

Published October 2022

---

# Provision of Directorship Services by Corporate Service Providers

Thematic Review 2020



# Table of Contents

1.	Scope of the Thematic Review	03
<hr/>		
2.	The Risk-Based Approach	04
2.1	The BRA	05
2.2	The CRA	08
<hr/>		
3.	CDD Measures	12
<hr/>		
4.	The Purpose and Intended Nature of the Business Relationship	14
4.1	The anticipated level and nature of activity (including the expected value and frequency of transactions) that is to be undertaken throughout the relationship	15
4.2	Enhanced Due Diligence - The Source of Wealth and Source of Funds	16
<hr/>		
5.	Ongoing Monitoring of the Business Relationship - Scrutiny of Transactions	21
<hr/>		
6.	Conclusion	26
<hr/>		
7.	Glossary	28

## CHAPTER 1 | SCOPE OF THEMATIC REVIEW

During the last quarter of 2020, the FIAU's Supervision Section carried out a thematic review on Corporate Service Providers' (CSPs) adherence to anti-money laundering and combatting the financing of terrorism (AML/CFT) obligations. These originate from the intervention of the Prevention of Money Laundering Act, the Prevention of Money Laundering and Funding of Terrorism Regulations (PMLFTR) and the FIAU's Implementing Procedures (IPs) when providing directorship services to their customers. The review covered 11 CSPs, and a total of 10 business relationships<sup>1</sup> per CSP were examined.

### THE OBJECTIVE

The thematic review was to understand how CSPs had structured their AML/CFT frameworks to assess and mitigate the inherent risk resulting from the provision of directorship services. The thematic review consisted of 11 examinations carried out remotely, which were designed to test CSPs' understanding of inherent risks encountered when providing directorship services, and the adequacy of the policies, procedures, controls, and measures applied to mitigate the identified risks. The AML/CFT compliance examinations consisted of:

- A review of CSPs' risk assessment of directorship services in the Business Risk Assessment (BRA);
- A review of the CSPs' risk assessment of directorship services within the context of the Customer Risk Assessment (CRA);
- Discussions with the MLROs and other key officials, where applicable, to gain an overview of the systems and process in place relating to the subject person's compliance with AML/CFT obligations;
- Sample-based testing on the practical application of controls in place, including measures to identify the purpose and intended nature of the business relationship; and
- A review of the transaction monitoring procedures adopted in respect of corporate customers to which directorship services were provided.

**11** Subject Persons reviewed

**10** Customer files per subject person reviewed

**110** Total of customer files reviewed

<sup>1</sup> That is, corporate customers to which directorship services were provided.

## CHAPTER 2 | THE RISK-BASED APPROACH

The risk-based approach has been a major development in the dynamic sphere of AML/CFT. Since its mandatory introduction, subject persons have been required to take appropriate steps, proportionate to the nature and size of their business, to identify the risks of Money Laundering and Funding of Terrorism (ML/FT) they are exposed to and address the same.

To effectively apply the risk-based approach, subject persons must understand their exposure to ML/FT risk. The initial step is to determine what is one’s inherent risk, i.e. one’s risk exposure prior to adopting and applying any measures, policies, controls, and procedures to mitigate the same. To this end, it is key to understand how risk may manifest itself or what are the threats and the vulnerabilities that may lead to the subject person being abused for ML/FT. This is then followed by an assessment of the likelihood and impact of the vulnerabilities and the threats manifesting themselves, which will determine the inherent risk. Once AML/CFT measures, policies, controls and procedures to mitigate inherent risk are applied, the residual risk can be determined to assess how effective the said measures, policies, controls and procedures are.

The residual risk should be determined irrespective of the subject person’s size. The assessment of one’s exposure to risk and ways how to mitigate this must reflect the subject person’s risk appetite and risk tolerance.

### Notions of Risk

Chart 1



## 2.1 | THE BRA

As the foundation of the risk-based approach, Regulation 5(1) of the PMLFTR requires subject persons to take appropriate steps, proportionate to the nature and size of their business to identify and assess the ML/FT risks that arise out of their activities. Through the BRA, subject persons are to consider how specific risk factors, including those relating to customers, geographical areas, products, services, transactions and delivery channels, may impact risk exposure. In so doing, consideration should be given to the national risk assessment (NRA) and supranational risk assessment (SNRA) relating to ML/FT risks. Both the NRA and the SNRA can provide important insights into how ML/FT risk can manifest itself for specific sectors and for the country at large.

Throughout the thematic review, it was positive to note that overall, subject persons had carried out and documented their BRAs and duly documented their assessment of their risk exposure. The exercise of assessing the inherent risks includes the evaluation of the complexity of the structures of corporate customers, and the jurisdictions they are connected to. This assessment needs to consider other risk factors which subject persons are exposed to, including other services offered by the subject person.

However, 46% of subject persons under review identified the inherent risks they were exposed to through the provision of directorship services. Subject persons should be aware of all the risks they are exposed to, especially prominent ones, such as when providing directorship services by way of business.



The IPs Part II for CSPs<sup>2</sup> identify the following key inherent risk drivers which subject persons are exposed to:

- A significant volume of high-risk customers;
- The services provided are risky in nature;
- High level of geographical risk;
- Large volume of international business handled by CSPs; and
- Higher service interface risk.



As part of a thorough analysis, subject persons must consider the specific controls put in place to address specific ML/FT risks and assess the same as thoroughly as possible. In this case, whilst 46% of subject persons under review identified general measures to mitigate their risk exposure, 54% of subject persons under review identified specific control measures to mitigate the risks specifically derived through the provision of directorship service.

**Subject persons are not only to identify the risks, but in accordance with the provisions set out in the IPs, they must identify the likelihood and impact of the risk manifesting itself and adopt commensurate measures.**

<sup>2</sup> The Implementing Procedures Part II for CSPs were issued by the FIAU on 16 December 2020, following the commencement of the thematic AML/CFT compliance examinations of CSPs. The IPs Part II of the CSPs can be accessed electronically through the following link: [https://fiaumalta.org/wp-content/uploads/2020/12/FIAU\\_IPs-Part2-CSPs-FINAL-Version.pdf](https://fiaumalta.org/wp-content/uploads/2020/12/FIAU_IPs-Part2-CSPs-FINAL-Version.pdf)

Most subject persons reviewed during the examination identified the risks emanating from the provisions of directorship services as low to medium risk of ML/FT. In respect of 55% of the BRAs reviewed, the FIAU concluded that the residual risk rating assigned to directorship services in the BRA was not calculated correctly when compared to the CSP's operations. The FIAU encourages subject persons to apply a more thorough approach when identifying and concluding the residual risk of their operations, which should be within the subject person's established risk appetite.

Identifying the risks associated with jurisdictions one has links to is a core component of a BRA. Jurisdictional risk exposure is determined through an analysis of jurisdictional connections, by identifying the risks applicable to each jurisdiction one has tangible connections to and by identifying and quantifying the number of customers connected to each country. The geographic connections should not be limited to nationality, which may not even be of any relevance in this context. Other factors to be considered, include, the place of incorporation, the customers' main place of business, and the main markets targeted by customers.



Whilst the requirement to identify connected jurisdictions is essential to recognise the geographical risks,

only

# 27%

of subject persons reviewed identified all relevant jurisdictional connections.

During the thematic review, it was noted that 55% of subject persons assessed the geographical connections of customers/beneficial owners in the BRA, by solely referring to a category without recording the specific jurisdictions in the document itself (for example, 'a non-Maltese European Union (EU) or European Economic Area (EEA) member state jurisdiction' and 'non-EU or non-EEA member state jurisdiction').

**It is essential that the BRA includes a granular assessment of the jurisdictions that the subject person is exposed to. This allows for a correct assessment of the ML/FT risks emanating from each of the jurisdictions connected to the business relationships. This is since not all countries present the same level and type of ML/FT risks and therefore, different control measures may be required.**

For further guidance and best practices on how to carry out the BRA satisfactorily, subject persons are encouraged to refer to section 3.3 of the IPs and the **Business Risk Assessment Paper** issued by the FIAU on 9<sup>th</sup> April 2021.<sup>3</sup>

<sup>3</sup> The Business Risk Assessment Paper can be accessed electronically through the following link: [https://fiaumalta.org/wp-content/uploads/2021/04/1178-FIAU-The-Business-Risk-Assessment-Document\\_DM\\_Working-File-V3-2.pdf](https://fiaumalta.org/wp-content/uploads/2021/04/1178-FIAU-The-Business-Risk-Assessment-Document_DM_Working-File-V3-2.pdf)

## 2.2 | THE CRA



Regulation 5(5)(a)(ii) of the PMLFTR requires the implementation of CRA procedures. This obligation is further explained in Section 3.5 of the IPs which states that the CRA is expected to be conducted prior to entering into a business relationship or carrying out an occasional transaction. This allow a subject person to be able to properly formulate the customers' risk profile. Through this process, a subject person should formulate its customer's overall risk rating to determine whether the customer falls within its risk appetite and the applicable level of Customer Due Diligence (CDD) to be applied to mitigate the risks posed by the customer.

Furthermore, given that risk is dynamic, it is important that in the case of a business relationship such as when one is providing directorship services, the CRA is reviewed from time to time, depending on the risk presented by the particular business relationship and especially, where there is an event marking a material departure from the known business and risk profile of the customer which may be noted through the ongoing monitoring of transactions.

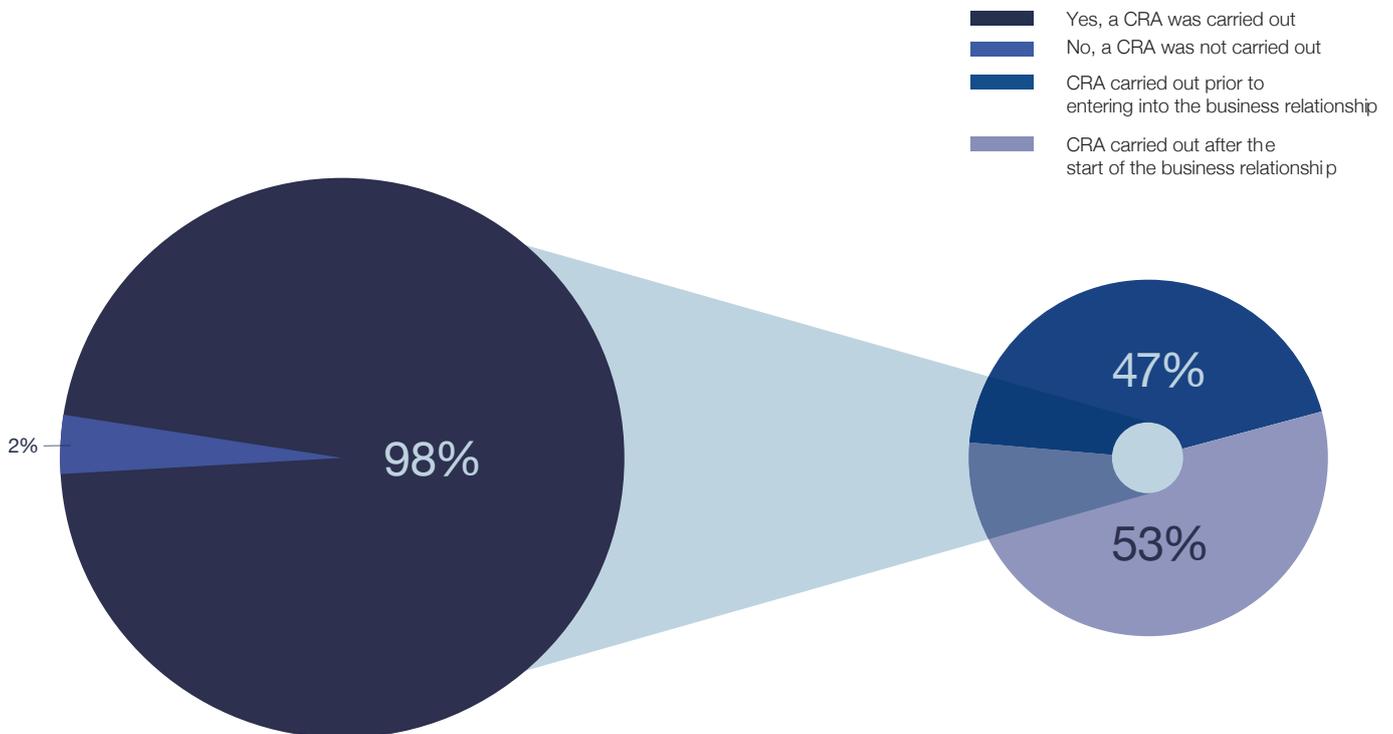
As stated in Section 3.5.2 of the IPs, the methodology behind the CRA, and any decisions related thereto, should be duly documented to evidence that an appropriate assessment has taken place. It is equally important that both the CRA and any updates thereof, be recorded and duly dated.

It was positive to note that all subject persons under review had CRA procedures in place. In fact, a CRA was carried out in respect of 98% of the files reviewed. However, only 47% of the CRAs were carried out prior to entering into the respective business relationships.<sup>4</sup>

<sup>4</sup>The file reviews all related to business relationships initiated after the requirement to compile a CRA came into force

## CRA Carried Out

Chart 2



Subject persons must ensure that all known risks they will be exposed to arising from the business relationship and/or where applicable, the occasional transaction offered, are assessed in the CRA to ensure they are mitigated accordingly, prior to the provision of services. The necessary level of CDD can then be applied as stipulated in the Customer Acceptance Policy and in a manner which effectively addresses the risks identified. Section 3.2.3 of the IPs states:

“ The product, service or transaction risk is the risk one is exposed to as a result of providing a given product or service or carrying out a particular transaction. ”

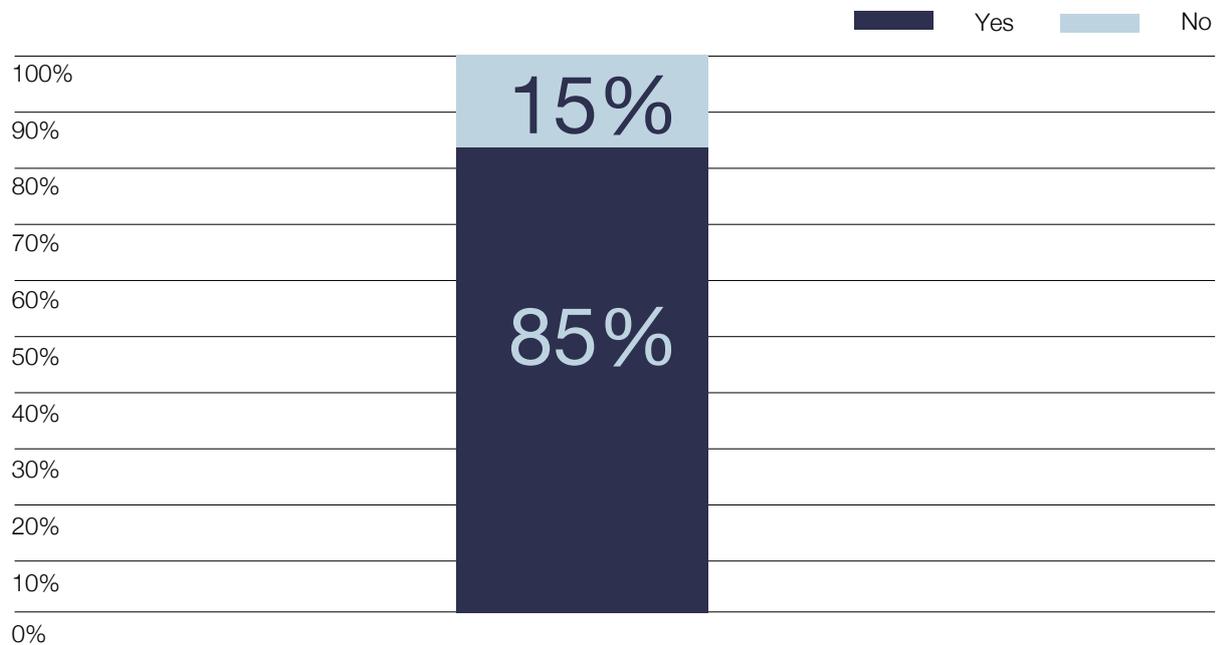
However, in some instances, it was observed that directorship services were not considered separately but rather were factored in under the umbrella of CSP services, therefore encompassing directorship services, company incorporation services, company secretarial services and registered address services.

**The FIAU stresses the importance of understanding and assessing each service provided, to be in a position to clearly identify the threats and vulnerabilities of each service and subsequently apply adequate and commensurate measures to mitigate the same.**

In this respect, it was positively noted that 85% of the subject persons reviewed specifically factored directorship services in their CRA methodology.

### Were Directorship Services Factored in the CRA?

Chart 3



Subject persons are also obliged to assess their customers' geographical connections and to understand whether such jurisdictions are considered non-reputable jurisdictions or are otherwise to be regarded as high-risk jurisdictions. Regulation 5(5) of the PMLFTR requires subject persons to have procedures in place to manage the ML/FT risks posed by their customers, products, services and transactions, delivery channels, and countries and geographical areas. The thematic review revealed that only 50% of the overall sample of files tested considered the geographical risk presented by the customer in the CRA.

Subject persons are reminded to include the geographical risk factor in their CRA, as this will determine the level of ML/FT risk posed by the customer from a geographical aspect. Geographical risk arises from links with one or more geographical areas, usually related to those jurisdictions:

- A Where the customer or its beneficial owner are based, have their main place of business or where the activity generating customer's or beneficial owner's wealth is carried out, and the jurisdictions with which the customer has particularly strong trading or financial connections; and/or;
- B With which the customer or its beneficial owner have relevant personal links (for example the individual's residence in a specific jurisdiction).

Among other things, the CRA needs to include the identification of risks posed by a business relationship or where applicable, an occasional transaction established or carried out with a natural or legal person from a particular jurisdiction, particularly those considered to pose a higher risk of ML/FT.

## Best Practice

- 

From the review, it was positive to note that in most cases, the risks pertaining to directorship services were assessed on their own and not simply under the umbrella of CSP services.
- 

In one instance, the subject person implemented the assessment of the directorship services into different categories, such as whether the customer was requesting directorship services as the sole service, whether the customer was requesting directorship services combined with company secretarial services and whether the customer was requesting directorship services in conjunction with bank signatory services. As detailed above, considering each service in isolation, assists in identifying the threats and vulnerabilities of each service and will allow the application of adequate and commensurate measures to mitigate the services.

## Bad Practice

- 

Directorship services were sometimes factored in under the wrong risk factor, in that, instead of being factored under product/service risk, they were factored under customer risk, which may have impacted the overall risk score of the business relationship, as the scores allocated to customer risk and product and service could vary.

## CHAPTER 3 | CDD MEASURES

### IDENTIFICATION AND VERIFICATION

The requirement to apply CDD measures ensures that subject persons have adequate mechanisms in place to:

- Determine who the customers, and beneficial owners are;
- Verify whether the customer is the person they purport to be;
- Determine whether the customer is acting on their own behalf, or on behalf of another person or legal entity;
- Establish the purpose and intended nature of the business relationship, and the customer's business and risk profile; and
- In the case of a business relationship, monitor that relationship on an ongoing basis and keep information, documents and data held on the customer up to date.

Along with the CRA, the CDD measures adopted assist the subject person in determining whether the customer falls within the subject person's risk appetite. It is good to note that in line with Regulation 7(1)(a) and 7(1)(b) of the PMLFTR,

for over

# 95%

of the files reviewed, subject persons had identified and verified both the customers and their beneficial owners.<sup>5</sup>

While it is important that information and documentation to establish and verify the identity of the customer and the beneficial owner is obtained prior to entering a business relationship, it is equally important that said information and documentation is kept current and updated. Hence the importance of Regulation 7(1)(d) and of Regulation 7(2)(b). This is especially the case where there are changes within a corporate customer's structure (e.g. a share transfer or the allotment of new shares) that may denote a change in beneficial ownership.

Subject persons are reminded to ensure that data, information and documentation obtained as part of the CDD process are kept up to date, especially whenever there are changes in the involved parties of a particular corporate customer (e.g. changes in shareholders or beneficial owners).

<sup>5</sup> This finding is similar to what was noted in the Beneficial Ownership Thematic review which was carried out during 2021. The 'Compliance with Beneficial Ownership obligations by CSPs' can be accessed in the following link: <https://fiaumalta.org/wp-content/uploads/2022/04/Compliance-With-beneficial-Ownership-Obligations-by-CSPs.pdf>



Furthermore, although this obligation was not within the scope of the thematic review and therefore was not tested, it is important to note that the second proviso of Regulation 7(1)(a) of the PMLFTR<sup>6</sup> obliges subject persons to obtain proof that beneficial ownership information has been duly registered with a designated beneficial ownership register. This holds true whether the customer is a body corporate, a body of persons or any other form of legal entity incorporated in an EEA Member State or a trust or similar legal arrangement administered in an EEA Member State. Thus, subject persons are required to obtain proof that information regarding the beneficial owner(s) and/or the natural person(s) exercising control of the customer has been duly registered. Subject persons are to ensure that beneficial owners are identified, and their characteristics must be considered for risk assessment purposes. Customers who seek to utilise corporate services in an adverse manner, such as to hide their identity will heighten the risk of the subject person.

For further guidance on beneficial ownership obligations, subject persons are encouraged to refer to the **‘Compliance with Beneficial Ownership obligations by Company Service Providers’** Paper issued by the FIAU on 30<sup>th</sup> March 2022.<sup>7</sup>

<sup>6</sup>. Introduced by Legal Notice 26 of 2020.

<sup>7</sup>. The Compliance with Beneficial Ownership obligations by Company Service Provider can be accessed electronically on the following link: <https://fiaumalta.org/wp-content/uploads/2022/04/Compliance-With-beneficial-Ownership-Obligations-by-CSPs.pdf>

## CHAPTER 4 | THE PURPOSE AND INTENDED NATURE OF THE BUSINESS RELATIONSHIP

The requirement to understand and, as appropriate obtain information on the purpose and intended nature of the business relationship is highlighted in Section 4.4 of the IPs and Regulation 7(1)(c) of the PMLFTR. The outcome of the CRA conditions the extent of the information and the level of detail which is required on the purpose and intended nature of the business relationship. It also influences the extent of documentation required (hence requested) to substantiate the information provided by the customer.

Subject persons need to understand why a customer is requesting their services and/or products and how those services and/or products are expected to be used throughout the business relationship. Sufficient information obtained during the commencement of the business relationship also serves as a good basis to carry out appropriate monitoring, as well as to determine that the product or service requested makes sense when compared to the customer’s profile.

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

It was positive to note that

**86%**

of the subject persons under review obtained information and/or documentation on the purpose and intended nature of the business relationship.

For the remaining 13% of subject persons, the information and/or documentation on the purpose and intended nature of the business relationship was not obtained and/or was considered as insufficient.<sup>8</sup>



<sup>8</sup> By limiting to obtaining the Memorandum and Articles of Association

## 4.1 | THE ANTICIPATED LEVEL AND NATURE OF ACTIVITY (INCLUDING THE EXPECTED VALUE AND FREQUENCY OF TRANSACTIONS) THAT IS TO BE UNDERTAKEN THROUGHOUT THE RELATIONSHIP

The FIAU noted that most subject persons obtained information on the anticipated level and nature of the activity to be undertaken throughout the business relationship. In fact, the information of the anticipated level and nature of activity that was to be undertaken throughout the respective business relationships was not obtained in only 14% of the files reviewed. As a result of this, subject persons were not able to build a customer risk profile which could assist the subject persons to fully understand the business relationship.



All the subject persons selected for this thematic review offered directorship services, which are considered as business relationships. Therefore, in line with Section 4.5 of the IPs Part I and Section 2.4 of the IPs Part II for Customer Services Providers (IPs Part II) ongoing monitoring is expected to take place for the business relationships. When providing directorship services, subject persons need to obtain information on the nature and the anticipated level of the activity that is to be undertaken during the relationship. This should include the type of activity being carried out, the expected volume of transactional activity, projected turnover and proposed suppliers and customers to understand the eventual source of funds flowing through the customer company. Furthermore, this information is necessary for the subject person to be able to formulate an understanding of the typical transactional activity expected from the customer. This understanding is crucial for the carrying out of effective ongoing monitoring of the customer's activities and transactions.

## 4.2 | ENHANCED DUE DILIGENCE - THE SOURCE OF WEALTH AND SOURCE OF FUNDS

It resulted that out of the 98% of customers for whom a CRA was carried out, almost 25% were rated by the CSPs as presenting a high risk of ML/FT. In terms of Regulation 11(1)(b) of the PMLFTR, subject persons are required to apply enhanced due diligence (EDD) measures when servicing a business relationship or carrying out an occasional transaction that is considered to present a high risk of ML/FT. Therefore, in addition to the CDD requirements as laid down under Regulation 7 of the PMLFTR, subject persons must also apply additional measures to mitigate the high risk of ML/FT.

As per the IPs, a subject person is to collect information on a customer's source of wealth and expected source of funds at the outset of a business relationship. Subject to what is set out in Section 3.6 of the IPs, this information serves to assist the subject person to further understand the actual ML/FT risk it is exposed to, especially when it comes to the customer risk factor. The source of wealth is identified at the beginning of the business relationship, with the necessity to update this information throughout. On the other hand subject persons are required to identify and obtain information on the source of funds of

individual transactions when necessary, in accordance with the obligation of ongoing monitoring.

The nature of the relationship and the risk allocated to it determine the level of information and/or documentation to be collected with regards to the source of wealth and funds of the customer. In a low-risk scenario, the subject persons may limit the amount of information gathered and verified. However, in higher risk situations, it is pertinent for subject persons to be more rigorous and they should not just rely on the information provided by the customer. The CSP needs to take additional measures to ensure that such information is representative of the transaction or business relationship. Consequently, subject persons should take necessary measures in line with the risk allocated, to establish the source of wealth and source of funds of the customer and/or beneficial owner (where applicable).

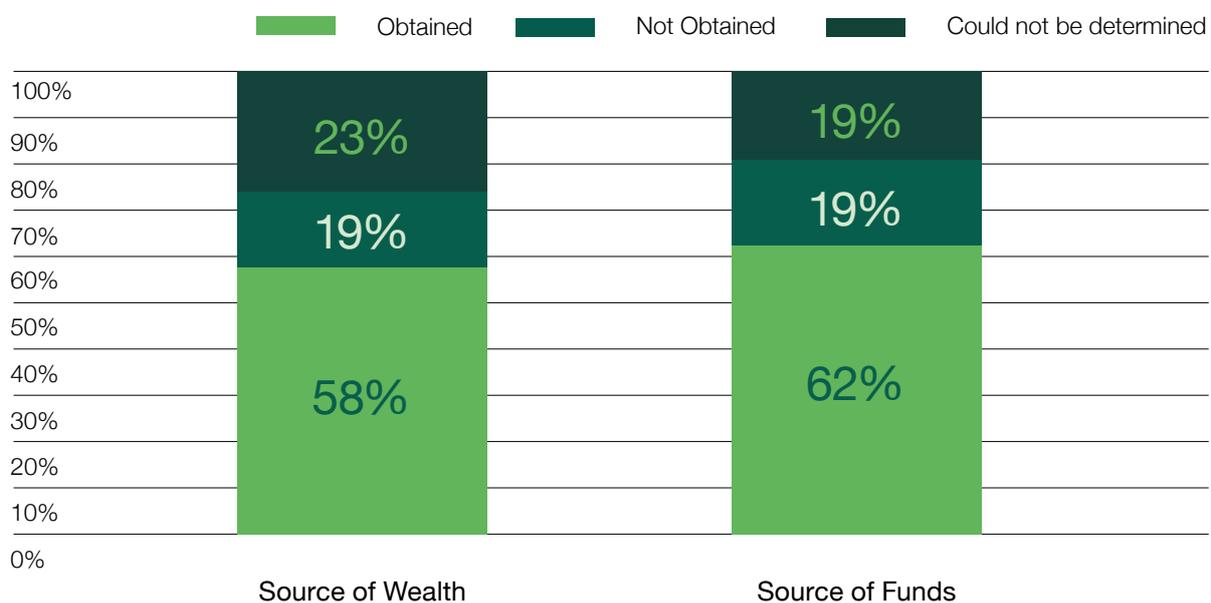
The thematic review revealed that EDD was not applied in some cases, and on other occasions not applied in line with the heightened risk of the customer business relationship. The latter was observed in 19% of the cases in relation to the source of wealth and source of funds.

It was also noted that for the high-risk business relationships tested, subject persons sought information on the source of wealth (in 58% of the high-risk files reviewed) and source of funds (in 62% of the high-risk files reviewed) of all their customers/beneficial owners during the on-boarding process.

In 12% of high-risk business relationships reviewed, the information and documentation on the source of wealth and source of funds was obtained between two years to six years following the commencement of the business relationship. Furthermore, in 23% (for source of wealth) and 19% (for source of funds) of the high-risk business relationships, the FIAU could not determine whether the information and documentation on the source of wealth and source of funds was obtained during the on-boarding process or post-onboarding.

### Information Sought on the SoW and SoF on High Risk Customers

Chart 4



Following the collection of information on the source of wealth and source of funds of the customer, the subject person needs to determine the extent to which that information must be corroborated by any further information and/or official documentation. This may be obtained both from the customer and/or reliable external sources. This will allow the subject person to understand whether the funds used for the customer’s operations are legitimate and that the company is not being used for the purpose of ML/FT. Where the collection of this information is deemed relevant, subject persons must not limit themselves to obtaining information of a generic nature, the mere reference to ‘business’, ‘employment’ or ‘inheritance’ will never be deemed sufficient to meet this obligation, independently of the risk presented. Information and documentation to corroborate the customer’s source of wealth and source of funds can be obtained from a variety of sources.

The table below highlights sources which may be referred to in order to corroborate source of wealth and source of funds:

<p><b>Customer sourced information</b></p>	<ul style="list-style-type: none"> <li>• Tax declarations</li> <li>• Bank statements</li> <li>• Payslips</li> <li>• Dividend warrants</li> <li>• Declaration causa mortis</li> <li>• Audited financial statements</li> </ul>
<p><b>Third party sourced information</b></p>	<p>Information obtained from professionals such as legal or accountancy professionals or entities/persons undertaking relevant financial business or equivalent activities in reputable jurisdictions, etc.</p>
<p><b>Open-source information</b></p>	<p>Open-source internet searches and access to constitutive documents from companies' registries such as the Malta Business Registry or equivalent body.</p>

Where the customer is a body corporate, subject persons must establish the source of wealth of the customer. In situations where the customer is a trading company and has developed its commercial activities, the source of wealth needs to be determined through obtaining information on the nature and extent of these commercial activities, supported by audited financial statements. This would be sufficient to satisfy the obligation to establish a customer's source of wealth, so long as the financial statements attest to a sound financial situation resulting from the company's turnover generated from the carrying out of its own activities.

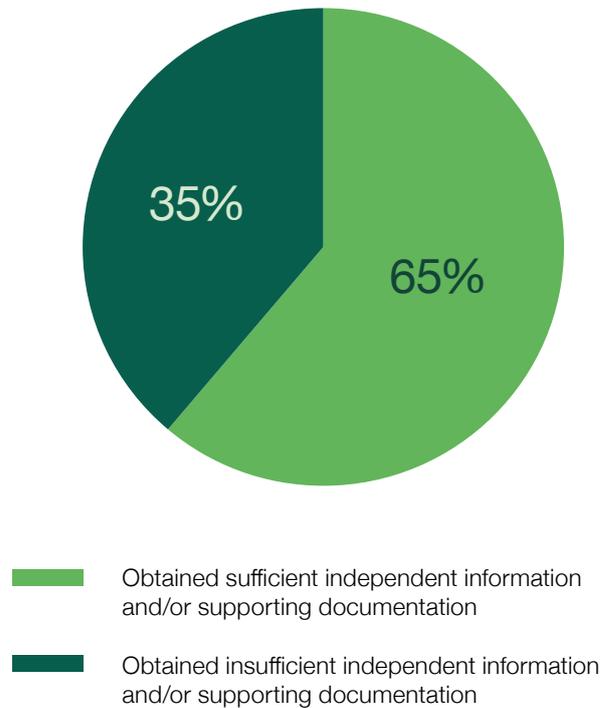


**‘The Guidance note: on obtaining source of wealth information related to parties other than the customer’** issued by the FIAU in July 2022,<sup>9</sup> elaborates further on scenarios where the subject person is required to obtain the source of wealth information in relation to the customer and to parties other than the customer.

It was noted that in 65% of the high-risk business relationships, the subject persons reviewed have sought to obtain independent documentation on their customers’ source of wealth and source of funds. For the remaining 35% of high-risk business relationships, the FIAU identified issues relating to insufficient supporting documentation. It was also observed that there were instances where subject persons relied too heavily on open-source information to corroborate the customer’s source of wealth and source of funds information. Although subject persons may refer to open-source information as an additional measure for high-risk business relationships, it cannot be the only source of information relied upon, sufficient documentation from other sources should also be retained on file.

### Independent Documentation on The Customers’ SoW and SoF Obtained

Chart 5



<sup>9</sup> The Guidance Note can be accessed electronically through the following link: <https://fiaumalta.org/wp-content/uploads/2022/07/Guidance-Note-On-obtaining-Source-of-Wealth-Information-related-to-Parties-other-than-the-Customer.pdf>

## Best Practice

The below instances are examples of good practices regarding information and/or documentation that need to be requested to corroborate the information provided by the customer:



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



The beneficial owner of the customer company indicated, amongst other factors, that he is the beneficial owner of a number of entities, holds investments in several entities and was a director of numerous listed entities. To corroborate this information, the subject person collected various documents such as an overview of the customer company, financial statements and annual returns for a number of entities where the beneficial owner acts as a director. A letter from the beneficial owner's warranted accountant from a reputable jurisdiction was also obtained and was substantiated with supporting documentation. This letter confirmed that the beneficial owner had net assets in his personal name, that he was a member of a company whereby he received a fixed priority profit share, was paid additional/bonus profit share and that he received significant carried interest and co-investment distributions. The subject person also collected additional information of investment portfolios which accounted for proceeds generated from monetary donations given by a family member of the beneficial owner.

## Bad Practice



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



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

## CHAPTER 5 | ONGOING MONITORING OF THE BUSINESS RELATIONSHIP - SCRUTINY OF TRANSACTIONS

Subject persons who provide directorship services are expected to carry out ongoing monitoring of the business relationship. Section 4.5 of the IPs requires subject persons to scrutinise transactions through transaction monitoring by using the information gathered on the purpose and intended nature of the business relationship and the customer's business and risk profile to identify any transactions that are unusual.

As described in the IPs Part II for CSPs, by carrying out effective ongoing monitoring and effective scrutiny of transactions, the subject person will be able to:

- Identify transactions and/or activities that are not in line with the corporate customer's operations and business;
- Identify unusual/dubious transactions or activities, and generate internal reports; and
- Communicate suspicions or knowledge of ML/FT or proceeds of crime to the FIAU in a timely manner.

Effective on-going monitoring and scrutiny of transactions is also a key element to ensure that the subject person's risk understanding of its customers is kept current and updated as it may reveal changes from the known business and risk profile.

Scrutinising transactions is vital to ensuring the effectiveness of ongoing monitoring. Moreover, it must be seen as an integral part of effectively ensuring the required AML/CFT systems and controls are in place while the extent of the scrutiny as well as information and documentation to be gathered will vary according to the ML/FT risks connected with that specific business relationship.

Furthermore, transaction monitoring does not necessarily require sophisticated electronic systems. The scope and complexity of the process will be mainly influenced by the subject person's business activities and size. The key fundamental of any transaction monitoring system or process is to ensure that information is kept up to date. Through this, the system or process implemented will make it easier to detect unusual activities and serve to prompt one to gather information as to why such unusual transactions or activities are carried out. The subject person may then flag the divergence as suspicious or may utilise it to form a better judgement of the relationship and the services offered.

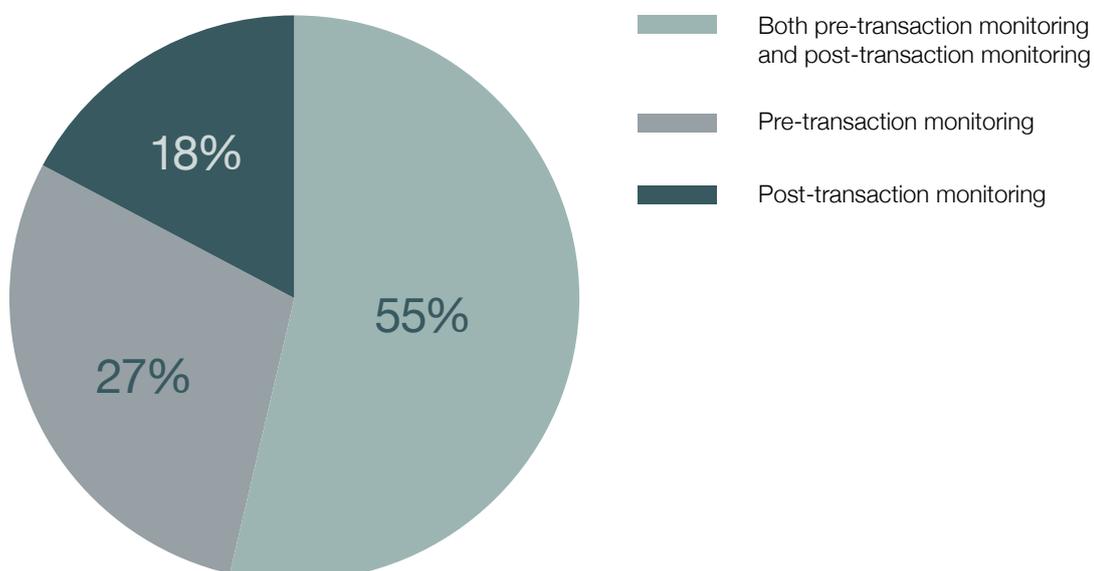
The FIAU acknowledges that most of the subject persons reviewed had established policies and procedures on how to carry out transaction monitoring. In fact, most of the subject persons (82%) incorporate transaction monitoring processes in their respective policies and procedures. It was noted that subject persons effectively carried out monitoring of transactions and controlled the provision of service overall through various methods, such as:

- By attending board meetings, where major investments decisions are taken by approving payments during the meetings;
- Obtaining invoices, loan agreements, relative agreements and supporting documentation related to specific transactions;
- Via the approval of banking transactions (when the subject person is the signatory on the bank account/s);
- By obtaining copies of board resolutions which explain the rationale of specific transactions;
- By obtaining contracts of employment; and
- By obtaining the source of funds to support the transaction and any other information that is reasonably necessary to identify that the funds are derived from legitimate sources.

Transaction monitoring can take place in several ways. Transactions may be monitored in real time (pre-transaction monitoring), after the event (post-transaction monitoring) and on the basis of a customer’s specific profile. 55% of the subject persons under review adopted both pre-transaction monitoring and post-transaction monitoring, while 27% only adopted pre-transaction monitoring and the remaining 18% only adopted post-transaction monitoring.

### Transaction Monitoring

Chart 6



Section 2.4.4 of the IPs Part II for CSPs, requires directors who are legal representatives of the corporate entity (solely or jointly) or are granted representation powers (e.g., through a Power of Attorney or Directors' Resolutions) and are responsible for approving payments or undertaking transactions (e.g., signing contracts) to monitor transactions or payments prior to their execution (pre-transaction) in order to ensure that they are in line with the customer company's expected business activities. Furthermore, the CSP should request supporting documentation and information when this is not clear and necessitates further scrutiny to ascertain the purpose and nature of the transaction or payment and, where appropriate, the source of funds.

The FIAU is aware that subject persons acting as directors are not able to carry out pre-transaction monitoring in all instances, for example, where CSPs act as directors in a company where the legal representation

or other powers to bind the corporate customer are vested in different directors acting individually. In such a scenario, the legal representation or binding powers may be exercised by other directors or individuals without that CSP's involvement. In such cases, subject persons should adopt post-transaction monitoring, by periodically requesting information on transactions, contracts or payments undertaken by the customer company to determine whether these are in line with the customer company's known activity. The subject person must determine the best approach towards keeping information up to date, and base this on several factors relating to the subject person itself - such as size, number of customers, type of services offered, resources, and the customer base - such as the risk rating, range of products/services offered, among other considerations. The methods adopted may also vary to better address the circumstances presented by different customer groups or services.



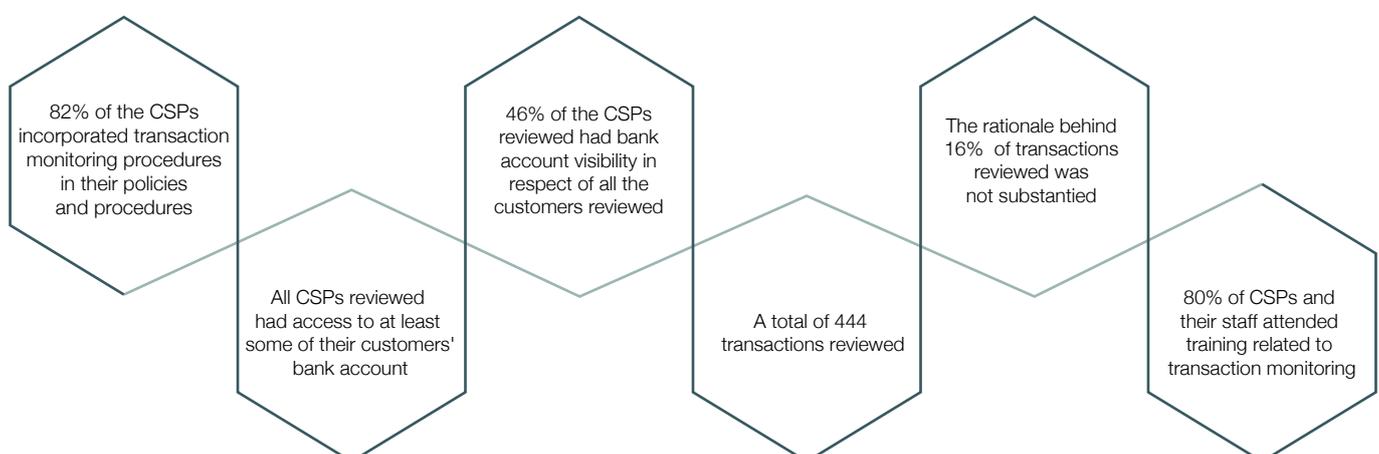
All of the subject persons reviewed had access to at least some of their customer’s bank accounts, and 46% of subject persons reviewed had bank account visibility in all the customer files reviewed. The FIAU acknowledges that directors who act as signatories on a bank account may still be exposed to an element of ML/FT risk. Section 2.4.4 of the IPs Part II for CSPs further explains that good practice in this regard is to have measures in place to monitor and scrutinise the transactions being undertaken through the client’s accounts, to understand their nature and purpose, and to ensure that they are in line with the customers’ business activities and the expected use of the customers’ account.

The thematic review also included a review of the subject person’s scrutiny of the transactions effected by their customers. Out of a total of 444 transactions examined, the FIAU identified that in 70 transactions (16%), the subject persons did not flag the transaction and as a result no documentation to substantiate the rationale behind the transactions was obtained. This deficiency was noted in 3 out of 11 subject persons reviewed. Despite this when considered holistically, the indication is clear that most subject persons were found to carry out effective transaction monitoring.

It was also noted that over 80% of subject persons and their staff attended training related to transaction monitoring during the past three years. The FIAU highlights the importance for subject persons to attend relevant training regularly. This will ensure that the subject person’s personnel are aware of the relevant AML/CFT legislation, AML/CFT measures, policies, controls and procedures as well as of the main ML/FT risks to which the activities carried out are exposed to. Subject persons are required to provide training in relation to the recognition and handling of operations and transactions that may indicate proceeds of criminal activity or ML/FT. By way of example, compliance staff members who are responsible for carrying out transaction monitoring need to be provided with detailed and regular training to enable them to detect unusual and/or suspicious transactions, behaviour, and ML/FT trends as these evolve over time. A training program which educates in the identification of unusual transactions and high-risk situations as applicable to the subject person is critical to the success and effectiveness of a subject person’s efforts at combatting ML/FT.

## Transactions Reviewed

Chart 7



## Best Practice

-  Through manual transaction monitoring, one of the subject persons under review obtained information and, where necessary, documentation in a systematic and organised manner. When information and documentation in relation to a sample of transactions was requested, the subject person was able to provide the FIAU with sufficient information to substantiate the relationship between the transferee and transferor, the purpose of the transaction and the source of funds.
-  Certain subject persons ensure that they always have visibility or access to the customers' bank accounts. This is done by having direct access to their customers' bank account or by requesting monthly statements.
-  Through compliance examinations, the FIAU has also come across cases where the subject person acts as signatory on bank accounts and signs off on every banking transaction.

## Bad Practice

-  A deposit made by the beneficial owner was treated as a shareholder's loan. The subject person obtained a copy of the bank transfer order made by the beneficial owner to affect the transfer but did not request a copy of the shareholder's loan agreement to thoroughly substantiate the source of funds of the transaction. This transaction was not in line with the anticipated nature of the business relationship and therefore more information was required at the time of the transaction.
-  In another file reviewed, the total amount of a particular outward payment did not tally with the invoice obtained to justify the transaction. In such a scenario, the subject person was expected to obtain an explanation on the discrepancy in the values of the transaction and the relative invoice.
-  The subject person explained that several outward transactions were loan repayments made by the subsidiary of the customer company to the beneficial owner. Nonetheless, the subject person was required to substantiate these transactions by obtaining supporting documentation such as the loan agreement which would include repayment terms.
-  For an inward payment relating to a shareholder's loan, the subject person retained a loan agreement which did not correspond with all the details of the transaction highlighted, such as the amount and the expected repayment date.

## CHAPTER 6 | CONCLUSION

Throughout the thematic review, it was positive to note that subject persons are generally aware of their obligations and the importance of having a sound AML/CFT control framework to mitigate the risks arising from the provision of directorship services.

The FIAU expects that all CSPs and their MLROs go through this document and familiarise themselves with the findings, and implement any updates, if necessary, to their internal controls to ensure that they do not incur weaknesses reported in this paper.

The thematic review revealed minor to moderate deficiencies in the compliance programme of six CSPs, because of which the FIAU required these CSPs to

remediate these deficiencies within a given time frame. In the case of another two CSPs, serious potential breaches of AML/CFT obligations were identified, and have resulted or may result in the imposition of more dissuasive administrative measures.

For the remaining three CSPs, only minor shortcomings were observed, and these examinations ended with the issuance of a closure letter.



## KEY OBSERVATIONS

BRAs were carried out and the assessment of their risk exposure was duly documented.

46% of subject persons under review identified the inherent risks they were exposed to through the provision of directorship services.

54% of subject persons under review identified specific control measures to mitigate the risks specifically derived through the provision of directorship service.

27% of subject persons under review identified all relevant jurisdictional connections in their BRA.

All subject persons under review had CRA procedures in place. In fact, a CRA was carried out in respect of 98% of the files reviewed.

Only 47% of the CRAs were carried out prior to entering the respective business relationships.

85% of the subject persons reviewed specifically factored directorship services in their CRA methodology.

50% of the overall sample of files tested considered the geographical risk presented by the customer in the CRA.

In over 95% of the files reviewed, subject persons had identified and verified both the customers and their beneficial owners.

86% of the subject persons obtained information and/or documentation on the purpose and intended nature of the business relationship.

Most subject persons obtained information on the anticipated level and nature of the activity to be undertaken throughout the business relationship.

For the high-risk business relationships tested, subject persons sought information on the source of wealth (58%) and source of funds (62%) of all their customers/beneficial owners during the on-boarding process.

In 65% of high-risk business relationships, the subject persons reviewed sought to obtain independent documentation on their customers' source of wealth and source of funds.

Most of the subject persons reviewed had established policies and procedures on how to carry out transaction monitoring. In fact, 82% of the subject persons reviewed incorporate transaction monitoring processes in their respective policies and procedures.

Subject persons had effectively carried out monitoring of transactions.

All the subject persons reviewed had access to at least some of their customer's bank accounts.

Over 80% of subject persons and their staff attended training related to transaction monitoring.

# Glossary

---

AML/CFT	Anti-Money Laundering and Counter Funding of Terrorism
BRA	Business Risk Assessment
CDD	Customer Due Diligence
CRA	Customer Risk Assessment
CSP	Customer Service Provider
EDD	Enhanced Due Diligence
EEA	European Economic Area
EU	European Union
PMLFTR	Prevention of Money Laundering and Funding of Terrorism Regulations
IPs	Implementing Procedures Part I
IPs Part II	Implementing Procedures Part II for Corporate Service Providers
NRA	National Risk Assessment
ML/FT	Money Laundering and Funding of Terrorism
SNRA	Supranational Risk Assessment

---

© Financial Intelligence Analysis Unit, 2022

Questions on this document or on the application of AML/CFT measures may be sent to [queries@fiaumalta.org](mailto:queries@fiaumalta.org)

Reproduction is permitted provided the source is acknowledged.

**Telephone:** (+356) 21 231 333

**E-mail:** [info@fiaumalta.org](mailto:info@fiaumalta.org)

**Website:** [www.fiaumalta.org](http://www.fiaumalta.org)