of risk.

These categories are referred to as **customer risk**; **geographical risk**; **product, service, and transaction risk**; and **delivery channel risk**.



Section 3.2 of the Implementing Procedures Part I explains these categories in more detail and provides examples of risk factors that apply and are relevant to all sectors. The following section of the document explores additional elements of risk that are relevant to practitioners. Practitioners are to bear in mind that risk factors are those elements which increase the risk of ML/FT, and hence increase the potential of ML/FT to take place. With appropriate and commensurate controls and due diligence measures, the risks can be eliminated or reduced to a manageable level.

3.3.1 Customer Risk

The following are examples of customer risk factors that practitioners may be exposed to and that may increase or indicate a higher risk of ML/FT, together with an explanation of the cause giving rise to the risk:

The customer is or forms part of a Complex Corporate Structure

Complex corporate structures are ownership structures that are not immediately transparent as to who ultimately owns or controls them. A structure may be complex due to having multiple tiers of shareholding levels. Such structures could also involve shareholding through different types of entities and arrangements, such as trusts and foundations. These entities and arrangements may also be incorporated in multiple different overseas jurisdictions, further increasing the complexity. The structure becomes more complex if one or more entities involve bearer shares or shares held in a nominee or fiduciary capacity.

How do complex corporate structures affect ML/FT risk? Servicing a complex structure increases the ML/FT risk for the practitioner due to the inherent opacity of the structure. This makes it more challenging to establish the ownership and control structure and determine who the beneficial owners are.

Where the entities and arrangements within the structure are established in multiple overseas jurisdictions, practitioners may encounter obstacles in obtaining company information from reliable and independent sources to verify ownership and control.

Within complex structures, it becomes more complicated to obtain a clear understanding of the purpose of the setup and of the customer company's role within that structure.

The use of complex corporate structures is a known means for facilitating ML/FT, the mentioned factors make such structures attractive vehicles to purposely obscure ownership and/or to layer transactions throughout the various entities. This increases the risk of misuse of legal entities (such as companies) and arrangements (such as trusts and foundations) for criminal purposes.

Mitigating Measures

Practitioners must ensure that they identify and verify the identity of the beneficial owners and take steps to understand and document the ownership structure. Registers of beneficial ownership information contribute to increasing transparency and practitioners are to use these to complement their due diligence measures.

Understanding, documenting and corroborating the ownership structure together with understanding the reasons for that particular set-up provides practitioners with much needed information for risk assessment purposes and the actual determination of ML/FT risk they are exposed to. There may be legitimate tax, business, or economic reasons to justify such complexity.

In addition to understanding the activity conducted by its corporate customer, where the customer forms part of a group structure, the practitioner must also seek to understand the overall activity/operations of the group, and understand the role of the subsidiary (the customer) within the group.

The Customer operates within the VFA sector

Having customers who are active in the VFA sector may expose practitioners to a higher risk of ML/FT. When assessing the risk associated with entertaining business relations with a VFA operator, practitioners should have regard to the below considerations[13]:

- **The operator's regulatory status:** an operator that carries out its activities from or in a jurisdiction that does not regulate or supervise the activity in question exposes the practitioners to a significantly high risk of ML/FT when compared to an operator that is regulated and supervised for AML/CFT purposes. One needs to have regard to the jurisdiction which is regulating the VFA operator in question. Being subject to regulation in a non-reputable or in a high-risk jurisdiction dilutes the relevance of regulatory oversight exercised over the VFA operator.

- **The activities of the operator:** VFA operators provide different types of services, each giving rise to varying levels of ML/FT risks. For instance, providing services consisting in the transfer of VFAs increases the practitioner's risk, particularly due to the ability to transfer high values and volumes of transactions.

The Customer is or owns a Cash-Intensive Business

The provision of services to entities that carry out primarily or substantially cash transactions increases the ML/FT risk exposure for practitioners.

Businesses that are cash intensive receive significant amounts of payments in cash, such as catering establishments, supermarkets and fuel stations, traders in high value goods (e.g.: cars, jewellery, arts, antiques), and entertainment establishments such as land-based casinos**.**

Cash has historically been the most popular means of currency in the criminal underworld, as it allows anonymous transactions, and can be moved around without leaving a trail, allowing criminals to disconnect themselves from the activity which generated the illicit cash.

Most cash intensive business operate legitimately, but nevertheless are at an increased risk of being misused for ML/FT purposes. Cash-intensive operations provide a potentially efficient way for commingling illicitly obtained cash with proceeds derived from the genuine operations of the business. In turn, these are placed into the financial system under the guise of legitimate business transactions and earnings.

Additionally, owners of cash intensive businesses may be less likely to declare their full earnings, exposing practitioners to tax evasion. One has to also consider the Use of Cash (Restriction) Regulations[14], which restrict the use of cash when it comes to transactions involving the sale or purchase of determinate high value goods. Practitioners may be especially well placed to detect if these regulations are being breached and whether the customer is in fact making use of proceeds of crime.

The Customer is or owns a High-Volume Trading Business

High-volume trading activity involves the processing (or facilitation thereof) of high volumes of transactions. Examples of such operations include online and land-based casinos, financial institutions such as payment service providers and electronic money institutions, and virtual financial asset exchange services.

[13] Subject persons may wish to refer to the FIAU and MFSA joint publication 'Guidance for Credit Institutions, Payment Institutions and Electronic Money Institutions Opening Accounts for Fintechs' for general principles that can be taken into account when assessing the risks they may be exposed to when providing services to FinTechs including VFA operators: https://fiaumalta.org/wp-content/uploads/2020/05/Guidance-20190618_Guidance_OpeningAccountsForFinTechs.pdf

[14] S.L. 373.04 of the Laws of Malta.

The risk associated with servicing these entities is driven by the high volume of transactions processed, which increases the challenges of identifying suspicious transactions. The risk is further increased by the fact that the practitioner does not have a relationship with or any control over the end client (the customer's clients), and so is not able to conduct due diligence on such end clients. Thus, the practitioner is exposed to the many risks that may be posed by the customer's clients.

Factors indicative of a Lower Customer Risk

The following are examples of customers who typically present a lower customer ML/FT risk. This does not mean that the business relationship is one of low risk, but merely that the risk presented by the customer (prior to assessing other risk factors) may be lower. Practitioners must bear in mind that it is the customer risk assessment that ultimately dictates the level and type of risk associated with a given business relationship/occasional transaction:

- public companies listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means), which impose requirements to ensure adequate transparency of beneficial ownership,

- public administrations or enterprises in reputable jurisdictions in terms of Section 4.8.1 of the Implementing Procedures Part I.

3.3.2 Geographical Risk

This refers to the risk that arises from connections with one or more geographical areas. The jurisdictions to be taken into consideration for this purpose are those (a) where the customer or its beneficial owners are based, have their main place of business or where the activity generating their wealth is carried out, and the jurisdictions with which the customer has especially strong trading or financial connections; or (b) with which the customer or its beneficial owner have relevant personal links (e.g., the individual's residence in a given jurisdiction). If these jurisdictions pose a higher risk of ML/FT or their AML/CFT frameworks are deemed to be non-reputable, there is a higher risk that funds connected to the relationship are tainted.

Section 3.2.2 and Chapter 8 of the Implementing Procedures Part I provide detailed guidance on the factors that are to be taken into consideration when assessing geographical risk. The below may provide further sector specific examples of connections that may be taken into consideration when assessing geographical risk:

- Where the activity generating their wealth is carried out.
- Where the place of management is located.
- Where the customer undertakes its financial activity – this would include the countries where the customer has branches or agents.
- With respect to potential acquisitions, where the target company is registered and has its major operations located.

3.3.3 Product, Service and Transaction Risk

Practitioners provide a range of services and activities that differ in their methods of delivery, the depth and duration of the relationships formed with customers, and the size of their operation. The ML/FT risks associated with the various services can differ, depending on the inherent features of the service offered.

The level of transparency and complexity associated with the service, and the value and volume of transactions permitted through the service, drive the practitioner's risk exposure. These elements are outlined in more detail below:

Anonymity: The ML/FT risk is higher where the service provided by the practitioner provides or facilitates anonymity. This occurs by allowing the customer or beneficial owner to remain anonymous or by obscuring the beneficial owner's identity or the audit trail of transactions. A case in point would be where the service provided involves the transfer of funds and use is made of the practitioner's clients' account.

Complexity: Risk can also be driven by the complexity of the transactions that may be carried out through, or as a consequence of, the service provided. As an example, this would include services which facilitate or result in the movement or change in ownership of multiple assets across entities or jurisdictions.

Large value or volume of transactions: Practitioners are exposed to a higher risk when their services facilitate in the planning or execution of large value transactions, for instance through their involvement in mergers or the provision of advice on the acquisition of high value assets or finance raising transactions.

Client Accounts

Client accounts held by practitioners, particularly accountants, are attractive to criminals and money launderers since the practitioner's professional designation lends trust and legitimacy to a transaction. Hence, the misuse of client accounts by criminals is a known money laundering typology. It is not within the FIAU's competence to regulate client accounts. However, this section provides practical guidance for practitioners to ensure that they do not unwittingly participate in facilitating money laundering through the use of their client account.

Limiting the use of the client account: Practitioners should avoid permitting the use of their client account when they are not providing their professional services. In this regard, practitioners may wish to avoid disclosing the details of their client account, unless this is necessary to carry out a specific service, which they are fully aware of and in agreement with. Likewise, practitioners should discourage customers from passing the details on to third parties.

Using the client account only as necessary: To prevent misuse, client accounts should only be used to hold client money for legitimate transactions, which are incidental to the services provided. Practitioners should know who they are receiving funds from and should ensure that the value is commensurate with the purpose for which they are intended. It is considered good practice to cross-check information about payments received against the services being provided.

Limiting funds received in the client account: Practitioners should consider limiting incoming funds if they do not come from an account held in the customer's name from a local or EU/EEA bank or financial institution, or one held in a reputable jurisdiction. Practitioners should likewise be careful about the ML/FT risk associated with the use of cash and cash deposits into client accounts and may wish to consider accepting only electronic transfers of funds. When in doubt of the source of the funds, practitioners may enquire further and obtain relevant information and/or documentation to substantiate the source. Practitioners should be wary of receiving funds from any sources that may give rise to concern to them.

Prior acceptance of customer instructions: Practitioners should be satisfied that funds received through the account are for purposes that they have explicitly agreed to. Customer instructions should be scrutinised and practitioners should ensure that funds are only transferred out of the client account in the manner and to the beneficiaries agreed upon. These instructions should make logical and economic sense. Importantly, the transfer of funds to third parties should be in line with the transaction being carried out.

Reimbursement of funds: When a transaction is aborted and given there is no suspicion of ML/FT or proceeds of crime, funds should be transmitted back to the customer through the same channels and in the same manner in which they were received. If this is not possible and if there are no suspicions of ML/FT, practitioners should seek to transfer funds to another account in the customer's name held by a bank or financial institution in a reputable jurisdiction. The request to transfer unused customer funds to third parties designated by the customer is a red flag that is typically indicative of money laundering.

As a general principle, practitioners expose themselves to a high risk of ML/FT when they permit their client account to be used by their customers instead of the customer opening their own banking or payment account to facilitate payments or transfers of funds. This is tantamount to the provision of shadow banking services, which should be avoided.

3.3.4 Interface Risk

The interface risk, which is also known as 'delivery channel risk' is the risk arising from how the practitioner interacts with its customer, and the channels it uses to provide a given product or service. Practitioners conduct business through varying channels, and these affect exposure to ML/FT. The following are a few considerations that need to be made when determining the interface risk of a given business relationship or occasional transaction:

Non-Face-to-Face Interaction

The Implementing Procedures Part I provide an example of an interface risk, namely non-face-to-face interaction. This includes non-face-to-face onboarding (the risks of which can be mitigated through the adoption of various due diligence measures[15]), but also ongoing non-face-to-face interaction such as taking instructions and processing transactions in a non-face-to-face manner. Implementing technological means that address the risk of impersonation or identity fraud, where relevant, is one way of mitigating the risks of such exposure.

Communicating through an Intermediary

There are situations when practitioners do not communicate directly with their customers, but through an intermediary.[16] The practitioner's relations with the intermediary may increase the level of ML/FT risk. The risk arises from the lack of contact with the customer throughout the duration of the business relationship, as well as due to exposure to any risks posed by the intermediaries themselves. The reputation and integrity of the intermediary impacts the type of customers that the intermediary deals with and the way business is conducted.

Thus, prior to entertaining relations with the customer, practitioners need to be reassured of the reputability and integrity of the intermediary. If the intermediary is not already well-known and enjoys a positive reputation, the practitioner may need to undertake checks on the intermediary using public (open source) information. Further guidance on dealing with intermediaries is provided in Section 5.1 of this document.

Other elements that affect the level of ML/FT risk of a given intermediary include for instance, when an intermediary is established or operating in a high-risk jurisdiction or a jurisdiction known to have deficiencies in its AML/CFT framework.[17] This factor would expose a practitioner to a higher degree of ML/FT risk, as opposed to when dealing with an intermediary in a reputable jurisdiction that is supervised for AML/CFT purposes.

3.4 External Risk Assessments

The PMLFTR and Section 3.2.7 of the Implementing Procedures Part I require practitioners to take into consideration any relevant risk information emerging from risk assessments such as the Supranational Risk Assessment, the National Risk Assessment and sectoral risk assessments.[18] These documents are vital for informing authorities and subject persons on those areas and sectors that are at greater risk of ML/FT, so that the actions of the respective persons and entities can be tailored towards addressing and mitigating that risk.

[15] Refer to Section 4.3.1.2 of the Implementing Procedures Part I for guidance on non-face-to-face on-boarding.
[16] Refer to the Section 5.1.1 of this document for more guidance on dealing with intermediaries.
[17] Refer to Chapter 8 of the Implementing Procedures Part I for guidance on determining high-risk and non-reputable jurisdictions.
[18] National risk assessments are coordinated by the National Coordinating Committee on Combating Money Laundering and Funding of Terrorism (NCC) and key results of national and sectoral risk assessments are published on the NCC's website https://ncc.gov.mt/resources/#annual-reports-section.

3.4.1 Supranational Risk Assessments

The **SNRA** is an assessment of the ML/FT risks that may affect the European Union, conducted by the European Commission and revised every two years. The SNRA assesses the areas of the internal market that are at greater risk of ML/FT, the risks associated with each sector, and the most widespread means used by criminals to launder illicit proceeds[19].

The SNRA published in 2022[20] states that *"professionals in these areas are among the actors most misused by organised crime groups to launder criminal proceeds; this is due to the types of services that they can provide to their clients and their sector of expertise. They can use financial engineering techniques and set up corporate structures, involving not cooperative jurisdictions, fabricating accounting systems, providing bookkeeping services, preparing financial statements or fiscal declarations, reporting false information, acting as insolvency administrator and providing general accounting and tax advice. These services are used by organised crime groups to disguise their identity, to commit predicate offences and laundering the proceeds of these crimes". .*

3.4.2 National and Sectorial Risk Assessments

The **NRA** and sectoral risk assessments provide information on the local ML/FT risk context, and so their findings are vital for strengthening risk understanding and enhancing the implementation of the RBA. As the first line of defence, subject persons have to be aware of the country's ML/FT risks and be able to effectively deter them from materializing or, detect them and avoid misuse. To factor findings of the NRA and sectoral risk assessments into their business and customer risk assessments, practitioners need to understand and assess the likelihood of the risks highlighted in the results of such assessments manifesting themselves within their operations. This will require an analysis of exposure from both a qualitative and a quantitative perspective.

For instance, the 2018 NRA indicated that tax evasion was one of the highest drivers of domestic ML/FT vulnerability.[21] For practitioners, this information means that when servicing local customers, there is a higher risk of misuse of their services to evade tax and/or to launder the proceeds of tax evasion.

To assess the extent of such exposure, one needs to analyze factors such as the type of local customers that are more likely to pose such a risk, and the distribution of such customers within the client base. Self-employed persons, contractors, and cash-intensive businesses are likely to pose a higher risk of tax evasion, as are those customers who have benefitted from tax amnesty schemes.

From a service point of view, practitioners need to understand which of their services are more at risk of being misused to facilitate tax evasion or the laundering of proceeds of crime. This would then be followed by an assessment of the volume of business that such services represent.

Practitioners are to always refer to the latest available versions of the NRA and of any sectoral risk assessments, as the risk environment is bound to change over time. Sectors or services previously considered high risk may become less risky due to an improvement in controls by subject persons and competent authorities, while emerging risks may also be identified based on new information.

[19] Article 6 of the 4th AMLD.
[20] The Supranational Risk Assessment is available on the website of the European Commission - https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022SC0344&from=EN.
[21] Table 1, Section 4.3 of the Results of the ML/TF National Risk Assessment 2018 - https://finance.gov.mt/en/library/documents/result_of_the_nra_2018.pdf.

4. Guidance on Specific Services

4.1 Audit Services

Due Diligence for Audits

The engagement of an auditor implies an element of duration since auditors are expected to conduct recurring audits. This is achieved by having their engagement confirmed annually by virtue of a Board resolution, ahead of the start of each audit cycle. For this reason, the relationship of audit is one which constitutes a business relationship between the auditor and the audited entity.

Ongoing Monitoring (including Transaction Monitoring)

Once a business relationship is formed, Regulation 7(1)(d) of the PMLFTR requires subject persons to carry out on-going monitoring. Monitoring comprises the scrutiny of transactions and ensuring that information, documents, and data on the customer are kept up to date and relevant.

The duration of an audit process varies depending on the circumstances and scale of the entity being audited. In most cases, the audit has a foreseeable end date and once the audit is completed, there is usually no ongoing communication with the customer or a review of their file until the start of a new audit. For this reason, to fulfil their ongoing monitoring obligations, auditors are expected to:

(i) Review and assess existing information and documents concerning the customer, and update these as necessary to reflect any material changes identified either during the audit, or during any other service provided which is considered to be relevant activity, or through the periodic review of the said information and documents carried out on a risk sensitive basis.

(ii) Review and assess the previous audit/s to compare the closing balance of the previous audit with the opening balance of the new audit. Where any discrepancies between the two balances occur, the auditor has to consider the reasons for the same and whether this gives rise to suspicion of ML/FT.

Based on the above, the auditor should determine whether the customer's risk profile has remained the same or not, and where there is a change in risk adjust CDD measures accordingly. As with all business relationships, the review is to be carried out:

(i) Periodically, the frequency of which must reflect the customer's risk; or

(ii) Earlier whenever there is a trigger event wherein a change occurs in the business relationship. Examples of a trigger events include where a change occurs in the activities of the customer, where

additional services are provided to the customer, or where there is a change in the customer's beneficial owner.

All aspects of due diligence information and documents held on the customer are expected to be reviewed to ensure that these are kept updated. However, the following are more likely to change over time, and any such changes are more likely to impact the risk profile of the customer:

- the identification and verification of information and documents including information on the identity of the directors
- the ownership and control structure
- the beneficial owners
- the purpose and range of the objects and/or activities of the audited entity
- the markets and/or jurisdictions in which the audited entity trades or has links with.

Having said this, if at any stage of the audit process doubts arise on the accuracy or veracity of any information or documents, auditors are to request additional information and/or documentation as needed.

The above requirements ensure that information and documentation held on the customer are kept current and valid, and that the CRA reflects the ML/FT risk arising from a business relationship. This way, the auditor will be in a better position to adjust any CDD or other mitigating measures taken or to be taken, including the level of ongoing monitoring, to reflect the risks posed by the customer. Section 4.5.3 of the IPs Part I provides further guidance on maintaining information, documents and data up to date.

Another aspect of ongoing monitoring which must be fulfilled is transaction monitoring. While it is acknowledged that auditors do not per se carry out transactions for their customers, the carrying out of an audit involves examining the activities and transactions carried out by the customer on a sample basis to assess whether the customer's financial statements reflect a true and fair view in accordance with the relevant accounting framework. In this regard, auditors should consider the knowledge and information obtained from previous audits carried out by that same auditor on the customer. This enables the auditor to compare the customer's yearly transactions and overall activity, thereby observing whether the activity of the current cycle is in line with previous ones. More guidance on the importance of transaction monitoring and how this may be achieved may be found below in the section "*Reporting executed transactions"*, whilst broader guidance on ongoing monitoring (including transaction monitoring) may be found in Section 5.3 of this guidance document.

In the case of group audits, each component auditor who has carried out an audit for a subsidiary of the group is deemed to be a subject person in his/her own right and therefore is expected to comply with his/her own AML/CFT obligations. The group auditor consolidating the group audit, who also falls to be considered as a subject person, would be expected to consider the visibility over the group's activities by virtue of the group audit and the accounts of the subsidiaries. The fact that part of a subsidiary's audit was conducted by a component auditor would not automatically exonerate the group auditor from responsibility **if** the said auditor is in a position to detect any unusual matters or suspicious activity or transaction. Therefore, group auditors are expected to ensure compliance with their own AML/CFT obligations by reporting any knowledge or suspicion of ML/FT, where they have visibility or awareness of the same.

Reporting

This section provides additional guidance on the obligation to report suspicious transactions in terms of Regulation 15(3) of the PMLFTR, with respect to situations that auditors are likely to encounter.

Reporting Executed Transactions

The obligation to report suspicious transactions has to be complied with promptly from when the practitioner knew, suspected, or had grounds to suspect ML/FT or that a given transactions involved the proceeds of crime. Although each audit year is considered separately for auditing purposes rather than a continuation of the previous year, this does not mean that the subject person may ignore previous audits and is therefore exempted from the requirement to report should they suspect ML/FT when comparing the information, activity, or transactions of one audit cycle to another. Hence, auditors are not to look at each audit year in isolation. In reality, while providing their services, auditors may come across unusual transactions that were executed or concluded well before the start of the audit cycle or even before their engagement. Practitioners must report even when the transactions or activities in question took place significantly prior to the practitioner's review and when transactions may have already been concluded.

This is particularly relevant for auditors as an audit can, for example, shed light on a dubious or suspicious contract that was entered into between the audited entity and another third party. Notwithstanding the lapse of time and the fact that the unusual or suspicious transaction would have already been carried out, auditors are still expected to scrutinise such transactions and if necessary, request additional information from the customer to justify or substantiate the transaction. This will enable the auditor to determine whether there is suspicion of ML/FT or proceeds of crime, in which case the auditor is required to report to the FIAU. The passage of time between the contract and the detection should not preclude the auditor from reporting, and the requirement applies regardless. Thus, the lapse of time does not create an exemption from the obligation to scrutinise transactions which might have raised a concern and to report suspicions of ML/FT. The obligation to report on the same day when knowledge or suspicion of ML/FT is still considered to subsist.[22]

Reporting on the basis of Adverse Media

Should auditors encounter adverse media or information which gives rise to suspicion of ML/FT or proceeds of crime regarding audit customers, even if this discovery is made in between one audit cycle or another or prior to the auditor's first engagement, they are nonetheless expected to consider their obligation to report suspicions to the FIAU in terms of Regulation 15 of the PMLFTR.

Practitioners may refer to Section 3.5.1(a) of the Implementing Procedures Part I for guidance on dealing with adverse information and media.

Prohibited Disclosures

There may be situations where an auditor terminates their relationship with an audit customer for reasons connected to knowledge or suspicion of ML/FT. In such cases auditors are expected to file a report with the FIAU in terms of Regulation 15(3) of the PMLFTR.

The Accountancy Profession Act requires resigning auditors to inform the Accountancy Board in writing of such resignation and provide adequate explanations for the said decision[23]. The Companies Act likewise requires a resigning auditor to deposit with the company a statement of any circumstances connected with their ceasing to hold office[24].

When abiding with these requirements, auditors must be mindful of rules on prohibited disclosures as set out in Regulation 16 of the PMLFTR. Regulation 16 prohibits subject persons from disclosing the fact that a report was submitted to the FIAU, or that the FIAU has requested information from that subject person. Thus, any communications made in fulfilment of other obligations, including those emanating from Article 161(1) of the

[22] Refer to Section 5.5 of the Implementing Procedures Part I.
[23] Article 17 of Cap. 281 of the Laws of Malta.
[24] Article 159 and Article 161(1) of Cap. 386 of the Laws of Malta.

Companies Act or from the Code of Ethics (Directive 2 issued by the Accountancy Board in terms of the Accountancy Profession Act) and the Accountancy Profession Regulations should not include wording that might lead to the customer being tipped off in breach of the PMLFTR.

4.2 Liquidation Services

Liquidation Services as Relevant Activity

Certified public accountants and auditors may act as liquidators, as set out in Article 305 of the Companies Act. Liquidation is a form of operation and management of a company, and is hence deemed to be a relevant activity, in terms of part (c)(v) of the definition of "relevant activity"[25], which applies equally to both accountants and auditors. Accountants and auditors acting as liquidators or assisting liquidators in insolvency or winding up proceedings are deemed to be carrying out relevant activity, even when so appointed by a court or tribunal.

Accountants and auditors are usually appointed to act as liquidators in their own name, regardless of whether they are employed within a firm or form part of a partnership. In all such cases, accountants and auditors are not required to consider themselves as subject persons in their own right (separate from the entity they work with), and would only be considered as such if they provide their service in their personal capacity (i.e. outside of the firm's activities). This applies even if any reports or deliverables are signed off in the individual's name. The circumstances in which the services are being provided indicate whether a liquidator is carrying out their role in their own personal capacity (in which case they are to be considered as a subject person in their own right) or whether they are doing so as part of the firm. The following may assist in distinguishing between the two scenarios:

- Whether the person is marketing the services in their own personal name/personal brand as opposed to the firm's.
- Whether that person is following their own procedures (AML or any other procedures) or the procedures of the firm.
- Whether payment is ultimately made to the individual or to the firm.
- Whether the letter of engagement is issued on the firm's letterhead.
- Whether correspondence is made using the individual's own email address or that provided by the firm.

The Customer Risk Assessment

When conducting a CRA in terms of Regulation 5(5) of the PMLFTR, accountants and auditors should take into consideration ML/FT risk factors that are specific to liquidation services. Factors that increase the ML/FT risk of the service being provided include:

- Where the company, its beneficial owners or any of its officers or directors are linked to material adverse media, particularly if they are subject to criminal investigations or allegations of fraud.

- Where the liquidation process requires the sale or distribution of the company's assets.

- In terms of geographical risk factors and in addition to those set out in Section 3.2.2 of the Implementing Procedures Part I, where the assets of the company are located in a high-risk jurisdiction or where payments are to be made to or received from high-risk jurisdictions.

- Where the beneficial owners of the company being liquidated have ceased to remain in contact or cannot be reached.

[25] Regulation 2(1) of the PMLFTR.

Due Diligence Measures

The liquidation of a company involves an element of duration that does not usually have a foreseeable end date, and for this reason, the provision of such services is considered to constitute a business relationship. The company being liquidated is deemed to be the customer of the liquidator. In this respect, the identification and verification obligations set out in Regulations 7(1)(a) and (b) apply with respect to the company and its beneficial owners.

In terms of Regulation 7(1)(c), practitioners are to assess and obtain information on the 'purpose and intended nature of the business relationship'. The purpose of liquidation services is self-evident and so in this respect it is considered more useful for accountants and auditors to understand why the company is being liquidated. This would be particularly important in cases where the purpose behind the liquidation is not immediately evident or does not make economic or business sense, for instance in cases where a company is being liquidated shortly after having been set up.

The ongoing monitoring obligations set out in Regulation 7(1)(d) of the PMLFTR consist of two separate requirements: keeping information, data, and documents up to date, and the ongoing scrutiny of transactions. In situations where liquidation services are being provided to a company that is no longer trading or conducting commercial activity, it is unlikely that the liquidator will need to assess, review, and update the information and data held on the customer. Where the company is still carrying out some form of commercial activity, additional or updated due diligence information and documents are to be requested on a risk-sensitive basis with consideration being given to the duration of the services being provided.

In all cases, where the liquidator has doubts about the veracity or accuracy of the information and/or documents provided at onboarding stage, the liquidator may need to request new and/or additional information and/or documentation.

With respect to the scrutiny of transactions, liquidators should take measures to understand the recipients of any assets that are being distributed. Such measures should be focused on ensuring that assets are not distributed to persons connected to ML/FT, proceeds of crime, or criminality. In cases where assets are being distributed to persons with no apparent connection to the business, liquidators need to understand the reasons for the arrangement and the connection between the recipient and the company. In all cases, liquidators should be mindful of their obligation to report knowledge or suspicions of ML/FT or proceeds of crime.

4.3 Services related to the Operation, Management, or Administration of Companies

Accountants and auditors may also be appointed by supervisory authorities or by the court in roles that entail the operation, management, or administration of a company. Examples of these roles include being appointed as controller, administrator or as a competent person in terms of the Banking Act[26] or any other relevant laws, where the specific appointment requires taking or assuming control of a business, or carrying on a part or a function of the business.

Any such appointment would have usually been the result of either issues related to the possible misuse of the entity for the conduct of criminal activity or serious failures by the entity in question to abide by its regulatory obligations, which may also include serious failures with respect to its AML/CFT obligations. Notwithstanding that the appointment is being made by a reputable competent authority, the nature of the engagement and the service being provided in this case must still be regarded as one of high risk from an ML/FT point of view.

In such cases, the main mitigating measure that can be applied by the practitioner is that of monitoring any transactions carried out by the entity, bearing in mind the scope and objectives of the services to be provided

[26] Cap 371 of the Laws of Malta.

by the practitioner which would be specified in the letter/order sanctioning the appointment. The same instrument is likely to set out the respective reporting obligations by which the practitioner has to abide, with any reporting usually being done to the authority or court that would have appointed the practitioner to any of the said roles.

In this context, it therefore becomes key for the practitioner to thoroughly understand the activities of the particular entity entrusted under his/her administration and management and, where applicable, the extent and nature of the AML/CFT obligations which it may have applied. This allows the practitioner to better understand when checks are to be carried out and additional information or documentation is to be requested in relation to transactions to be carried out.

The importance of doing so is especially high where the entity in question is a subject person and the practitioner is to also return funds and/or assets to the customers of the entity under his/her administration and management. It is possible that the instrument of one's appointment will itself set out what checks are to be carried out but the absence of any such instructions or directions does not mean that the practitioner does not have any obligations in this regard.

In doing so, the practitioner may come across instances where there may be a suspicion that funds or assets are the proceeds of criminal activity, triggering the obligation to submit an STR to the FIAU. Should any such report be filed, practitioners are reminded of their non-disclosure obligations under Regulation 16(1) and therefore they are not to disclose the fact that they filed an STR other than in those instances set out in Regulation 16(2) which allow such disclosure.

5. Aspects of Due Diligence

The following sections provide guidance on select aspects of CDD that merit sector-specific guidance and interpretation. This document does not provide guidance on the entire set of due diligence measures that practitioners are to carry out, and practitioners are to read the following sections in conjunction with the corresponding chapters of the Implementing Procedures Part I.

5.1 Agents, Intermediaries & Introducers

The person requesting the practitioner's services may be the customer himself/herself but there may be circumstances where the customer is represented by another person or entity. This section provides guidance on how the different scenarios and relationships are to be treated and the due diligence measures to be conducted.

5.1.1 The Agent

In addition to carrying out due diligence measures on the customer and beneficial owner, Regulation 7(3) of the PMLFTR requires subject persons to identify and verify the identity of any person who **acts on behalf of a customer**, and to ensure that this person is duly authorised in writing to act on behalf of that customer.

An agent is a person who acts on behalf of the customer, be it the corporate customer itself, or a prospective shareholder, partner, or beneficial owner. This person has the authority to bind the customer, for example when duly appointed to act as a signatory on the customer's bank account, or when duly authorised to sign contracts or agreements binding the customer (such as the director(s) vested with legal and judicial representation). Sections 4.2.1 and 4.3.3 of the Implementing Procedures Part I provide more information on the concept of the agent acting on behalf of the customer and the measures that are to be carried out in those circumstances where the customer is represented by another person or entity.

Where the customer is a company or commercial partnership, the agents in terms of Regulation 7(3) of the PMLFTR would usually be those directors and partners who are legally empowered to represent and bind the company or commercial partnership. These individuals are typically involved in the carrying out of an occasional transaction or business relationship by giving instructions to the practitioner, or taking actions that likewise bind the company or commercial partnership (e.g.: signing of letters of engagement with the practitioner). This means that not all directors and partners are to be considered as agents, but only those that have and are in fact exercising powers to bind the customer throughout the course of the business relationship or the carrying out of the occasional transaction. The due diligence requirements set out in Regulation 7(3) would need to be carried out with respect to these persons.

Persons with legal and judicial representation of a company are usually listed in the Memoranda/Articles of Association as such. A copy of the document attesting to the said representation would satisfy the requirement to ensure that the person is duly authorised in writing to act on behalf of the customer. Authorisation may also be granted to individuals through a resolution of the Board of Directors, in which case the practitioner is to obtain a copy of the board resolution.

In the case of foundations or associations, authorisation is usually granted through the statute, through a resolution, or written down in the minutes of meetings of the supervisory board or council.

Where the agent is acting on behalf of a natural person, authorisation is usually provided through a power of attorney or other legal document or instrument that demonstrates that the agent is indeed authorised to act on behalf of the customer.

5.1.2 Introducers and Intermediaries

Even though auditors usually have direct access to the customer, at times, practitioners (particularly accountants) may deal with other persons or entities that would be representing their customer. However, unlike in the case of agents, these other persons or entities would not have the power to bind, execute transactions, or enter into contracts for the customer. This would be the case when dealing with introducers or intermediaries. The following section examines the concept of the introducer and the intermediary and provides guidance on how practitioners are to treat such relationships.

The Introducer

Practitioners may face situations where a prospective customer is introduced to them by a third party. A typical example would be where a CSP requests an accountant to provide professional services constituting a relevant activity to a customer. The intention would be for the prospective customer to form a relationship or conduct an occasional transaction directly with the practitioner. Where the role of the introducer is to merely place a prospective customer in contact with the practitioner, without any further involvement in the business relationship, they are not to be considered as an agent. Practitioners would therefore not be required to carry out any due diligence on the **introducer**.

The Intermediary

There are situations where an introducer introduces a customer to the practitioner, then proceeds to remain actively involved in the carrying out of a transaction or in the business relationship established between the customer and the practitioner. The involvement could include the communication of the customer's instructions to the practitioner (prior to or during the business relationship or the carrying out of the transaction), without necessarily being legally authorised to bind or act on behalf of the customer in the same way as an agent would.

In such a scenario, the person making the introduction does not remain an introducer as explained in the previous sub-section but becomes an **intermediary.** An intermediary may be an individual who enjoys the customer's trust and communicates the customer's intentions, instructions, and decisions to the practitioner, and/or undertakes specific tasks or activities (e.g.: project management, vetting of documents, and giving legal advice to the customer), without having any powers to bind or sign on behalf of the customer.

Typically, an intermediary remains involved as the point of reference to carry out the transaction or during the business relationship, again without having the power to bind the customer. Intermediary relationships typically involve another local or foreign practitioner, CSP, trustee or wealth management firm, law firm or other professional firm. The following are examples of situations that indicate that a person or entity is more than an introducer and is actually an intermediary:

- Correspondence takes place between the practitioner and the introducing person or entity (e.g.: the introducing law firm or CSP), irrespective of whether the customer is always, often or never copied in.
- Instructions are always or mostly provided by the person acting as the introducer.
- The letter of engagement is entered into with the purported Introducer, who continues to co-ordinate other matters relevant to the transaction or relationship.
- The letter of engagement is entered into with the customer directly, but interaction and relations between the practitioner and the customer take place through the introducer.

In other words, any situation in which an individual or entity carries out additional activities beyond merely introducing the customer to the practitioner and stopping there, renders that individual or entity an intermediary, **thereby necessitating the application of due diligence measures on that intermediary.**

Due Diligence Measures to be conducted on Intermediaries

Practitioners should have internal processes to **review and approve intermediaries** before servicing customers who are introduced and represented by these intermediaries. These internal processes are necessary to ensure that practitioners deal with intermediaries who are reputable and of good standing, which will itself reflect on the quality, standing and intention of customers who are introduced to them.

Except in the case of sole practitioners, such internal processes should require **senior management approval** before any working relationships with intermediaries are initiated.

These processes should also require **scrutiny and due diligence** to be carried out on the intermediary for the determination of senior management (or the practitioner themselves in the case of sole practitioners) to be a well-informed one. The scrutiny and due diligence should include the following:

Basic checks for all Intermediaries

(a) Determine whether the intermediary would be representing end customers to whom services will be provided, or whether the intermediary will be passing on instructions from another intermediary/other intermediaries, one of which would ultimately represent the end customer (i.e.: intermediary chains).

(b) Establish the existence of the intermediary through public sources.

(c) Assess, and be satisfied with, the intermediary's reputability and integrity. This would involve carrying out public searches (e.g.: using online search engines, metasearch engines or commercial databases) to assess whether any adverse information exists on the intermediary, which would raise doubts about the intermediary's integrity, such as involvement in any wrongdoing (e.g., criminal offences or breaches of AML/CFT, prudential or other professional obligations). In cases where the intermediaries are professional law, accountancy, tax advisory or CSPs/firms, practitioners should confirm that these intermediaries are licensed, regulated or are accredited professionals, as the case may be.

(d) When the relationship with the intermediary is ongoing, practitioners are to carry out regular checks to ensure that the information obtained at the point of establishing the working relationship with the intermediary remains current and to be aware of any new information that might concern the intermediary's reputability and integrity. These ongoing checks are expected to be carried out at least on an annual basis.

Additional checks for higher risk Intermediaries

Higher risk intermediaries would include intermediaries who are:

- not subject to any licensing, regulation or professional accreditation
- situated in high-risk or non-reputable jurisdictions
- less renowned and about whom it is difficult to find information through public sources.

Before establishing working relationships with higher risk intermediaries, practitioners should be more cautious and should carry out additional and more in-depth checks. These additional checks may include:

(a) Identifying and verifying the intermediary's identity by collecting the necessary identification details and verifying those details based on data, documents or other information, as is explained under Section 4.3.1 of the Implementing Procedures Part I. In the case of intermediaries that are firms or entities,

practitioners should also identify the directors, partners or administrators of these intermediaries and also identify and verify the identity of their beneficial owners. See section 4.3.2 of the Implementing Procedures Part I for further details on the identification and verification procedures to be applied in the case of intermediaries that are entities or firms.

(b) In the case of intermediaries that are entities or firms, extending the reputability and integrity checks envisaged under paragraph (c) of the list of basic checks for intermediaries, to not only cover the intermediary but also its directors, partners or administrators, and its beneficial owners.

(c) Gathering further information on their internal AML/CFT procedures (where applicable) to formulate an understanding of the intermediary's compliance culture.

(d) Holding introductory meetings (physical or virtual meetings using a video-conferencing facility).

(e) In the case of intermediary chains, carrying out the above procedures on every intermediary in the chain.

(f) Where the relationship with the intermediary is ongoing, practitioners are to carry out regular checks to ensure that the information obtained at the point of establishing the working relationship with the intermediary remains current and to be aware of any new information that might concern the intermediary's reputability and integrity. These ongoing checks are expected to be carried out at least on an annual basis.

5.1.3 Situations indicating that the presumed customer is acting on behalf of somebody else

Notwithstanding the requirement to determine the beneficial owner(s) of a customer when dealing with a legal entity or arrangement, there may be situations that indicate that the person presumed to be the customer or beneficial owner is acting on behalf of another person.

This may be due to legitimate changes in the ownership structure of the customer, in which case practitioners must update their due diligence and customer profile and review their CRA to determine whether it needs to be updated to reflect new risks presented by the new beneficial owners. However, this may also suggest that the presumed customer/beneficial owner is not acting in their name as originally disclosed to the practitioner, but on behalf of another person, as a *prestanome,* mandatory, front man or straw man. In such instances, practitioners should consider the possibility that the customer is intentionally concealing the identity of the end customer or beneficial owner. Unless there exists a legitimate explanation, practitioners should consider whether there is reason to submit a suspicious activity report to the FIAU and should desist from providing further services to the customer.

Practitioners may become aware of such situations through behavioral indicators, such as the below:

i) The presumed customer/beneficial owner is not able to provide outright instructions on the entity's operations and has to refer decisions to another person.
ii) Correspondence between the practitioner and the customer/beneficial owner involves a third party who is not known the practitioner.
iii) The practitioner's fees are being settled by persons other than the presumed customer/beneficial owner in a way that does not make practical business sense.r
iv) The presumed customer/beneficial owner does not appear to understand in detail the operations of their entity.

5.1.4 Network Firms

Practitioners are likely to find themselves dealing with intermediaries and introducers particularly when they form part of an international member network (also sometimes referred to as an international correspondent firm).

"Network" is defined in Article 2(1) of the Accountancy Profession Act as the larger structure which is:

(a) aimed at cooperation and to which an auditor belongs; and
(b) clearly aimed at profit or cost sharing or shares common ownership, control or management, common quality control policies and procedures, common business strategy, the use of a common brand-name, or a significant part of professional resources.

These international networks serve, amongst other things, to facilitate cross-border activity for the customers of the network firms. These relationships may give rise to AML/CFT obligations, and the section below provides guidance on the application of these within various scenarios.

The type and extent of due diligence to be carried out by the practitioner depends on whether that practitioner will communicate with and provide services **directly to the customer** of the counterpart firm, or whether the practitioner will continue to correspond through or provide services **to the network firm**. The following section provides more guidance on the due diligence to be applied in such situations.

When a foreign network firm refers a customer to the local correspondent firm (subject person) in Malta

Where the role of the foreign network firm is limited to referring a customer to the local correspondent firm (the practitioner) without remaining involved in the relationship, the customer of the foreign network firm becomes a direct customer of the practitioner. In such instances the foreign network firm is deemed to be an **introducer** in the manner set out in previous sections of this document. In such cases, no due diligence is required to be undertaken on the introducing foreign network firm. However, practitioners may wish to assess the reputability of the foreign network firm for any adverse media linking them to ML/FT or proceeds of crime.

Since the practitioner is establishing a direct relationship with the customer, he must undertake all the obligations applicable to a business relationship (or occasional transaction) with respect to the said customer and all relevant involved parties.

In cases where the foreign network firm continues to remain involved in the provision of the service by, for instance, assisting or liaising in the communication of instructions or documentation, the foreign network firm is considered to be an **intermediary**. Nevertheless, practitioners are to apply the due diligence measures for foreign network firms as laid down below.

Where the practitioner provides a service to a foreign network firm

There may be instances where the foreign network firm requests the practitioner to participate in the undertaking of a service to its customer, but engagement with the customer continues to remain with the foreign network firm. For example, a foreign network firm is engaged by its customer to provide advice on an international taxation structure. The foreign network firm contacts the practitioner to assist through the provision of advice from a Malta perspective. The practitioner will report directly and provide deliverables to the foreign network firm and would charge the foreign network firm for services rendered. Thus, the provision of the service is limited to the foreign network firm. In this regard, the practitioner is considered to have entered into a business relationship/occasional transaction directly with the foreign network firm, and **not** with the firm's customer.

In those cases where a firm forms part of a network that meets the criteria set out in Article 2 (1) of the Accountancy Profession Act, and therefore shares a common set of standards and common quality-control policies and procedures with the other firms that are members of the same network, the customer due diligence to be carried out can be limited to the following:

i. The identification of the network firm, i.e. depending on the form of the network firm, obtaining its official name, its registration number, its date of incorporation or registration, and its registered office or principal place of business address.

ii. The identification of the Chief Executive Officer, managing partner or other person holding an equivalent position. This can be done through the collection of the necessary information from the network firm itself or, if available, by consulting the network firm's portal. In the latter case, the practitioner has to retain a printout of the portal to demonstrate that such a check was carried out.

The above is without prejudice to the obligation of the practitioner to request, collect and consider the necessary information and/or documentation to understand the rationale of the transaction or transactions in relation to which its services are being requested, mitigate any risks associated the same and, where necessary, file an STR with the FIAU.

5.2 Assessing the Purpose and Intended Nature of the Business Relationship

Regulation 7(1)(c) of the PMLFTR requires practitioners to assess and, where appropriate, obtain information and/or documentation on the purpose and intended nature of the business relationship. Section 4.4 of the Implementing Procedures Part I provides comprehensive guidance on the measures to be taken and is to be read in conjunction with the following sections. In addition to the measures laid out in the Implementing Procedures Part I, practitioners are to obtain information on the rationale for the services being requested, to understand whether these make legitimate economic and business sense for the customer. This is especially relevant when the customer requesting the services has little or no apparent connection with Malta.

Where the customer is a company, practitioners are to also understand the commercial or trading activity carried out by the company. This would also include understanding the actual or expected principal activity and financial flows with respect to size and geographical distribution.

In the case of companies set up to hold assets (e.g.: shareholding in another entity), practitioners are expected to understand the commercial or trading activity carried out directly by the holding company's subsidiary or subsidiaries. This information would allow the practitioner to understand the type of activities or the purpose which its customer is connected to. Merely understanding that the customer is a holding company would not be sufficient.

Practitioners need to also seek to understand whether, in the course of the business relationship, they will be expected to provide ad-hoc or other services in addition to those initially agreed to.

Purpose and Intended Nature in the context of Occasional Transactions

While the requirement to establish the purpose and intended nature is to be carried out in the context of a business relationship, there may be situations where the ML/FT risks associated with an occasional transaction can only be mitigated through obtaining information and, where applicable, documentation on the purpose and intended nature, including information and documentation on the source of funds or the customer's source of wealth.

Thus, the requirement to obtain information and documents on the purpose and intended nature of the business relationship, including source of wealth and source of funds, is to also be applied in a risk-based manner with respect to occasional transactions where the identified ML/FT risks can only be mitigated through obtaining this information. When the customer is a company, practitioners are to understand the commercial or trading activity carried out by the company. In the case of companies set up to hold assets (e.g.: shareholding in another entity), practitioners are expected to understand the commercial or trading activity carried out directly by the holding company's subsidiary or subsidiaries. This information would allow the practitioner to understand the type of activities or the purpose which its customer is connected to.

5.2.1 Establishing the Source of Wealth and the Source of Funds

Part of the information required to understand the purpose and intended nature of the business relationship or of an occasional transaction is information on the source of the customer's wealth and the source of funds to be used throughout the relationship or to fund an occasional transaction. In addition to helping with the establishment of the business and risk profile of the customer, information on the source of wealth and/or funds, supported by documentation where necessary, is also essential to ensure that the customer's wealth and any funds to be used have been generated legitimately, and will also allow the practitioner to conduct meaningful ongoing monitoring and detect unusual or suspicious transactions.

Section 4.4.3 of the Implementing Procedures Part I defines the source of wealth as '*the economic activity or activities that generate the customer's wealth*'. By way of example, the source of wealth may be comprised of income through employment, business, or inheritance in the case of a natural person, revenue or share capital in the case of a company, and donations or endowments in the case of a foundation. The term 'source of funds' is then defined as '*the activity, event, business, occupation or employment generating the funds used in a particular transaction, or to be used in future transactions*'. Section 4.4.3 of the Implementing Procedures Part I provides more guidance on establishing the source of wealth and source of funds, and is to be read in conjunction with the following sections which provide sector-specific guidance and examples on the application of this requirement.

Source of Wealth

The overarching principle when understanding the source of wealth of a customer is to form a reasonable conclusion that the customer's wealth has been accumulated legally. In this regard, the measures taken may be varied depending on the level of ML/FT risk posed by the relationship and by the nature of the risks.

When establishing the source of wealth of customers that are legal entities, practitioners may request and refer to recent financial statements prepared by the customer, paying particular attention to the statement of financial position, statement of cash flows and related notes. Legal entities may be financed through various means, including equity, retained earnings, other reserves, third party debt, shareholders and related party debt, and working capital. Practitioners should seek to understand these elements and their contribution to the source of wealth of the company. When doing so, practitioners may request the customer to provide additional information such as financial statements from previous years and details on any shareholders loans.

Where the entity has only recently been established and is not able to provide such information, the practitioner's role is to understand how the legal person will be financed, and then determine the source of such funds and the source of wealth of any persons making any significant capital injections or financial contributions.

Source of Funds

The purpose behind the requirement to establish the source of funds is to ensure that funds used throughout the duration of the relationship are legitimate and that transactions are conducted in line with the customer's profile. In requesting information and, where necessary, documentation on the expected source of funds, practitioners may, on a risk-sensitive basis, consider the following:

- volume and frequency of expected cash inflow and outflows; geographical distribution of main money flows
- details of major customers and suppliers
- details on expected funding through borrowings (related party or third party)
- source of initial equity funding and related entity debt financing (where applicable).

Throughout the duration of the business relationship, practitioners are not expected to understand or request the source of funds of every transaction. However, when activities or transactions appear to be unusual, or not in line with what is known about the customer, or represent a new source of funding, when assessed based on both materiality and risk, information and any supporting documentation on the actual source of funds used to

finance the unusual activity or transaction should be collected. This will lead the practitioner to determine whether the funds were derived from a legitimate source.

The following are examples of sources of funds which attract higher ML/FT risks:

- the use of crowdfunding to raise capital
- assets denominated in virtual currencies
- funds raised through initial coin offerings or security token offerings
- debt with related entities, if they are incorporated in high-risk or non-reputable jurisdictions, especially without a legitimate reason
- debt from parties which are not related to the customer, that are not licensed credit/financial institutions.

Within certain business activities, it may be normal for customers to conduct high and very high value transactions, and the customer's risk profile would indicate that such values of transactions are indeed in line with their business. In these cases, practitioners should still request substantiating documentation from time to time so that they may continue ensuring that the transactions are indeed related to the business activity.

Source of Wealth of Beneficial Owners

The requirement to understand the source of wealth of the customer should not always be interpreted as requiring the practitioner to obtain information on the source of wealth of the beneficial owner(s).

Information and, where applicable, on the wealth of the beneficial owner(s) would be relevant when, while obtaining information on the purpose and intended nature of the business relationship, or at any time during the provision of the service or prior to conducting an occasional transaction, it is noted that the customer's funds or wealth have been or will be provided or contributed by the beneficial owner(s). In these cases, practitioners will need to obtain information on their source of wealth/funds to establish that they have been derived legitimately.

Examples of such instances include:

- Where the capital is provided by the beneficial owner and the amount is substantial.
- Where the capital or funding of the company does not appear to be sufficient (e.g.: in the cases where the company has been set up with minimal or very low share capital). In such cases the practitioner is to ask and understand how the company will be operating and whether there will be capital increases. It should also establish how these funds will be provided by the beneficial owner, as well as the source of said funds.
- With respect to trusts and foundations, if these are being serviced at a stage where assets are still to be placed or the foundation is not yet generating the funds needed to support its activities, practitioners are to establish where the assets will come from and establish the source of funds of persons making any significant settlements or endowments.
- On an ongoing basis whenever significant assets or funds are placed or settled.

A contribution is significant when the value is high compared to that person's salary or income.

The above also applies in the case of shareholders, settlors (when the customer is a trust), founders (when the customer is a foundation) and other persons with a similar role. Practitioners should obtain information and, where applicable, documentation on the source of the funds and the source of wealth of the third parties.

This applies equally in the case of other non-related third parties providing or lending assets into the company or entity (unless these are licensed credit or financial institutions). In such cases, the practitioner is to understand the connection between the third party and the company. Where the connection is not apparent or there does not appear to be any economic or business rationale behind the arrangement, practitioners are to request additional information and/or documents to understand the purpose and the source of the fund. In case of suspicion of ML/FT or proceeds of crime, practitioners are to report to the FIAU in terms of Regulation 15 of the PMLFTR. Practitioners should here refer to the FIAU's Guidance Note on *Obtaining Source of Wealth Information related to Parties other than the Customer*.

Extent of Information and Documentation

The extent and level of detail of the information required on the source of wealth and the expected source of funds, and whether and how much documentation should be requested to substantiate the information provided by the customer, would depend on the outcome of the CRA and the risks highlighted by it. In cases of lower risk, or where it emerges from the CRA that the ML/FT risk is not driven by the source of funds (e.g.: the source would be a ML/FT risk if the value of funds to be used is significant, if there is PEP involvement, or there are connections with high-risk jurisdictions), it would suffice to obtain information by way of a declaration from the customer. In higher risk scenarios, enhanced measures would need to be taken, which would include substantiating the information with documentation provided by the customer and/or information from open sources.

Ultimately practitioners need to reasonably conclude on the legitimacy of the source of wealth and funds. Measures undertaken should be commensurate with risk and practitioners should be mindful of taking measures that are excessive, disproportionate, or irrelevant when considering the ML/FT risks involved.

5.3 On-Going Monitoring

Business relationships are subject to customer due diligence procedures throughout their duration, in the form of ongoing monitoring obligations. The requirement to conduct ongoing monitoring is explained in detail under Section 4.5 of the FIAU Implementing Procedures Part I, and is comprised of two key elements:

(a) The scrutiny of transactions undertaken throughout the course of the relationship to ensure that the transactions being undertaken are consistent with the subject person's knowledge of the customer and of their business and risk profile, including where necessary, the source of funds.

(b) Ensuring that the documents, data or information held by the subject person are kept up to date.

Scrutiny of transactions

The scrutiny of transactions through transaction monitoring during the relationship requires practitioners to use their knowledge of the customer (including the information gathered on the purpose and intended nature of the business relationship and the business and risk profile) to identify transactions that are unusual. A transaction can be 'unusual' by its nature, because it is suspicious, illogical, unnecessarily complex, or unreasonable. A transaction may also be unusual when taking into consideration what one knows about a given customer, for instance because it is inconsistent with the customer's profile or is significantly different to the customer's usual activity or transactions.

Regulation 11(9) of the PMLFTR imposes a specific requirement to examine the purpose and background of transactions that are complex, unusually large, conducted in an unusual pattern, or have no economic or lawful purpose.

An unusual transaction is not automatically deemed to be suspicious but should, however, serve as a red flag or trigger for practitioners to assess the situation and undertake measures to establish whether that transaction is suspicious and ought to be reported, or whether there are legitimate explanations for the unusual transaction. Measures that can be undertaken to assess an unusual transaction include:

- Assessing the customer's profile to understand whether the flagged transaction makes sense in line with the known source of wealth, source of funds and business activities.
- Conducting searches on open sources to verify aspects of a transaction, such as the existence of any parties mentioned in an invoice.
- Asking the customer about any new operational activities that have given rise to changes in transactional behaviour.

- Requesting information on the transaction, such as the purpose of the transaction and/or the source of funds used or to be used to finance the transaction.
- Requesting documentation to substantiate the transaction and/or the source of funds used or to be used to finance that transaction.

In addition to the red flags provided in this document, practitioners should be wary of certain indicators within trade documents, such as invoices and contracts, provided by the customer. Such documents may contain certain defects, irregularities or features that should cause the practitioner to question further and assess whether there is cause for suspicion or knowledge of ML/FT:

- invoices for large sums with generic descriptions (e.g.: € 200,000 for 'consultancy services' without additional information or without a breakdown of what the sum consists of)
- recurring invoices for services without a contract or agreement regulating such services
- large value contracts for services without commencement dates or service periods
- inconsistencies between the name of the seller/exporter and the person or entity receiving the payment
- contracts that do not make business sense (e.g.: contract for tax, commercial and administrative support spanning only a few months)
- contracts for goods or services the value of which appears to be highly inflated (or deflated) when compared to the expected market value or what is usually charged
- incorrect or missing details (e.g.: incorrect VAT and registration numbers).

Practitioners are not expected to scrutinise each and every invoice or contract held by their customer. However, when such documents are provided to justify or substantiate a given transaction, particularly one flagged by the practitioner himself/herself, close attention should be given that there is already a degree of doubt or concern at that stage. These may be indicative of false transactions either to layer or structure funds or as part of a wider trade-based money laundering scheme. Reference may be made to Section 7 of this document for additional guidance in the case of auditors.

Ultimately, the purpose behind scrutinising transactions is to ensure that the transaction and the source of funds used are not connected to ML/FT or proceeds of crime. The type and extent of measures taken to scrutinise transactions should be risk-based and should provide the practitioner with a reasonable level of comfort that the transaction is legitimate. In cases of knowledge or suspicion of ML/FT or proceeds of crime, practitioners are to submit a report to the FIAU.

Not all unusual transactions will give rise to suspicions, as there may be legitimate reasons for the flagged activity. Sometimes, an assessment of an unusual transaction will lead the practitioner to identify important changes in the customer's profile, such as a significant change or expansion in the business activity. In this case, practitioners should ensure that the customer due diligence and the customer profile are up to date and should also assess the existing CRA to determine whether it needs to be updated.

Transactions falling outside the Scope of 'Relevant Activity'

Practitioners can provide a range of services to any one customer, some of which would fall outside the definition of 'relevant activity' and hence would not require the application of AML/CFT measures. However, the knowledge gained on the customer through the provision of these services should not be excluded or ignored from the subject person's overall knowledge of the customer. For instance, in cases where the practitioner comes across information that gives rise to suspicion of ML/FT while providing services falling outside the scope of 'relevant activity', the information cannot be ignored. Practitioners should seek to understand how this information impacts the relationship and the risk of ML/FT, and should they have suspicion or knowledge of ML/FT, they may still report this with the FIAU.

CASE STUDY

*A local audit firm submitted a STR to the FIAU on the basis of suspicions noted while conducting a statutory audit of consolidated financial statements. **

The subject of the STR was a Malta-registered company (Company A). During the audit, the subject person noted a contract between Company B and Company C. Company B is a subsidiary of Company A, registered in a high-risk jurisdiction. Company C is an unrelated third-party registered in the same high-risk jurisdiction as Company B. Some irregularities were noted in the contract, causing the subject person to ask its customer, Company A, for more information on the agreement.

The irregularities noted include:

- The agreement was for the provision of generic services ('administrative support').
- The services were to be provided over a short span of time where such services are usually recurring or provided over a longer period.
- The commencement period for the provision of the services was not specified in the agreement.
- The details of Company C were incorrect and, in some cases, false.

The explanations provided by Company A did not provide sufficient reassurance on the legitimacy of the transaction, leading the subject person to report its suspicions.

**Some details of the case have been changed to safeguard the confidentiality of information.*

Ensuring that the Documents, Data, or Information held by the Subject Person are kept up to date

The second aspect of a practitioner's ongoing monitoring requirement is to ensure that the documents, data, or information held on the customer are kept up to date. A practitioner's knowledge of the customer and its business activities continues to develop throughout the duration of the relationship. Through this requirement, customer information, including due diligence and the risk profile are reviewed and updated, so that they continue to reflect the current circumstances surrounding the customer and their activity. This requirement is also essential to ensure that the level and extent of due diligence being carried out continues to mitigate the actual risks posed by the relationship, since such measures would have been based on the information obtained on the customer prior to onboarding. The purpose is explained in more detail in Section 4.5.3 of the Implementing Procedures Part I.

The ongoing monitoring process also allows practitioners to determine whether the initial risk assessment requires updating, and whether, in view of the updated risk assessment or other considerations, the business relationship remains within the subject person's risk appetite and, if so, understand whether the level of due diligence and mitigating measures in place need to be adjusted in view of any changes from the initial risk understanding.

The need to update CDD information should be considered at appropriate times, following a risk-based approach. Reviews may be conducted periodically, with the frequency depending on the ML/FT risk of the business relationship, based on trigger events, or a combination of both periodic and trigger events.

Periodic reviews

The FIAU Implementing Procedures Part I and this document do not prescribe a specific frequency for carrying out ***periodic reviews***. However, these must be risk-based, with higher risk relationships being subjected to enhanced ongoing monitoring procedures which entail more frequent reviews.

Trigger events

Potential events that may trigger the need to review and update due diligence and risk profile information (**trigger events**) include:

- At the start of and when planning for recurring engagements.
- When requesting to provide a new service to the customer that would impact the risk of the relationship or which changes or presents a new risk factor in terms of the CRA.
- When a previously suspended engagement starts again.
- Whenever there is a change of control and/or ownership of the customer.
- Whenever there is a significant change to key office holders.
- When there is a material change in the level, type, or conduct of business (e.g. a change in the industry or jurisdictions in which the customer operates).
- Whenever a customer or its beneficial owner(s) is identified as being a PEP.
- Whenever there is any cause for concern or suspicion.

Ongoing monitoring procedures need not necessarily result in the collection of more documentation; this should only be necessary when information and documents held are no longer relevant, accurate or valid.

5.4 Reliance

It often happens that a customer contacts two or more subject persons in respect of the same transaction. Customers are also routinely introduced by one practitioner to another, or deal with one practitioner through another. Having multiple subject persons requesting the same information and documents from the same customer in respect of the same transaction does not necessarily mitigate the risk of ML/FT or add value to AML/CFT efforts being undertaken, resulting in inconvenience and inefficiency for both the customer and the practitioner.

Regulation 12 of the PMLFTR allows subject persons to rely on the CDD measures carried out by other subject persons or certain third parties subject to a number of conditions stipulating which elements of due diligence may be relied on, which entities may and may not be relied on, the circumstances under which a subject person may not place reliance, and the requirement to enter into a reliance agreement.

Section 4.10 of the FIAU Implementing Procedures Part I sets out how Regulation 12 is to be implemented and is to be followed by practitioners that intend to rely on others in such a manner. The following section explains some of the key rules and limitations.

It must be noted that in all cases, the practitioner remains ultimately responsible for compliance with their AML/CFT obligations, regardless of any reliance agreements that may be in place. This also includes the requirement to respond to FIAU requests for information in a timely manner.

Scope

A practitioner may **only** rely on the CDD measures undertaken by another subject person or third party in relation to Regulation 7(1)(a) to (c), namely:

- the identification and verification of a customer
- the identification and verification of beneficial owner(s), where applicable
- obtaining information on the purpose and intended nature of the business relationship, and on the business and risk profile.

Practitioners may **not** benefit from reliance with respect to other obligations such as establishing the purpose and intended nature of the business relationship, conducting the CRA, and carrying out ongoing monitoring[27]. These latter obligations are specific and tailored to the service provided by the individual practitioner and its policies, procedures, and risk appetite. Practitioners may rely upon PEP screening and checks conducted by the entity being relied upon, where the practitioner is comfortable that such checks were carried out appropriately and are up to date.

The customer may not necessarily present the same level and kind of ML/FT risk to the practitioner as it does to the entity being relied upon. This means that the due diligence measures being relied upon may be insufficient or inappropriate when it comes to mitigating the ML/FT risks to which the practitioner is exposed. Practitioners should therefore be cautious when opting to exercise reliance.

Entities that may be Relied On

Section 4.10.3 of the Implementing Procedures Part I sets out in detail which entities and subject persons may and may not be relied upon. It also provides additional guidance to assist subject persons in assessing whether a jurisdiction in which an entity is established is considered to apply CDD measures that are consistent with those of the PMLFTR. Practitioners are to read the said section carefully prior to relying on another entity.

Practitioners may not rely on third parties from a non-reputable jurisdiction (unless these third parties are branches or majority-owned subsidiaries of persons or institutions established in an EU Member State, subject to national provisions implementing the 4AMLD and which comply fully with group-wide policies and procedures equivalent to those listed in Regulation 6 of the PMLFTR).

Carrying Out Reliance

Section 4.10.4 of the Implementing Procedures Part I explains how reliance is to be carried out. When placing reliance, a practitioner must **immediately obtain** the information required under Regulation 7(1)(a) to (c) of the PMLFTR, before carrying out the occasional transaction or entering into a business relationship. Thus, a practitioner must at least have the customer and beneficial owner's identification data, information on the purpose and intended nature of the business relationship, and information on the customer's business and risk profile. Such information enables the practitioner to conduct its CRA and to comply with ongoing monitoring obligations.

For example: Firm A enters into a business relationship with, or undertakes an occasional transaction for, the underlying customer of Firm B. Firm A may rely on Firm B to carry out CDD measures, while remaining ultimately liable for compliance with the PMLFTR. The left-hand column indicates the measures to be taken by Firm A if it conducts its own due diligence, while the column on the right indicates the measures to be taken if placing reliance on Firm B.

If conducting own CDD	If placing reliance
Firm A has to identify and verify the customer.	Firm A has to obtain the information concerning the customer's identity from Firm B i.e. the entity being relied upon.
Firm A has to identify and verify the beneficial owner(s) by requesting the necessary documentation from the customer.	Firm A has to obtain information concerning the identity of the beneficial owner(s) (where applicable), from Firm B.

[27] An exception to this applies with respect to the requirement to keep due diligence documentation up to date. Section 4.10.4 of the Implementing Procedures Part I provides that *"in the case of verification data and/or documentation, the subject person has to rely on the entity with whom it has entered into a reliance arrangement even for keeping that documentation up to date since it would otherwise be impractical to seek updated documentation directly from the customer*".

Firm A has to obtain information and/or documents to understand the purpose and intended nature of the business relationship and establish the customer's business and risk profile.	Firm A has to obtain the information on the purpose and intended nature of the business relationship and the customer's business and risk profile from Firm B.
	Firm A must still carry out its own CRA and conduct ongoing monitoring.
Firm A has to request copies and receive copies of the identification and verification documentation and other supporting documentation.	Firm A is not obliged to request copies of the identification and verification data, and other relevant documentation (in relation to the purpose and intended nature of the business relationship and on the customer's business and risk profile) obtained by the entity being relied on, unless the subject person requests the entity being relied on to provide such information.
	Firm A and B have to enter into a written formal agreement, signed by both parties, regulating the procedures and conditions on data requests to ensure that the data and documents are made available immediately.
	Firm A should consider testing the reliance agreement to ensure that Firm B does indeed provide requested documents in a timely manner and that the due diligence measures being undertaken are satisfactory – this provides reassurance that Firm A remains compliant with its AML/CFT obligations.
Firm A has to monitor to ensure that documentation is up to date.	Firm A must enter into a reliance agreement with Firm B to ensure that the latter informs Firm A of any CDD documentation which is updated such as updating of identification documents, changes in address etc.
Firm A has to keep any CDD records securely for five years after the end of the business relationship and/or occasional transaction or for any such longer period as stipulated in the Implementing Procedures Part I.	Firm B shall keep any CDD records securely for five years after the end of the business relationship and/or occasional transaction or for any such longer period as stipulated in the Implementing Procedures Part I.

The Reliance Agreement

Practitioners are at all times expected to be able to respond to any requests for information from the FIAU, regardless of whether the practitioner has placed reliance or otherwise. This means that the practitioner needs to be able to retrieve documents in a timely manner so as to comply with such requests. In fact, rules on reliance require subject persons to take adequate steps to ensure that the entity relied upon immediately forwards relevant information and copies of documents. To this effect, practitioners must enter into a written formal agreement with the entity being relied upon, to regulate the procedures and conditions on such requests.

Practitioners should also consider testing the reliance agreement to ensure that the entity can be relied upon consistently. This can be done by requesting information and documents from time-to-time from the entity being relied upon. Through such testing, the practitioner can ensure that the entity does indeed provide information and documentation in a timely manner and provides insight on the whether the due diligence measures

conducted by it are satisfactory (e.g.: whether the entity is collecting the right documents and whether CDD is updated through ongoing monitoring). This is important as practitioners remain ultimately responsible for compliance with their AML/CFT obligations.

The below grid provides examples of permissible and non-permissible reliance relationships:

Practitioner	Entities that can be relied on	Entities that cannot be relied on
Firm A – Maltese accounting firm	Firm B – Maltese CSP	Firm C – CSP from a non-reputable jurisdiction (e.g.: FATF-listed).
Firm ABC – Maltese audit firm	Firm ABC – Audit firm in a reputable jurisdiction (for example: same group of companies or same network of firms)	/

Distinction between Entities acting as Intermediaries and Entities that may be Relied On

It is important to distinguish an Intermediary or Agent relationship from a situation where reliance is being placed in terms of Regulation 12 of the PMLFTR. The two instances should not be confused, and one does not necessarily involve the other. This means, for example, that a practitioner could be communicating with an Agent or an Intermediary without placing reliance on them. A reliance relationship must be explicit and regulated through an agreement as set out above.

In certain circumstances, an Introducer, Intermediary or Agent could be someone on whom the practitioner is permitted at law to place reliance in accordance with Regulation 12 of the PMLFTR. In this case, it is up to the practitioner to determine whether to conduct its own CDD or to place reliance.

6. Reporting

This section is to be read in conjunction with Chapter 5 of the Implementing Procedures Part I on Reporting Procedures and Obligations.

6.1 Reporting to the FIAU

Regulation 15(3) of the PMLFTR requires subject persons to promptly report to the FIAU any knowledge or suspicion of ML/FT, and any knowledge or suspicion that funds or property are the proceeds of crime. Section 5.5 of the FIAU Implementing Procedures Part I defines "promptly" as meaning that a report should be submitted on the same day when knowledge or suspicion is considered to subsist by the MLRO (or the practitioner in the case of a sole practitioner). In more complex cases where the compilation and submission of the report within the same day would be challenging in view of the extensive volume or complexity of information and documentation, the MLRO needs to ensure that the report is submitted within the shortest time possible.

After reporting, there is no obligation to terminate the relationship with the customer. If a practitioner does continue the business relationship, the below actions need to be taking after reporting:

a) classify that customer as a **high-risk** customer
b) remain vigilant and monitor the activities of that customer to a larger extent.

In some cases, suspicion or knowledge of ML/FT or proceeds of crime arises during the onboarding process. For instance, doubts may arise on the veracity of the information or the authenticity of the documents provided for due diligence purposes, or the purpose and intended nature of the relationship gives rise to concerns on the rationale for the service, or the prospective customer turns out to be the subject of worrying adverse media. The requirement to report such suspicion or knowledge subsists, even if the practitioner decides not to complete the onboarding process and not onboard the customer.

Reporting through goAML

In June 2020, the FIAU launched goAML – a fully integrated software solution developed by the United Nations Office on Drugs and Crime specifically for use by Financial Intelligence Units.

All subject persons are required to register on goAML. The goAML system is used to receive all suspicion reports and is also used by the FIAU to request information from subject persons. Practitioners are to refer to the FIAU's From Suspicion to Action document for guidelines on registering through goAML. [28]

The goAML reporting platform caters for various types of suspicion reports that may be submitted to the FIAU depending on the circumstances surrounding the person, activity or transaction being reported. For instance, a distinction is made between suspicious transaction reports (STRs) and suspicious activity reports (SARs). A STR is submitted when the transaction (or patterns of transactions) is suspicious for instance because it is not in line with the customer's profile, while a SAR is submitted when the suspicion stems from the customer's behaviour (rather than from a transaction). Other types of reports include PEPR (Politically Exposed Person

[28] https://fiaumalta.org/wp-content/uploads/2020/06/FIAU-goAML-Notification.pdf.

Report) and PEPTR (Politically Exposed Person Transaction Report), which are used when the subject of the report is a PEP, and TFR, which is used when there is a suspicion of terrorist financing activities.

The FIAU's Guidance Document on Reporting through goAML sets out the various reports with guidelines on selecting the most appropriate report in a given situation.[29]

6.2 Red Flags

The following section contains a list a of activities or circumstances that may indicate a higher risk of ML/FT. Not all the below circumstances would be relevant to all practitioners and across all services, as these red flags depend on the customer's specific profile and the circumstances surrounding the transaction or activity.

The existence of one or multiple red flags should not automatically give rise to suspicion and/or a report but rather, should cause the practitioner to analyse the transaction and customer in further detail to determine whether the activity is justified or whether there is indeed a suspicion of ML/FT. The list is based on information and typologies known to the FIAU and on guidance issued by the FATF from time-to-time, including the FATF's Guidance for a Risk-Based Approach, and FATF/EGMONT reports on Concealment of Beneficial Ownership[30] and on Trade-Based Money Laundering Risk Indicators[31].

As required under Regulation 15(3) of the PMLFTR, practitioners must report to the FIAU where there is knowledge or suspicion of ML/FT or proceeds of crime.

Red flags relating to the Customer

- The customer's registered address does not make sense when compared against its operational activity. E.g.: the address relates to an office or residential building when the customer's operations are more industrial or commercial, or else, the address is likely to be a mass registration address such as a post-box or an office building.

- The customer does not appear to have employees or business premises in a manner that is inconsistent with its business operations.

- The name of the company is very similar or almost identical to an unrelated, established business. This is a known typology where companies try to gain trust and repute by assimilating or appearing to form part of well-known businesses.

- Unexplained use of informal arrangements such as family or close associates acting as nominee shareholders or directors.

- Customers who appear to actively and inexplicably avoid face-to-face meetings or who provide instructions intermittently without legitimate reasons or are otherwise evasive or very difficult to reach, when this would not normally be expected.

- Adverse results from screening procedures.

- Customer starts or develops an enterprise with unexpected profile or abnormal business cycle or customer is entrant into new/emerging markets. Organised criminality generally does not have to raise capital/debt, often making them first into a new market, especially where this market may be retail/cash intensive.

[29] https://fiaumalta.org/wp-content/uploads/2021/02/Guidance-Document-on-Reporting-through-goAML.pdf
[30] https://www.fatf-gafi.org/publications/methodsandtrends/documents/concealment-beneficial-ownership.html
[31] https://www.fatf-gafi.org/publications/methodsandtrends/documents/trade-based-money-laundering-indicators.html

- Indicators that customer does not wish to obtain necessary governmental approvals/filings, or similar statutory documents.
- Frequent or unexplained change of professional adviser(s) or members of management.
- The customer is reluctant to provide all the relevant information or accountants have reasonable doubt that the provided information is correct or sufficient.
- Power of representation given in unusual conditions (e.g. when it is granted irrevocably or in relation to specific assets) and the stated reasons for these conditions are unclear or illogical.
- Unexplained urgency of assistance required.
- Unusual sophistication of customer, including complexity of control environment.
- The irregularity or duration of the customer relationship. One-off engagements involving limited customer contact throughout the relationship may present higher risk.
- Knowledge of previously undisclosed arrangements.
- New directors or shareholders, whose profile of a director or shareholder is inconsistent with the activities of the company.
- There are unexplained, frequent changes in the company's name, registered office or ownership structure.
- Multiple changes to a customer's accountants/auditors without a valid explanation.
- Change in trading partners that is not in line with expectations/nature of business.
- Customer lacks awareness of where business documentation is kept (indicating that the customer may be appearing on behalf of somebody else).

Red Flags relating to Transactions

- Company transactions do not indicate ongoing business activity in line with its stated activity, e.g.: lack of transactions relating to operational costs and employee salaries.
- High volume of trading with high-risk jurisdictions which does not make immediate economic sense when compared with the customer's known trading activity.
- Investment in or loans to entities that have no apparent legal or legitimate tax, business, economic or other reason or entities that may pose higher geographical risk.
- Holding of substantial or excessive amounts of cash considering the nature of the business.
- Injection of new funds into the business, from an unclear source or where the value appears to be disproportionate to beneficial owners' circumstances.
- Company transactions such as purchases exceeding its financial capabilities, especially where these are financed through cash injections or by third parties.

- Successive capital or other contributions in a short period of time to the same company with no apparent legal, tax, business, economic or other legitimate reason.

- Change in means of payment for a transaction at the last minute and without justification or where there is an unexplained lack of information or transparency in the transaction. This risk extends to situations where last minute changes are made to enable funds to be paid in from/out to a third party.

- Suspicion of customers' use of false loans, false invoices, and misleading naming conventions.

- Sudden activity from a previously dormant customer without clear explanation, or else the company is unusually dormant from time to time where this is not in line with what would normally be expected.

- Unexplained (where explanation is warranted) use of pooled client accounts.

- Transfer of real estate or other high value goods or assets between parties in a time period that is unusually short for similar transactions with no apparent legal, tax, business, economic or other legitimate reason.

- An unexplained and illogical change in the jurisdictions in which the customer trades, which does not make economic sense when compared to the customer's profile and known trading activity.

- Transactions where it is readily apparent to the practitioner that there is inadequate consideration, especially where the customer does not identify legitimate reasons for the amount of the consideration.

- Transactions using unusual means of payment (e.g. precious metals or stones).

- The postponement of a payment for an asset or service delivered immediately to a date far from the moment at which payment would normally be expected to occur, without appropriate assurances that payment will be made.

- Unexplained establishment of unusual conditions/clauses in credit arrangements that do not reflect the commercial position between the parties. Arrangements that may be abused in this way might include unusually short/long amortisation periods, interest rates materially above/below market rates, or unexplained repeated cancellations of promissory notes/mortgages or of other security instruments substantially ahead of the maturity date initially agreed.

- Contributions or transfers of goods that are inherently difficult to value (e.g. jewels, precious stones, objects of art or antiques, virtual assets), where this is not common for the type of customers, transaction, or with the accountant's normal course of business, such as a transfer to a corporate entity, or generally without any appropriate explanation.

- Acquisitions of businesses in liquidation with no apparent legal, tax, business, economic or other legitimate reason.

- Transactions involving closely connected persons and for which the customer and/or its financial advisors provide inconsistent or irrational explanations and are subsequently unwilling or unable to explain by reference to legal, tax, business, economic or other legitimate reason.

- Payments received from un-associated or unknown third parties and payments for fees in cash where this would not be a typical method of payment.

- Commercial, private, or real property transactions or services to be carried out by the customer with no apparent legitimate business, economic, tax, family governance, or legal reasons.

- Significant amount of cash sales by companies trading in goods that are subject to cash restrictions.

- Existence of suspicions regarding fraudulent transactions, or ones which are improperly accounted for. These might include:

    - Over and under invoicing of goods/services.
    - Multiple invoicing of the same goods/services.
    - Falsely described goods/services - over and under shipments (e.g. false entries on bills of lading).
    - Multiple trading of goods/services.

Red Flags indicative of Tax Evasion

Reference should be made to the Factsheet published by the FIAU on Typologies & Red Flags: Indicators of Tax-Related ML[32].

Audit Standards that may be relevant in detecting ML/FT

When determining whether a transaction is unusual or otherwise, auditors may find it helpful to consider any adverse results of procedures carried out when auditing financial statements in the normal course of the audit, particularly those carried out in accordance with International Standards including:

- International Standard on Auditing 240: The auditor's responsibilities relating to fraud in an audit of financial statements (ISA 240);
- International Standard on Auditing 315: Identifying and assessing the risks of material misstatement through understanding the entity and its environment (ISA 315); and
- International Standard of Auditing 550: Related Parties (ISA 550).

The following section is not intended to interpret the application of the above international standards, and neither does this document require practitioners to follow these procedures and standards for AML/CFT purposes (the use of the term 'should' refers to what is required by auditors following these standards). Rather, the purpose is to highlight those audit standards that may also assist in determining unusual transactions or possible suspicions of ML/FT or proceeds of crime.

The procedures expected under ISA 240 to address the risk of fraud would include, amongst other procedures:

- Evaluation of unusual or unexpected relationships that have been identified in performing analytical procedures, including those related to revenue accounts, which may indicate risks of material misstatement due to fraud.

- For significant transactions that are outside the normal course of business for the entity, or that otherwise appear to be unusual given the auditor's understanding of the entity and its environment and other information obtained during the audit, the auditor shall evaluate whether the business rationale (or the lack thereof) of the transactions suggests that they may have been entered into to engage in fraudulent financial reporting or to conceal misappropriation of assets.

Other procedures that may be relevant from an AML/CFT point of view are those carried out under ISA 550 dealing with related parties:

[32] https://fiaumalta.org/wp-content/uploads/2021/12/FIAU-Intelligence-Factsheet-Tax-Related-ML-final.pdf.

- If the auditor identifies transactions that are both significant and non-routine, the auditor should establish whether they involve known related parties. The auditor should understand the rationale for these transactions and determine whether high level approval has been given for these transactions.

- This Standard also describes procedures that should be considered should the auditor come across any transactions involving related parties that had not previously been identified or disclosed by the customer.

Appendix 2 of ISA 315 (Revised) includes a list of conditions and events that may indicate the existence of risks of material misstatement, which may likewise give rise to suspicion of ML/FT, including amongst others:

- changes in the industry in which the entity operates
- changes in the supply chain
- the existence of complex alliances and joint ventures
- significant transactions with related parties
- changes in key personnel including departures of key executives
- inception of investigations into the entity's operations by regulatory or government bodies
- significant amount of non-routine or non-systematic transactions including intercompany transactions and large revenue transactions at period end.

These events may serve as indicators in assessing whether a given activity or transaction gives rise to suspicion of ML/FT.

If the results of any of these procedures carried out as part of the audit reveal an instance of fraud and/or are unsatisfactory (in the sense that no valid explanation is available), the auditor should consider whether any of the above raises any ML/FT red flags and whether more information should be obtained to assess the circumstances and determine whether there is knowledge or suspicion of ML/FT.

It is also worth noting that ISA 240 includes a list of fraud risk factors and ISA 315 also includes examples of conditions and events that may indicate risks of material misstatement. These lists can also be useful tools in determining red flags for auditors.

Exemptions from Reporting Obligations

Recitals (9) and (10) of 4AMLD set out the principle behind this exemption, and its application to professionals other than lawyers. In brief, and even as set out in Section 5.10 of the Implementing Procedures Part I, legal advice and information obtained before/during/after judicial proceedings or in the course of ascertaining the legal position of the customer remains the subject of professional secrecy (except of course where the customer seeks advice to launder funds or attempts to involve the lawyer in laundering). This is done in order to ensure the right to a fair hearing, which includes the right to have the possibility of being advised, defended and represented, as per the Charter of Fundamental Rights of the EU.

The Directive then explains that comparable services should be treated in the same manner when provided by the professionals covered in the Directive (notaries, auditors, accountants). This is done in view of the possibility that auditors and accountants are, in some Member States, entitled to defend or represent their customer in the context of judicial proceedings. This principle is transposed into Maltese laws and into the Implementing Procedures, and would find its application in cases where auditors or accountants represent their customers or assist in ascertaining their legal position.

Indeed, the law envisages some exceptions to reporting obligations as set out in Regulation 15(9) of the PMLFTR and further explained under Section 5.10 of the FIAU Implementing Procedures Part I.

Regulation 15(9) creates an exception to the requirements under Regulation 15(3), (4) and (8), namely:

- Regulation 15(3): the requirement to report suspicion or knowledge of ML/FT or proceeds of crime to the FIAU.
- Regulation 15(4): the requirement to notify the FIAU of a pending transaction that is known or suspected to be connected to proceeds of crime of FT (and to refrain from executing out that transaction).
- Regulation 15(8): the requirement to respond to a request for information from the FIAU.

This exemption applies only to auditors, external accountants, tax advisors, and independent legal professionals (primarily advocates). Furthermore, the exemption **only** applies in relation to information that the practitioner receives in the course of ascertaining the legal position of their customer, or performing their responsibility of defending or representing their customer in judicial proceedings. This includes advice on instituting or avoiding procedures. Set out below are some examples of work which may fall within privileged circumstances:

- When the practitioner's services are requested to regularise one's position with the tax authorities and avoid future legal proceedings, as long as the request for such services is not intended to advance a crime.
- When having a clear indication that someone is suing one's customer or the customer is subject to legal proceedings (e.g. where the customer receives a legal letter on a tax assessment being carried out by the respective authority on the same).
- Representing a customer, as permitted, in front of a tax tribunal.
- When engaged by a customer as an *ex-parte* expert in relation to judicial proceedings.

Thus, in any instance where an accountant or auditor is entitled to defend or represent a customer in the manner set out in Section 5.10 of the Implementing Procedures Part I, if at all, then information obtained directly as a result of the provision of such services would not be reportable.

7. Record Keeping

Practitioners are required to retain records pursuant to their customer due diligence obligations as well as documents and information collected to comply with their ongoing monitoring requirements. Records must include any documents and information produced or obtained in complying with obligations under the PMLA, PMLFTR and any FIAU guidance and implementing procedures as set out in the Implementing Procedures – Part I. The said documents and information are to.

The said information and documentation is to be retained for five (5) years which start running from the end of the business relationship or the carrying out of an occasional transaction. The retention period of five years may be extended by the FIAU or other relevant supervisory authorities or law enforcement agencies where necessary for the purposes of the prevention, detection, analysis and investigation of ML/FT activities.

Upon the lapse of the applicable record-keeping period, the data, documents and information are no longer required to be maintained for AML/CFT purposes. The FIAU does not impose the deletion of such data, as the practitioner may be subject to other record-keeping obligations under any other applicable laws.

While in the case of customer due diligence, the requirements apply in a similar way to both accountants and auditors, a distinction must be made in the case of documentation retained in relation to transaction records which may vary depending on the service being provided.

The provision of audit services results in the collection of information and possibly of documentation on specific transactions and activities, constituting what are often referred to as audit working papers. The auditor is **not** required to collect and retain information on **all** transactions carried out by a customer but is only obliged to prepare documentation that provides a sufficient and appropriate record of the basis for the auditor's report and that provides evidence that the audit was planned and performed in accordance with the applicable audit standards. Neither does this mean that the practitioner has to retain a copy of the actual documentation received and forming part of the sample selected for audit testing purposes (e.g. invoices, agreements, etc.). The auditor is considered to have met his obligations if the information collected is sufficient for the proper and efficient identification of the transaction tested. By way of example, depending on the nature of the transaction being tested, this may include details such as invoice/agreement number, date, parties, amounts involved, etc.

Given that any transactions and/or activities so considered by the auditor would have already been carried out by the customer, the said practitioner cannot be considered as either being a party thereto or as somehow having facilitated their planning and/or execution. Thus, Regulation 13(1)(b) of the PMLFTR, which requires practitioners to retain "*supporting evidence and records necessary to reconstruct all transactions carried out by that person in the course of a business relationship or any occasional transaction, which shall include original documents or other copies admissible in court proceedings*;" cannot be considered as being applicable with respect to the retention of any such working papers.

This does not mean that there are no record retention obligations with respect to audit working papers but these can be aligned with what is required by audit standards. In line with auditing standards, this documentation is retained for a period from the date of the auditor's report. Locally, auditors generally align their retention period to the period prescribed in Article 163 of the Companies Act, which requires companies to keep their accounting records for a period of ten years. An auditor would therefore only dispose of the audit working papers after the 10-year period from the date when the audit report elapses. During this 10-year retention period, an auditor may be requested by the FIAU to provide information that is included in the audit working papers.

The above is without prejudice to situations where an internal report has been made to the MLRO or an STR is submitted to the FIAU, in which case the practitioner would need to retain a copy of the documentation that substantiates the reasons for reporting.

65C, Tower Street,
Birkirkara BKR 4012,
Malta

Questions on this document or on the application of AML/CFT measures may be sent to **queries@fiaumalta.org**

Financial Intelligence Analysis Unit
65C, Tower Street,
Birkirkara BKR 4012,
Malta

Telephone: (+356) 21 231 333
Fax: (+356) 21 231 090
E-mail: info@fiaumalta.org
Website: www.fiaumalta.org