FIAU Financial Intelligence Analysis Unit Malta

MFSA Malta Financial Services Authority

Application of Simplified Due Diligence by Collective Investment Schemes

Practical guidance on dealing with Customers Carrying out Relevant Financial Business

Thematic Review 2023

Published December 2025

Table Of Contents

Glossary

AML/CFT	Anti-Money Laundering and Counter Funding of Terrorism
CDD	Customer Due Diligence
CIS/CISs	Collective Investment Scheme/Collective Investment Schemes
CRA	Customer Risk Assessment
EU	European Union
FIAU	Financial Intelligence Analysis Unit Malta
IPs	Implementing Procedures Part I
MFSA	Malta Financial Services Authority
ML/FT	Money Laundering and Funding of Terrorism
MLRO	Money Laundering Reporting Officer
PMLA	Prevention of Money Laundering Act
PMLFTR	Prevention of Money Laundering and Funding of Terrorism Regulations
SDD	Simplified Due Diligence
SoF	Source of Funds
SoW	Source of Wealth

1. Executive Summary

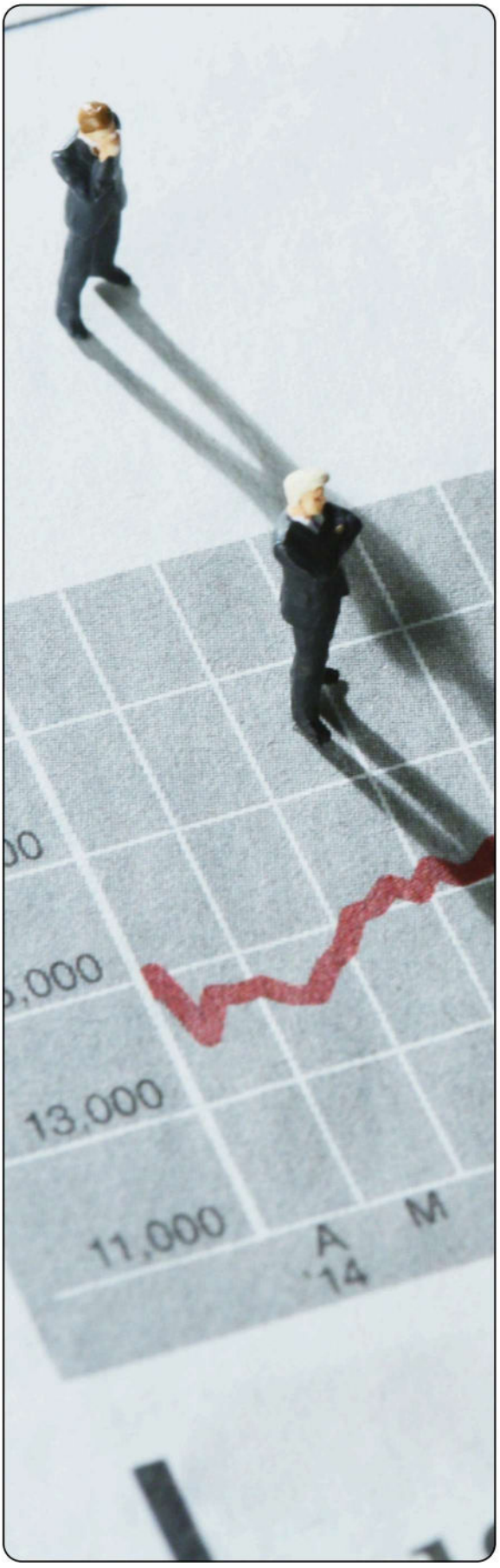
During the last quarter of 2023 the FIAU's Supervision Section in collaboration with the Malta Financial Services Authority (MFSA) conducted a thematic review on the Collective Investment Schemes (CISs) sector focused on dealing with customers providing relevant financial business, be it when the customers are investing on their own behalf or when they invest on behalf of underlying investors.

The thematic exercise indicated that the majority of CISs follow robust practices in obtaining the necessary information and documentation for customers. Furthermore, it was observed that most CISs have established procedures to collect data aimed at developing comprehensive business and risk profiles of their regulated customers. However, two main issues were identified: first, the challenge in obtaining information that can assist in having an understanding of what level of activity can be expected by the regulated customer; and second, the extent of information gathered to understand the nature of the business conducted by these customers. This includes having a clear understanding of the scope of services and products offered by the regulated entity, as well as gaining a broad understanding of its customer base, including main customer categories and key geographical markets. A complete assessment of all these elements is crucial in determining the level of ML/TF risk the customer presents and whether applying Simplified Due Diligence (SDD) is appropriate. It is crucial to remember that not all customers carrying out relevant financial business pose by default a low risk of ML/FT. Maintaining continuous awareness is essential, and consistent ongoing monitoring ensures that no higher-risk indicators are present.

Furthermore, the thematic review highlighted a recurring weakness in documenting the customer risk assessments and transaction monitoring. Several CISs were observed to justify significant changes in transaction patterns or large transactions as 'expected' due to the entity's size or profile, often without conducting a sufficient analysis. Effective transaction monitoring requires a thorough comparison of transactional behaviour with a well-established and dynamic customer profile. CISs should avoid treating large transactions as self-explanatory or assuming that smaller transactions are automatically insignificant.

While the thematic review generally highlighted a good level of compliance by CISs with SDD and related obligations, improvements are recommended to ensure that risk assessment and ongoing monitoring procedures are properly implemented and that any higher-risk indicators are not dismissed on the assumption that SDD should automatically be applied to customers conducting relevant financial business.

CISs are encouraged to consult the relevant sections of this document for a deeper understanding of the thematic review's findings, key takeaways and recommendations for improvement. The analysis in this document is based on the obligations as they currently result from the PMLFTR and the Implementing Procedures. CISs are encouraged to stay informed about any changes that could affect their AML/CFT obligations, particularly those arising from the implementation of the AML Package.



2. Scope of the Thematic Review

The CISs sector holds significant importance within Malta's financial services landscape. Consistent application of ML/FT safeguards is crucial, given the sector's size, complexity, and links with European and global markets.

In this context, the FIAU, in collaboration with the MFSA, conducted a thematic review on the CISs sector in the last quarter of 2023. The thematic review focused on the adoption of SDD measures and the accompanying transaction monitoring practices of CISs, particularly in respect of customers that are regulated entities conducting relevant financial business either investing monies on their own behalf, or as nominees on behalf of underlying investors. The review also examined related policies and procedures, as well as the Customer Risk Assessment (CRA) process, focusing on how CISs evaluated their customers' business and risk profiles and classified customers as low risk for ML/FT.

3. Methodology

The thematic review focused on **20 CISs**[1], particularly those serving clients that are regulated entities, such as credit or financial institutions and have adopted SDD measures. The thematic review consisted of interviews with the Money Laundering Reporting Officer (MLRO) of each CIS and the review and analysis of 124 client files[2] and 97 transactions.

[1] 11 Professional Investor Funds, 5 Alternative Investment Funds, 4 Retail.

[2] The number of customer files reviewed per CIS varied depending on the size of the CIS.

Table 1 - *Transactions selected*[3] *for review:*

Unusually large transaction (compared with the business profile)	44
One-time transactions	12
Transaction in - out in a short timeframe	10
Most recent transaction/Last redemption	9
Initial subscription / transfer	6
Random selection	6
Transfer to 3rd parties	3
Subscription in kind	2
Transfer in from a fund of a different customer	1
Transaction not in line with customer's profile	1
Multiple subscriptions on the same day	1
Transfer after two years of inactivity	1
Switch in transfer between funds of the same customer	1

[3] The sample was selected to ensure broad coverage of all transaction types carried out by the customers under review

As shown in the customer sample selection charts below, the FIAU aimed to choose a representative sample of CIS-regulated customers, considering factors such as the customer's authorisation type[4], business relationship status and the latest customer's risk[5] rating .

Chart 1 - *CISs' customers authorisation category*

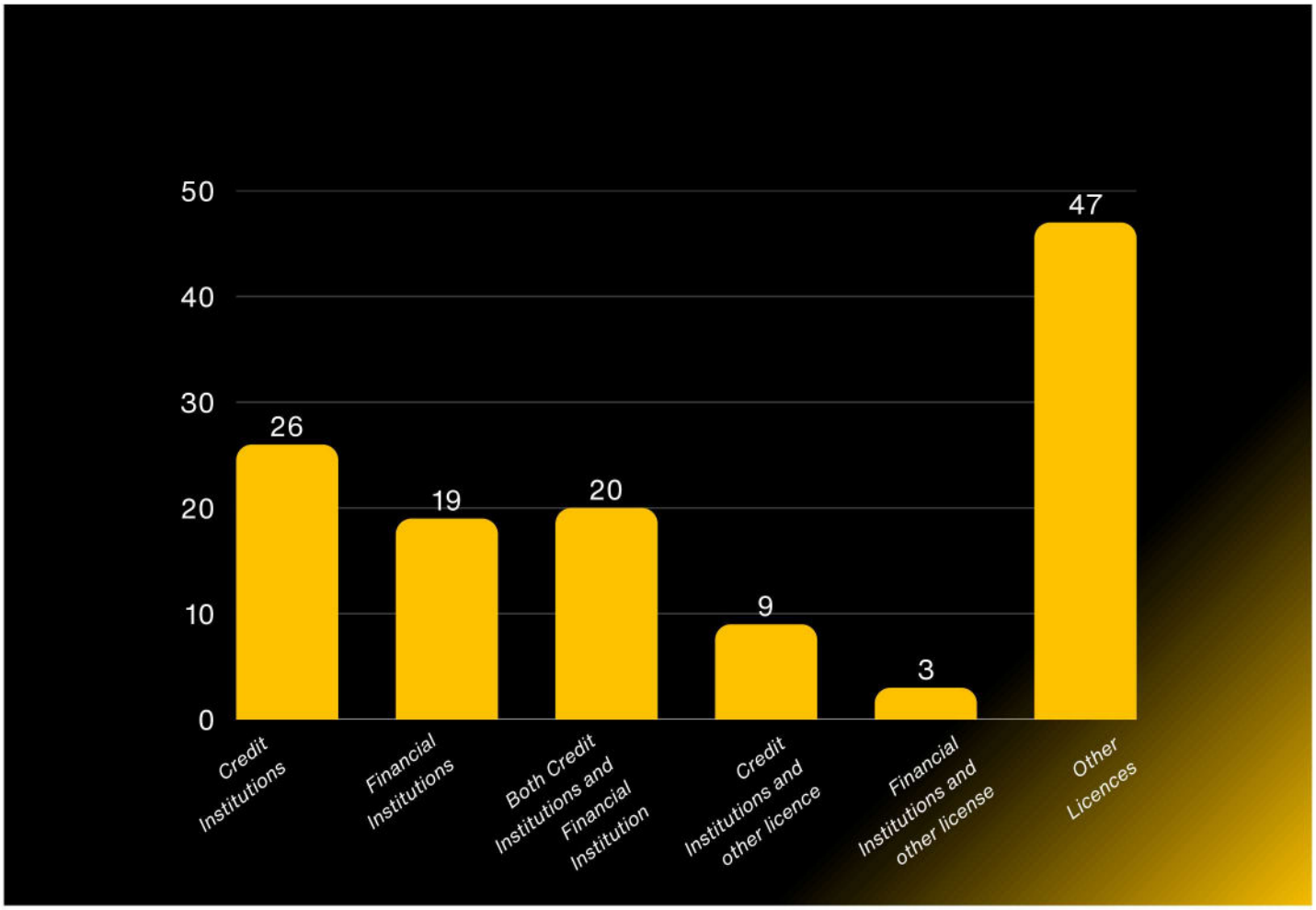
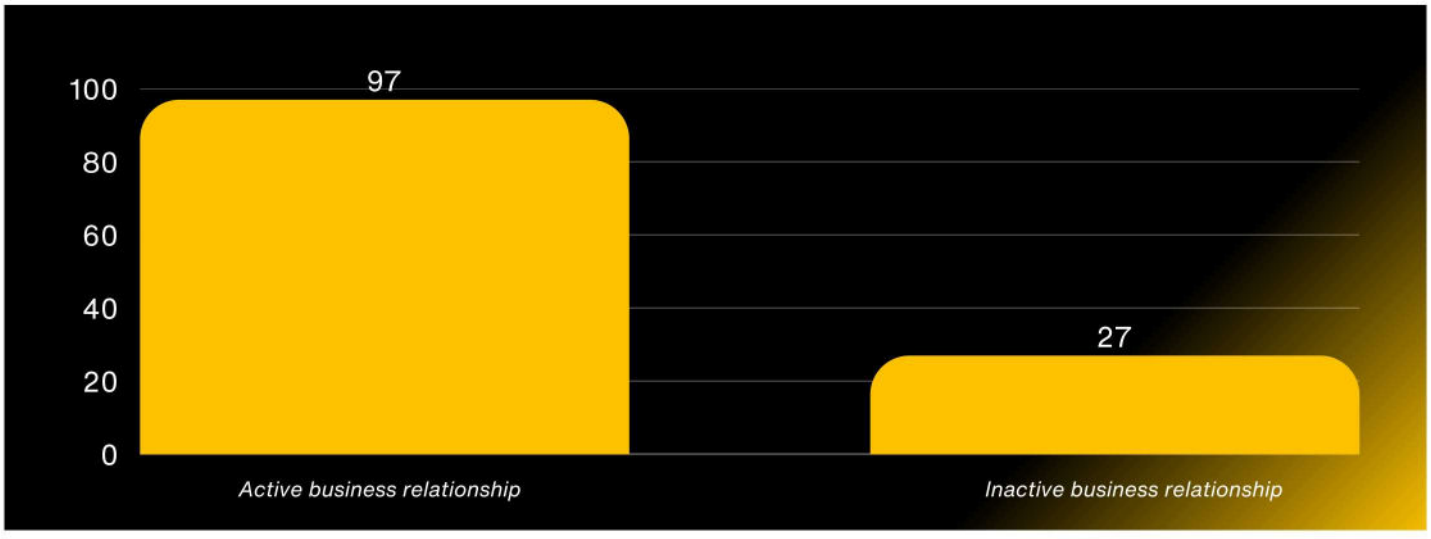


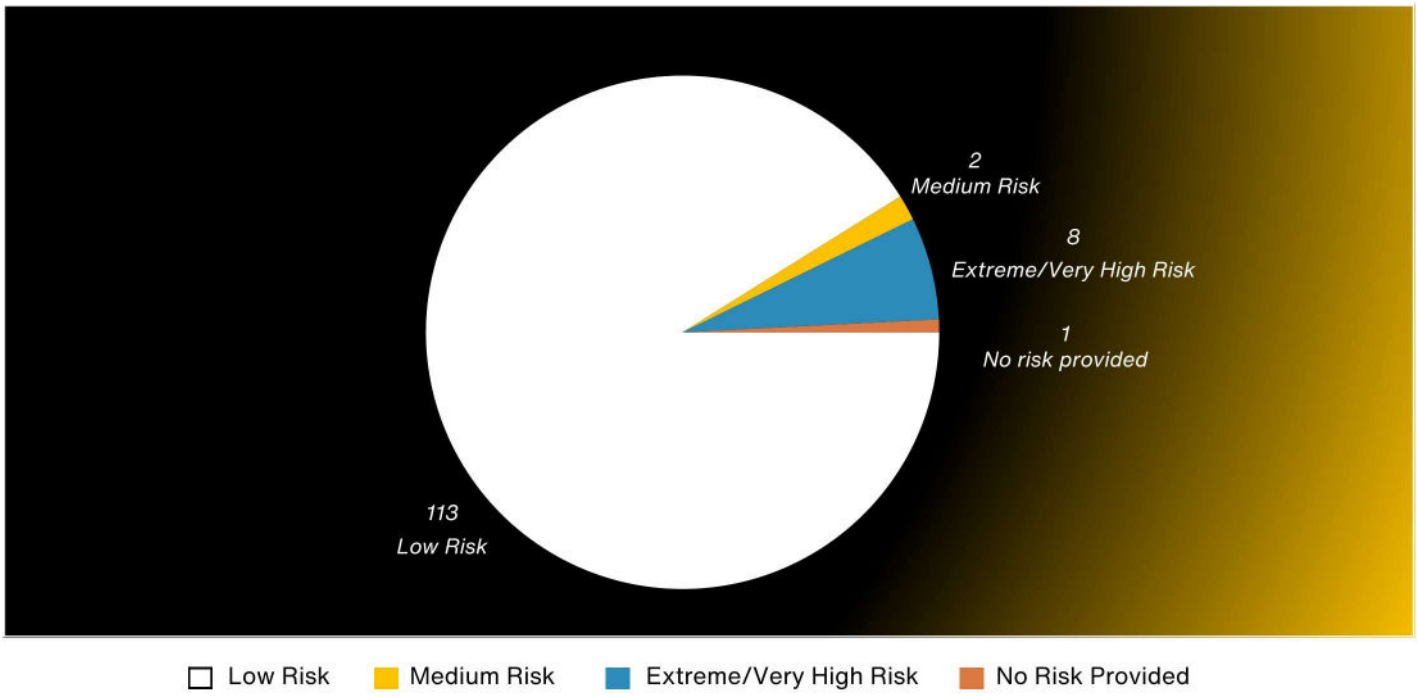
Chart 2 - *Business relationship status*



[4] The customers' authorisation category indicates the type of licence recorded by the CISs for each customer, based on the documentation held on file

[5] The customer's risk rating reflected the rating at the time when the thematic review took place.

Chart 3 - *Risk rating assigned to the CIS's customers selected for review*



The thematic review consisted of two parts:

Initial meeting with the MLRO of the CIS and review of the policies and procedures

To gain an understanding of the controls design and processes adopted by the CIS in relation to the topics covered by the thematic examinations.

Customer file reviews

To verify whether the CIS was implementing effective controls in compliance with AML/CFT regulations applicable to the topics in scope of the thematic examinations.

4. Outcome

4.1 Customer Risk Assessment and Policies and Procedures

Regulatory Obligation

Regulation 5(5)(a)(ii) of the PMLFTR and Sections 3.4 and 3.5 of the IPs.

Key Findings:

Chart 4: *When and was a CRA carried out at some point during the business relationship?*[6]

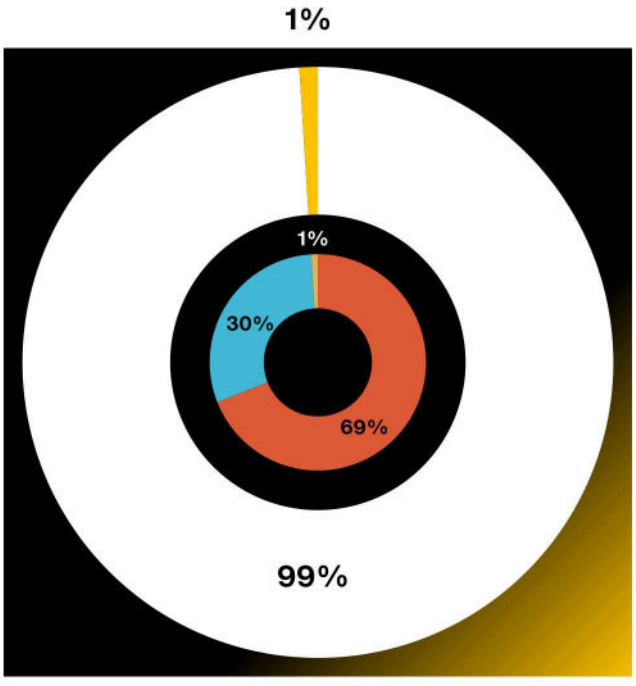
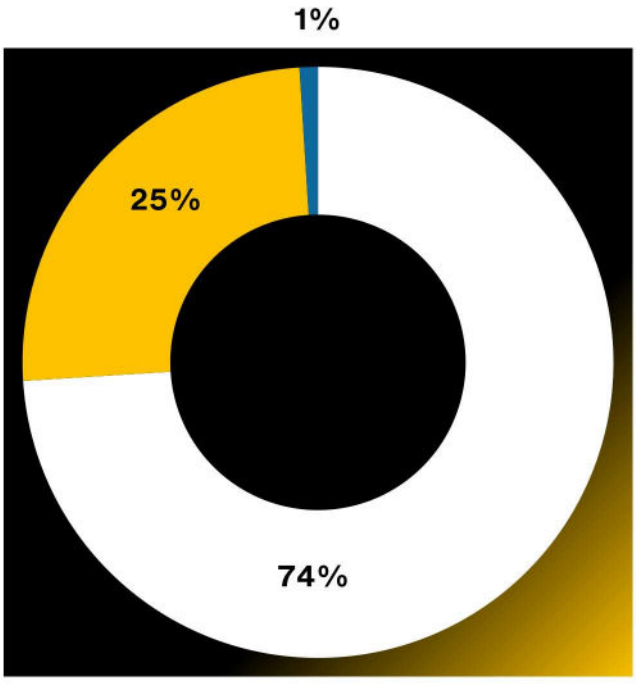


Chart 5: *Has the CRA been updated during the course of the business relationship?*



The Officials observed that, in 89% of the customer files examined, the assigned low-risk rating for the respective customers was adequate and justified as it was supported by a documented assessment outlining the absence of any high-risk factors.

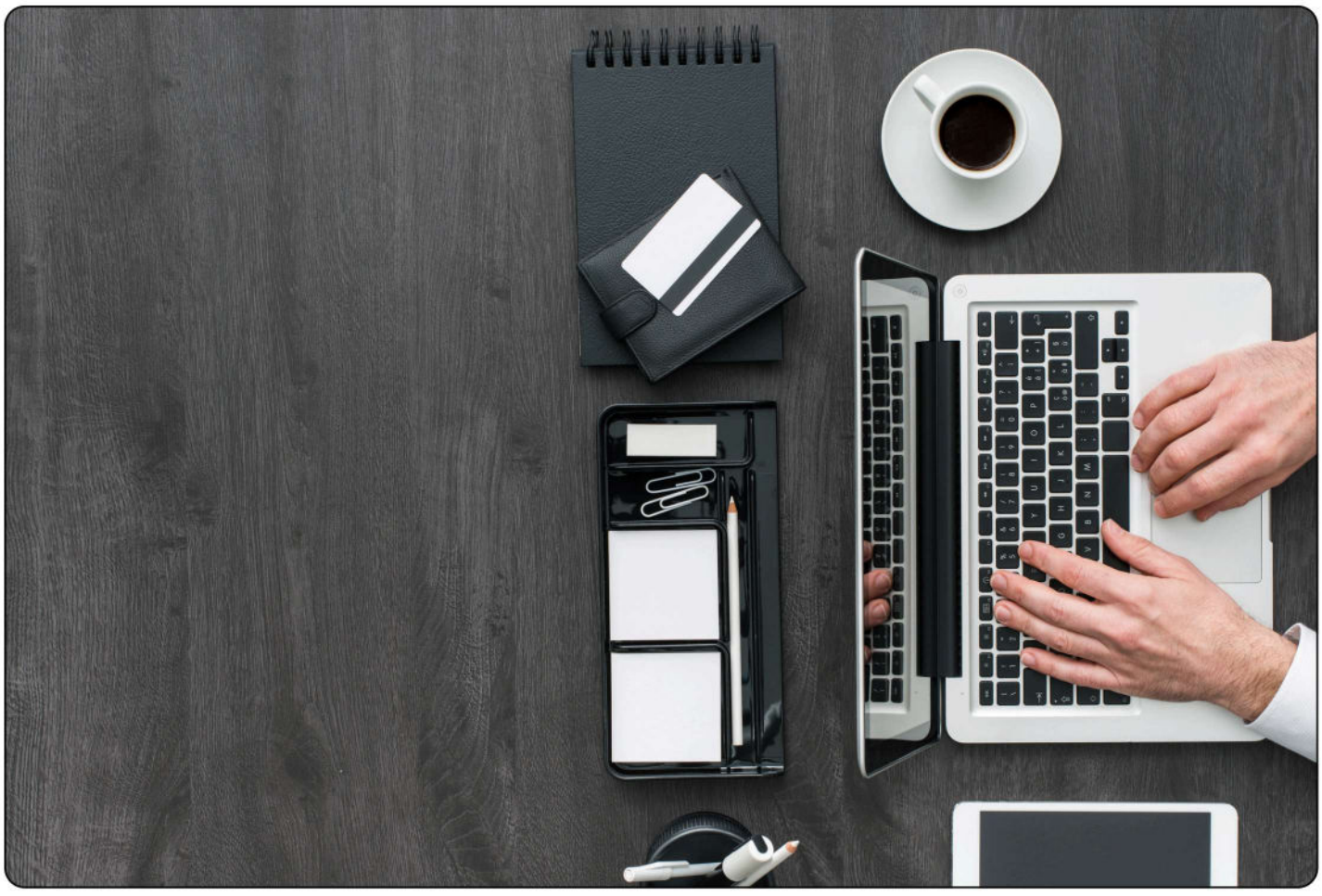
[6] In some instances when the CRA was carried out after onboarding, this might have been due to restrictions related to the dealing days

Good practice: Considering all known risk factors when assessing the CRA

When assessing the adequacy of customers' low-risk rating, one CIS implemented a comprehensive set of checks to support its risk assessment. Specifically, the CIS assessed whether customers were regulated entities registered within the EU, operated exclusively in EU jurisdictions, and if there was any adverse media associated with them. The CIS also checked for any adverse media linked to the customers and ensured that the industries in which the underlying customers of the regulated entity operated were not posing a high ML/FT risk.

Bad practice: Failure to tailor AML/CFT framework to Maltese requirements

A CIS adopted the AML/CFT policies and procedures of its Fund Administrator, which were developed in line with the legal framework of another European Union (EU) Member State. However, the CIS failed to ensure that these policies and procedures were appropriately adapted to reflect Maltese legal and regulatory requirements. Specifically, the CIS was unable to demonstrate that it had assessed how the AML/CFT framework of the respective jurisdiction diverges from the Maltese framework, for example, in terms of differences in CDD requirements. Furthermore, it was observed that while the policies and procedures in use incorporated the relevant AML/CFT obligations, they did not make any reference to the PMLA, the PMLFTR, the IPs, or any applicable guidance issued by the FIAU.



Key Takeaways

1 Key Takeaway 1: Not all regulated entities present a low risk of ML/FT by default

When evaluating a customer's risk level, CISs should consider all known risk factors and ensure these are reflected in the customer's risk profile. CISs should not automatically classify a customer as low risk simply because the customer is a regulated entity. Instead, all information collected should be reviewed holistically to determine whether the customer truly presents a lower ML/FT risk. This assessment should be properly documented, and the information gathered must be thoroughly evaluated rather than treated as a simple tick-box exercise.

2 Key Takeaway 2: Monitoring and understanding outsourced risk assessment procedures

CISs frequently outsource the implementation of AML/CFT risk assessment procedures to a third-party service provider, such as a fund administrator. It is common for a fund administrator to have a defined CRA methodology, including procedures and templates, to be used to risk-assess the customers of the CIS. In these cases, the CIS needs to assess whether these policies, procedures and templates are adequate to its particular circumstances. Then, effectively monitor that the risk assessment is carried out in line with the CIS's own risk understanding and risk appetite. A CIS should not rely solely on the CRA carried out by the fund administrator; it must ensure that the fund administrator applies a methodology that is understood and approved by the CISs' senior management and is adequate for the business model, specifics and customer base. Ultimately, the CIS is fully responsible for complying with AML/CFT requirements.

3 Key Takeaway 3: Understanding the Fund Administrator's policies and procedures

Similarly to the CRA framework, CISs must understand that even though the fund administrator may be the one drafting the scheme's AML/CFT policies and procedures and/or applying its own policies and procedures to the CISs, it is ultimately the responsibility of the CIS to determine if the policies and procedures address the specific ML/FT risks to which it is exposed. Standardised policies and procedures may be adopted as long as they are adequate and commensurate with the CIS's risk profile. It is no justification for the CIS to argue that the policies and procedures were provided to it by the fund administrator or that these are the same ones implemented by the fund administrator to meet its own AML/CFT obligations.

4.2 Purpose and Intended Nature of the Business Relationship and the Customer's business and risk profile

Regulatory Obligation

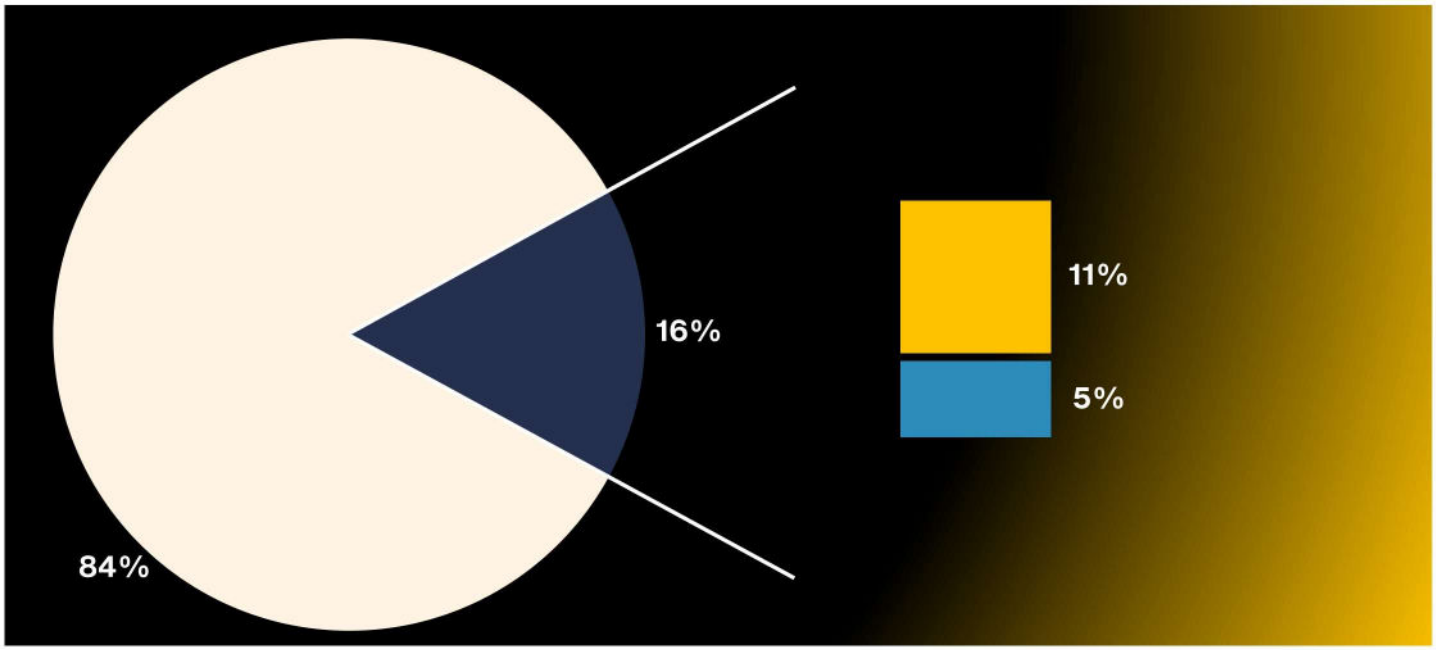
Regulation 7(1)(c) of the PMLFTR and Section 4.4 of the IPs.

Key Findings:

The customer files analysis showed that in 16% of cases, information was obtained to evaluate whether the level of activity undertaken was reasonable. This would include an understanding of the SoW for those regulated entities that invest on their own behalf, and general information on the expected or actual source of funds in view of the CISs' underlying investors, in the case of nominees. This was obtained through the following means:

- 11% was collected by means of onboarding form; and
- 5% was collected by means of a declaration from the customer.

Chart 6 - *How was information collected by CISs?*



Good practice: Additional information and documentation to support the customer's business and risk profile

One of the CIS's customers was offering a nominee service to underlying investors. Given this client's significantly higher transaction volume in comparison to others, the CIS gathered additional details on the potential frequency and anticipated number of transactions to be conducted during the business relationship. Apart from obtaining information on the categories of the underlying customers serviced by the nominee, the CIS gained insights into the customers' operational processes for subscriptions and redemptions. Subscriptions were processed cumulatively, while redemptions were processed individually for each customer. This information allowed the CIS to develop a comprehensive business and risk profile on the customer, thereby supporting effective and appropriate transaction monitoring.

Bad practice: Expected Source of Funds in the context of the customers' profile

When building the customer profiles, CIS would request, amongst other elements, information on the expected SoF. The CIS often receive a generic or vague description, such as 'client monies'. This is particularly common in cases where customers provide nominee services and invest in funds on behalf of their underlying investors. In several instances, it was observed that the information was not assessed in the context of the profile that the CIS built. It was treated primarily as a compliance requirement rather than as a basis for developing a meaningful business and risk profile of the customers.

Key Takeaways

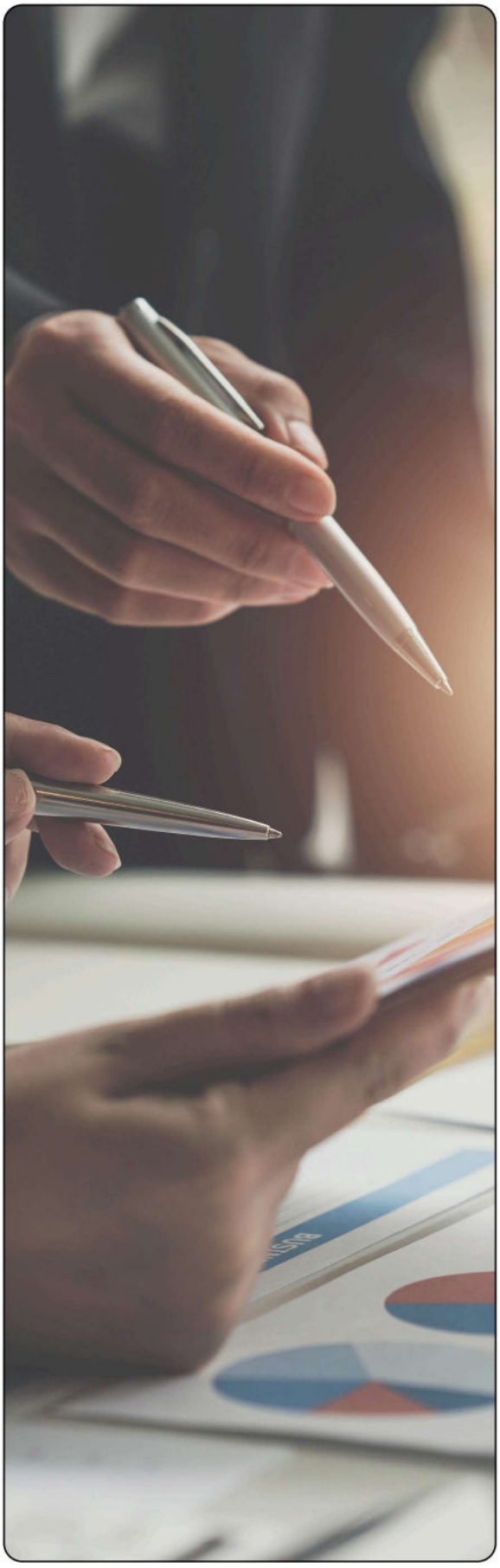
1 Key Takeaway 1: Source of Funds

Especially in the case of regulated customers acting as nominees, the CISs should not limit themselves to obtaining general information about the SoF, such as 'client monies', but focus on understanding the customer's business and risk profile. The information collected should allow the CISs to have a good understanding of what kind of customers the nominee is acting for. By understanding the underlying customers for which the nominee is acting, CIS should remain vigilant to identify any discrepancies between their overall understanding of the nominee's customer base and the actual volume and value of subscriptions. For instance, if the nominee's underlying customer is an institutional entity, there may be a significant flow of funds through the nominee to the CISs or its sub-funds. Conversely, if the nominee targets retail customers in jurisdictions with lower average incomes, then the flow of money into the Fund is expected to be somewhat lower. It is difficult for a retail CISs attract the same investment value as one used by institutional customers, even though a successful marketing strategy may increase the volume and value of subscriptions. In these circumstances, CISs are to seek an explanation about what may be generating this significant inflow of funds and assess its reliability.

Furthermore, from a transaction monitoring perspective, during the business relationship, if CISs encounter situations that require further information regarding the SoF, say due to unusually large transactions or a change in transaction patterns, CISs should go beyond simply asking for SoF (to avoid the customer merely responding with "clients' monies"). Instead, CISs should inquire whether the nominee customer has experienced any changes with their underlying investors, such as targeting new customer types or expanding to new jurisdictions.

2 Key takeaway 2: Expected activity in the context of the business and risk profile

In the case of CISs, while some investors may change investment levels during a business relationship due to market opportunities, CISs should still strive to obtain an indication of expected transaction levels at the onboarding stage, including the jurisdictions from which the funds will be channelled. This information is to be regarded in the context of the overall assessment that a CIS would undertake on its regulated customers. This would include, amongst other elements, an understanding of the services and products offered by such customers, as well as a general understanding of their customer base. The customer's business and risk profile may be updated throughout the business relationship by referring to the customer's transaction profile. CISs should refrain from requesting generic information. This information is intended to both assist them with the risk assessment of their customers and with their ongoing monitoring obligations to detect any unusual spikes in activity. This is particularly important for customers rated as low risk, since generally no other information would be available for them.



4.3 Application of Simplified Due Diligence

Regulatory Obligation

Regulation 10 of the PMLFTR and Section 4.8 of the IPs

Situations that are deemed to present a low risk of ML/FT[7]

Section 4.8.1 of the IPs lays out several factors that CISs need to consider to determine whether a business relationship with a regulated customer presents as low risk of ML/TF and therefore allows for the application of SDD to such customers. These are:

a. Checking whether the customer of the CIS is licensed or authorised to conduct financial and/or banking business.
b. Checking for any publicly available and relevant adverse regulatory or supervisory information.
c. Establishing whether the customer is a subject person carrying out relevant financial business or a third party established in an EU Member State or in a reputable jurisdiction carrying out an equivalent activity and subject to equivalent AML/CFT requirements and supervision as those required by Directive (EU) 2015/849.
d. Obtain an understanding of the activities that the regulated customer is undertaking, i.e. an understanding of the services and products offered as well as a general understanding of its customer base (e.g. main customer categories, main geographical locations of the same, etc.).

In addition to the above, where the regulated entity is acting as a nominee, the CIS has to:

e. Obtain confirmation from the regulated entity, as customers of the subject person, that it has carried out CDD on all the underlying investors and beneficial owners.
f. Obtain an undertaking from the customer, ensuring that the regulated entity will provide all the information and documentation to the CIS upon demand so that the subject person can fulfil all its AML/CFT obligations as may be applicable.
g. Obtain an undertaking that the regulated entity will immediately inform the CIS about any changes in the information provided at the inception of the business relationship so the CIS may factor this into its customer risk assessment as applicable.

Section 4.8.1 of the IPs also requires that CISs keep a record of the checks conducted to ensure their customer meets the conditions for the SDD to be applied.

[7] The following situations are relevant to those CISs which were part of the thematic review. These include cases where the customer of the CISs is:

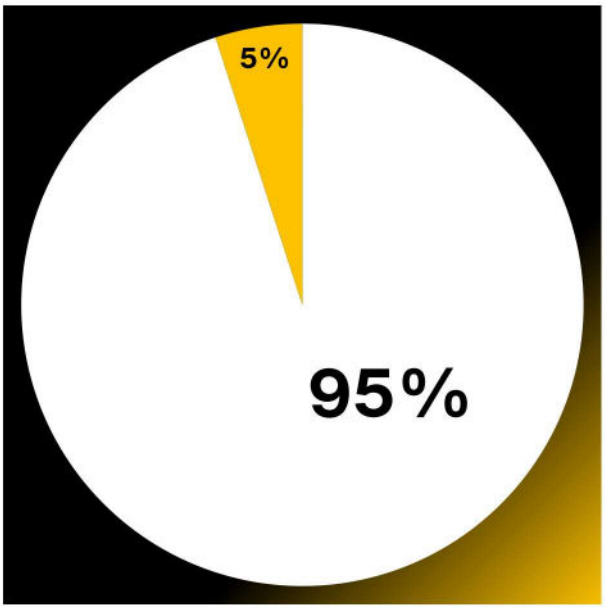
1. a subject person carrying out relevant financial business or a third party established in an EU Member State or in a reputable jurisdiction carrying out an equivalent activity and subject to equivalent AML/CFT requirements and supervision as those required by Directive (EU) 2015/849;
2. a collective investment scheme; and
3. a regulated entity holding financial instruments such as bonds, shares, and units in the scheme in a nominee capacity for its own customers or through an omnibus account.

Key Findings

Was SDD applied?

Out of the **124 customer files** reviewed where SDD was applied, checks were carried out to assess whether the application of SDD complies with Section 4.8.1 of IPs.

Chart 7: *Could SDD be applied in line with Section 4.8.1 of the IPs?*



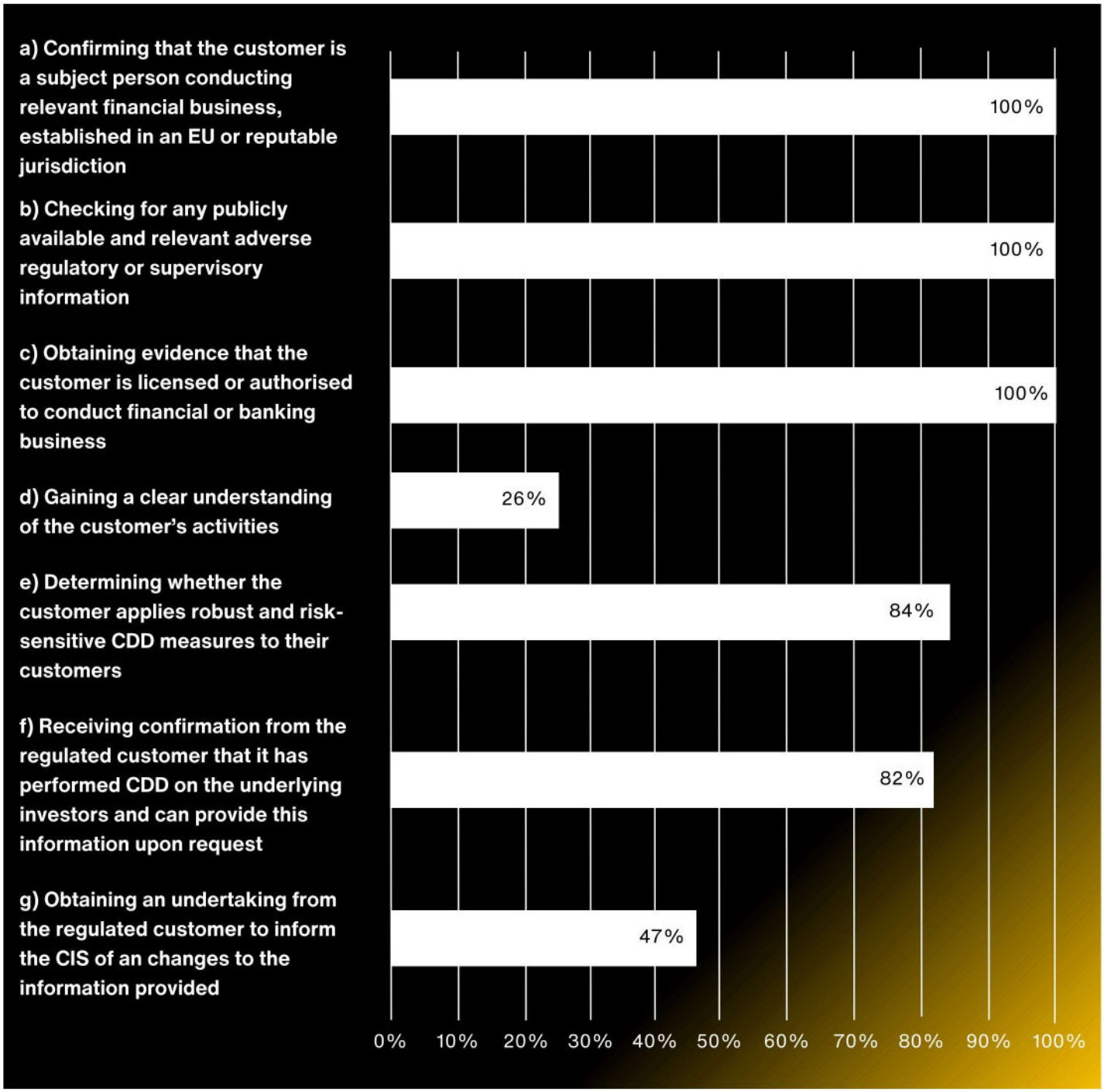
It was found that in **95%** of these cases, the application of SDD was justified.

However, in the remaining 5%, SDD should not have been applied.

This was due to the latest customer risk rating being either medium or high, which should have automatically excluded the application of SDD by the CIS in such circumstances.

Factors that CISs should consider to determine whether a business relationship presents a low risk of ML/FT

Chart 8: Percentage of the customer files analysed in which the Subject Person satisfied the respective condition



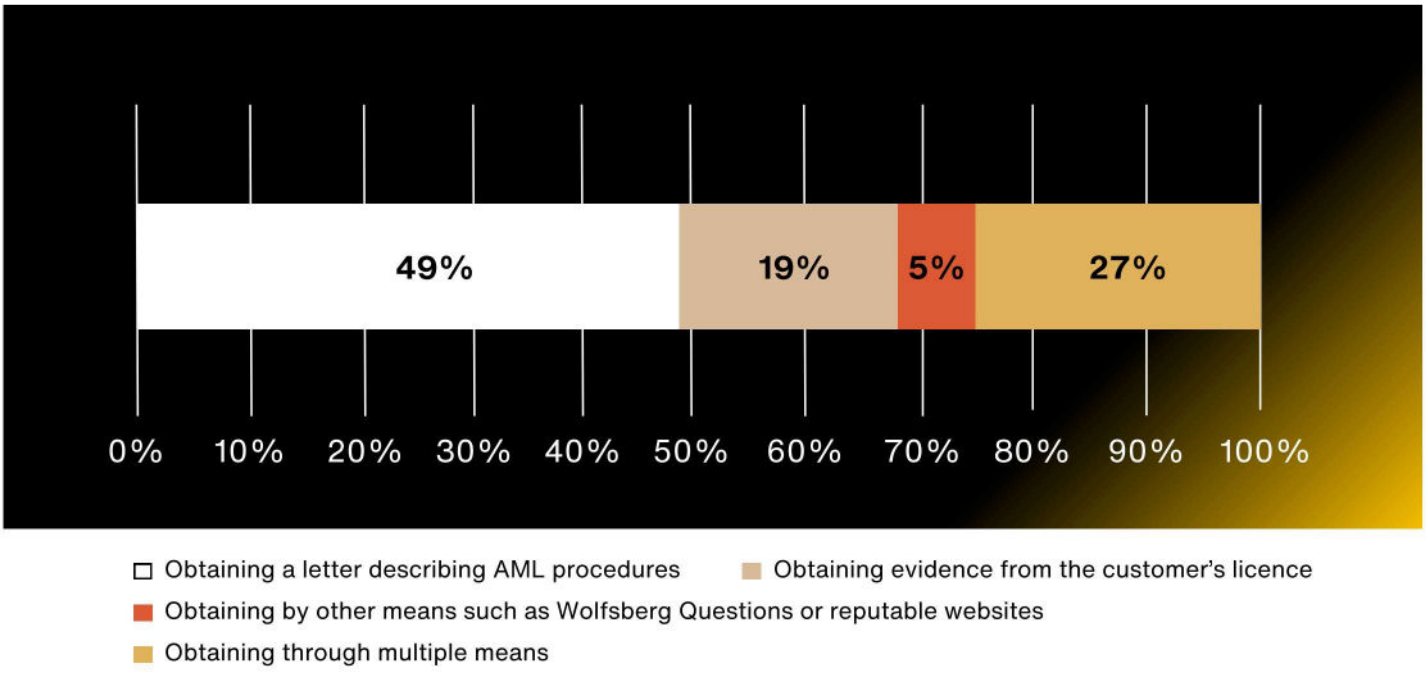
Applicability of SDD measures

a) Checks whether the customer of the CIS is a subject person carrying out relevant financial business or a third party established in an EU Member State or in a reputable jurisdiction carrying out an equivalent activity and subject to equivalent AML/CFT requirements and supervision as those required by Directive (EU) 2015/849

As shown in the Chart 8 above, it was observed that for **all** customer files reviewed, checks had been conducted to determine whether the customer was either a subject person carrying out relevant financial business or a third party established in an EU Member State or a reputable jurisdiction. These checks ensured that the customer was engaged in equivalent activities and subject to the same AML/CFT requirements and supervision as mandated by Directive (EU) 2015/849.

The information was collected through various means, as shown in the Chart 9.

Chart 9: *How was information obtained?*

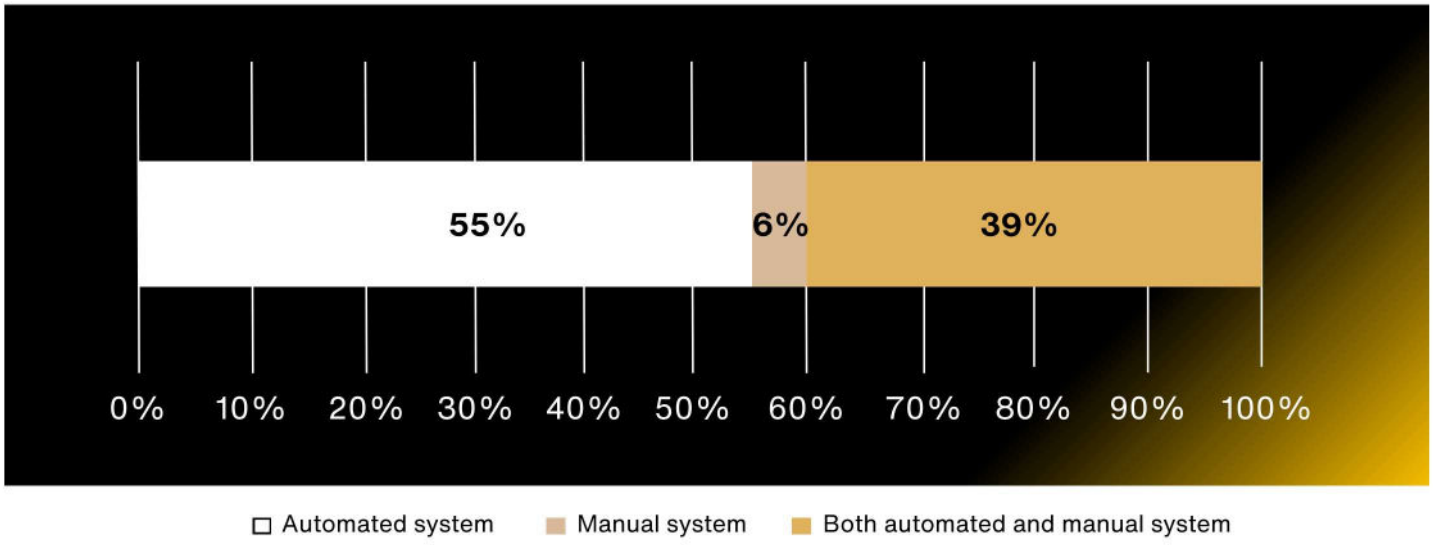


b) Checks conducted for any publicly available adverse regulatory or supervisory information

All the customer files reviewed had checks in place for publicly available adverse regulatory or supervisory information, which are to be assessed according to Section 3.5.1 (a) of the IPs.

Furthermore, as seen in Chart 10, the CISs reviewed used both automated and manual systems to collect adverse information on their regulated customers, with the majority opting for an automated system.

Chart 10: *How was information obtained?*

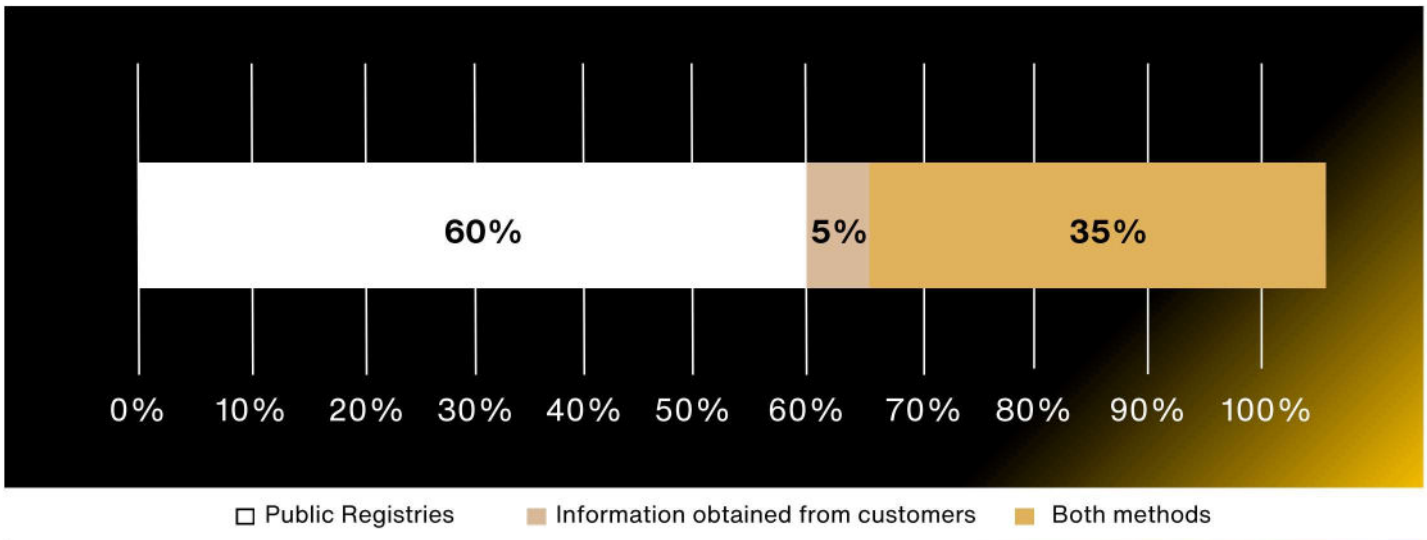


c) Evidence that the customer institution is licensed or authorised to conduct financial and/or banking business

All customer files reviewed provided evidence that the customer's institution is licensed or authorised to conduct financial and/or banking business.

The information was collected by the CIS under review through various methods, as shown in Chart 11 below.

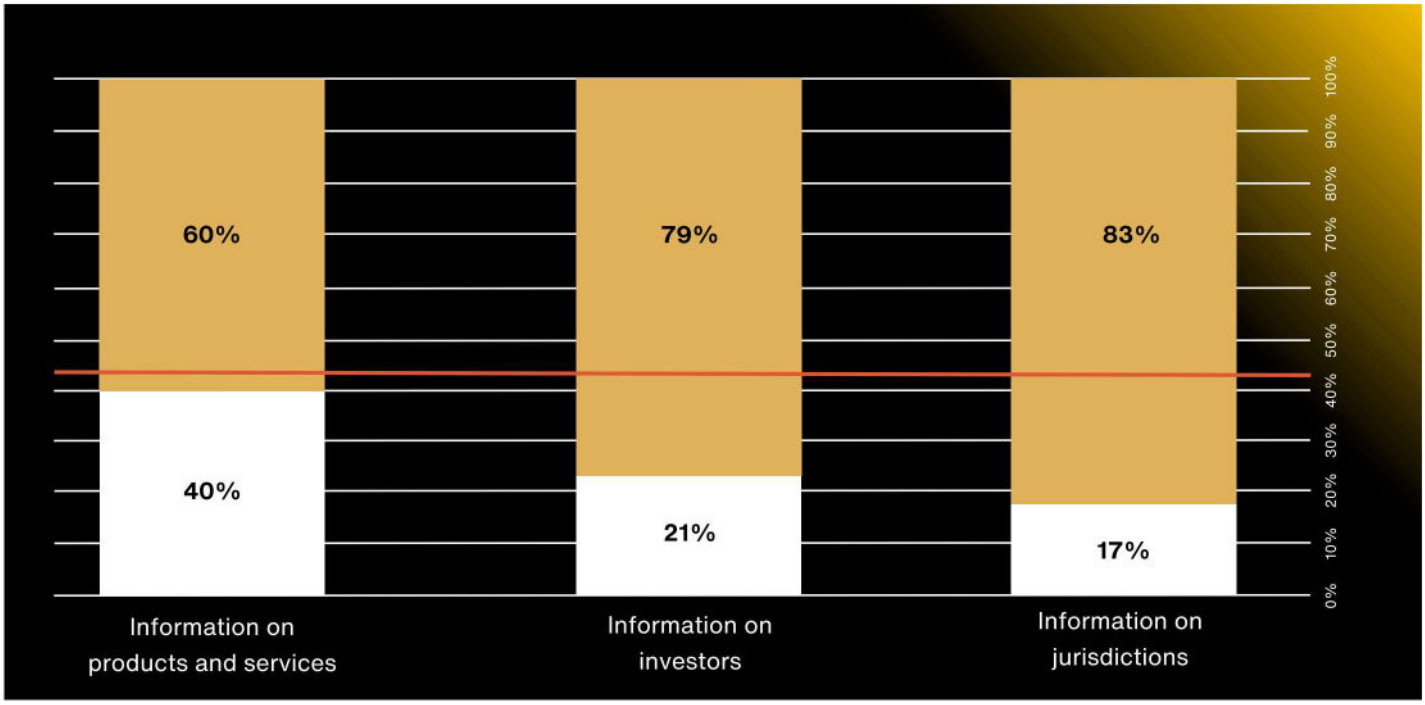
Chart 11: *How was information obtained?*



d) Evidence that the CIS has obtained an understanding of the activities of the regulated customer

When looking at the 26% of the cases where such information was obtained, the thematic review revealed the following:

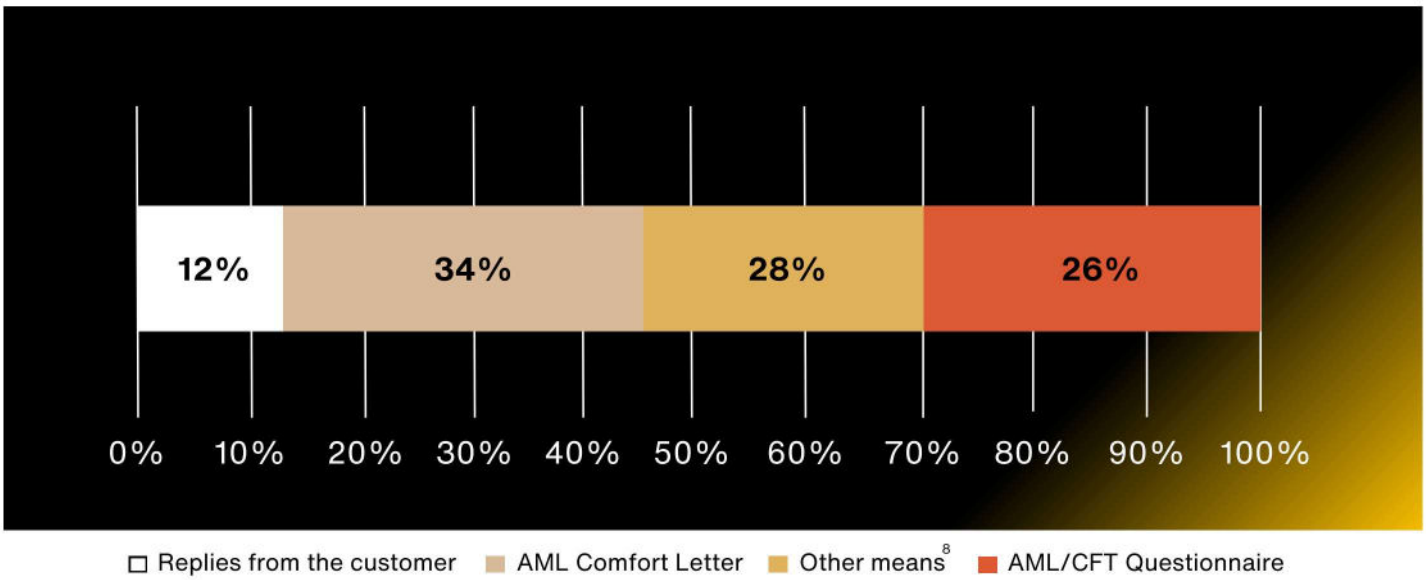
Chart 12: *Information obtained on the activities of the regulated customer*

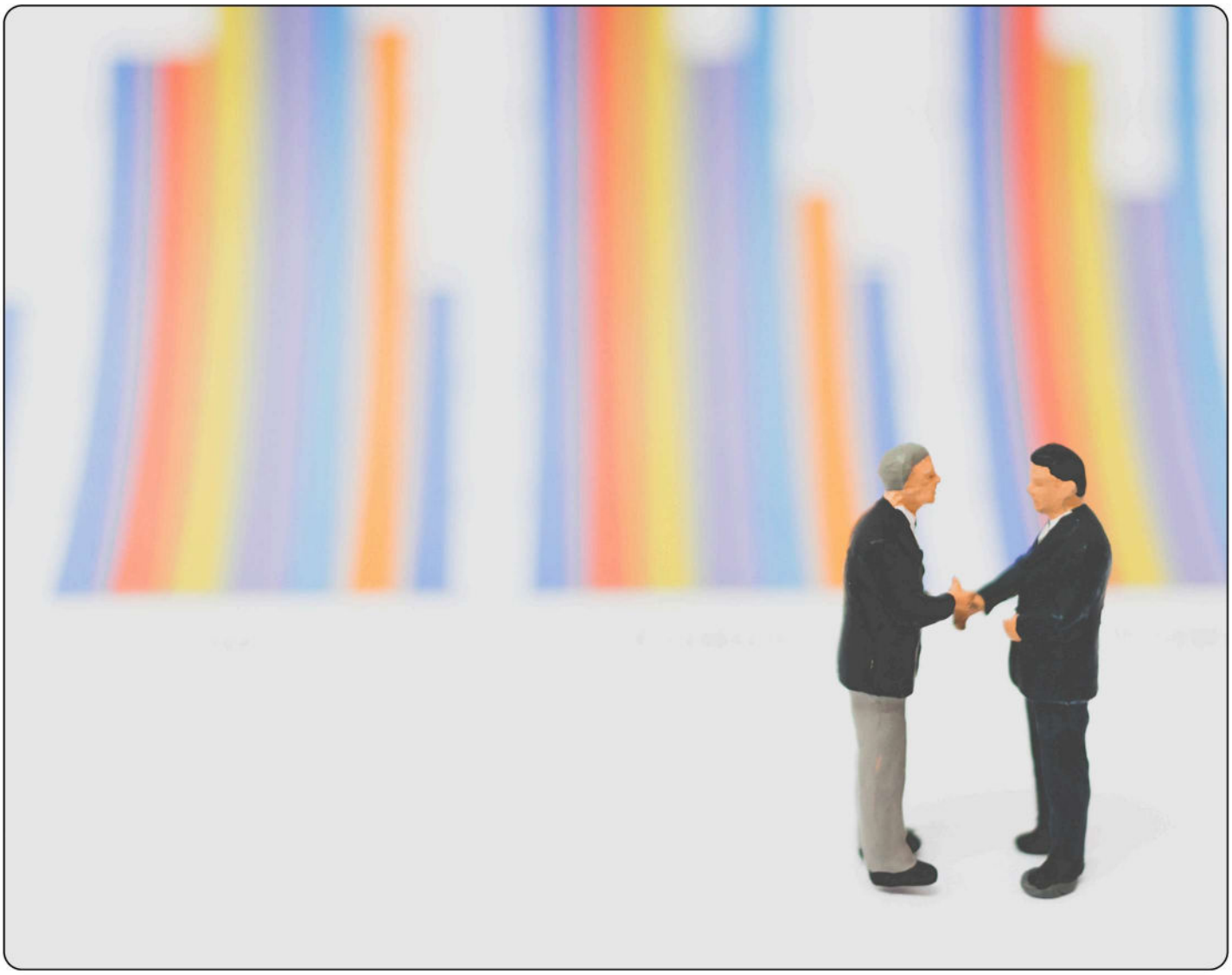


It is important to note that the expectation is not for CISs to obtain a general overview of all products or jurisdictions the customer serves. Rather, the information gathered should be specific to the products, customer segments, and jurisdictions relevant to the business relationship established with the CIS. For example, a customer may offer a broad range of services (e.g. pension funds and other investment vehicles) across several markets (e.g. France and Italy). However, in the context of its business relationship with a particular CIS, it may decide to offer only pension funds to clients located in France.

As such, relying solely on publicly available sources such as the customer's website is insufficient, as it may not provide visibility into the specific products or services offered through the business relationship with the CIS. A more tailored and specific understanding is therefore necessary to adequately assess the AML/CFT risks associated with the relationship. Requesting the information directly from the customers is one way of doing this.

Chart 13: *How was information obtained?*



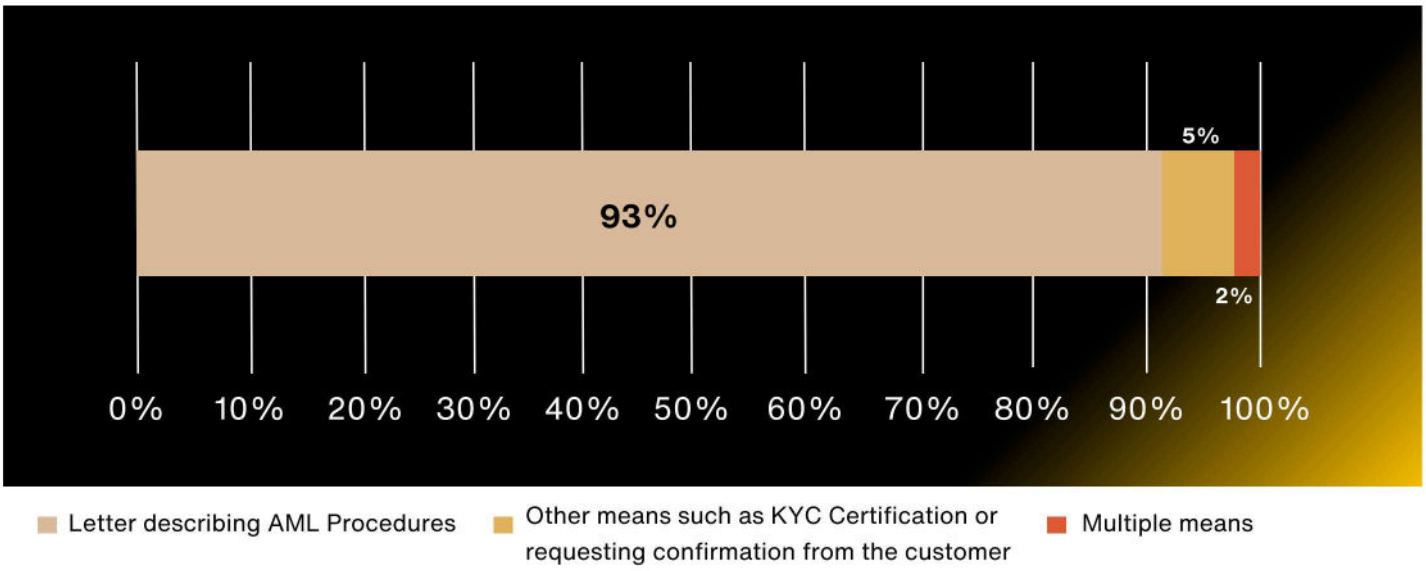


[8] Other means include the commercial registry, the Wolfsberg Questionnaire, websites, and documentation collected on the customers.

e) Checks done to determine whether the customer applies robust and risk-sensitive CDD measures

84% of the cases in which checks were made, information was obtained, as seen in Chart 14 below.

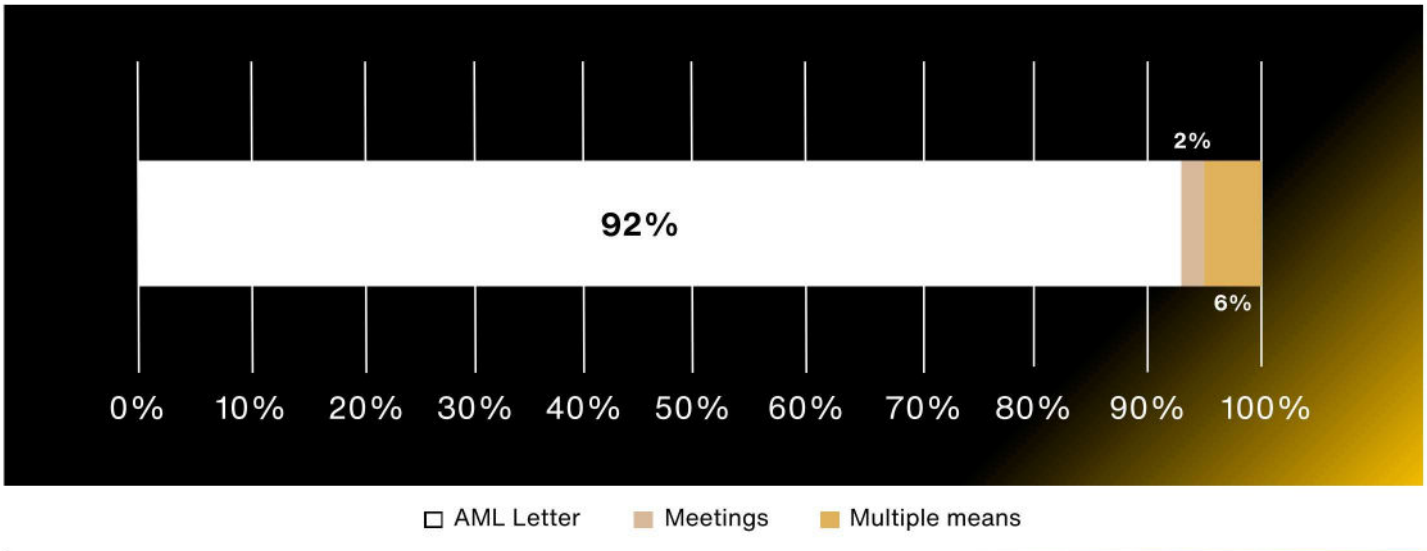
Chart 14: *How was information obtained?*



f) Ensuring that the regulated entity has carried out CDD on all of the underlying investors, and that the regulated entity will provide such information and documentation to the CIS upon demand

82% of the cases in which checks were made, information was gathered through various means, as seen in Chart 15 below.

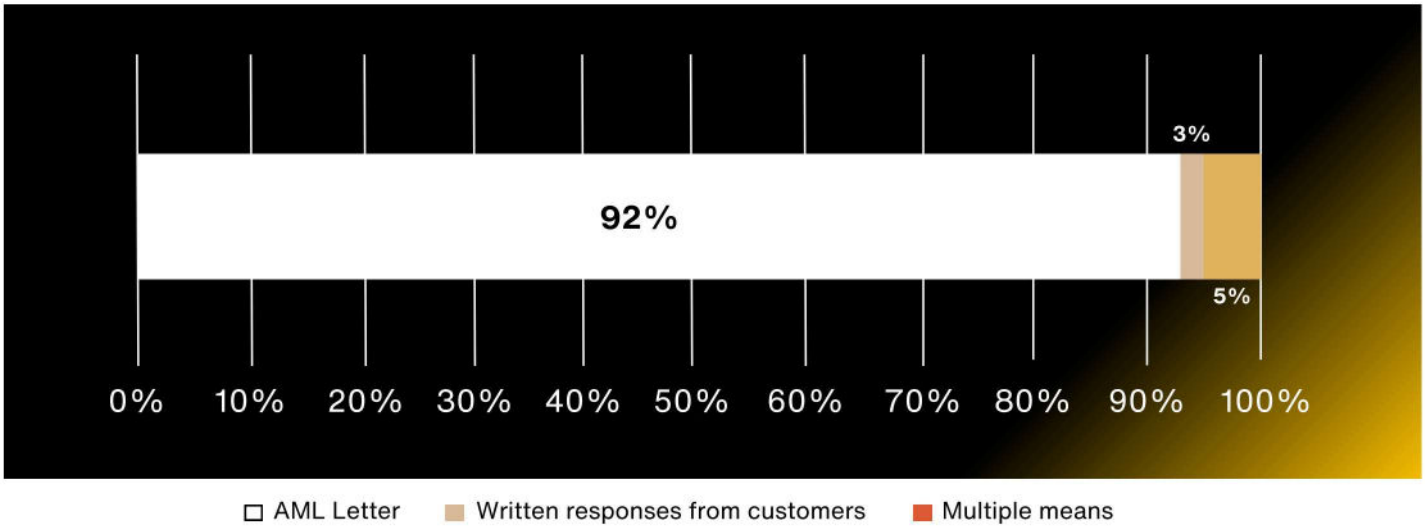
Chart 15: *Information obtained on the activities of the regulated customer*



g) Provide evidence that the regulated entity will immediately inform the CIS about any changes in the information provided at the inception of the business relationship

47% of the cases where checks were done, information was gathered through various methods, as outlined in Chart 16.

Chart 16: *How was the information obtained?*



Good practice: Understanding the activities of the regulated customer

A customer of the CIS held the majority shares in a fund as a nominee for its underlying clients. The CIS's MLRO undertook a thorough and enhanced review of the customer's AML/CFT framework, exceeding the standard measures typically applied to regulated entities. Beyond obtaining an AML Comfort Letter and a completed Wolfsberg Questionnaire, the CIS collected a tailored questionnaire specifically designed for this customer. This approach enabled the CIS to gain a deeper and more comprehensive understanding of the client's activities, including the nature and risk profile of the underlying investors, the jurisdictions involved, the services provided by the nominee, and the AML/CFT measures applied at the level of the underlying investors.

Bad practice: AML comfort letter about the regulated status received from Fund Administrator or Custodian on behalf of the customer

In one of the customer files reviewed, the CIS relied on an AML letter provided by the customer's Fund Administrator to confirm whether the customer qualified as:

- A subject person engaged in relevant financial business.

  or

- As a third party established in an EU Member State or in a reputable jurisdiction carrying out equivalent activities and subject to equivalent AML/CFT requirements and supervision in line with Directive (EU) 2015/849.

However, the AML letter in question was drafted and signed solely by the Fund Administrator, and not by the CIS's actual customer. The customer neither signed nor directly confirmed the declarations made on its behalf. In this case, best practice would require a direct declaration from the regulated customer itself, rather than relying on documentation submitted or signed by third parties such as fund administrators or custodians.

Bad practice: Incomplete AML Letters

One CIS had AML Letters that lacked specific details, such as an undertaking that the regulated entity would immediately inform the CIS of any changes or confirm that it carried out CDD on its underlying customers (in case of nominees). It appeared that the CIS did not assess the quality or adequacy of these documents, but instead merely retained them only to demonstrate compliance with AML/CFT requirements.

Bad practice: Application of SDD for customers that are not rated low-risk

A CIS had a customer initially rated as low risk but was then reclassified as high risk during the business relationship. Despite the increase in risk rating, the CIS continued to apply SDD and did not take any additional measures.

Key Takeaways

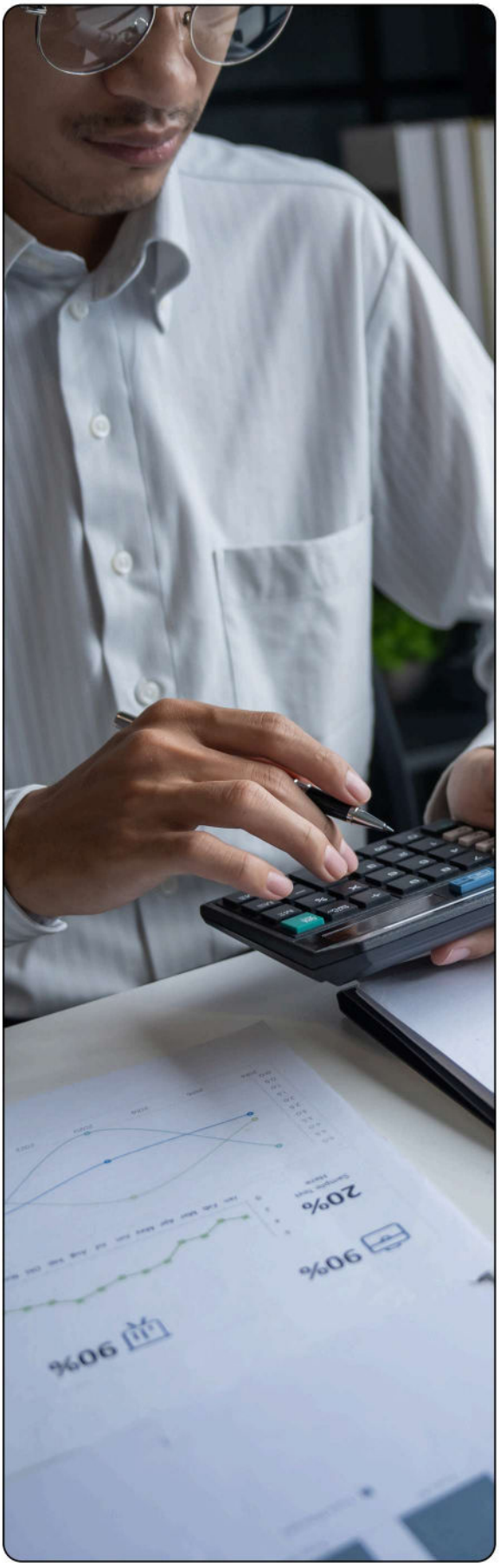
Key Takeaway 1: Application of SDD

CISs must keep in mind that SDD is only applicable in scenarios where a business relationship or an occasional transaction presents a low risk of ML/FT, per Section 4.8 of the IPs, and **is not applicable by default to any customers carrying out relevant financial business**. To determine and document such scenarios, CISs should have customer risk assessment procedures in place. Whenever a business relationship is assessed as posing a higher ML/FT risk, CISs must apply the full range of CDD measures and, in cases of high risk, further strengthen these measures.

Key Takeaway 2: Understanding the activities that the CIS's customers are undertaking

When servicing regulated entities engaged in relevant financial business and acting as nominees, it is essential to understand not only the products and services offered by the regulated customer but also the main types of underlying customers serviced and the main geographical exposure, as outlined in Section 4.8.1 of the IPs. This information will help to understand the ML/FT risks associated with the respective business relationship.

This means focusing on the actual customer segment the nominees are servicing in the context of the business relationship, rather than relying solely on general sources, such as the annual reports or generic information from the customer's website, which often provide an overview of the entire customer base. Instead, CISs must understand the regulated entities' business model, the category of underlying investors being serviced and provided with nominee services, as well as the volume of funds being invested through this arrangement, to determine whether the customers align with their risk appetite.



Key Takeaways

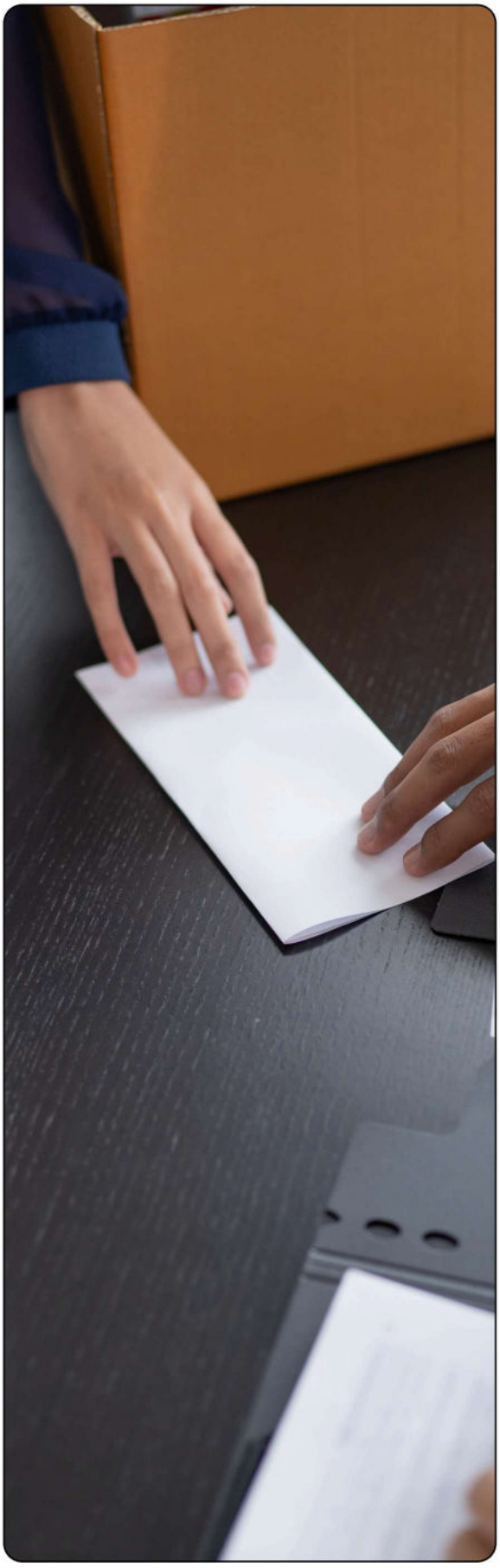
Key Takeaway 3: AML Comfort letters and confirmations received from third-party service providers or custodians

CIS must ensure that any written declarations and undertakings are provided by the nominee customer, not by a service provider or custodian to whom the nominee may have delegated the task of carrying out the CDD on the underlying investors. This is because the business relationship is between the CIS and the nominee, with the service provider or custodian being a third party that is not directly part of this relationship.

However, the following alternatives may also be considered as compliant with the requirements of the IPs:

a) There is communication between the CIS and the nominee, informing the CIS that CDD measures have been outsourced to a third-party service provider or custodian. The service provider or custodian then provides the necessary declarations and undertakings to the CIS. These declarations and undertakings should include a statement explaining the relationship between the nominee and the third-party service provider or custodian and that the nominee has authorised the third party to provide the CIS with the declarations and undertakings.

b) Both the nominee and the third-party service provider or custodian sign the written declarations and undertakings.



Key Takeaways

Key Takeaway 4: Undertaking to inform the CIS immediately about any changes in the information provided at the inception of the business relationship

An undertaking from a nominee that they will only provide information and/or documentation upon request from authorities in their jurisdiction, or report suspicions to the FIU of that jurisdiction, would not fulfil this requirement. The intention behind this requirement is to ensure that the CIS is proactively informed about any changes in the information provided at the inception of the business relationship. Other scenarios could include targeting new jurisdictions or new categories of customers. This ensures that the information provided by the nominee to CISs for risk assessment remains current and updated.

Key Takeaway 5: Ongoing monitoring

The application of SDD still requires ongoing monitoring to determine if the business relationship in question still merits being considered as low risk. CISs are to periodically confirm that any information obtained at the start of the business relationship remains current, even if the customer provided an undertaking stating it would inform the CIS of any changes.

As further stated in Section 4.8.1.1 of the IPs, CISs should consider whether:

- Any new regulatory or supervisory information has been made public, which may somehow impact the CIS's earlier CRA and rating of the business relationship as one presenting a low risk of ML/FT.
- Any increase in the volume of funds being channelled or invested through a nominee, omnibus or pooled account can somehow be considered to increase the risk of ML/FT posed by the given business relationship.
- Any data, information or documentation made available in relation to specific transactions, or the underlying investors or customers, is aligned with the information provided by the customer at the start of the business relationship. Any deviations may result in the CRA to be revised and possibly SDD not being applicable.

4.4 On-going Monitoring of the Business Relationships – Scrutiny of Transactions

Regulatory Obligation

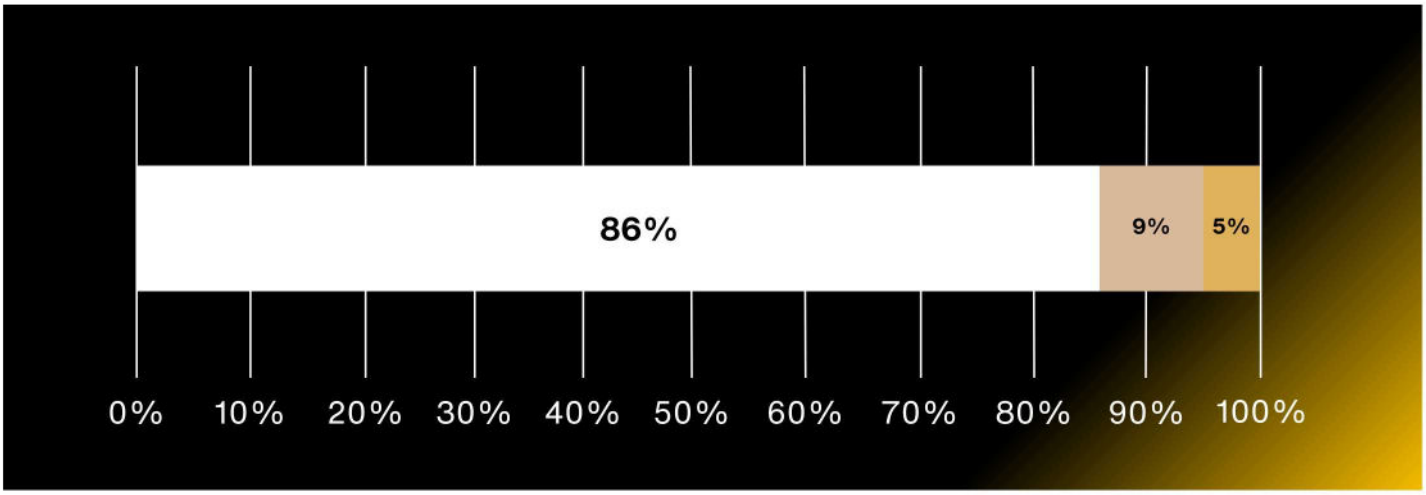
Regulation 7(1)(d) and Regulation 7(2) of the PMLFTR and Section 4.5.2 of the IPs.

In addition, Subject Persons are encouraged to refer to the Guidance Note on the Obligation of Transaction Monitoring issued by the FIAU in April 2023[9].

Key Findings

Who conducts Transaction Monitoring?

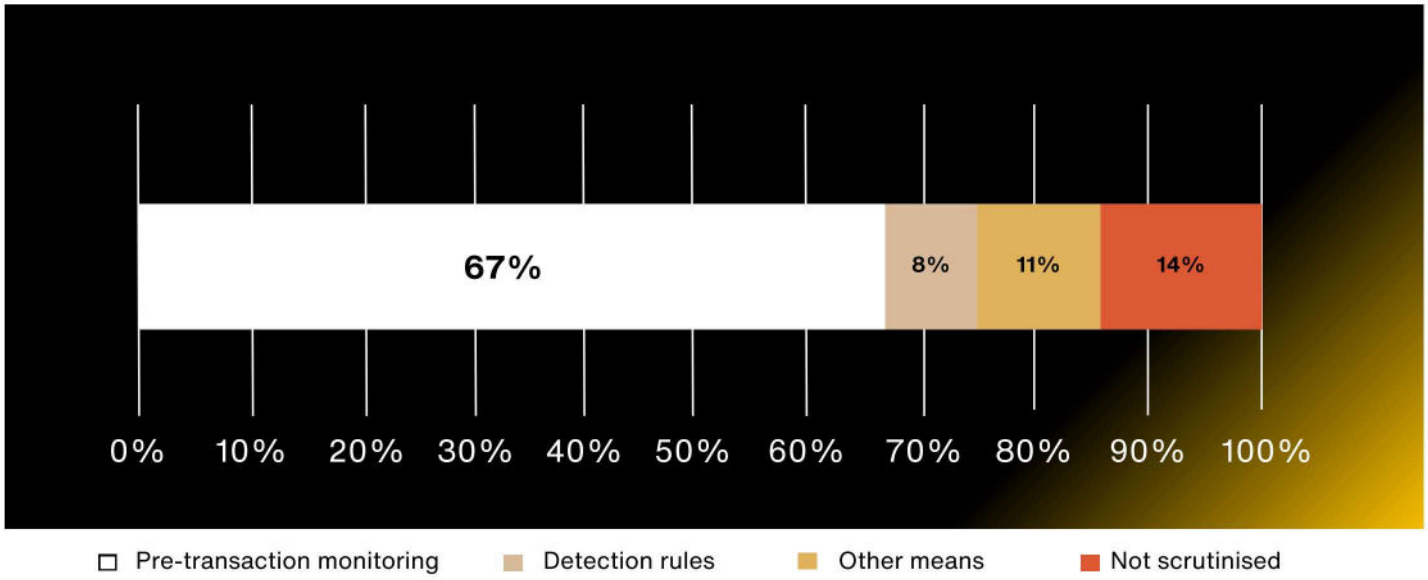
Chart 17: *Who conducts Transaction Monitoring?*



[9] The Guidance Note: A Look Through the Obligation of Transaction Monitoring can be accessed electronically through the following link: https://fiaumalta.org/app/uploads/2023/05/Guidance-Note-A-Look-Through-the-Obligation-of-Transaction-Monitoring.pdf

What type of transaction monitoring methods were used?

Chart 18: *Transaction monitoring methods used*

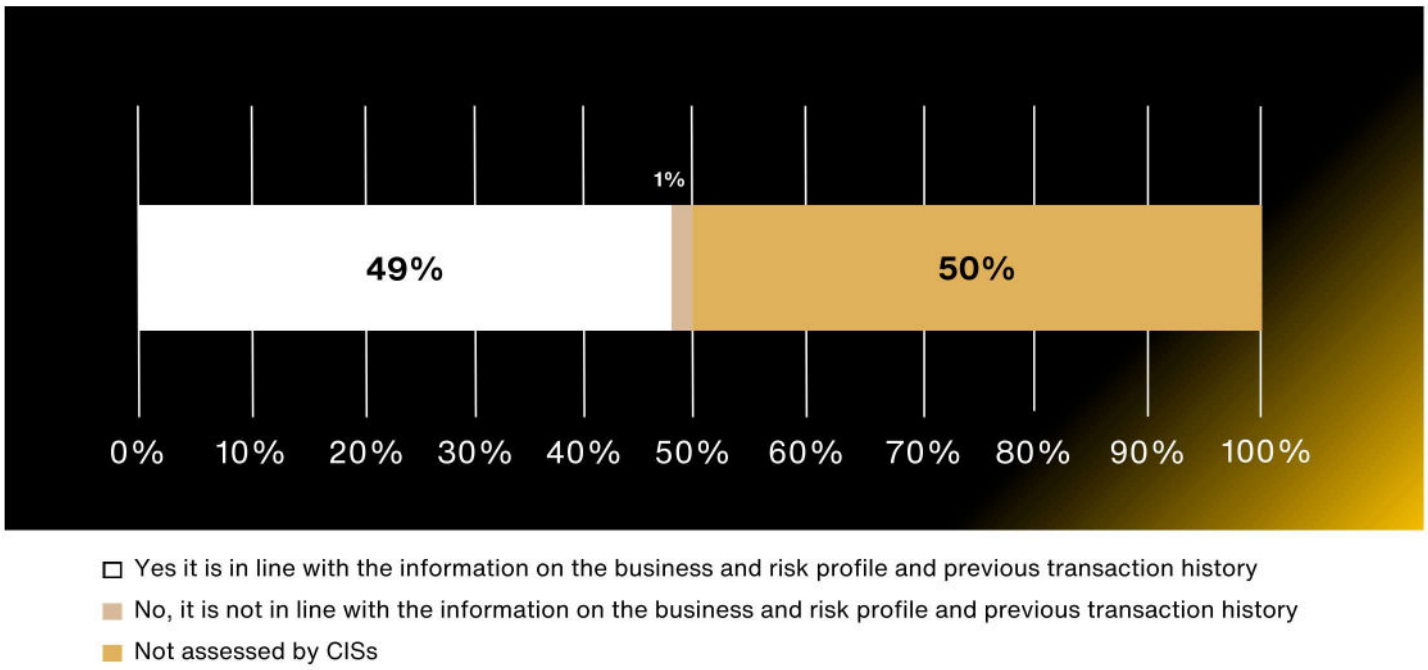


Was the transactional behaviour is in line with the business and risk profile of the customers or with the previous transactional history?

The customer files review also sought to assess whether transactions aligned with the customer's profile and with previous transaction patterns.

Findings revealed that in 50% of cases, the assessment was not carried out by the CISs so it could not be determined if the transactional behaviour is aligned with the business and risk profile of the customer or with the past transactional patterns. However, in 49% of the customer files reviewed, customers' transactional behaviour was in line with their previous historical transaction patterns and the business and risk profile. Only 1% of the files reviewed showed transactional behaviour that did not align with previous transaction history or the business and risk profile.

Chart 19: *Is the transactional behaviour consistent with the business and risk profile of the customer and with past transaction patterns?*



Review of transactions

The thematic review also assessed whether the transactions carried out by CIS's customers were scrutinised in scenarios where manual transaction monitoring was applied and when automated transaction monitoring was conducted.

Chart 20: *Review of transactions* ***when manual transaction monitoring was conducted***

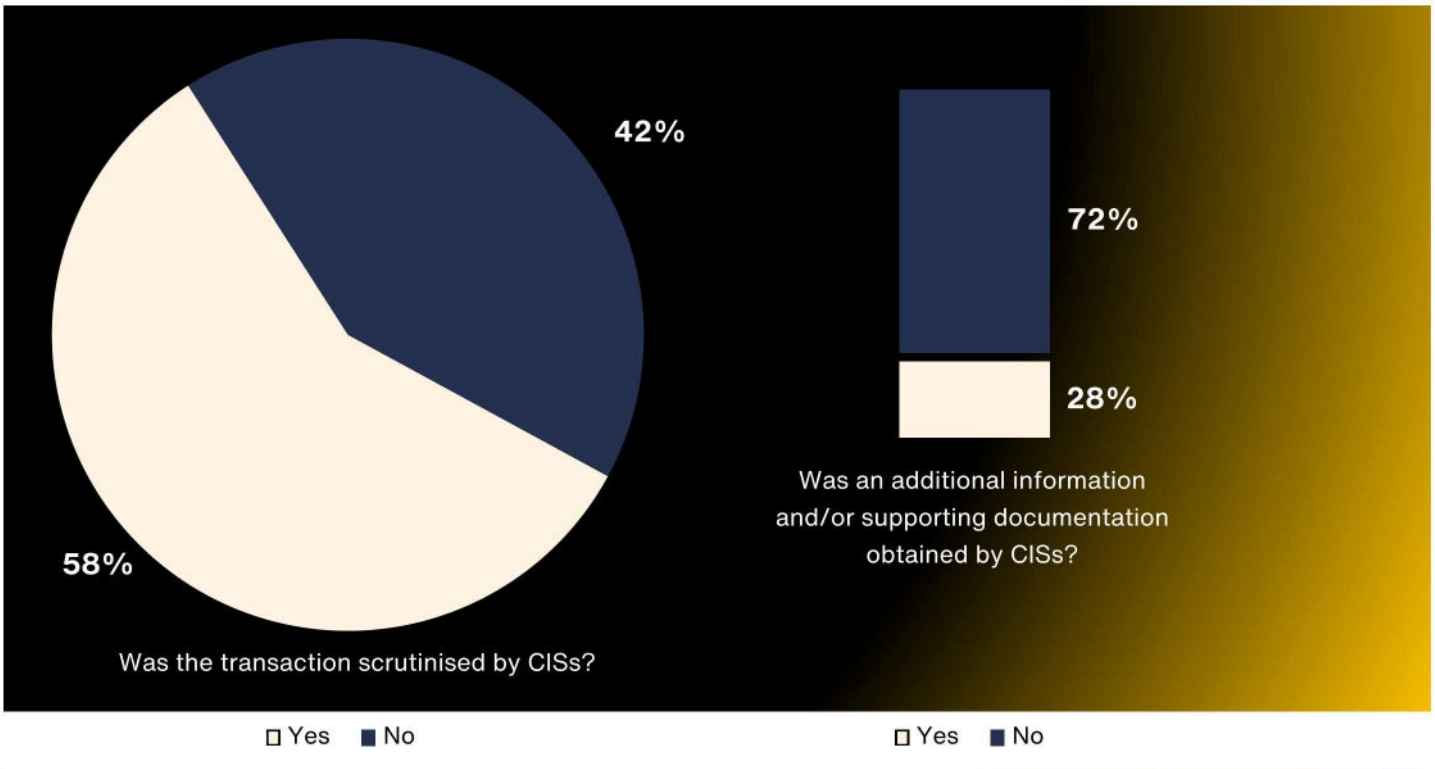
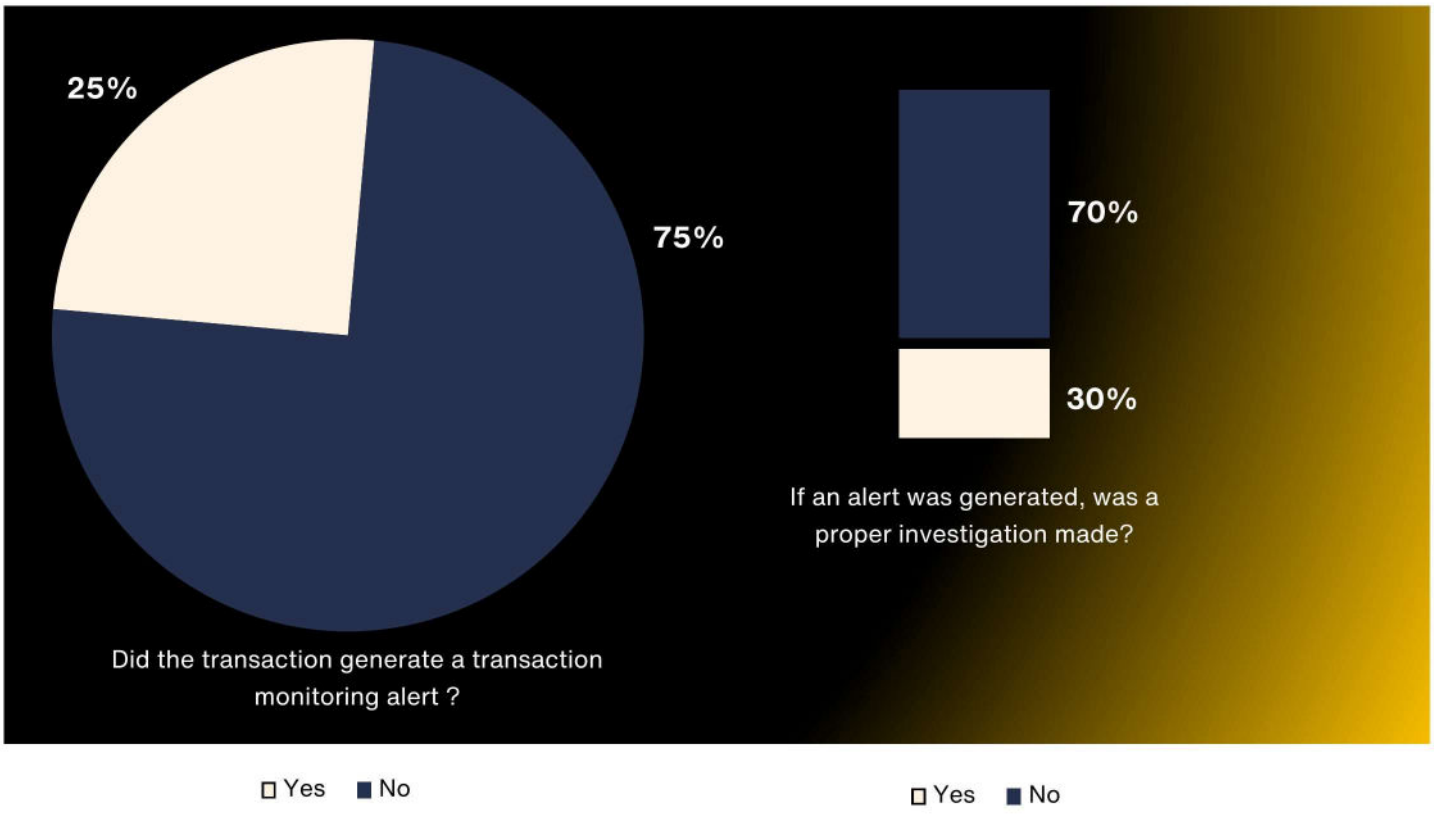


Chart 21: *Review of transactions* ***when automated transaction monitoring was conducted***



Adequacy of Transaction monitoring methods adopted

The thematic review revealed that 14 out of the 20 CISs (70%) were not carrying out transaction monitoring adequately or lacked the evidence to show that this was taking place. Some key issues identified included:

Lack of customer profiles	Lack of transaction scrutiny evidence	Inability to detect behavioural changes or unusual transactions
CIS did not maintain comprehensive profiles on all their customers.	Most of the CIS were aware of the transaction monitoring requirements and carried out some form of scrutiny, as per interviews conducted, several CIS were not able to provide any evidence of this.	The CIS were unable to detect changes in customer behaviour, transaction patterns, or unusually large transactions, presuming these activities are normal for large credit and/or financial institutions on which they apply SDD.

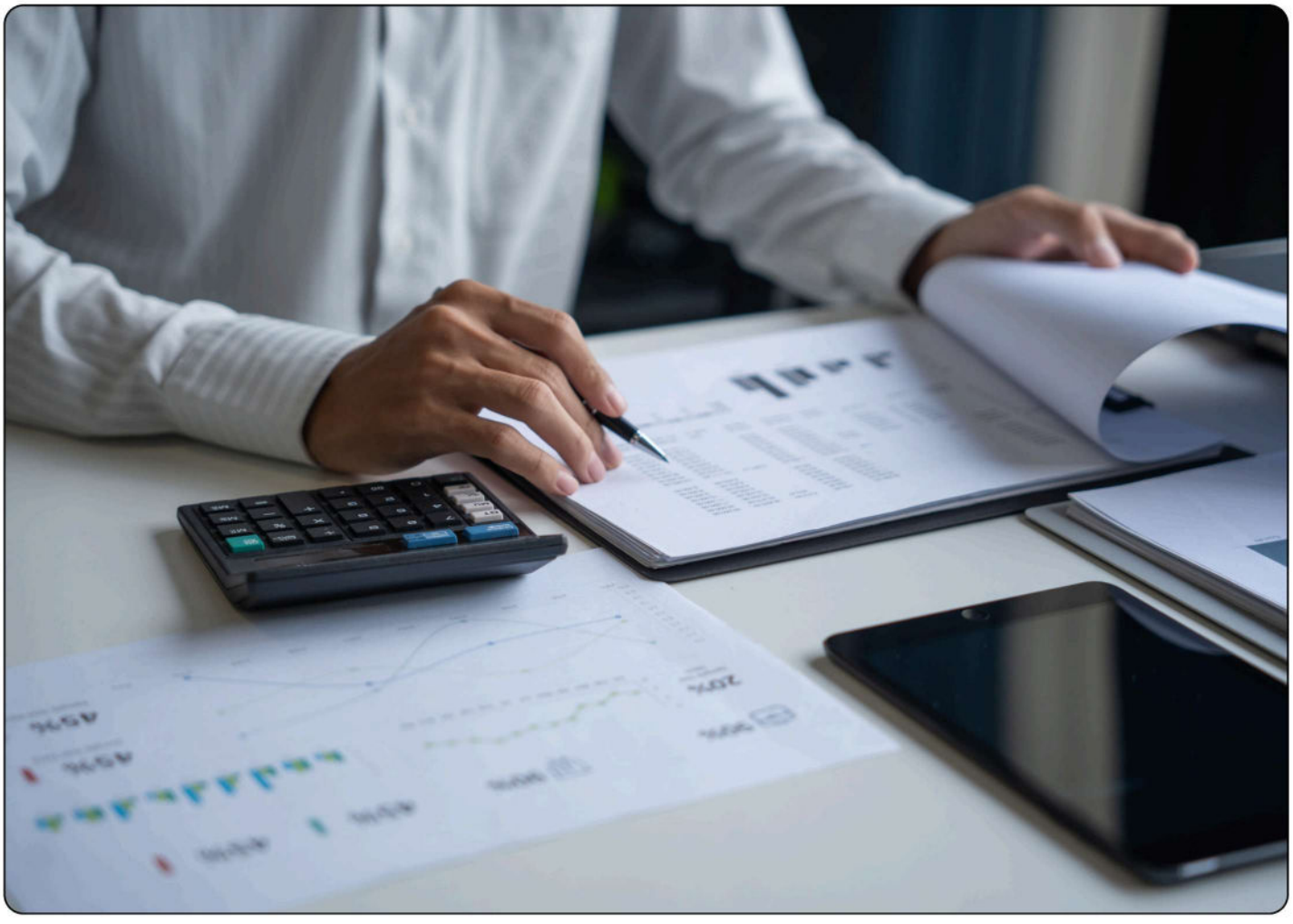
Bad practice: No Alerts generated from the system

The transaction monitoring system of a CIS did not effectively identify and address unusual activities. Specifically, it did not trigger any alerts for subscription transactions, and alerts for redemptions were frequently dismissed as a false positive without any additional justification.

Bad practice: Evidence of transaction monitoring was not recorded

A CIS relied solely on manual transaction monitoring, given that it processed only a limited number of transactions per year. However, when requested to provide evidence demonstrating that transaction monitoring was being conducted, the MLRO responded that no suspicious transactions had been identified and, as a result, no records had been maintained.

The absence of any documentation meant that the CIS was unable to demonstrate that transaction monitoring had in fact been carried out. This approach reflects a fundamental misunderstanding of regulatory obligations, where the effectiveness of transaction monitoring cannot be measured solely by the presence or absence of suspicious activity, but must also be evidenced through appropriate and consistent record-keeping.



Key Takeaways

1 Key Takeaway 1: Responsibility for carrying out transaction monitoring

Section 4.10.2 of the IPs specifies that the obligation to conduct ongoing monitoring of a business relationship, as outlined in Section 4.5 of the IPs, remains the sole responsibility of the CISs. This means that CISs cannot delegate their responsibility to another subject person or third party for scrutinising transactions or for ensuring that information, data, and documentation remain up to date, except as explicitly stated in Section 4.10.2 of the IPs.

Both CISs and Fund Administrators are considered subject persons under the Maltese AML/CFT regulations, and the obligations apply equally to both. Fund Administrators typically have insight into CIS transactions due to their operational roles, which may include back-office functions and acting as the CIS's transfer agent, handling subscription, redemption, and transfer requests.

However, the ultimate responsibility for ongoing monitoring, including transaction monitoring, lies with the CIS. This remains true even when the Fund Administrator is appointed as the MLRO under the exception provided in Section 5.1.2(a)(ii) of the IPs, since the underlying investors are the CIS's customers.

2 Key Takeaway 2: Understanding the activities that the CIS's customers are undertaking

The nature of transaction scrutiny in the case of CISs will be somewhat different from that carried out by other subject persons, as the nature of the business relationships they hold with customers is not characterised by frequent transactions.

In this context, the key form of transaction scrutiny that CISs are to undertake is to compare investments made into the scheme against what CISs know about a customer's business and risk profile to confirm that the amounts invested are in line with their knowledge and understanding of the regulated customer. It is not enough to look at every transaction in isolation. CISs need to consider the transactions taking place over a given period to assess whether, when taken into account together, they match the information provided in the customers' business and risk profile.

Key Takeaways

3 Key Takeaway 3: Transaction Monitoring in relation to investments made by nominees

With regards to investments made by nominees, there will be no SoW against which to compare new unit acquisitions through subscriptions, as the funds invested would not pertain to the nominee but to the underlying investors. This does not mean that no transaction monitoring is to be carried out. In this scenario, CISs must ascertain that:

a. A nominee provides information on the underlying customers that it services, which can be useful to understand whether the volume and value of transactions being processed are reasonable.
b. It is possible to compare investments made over a given period to identify outlier transactions which may represent an increase in funds transferred to the CIS compared to the rest. Where one or more of these transactions are identified, CIS must ask the nominee whether there is a reason for the increase in activity.

4 Key Takeaway 4: Adapting and fine-tuning the automated transaction monitoring systems

When CIS adopt transaction monitoring systems, these should be based on a set of risk-based detection rules tailored to the CIS's business model, customer base, transaction channels and historic transaction activity. There is no one-size-fits-all approach, and such rules should be calibrated based on the specific ML/FT risks associated with the CISs' customers. The following are to be considered:

- The values and/or volumes of the thresholds and parameters established for specific customer segments should be realistic. Setting thresholds and parameters that are too high may hinder the CIS's ability to effectively monitor transactions when considering the transaction amounts and ML/FT risks involved. Therefore, this may result in certain large transactions or deposit spikes not being detected and properly scrutinised.
- A set of parameters or factors within which transactions are considered 'normal' for a particular customer or customer segment should be defined. This will allow CIS to determine whether the customer's transactions or behaviour are consistent with their knowledge, and if necessary, question any discrepancies noted.

Furthermore, detection rules must be tested and fine-tuned periodically from both a technical aspect and an effectiveness standpoint. The need for such regular tuning is to allow for more granular analysis while minimising the likelihood of false positives being generated.

CISs can refer to the **Guidance Note on the Obligation of Transaction Monitoring** for a non-exhaustive list of the factors that may be considered when developing detection rules, as well as some practical examples of risk scenarios that can be applied.

Key Takeaways

5 Key Takeaway 5: Managing Alerts

When a transaction monitoring alert is generated, CISs should have an adequate process for the notification, prioritisation, handling and recording of these alerts, as well as of the actions taken. Where appropriate, transaction monitoring analysts may need to adopt a more holistic approach and consider all the following:

i) the alerted transaction in question
ii) the customer's transactional history
iii) past alerts for the customer

If the elements resulting in the alert provide reasonable grounds to suspect ML/FT, CISs must report this suspicious transaction to the FIAU without undue delay in line with Regulation 15(3) of the PMLFTR.

Conclusion

CISs must recognise that whilst Regulation 10 of the PMLFTR provides for the application of SDD, it does not represent an exemption from carrying out CDD. Rather, it is a variation of the extent and timing of the due diligence to be applied due to the lower risk of ML/FT that the circumstances present. It is also important to acknowledge that SDD should not be implemented by default for certain types of customers, such as customers providing relevant financial business, without a proper assessment of risks.

The FIAU expects all CISs servicing regulated entities providing relevant financial business to review the findings of this paper, and implement any required updates as necessary, to ensure that their controls are adequately designed to allow for accurate application of SDD.

Addressing the gaps highlighted in this paper is critical to ensuring that SDD is applied appropriately and consistently by CISs when servicing customers conducting relevant financial business. Such is essential to balance regulatory compliance with effective risk management, thereby contributing to safeguarding Malta's integrity and reputation as a strong, yet competitive investment centre.

Questions on this document may be sent to:
compliance@fiaumalta.org

Financial Intelligence Analysis Unit
Trident Park, No. 5, Triq l-Mdina,
Central Business District Birkirkara, CBD 2010

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

Timing of SoF and the anticipated level and nature of activity

Chart 13: *Timing of SoF and anticipated level of activity*