Frequently Asked Questions

Client Due Diligence (CDD)

The FAQ on AML/CFT & Sanctions is a dynamic document that is periodically updated by the ICPAC Monitoring & Compliance Team. Updates are based on questions received from ICPAC Members during support interactions and from participant inquiries raised in ICPAC seminars.

The information provided in this FAQ is intended for general informational purposes only and does not constitute legal or professional advice. While we strive to ensure that the information is accurate and up-to-date, regulations, laws, and procedures may change, and interpretations may vary depending on specific circumstances. For any legal, compliance, or regulatory concerns, it is strongly recommended that you consult with qualified legal or compliance professionals to ensure adherence to relevant laws and regulations.

Date of Issue: 16 April 2025

Last Updated:04 December 2025 (Questions 14-22 added)

FAQs

Client Due Diligence (CDD)

1. **Q.: How can the source of a company's wealth be verified if it holds assets, such as properties, acquired for example over 15 years ago that remain on its books, especially when the company has changed auditors twice since the acquisitions?**
   A.: As a first step, it is important to make a distinction between this very frequent question. From an AML/CFT perspective, the focus is not on the company's overall wealth as reflected in its net assets. Instead, what is relevant for AML/CFT risk assessment and customer due diligence (CDD) purposes is the legitimacy of the specific funds used to acquire the properties. This applies regardless of whether the funds originate from the activities of the company itself or are sourced externally, such as through a bank loan or capital contributions from the owners.

   The following steps may help:

i. **Gather Information from the Client**:
   - Request documentation related to the acquisition of the assets, such as purchase agreements, invoices, title deeds or any available financial records.
   - Obtain explanations from the client regarding the origin of the funds used to acquire these assets, including any loans, capital injections, or other financing sources.

ii. **Review the Historical Context:**
   - Evaluate whether the acquisition aligns with the company's economic profile at the time. Consider the company's financial position, industry, and operational scale during the period of the acquisition.

iii. **Audit Trail Examination:**
   - Review the audit reports and financial statements from the time of the acquisition to understand how these assets were recorded and whether there is sufficient continuity in the records.
   - Pay special attention to any discrepancies or missing information that may have arisen due to changes in auditing firms.

iv. **Assessment of Economic and Regulatory Fit:**
   - Check if the asset acquisitions make sense in the context of the company's historical activities and growth trajectory. Ensure that the acquisitions appear consistent with the company's stated objectives and practices during that time.

v. **Verification with External Sources:**
   - Use publicly available records (e.g., land registries)
   - Where necessary, obtain information on the historical market value of the assets at the time of acquisition to corroborate their financial impact.

vi. **Professional Judgment:**
   - Use professional judgment to assess whether the client's explanations and supporting documentation are credible and sufficient to justify the source of wealth.

- Consider the overall risk profile of the company and whether any additional checks are warranted, especially if there are indications of irregularities.

2. **Q.: When a client's UBO resides outside of Cyprus, has invested in multiple businesses, and the Cyprus-based company is managed by an ASP providing administrative services, would this situation raise any red flags and necessitate additional due diligence?**
   A.: Yes, this situation could raise red flags and necessitate additional due diligence depending on the specifics of the case. The following factors should be considered as potential red flags:

a) **UBO Residence in Higher-Risk Areas:** If the Ultimate Beneficial Owner (UBO) resides in a jurisdiction known for higher financial crime risks, inadequate regulatory frameworks, or political instability, this would require enhanced scrutiny.
b) **Nominee Shareholders or Bearer Shares:** The use of nominee shareholders or the existence of bearer shares within the ownership structure may indicate an attempt to obscure true ownership and should trigger further investigation.
c) **Unusual or Excessively Complex Ownership Structure:** If the company's ownership structure is unnecessarily intricate or disproportionate to the company's stated business, it could signal attempts to hide beneficial ownership or obscure illicit activities.
d) **Non-Face-to-Face Relationships or Transactions:** The absence of direct, in-person engagement in the business relationship increases risks and requires additional safeguards, such as robust electronic verification processes and supplementary checks.
e) **Nature of the Client's or UBO's Business Activity:** Activities in high-risk sectors (e.g., arms dealing, activities involving substantial cash handling, or unregulated industries) warrant heightened scrutiny, especially if there is a significant risk of corruption or illicit activities.

Additional Due Diligence measures may include:
a) Verifying the UBO's source of funds and wealth.
b) Conducting enhanced checks on the UBO's jurisdiction of residence and associated risks.
c) Reviewing the rationale for the complex ownership structure and seeking additional clarifications.
d) Assessing the adequacy of the ASP's internal controls and compliance frameworks.
e) Utilizing external intelligence tools, such as open-source checks or third-party databases, to identify any adverse information on the UBO or related entities.

Such measures are necessary to ensure that all risks are adequately addressed in line with applicable legal and regulatory requirements.

3. **Q.: Are firms required to perform due diligence on bank signatories and other individuals who have been granted power of attorney?**
   A.: According to Paragraph 5.2.1 of the AML Directive, firms are required to identify and verify any third parties authorized to represent the client and ensure that these individuals possess legitimate authority. Additionally, Paragraph 4.2 of the Sanctions Directive stipulates that screening must also be conducted on third/authorised parties.

4. **Q.: If a company undergoes a change in ownership, transferring shares from an individual with adverse media coverage, ongoing legal issues, and frozen assets to a new owner, does this transfer alone classify the company as high-risk and necessitate enhanced due diligence (EDD)? Furthermore, would such circumstances justify the submission of a suspicious activity report?**
A.: This situation could raise the company's risk to high-risk, requiring enhanced due diligence (EDD), and may also warrant the submission of a suspicious activity report (SAR).

The key considerations when assessing this case are as follows:

i. **Frozen Assets**: The freezing of assets indicates potential involvement in illicit activities or relates to a designated person under sanctions, elevating the risk profile of the company. When assets are frozen due to the application of sanctions, and conditional to the services provided (e.g. custodian/director services), the business relationship should be subject to enhanced scrutiny and ongoing monitoring to ensure that assets remain frozen and no funds or economic resources are made available to the designated person. In the event that a designated BO wants to transfer ownership of the company, circumvention of sanctions considerations should also be made.
ii. **Court Ruling Impact**: Even if the court ultimately rules in favor of the previous owner, the obliged entity must critically assess the reasons behind the decision. For example, the acquittal may be based on technicalities unrelated to the accusations, which may not necessarily mitigate the inherent risk.

Additional considerations include:

i. **Timing of the Ownership Transfer**: Examine when the transfer occurred in relation to adverse media and legal issues, as this may indicate whether the transfer was an attempt to shield the company or its assets.
ii. **Transaction Monitoring**: Implement robust transaction monitoring to identify any suspicious activity that could link the company to the accusations.
iii. **Source of Funds (SoF)**: Verify the source of funds to ensure that no funds related to the allegations have been funneled through the company.

It should be noted that the approach to be followed and the above considerations would remain the same even if only one of the two elements of the question was applicable, i.e., a change of ownership for designated person or BO with adverse media and legal issues.

5. **Q.: If we obtain confirmation from regulated professionals (e.g., accountants, lawyers) with knowledge of the client to corroborate the Source of Wealth (SoW), does this constitute reliance on a third party, requiring us to perform the relevant assessments on this party beforehand?**
A.: Obtaining confirmation from regulated professionals with knowledge of the client's Source of Wealth (SoW) can serve as an **additional method** of corroborating the information provided by the client.

The key factor is whether the regulated professional provides independent evidence or simply supporting documentation. If the professional's confirmation is being used to

corroborate specific evidence provided by the client (e.g., inheritance deeds, sale agreements, or bank drafts), then it enhances the robustness of your assessment rather than serving as a substitute for your due diligence.

It is essential, however, to ensure that the evidence aligns with the declared SoW. For a suggestive list of examples of appropriate information and/or supporting documentation required to establish SoW and SoF you may access ICPAC Guide on establishing Source of Wealth (SOW) and Source of Funds (SOF), here.

Whether or not reliance applies depends on the scope and nature of the professional's involvement. If they are performing functions such as gathering information or conducting due diligence on your behalf, this may require you to assess the third party's systems and procedures, in accordance with section 5.10 of the AML directive. However, in accordance with Article 67(5) of the Money Laundering and Terrorist Financing Activities Law of 2007 (L. 188(I)/2007), the requirements for assessing third parties for client identification procedures and client due diligence measures do not apply to outsourcing or agency relationships, where, based on a contractual arrangement, the outsourcing service provider or agent is to be regarded as part of the obliged entity.

Each case must be evaluated individually, as there is no universal "yes" or "no" answer.

6. **Q.: When onboarding new clients undergoing liquidation, are there any differences in the CDD procedures compared to the standard process?**
A: Client Due Diligence (CDD) procedures are conducted based on the firm's risk-based assessment, which allows for tailoring the due diligence process to mitigate the specific risks identified. While the overall process remains consistent, the depth and focus of the CDD measures may differ depending on the client's risk profile and specific situations.

For clients undergoing liquidation, it is essential to assess any heightened risks associated with this status and design appropriate measures to address them. Regardless of the client's risk category, identification and verification of the client must always be performed as part of the CDD process.

Furthermore, the firm must be equipped to address critical questions and considerations and conduct additional checks when performing due diligence on these clients, including but not limited to:

a) Whether the liquidation is voluntary or not.
b) Whether the assets held may have been acquired through illicit activities.
c) The identity of the Beneficial Owner (BO) and any recent changes to ownership.
d) Whether the assets are being sold at a significant profit/loss.
e) If third parties involved in the liquidation transactions have close ties to the BO.
f) Confirming ownership of assets before proceeding with liquidation.
g) Obtaining a detailed understanding of the company's activities prior to liquidation.
h) Establishing the background and legitimacy/validity of any creditors.
i) Establishing the validity of debtors, ensuring they are not fictitious clients, shell companies, or entities with inflated receivables, particularly in high-risk jurisdictions.

7. **Q.: What is the difference between "source of funds" and "source of wealth," of the client and how it should be assessed during due diligence?**
A.: Source of Funds: Refers to the specific origin of the money used for a particular transaction or investment, such as income generated from a trade activity, a loan, or proceeds from the sale of an asset.
Source of Wealth: Refers to the overall origin of an individual's or entity's accumulated wealth, including their lifetime financial history, such as inheritance, long-term investments, or business ownership.

   In essence, the source of funds is transaction-specific, while source of wealth provides a broader, holistic view of financial position.

   For detailed information, refer to ICPAC's guide titled "Guidance on establishing SOF and SOW".

8. **Q.: Is a firm allowed to adopt a certification method other than those specified in Annex III of the Directive to Members of ICPAC on Anti-Money Laundering and Combating Terrorist Financing Activities?**
A.: The certification methods mentioned in this Annex is a **suggested non-exhaustive list** of methods of certification. It is important that if a firm chooses a different certification method, it should make sure that this does not fall within the concept of the Third Party reliance as stated in paragraph 5.10 of the AML/CFT Directive. Whatever the method of certification the firm chooses, there should be evidence of the assessment of each method which should be clearly documented in the firm's AML/CFT Manual. This should include details on the procedures to be followed, including type of certification evidence, reference to the retention policy, and information about the credential of the individual certifying documents, for example, their profession, the requirement for them to be supervised under AML/CFT legislation, and whether they are located in the EU or equivalent countries. Additional checks should be performed in higher risk cases, for example, checking certified documents against official sources or public registries where possible.

   Irrespective of the chosen method, it is important that the firm establishes and maintains direct contact with the client.

9. **Q.: Can I use electronic verification for KYC/CDD purposes?**
A.: The AML/CFT Law allows for the use of electronic verification provided that a comprehensive risk assessment for AML/CFT purposes is performed prior to introducing it as part of the firm's compliance program.

   In assessing the risks associated with the use of electronic verification, the firm should consider the risks both at the client level and at the firm level.

   The risk assessment should recognize the **inherent risks** associated with electronic verification, including the risk of impersonation fraud, the risk that the client's identity is not the claimed identity, and the risk of the identity document provided may be stolen,

suspended, revoked or expired. The risk assessment should also consider the technical standards of the solution to be used, the reliability of the CDD measures regarding non face-to-face clients and electronic verification and the enhanced delivery channel and geographical risks.

Based on the results of the risk assessment, the firm should design and establish appropriate, adequate and proportionate procedures for mitigating those risks.

The use of electronic verification should be covered in the firm's documented policies and procedures which, as a minimum, should specify in which situations, for which type or category of clients, and for which services can electronic verification be used. The policies should also specify the features and functionality of the chosen solution.

Key considerations when assessing an electronic verification solution include:

a. **Check what the capabilities of the solution are**: does the system cover all three areas of KYC, risk assessment and verification of identity?
b. **Check the sources of the system**: Does the system draw from multiple sources, does it use only official sources, e.g. government records and how reliable are the sources?
c. **Check the system's control mechanisms**: Does the system support data integrity checks that are transparent as to allow the firm to assess the reliability and quality of data and are those checks available to the user for review?
d. **Ease and accessibility of data**: Can the data produced be extracted, saved and used and if so, do the exported reports include necessary information to identify the timing, source, name of user and system details?

It is strongly recommended that you test the solution and document the process prior to its introduction as part of your firm's policies, procedures, measures and controls, given particular attention to the quality, completeness, accuracy and adequacy of data provided.

When relying on third parties who use electronic verification methods, you should ensure that the solution used fully complies with the requirements of the AML/CFT Law. You should also satisfy yourself that the third party's KYC/CDD procedures relating to non face-to-face clients and the use of electronic verification are sufficient and consistent with the requirements of the AML/CFT Law and your firm's policies.

It is emphasized that the **responsibility** of ensuring that the information obtained through electronic means is accurate, reliable and sufficient remains with the firm and should not be extracted blindly from any single online solution. Furthermore, depending on the risk classification of the client, i.e. for higher risk clients, further enhanced measures might be required and should be assessed on a case-by-case basis.

10. Q. Is the use of video call considered as a face-to-face meeting?

A.: Although electronic verification of identity is not automatically considered equivalent to a face-to-face meeting, the firm may opt to utilize any electronic verification method, conditional to conducting and documenting a comprehensive risk assessment of the ML/TF/PF/sanctions risks involved and given that sufficient safeguards are put in place. For example, you may choose to conduct a video call to meet the client coupled with

scanning of biometric features capabilities, e.g., through the use of A.I. and scanning of the documents presented during the video call with the documents already provided. Alternatively, the firm may choose to accept dynamic selfies which support liveness detection given that the quality of the image and/or audio is sufficient to allow verification, while utilizing a built-in computer application that automatically identifies and verifies a digital image or video source, e.g., biometric facial recognition or a built-in security system that detects hampered images. In any case, proper filing and retrieval capabilities of the video call should be ensured.

Firms should keep evidence of the electronic method used at all times. It is once again highlighted that, whatever electronic method the firm wishes to employ, it must first perform a risk assessment for each verification method used, identifying the potential associated risks and implementing appropriate mitigation measures for the specific risks. The risk assessment should be documented and kept up to date at all times.

The use of electronic verification methods should also be reflected in the firm's AML/CFT and Sanctions Manuals with references to, as a minimum, the type of clients and services such method can be used and description of their features and functioning. Depending on the risk of the client, a video call might not be sufficient.

Finally, the firm should make sure the all staff involved in the specific process is duly and sufficiently trained.

11. **Q.: What is the extent of CDD required when providing tax services?**
A.: As a rule, the extent of CDD measures applied is linked to the risk level attached to each service line which should be assessed during the firm's firm-wide risk assessment and client risk assessment.

The following is a guide on how to approach the assessment:

i. Map out all services the firm offers and fall under the umbrella term of "tax services" and identify the level of risk associated with each one of the services listed.
ii. Based on the identified risks and the likelihood of those risks materializing along with the estimated impact they would have on the firm, appropriate, adequate and proportionate risk mitigation measures should be designed and implemented. For example, the risk associated with registering a client with tax authorities services or the preparation and submission of a standard statutory tax return form for an employee may be assessed as lower risk and as such identification and verification measures only may suffice, if there are no other risk factors that would elevate the client to a higher risk classification. If, on the other hand, the service provided is tax planning or advice on how to minimize taxes, then this could be assessed as carrying a higher risk element, and thus EDD measures for the specific element of risk should be carried out.
iii. Apply mitigating measures according to the firm's policies. For instance, the firm may restrict the particular high-risk service to clients that do not exhibit high-risk characteristics, for instance, clients that do not have complex structures or excessively large transactions. The firm may also apply EDD measures to clients requesting high-risk services, to address the specific risk factors associated with the service.

Beware, however, that the type of risk associated with a service may be very different when assessed under a different scope. For example, the preparation of tax forms for the distribution of dividend may be perceived as of lower risk when assessed from an AML perspective but may be much higher when assessed from a sanctions perspective, due to the potential involvement of designated individuals or persons linked to them.

12. **Q: What do I do if there is no shareholder with over 25% ownership? Who should I identify as a beneficial owner for KYC/CDD purposes?**
A: The AML/CFT Law clearly provides for both ownership and control criteria when identifying a beneficial owner (BO). More specifically it states that apart from the 25%+1 ownership percentage, the BO is the natural person that exerts control over the company via other means as well, e.g., by having dominant influence. The Law also provides that, if after exhausting all possible means, a BO cannot be identified, then the senior management official should be considered as the BO for KYC/CDD purposes.

13. **Q.: I am the trustee of a Trust. I have registered the Trust BO's in CySEC's CyTBOR. Do I still need to inform ICPAC?**
A: Yes. Registration of the Trust with ICPAC's Trust Registry and registration of the BOs of the Trust with the CySEC Registry are two distinct and unrelated legal obligations. Registration of the Trust with ICPAC's Trust Registry emanates from article 25A of the ASP Law (L. 196(I)/2012) and ICPAC's Trust Registry does not hold any information on the Bos of a trust, whereas registration of the BO's with CySEC's Registry emanates from article 61C of the AML/CFT Law and relates to the provision of BO information, such as identification details, date of birth etc. As such, where the trustee of Trusts is an ICPAC regulated person, then the Trust should be registered under both Registries for the Law requirements to be fulfilled.

14. **Q.: Does the initial client information profile collected at the commencement of the business relationship need to be a signed hard-copy form kept on file, or is an electronic submission—such as an email, online form, or e-signature—acceptable?**
A: An electronic submission is acceptable. The initial client information profile does not need to be a hard-copy form kept on file, provided that the information is accurately recorded and securely stored. Acceptable formats include email correspondence, online form responses, or electronically signed documents, as long as they meet the recordkeeping and authentication standards obligations derived by Law. It is important, however, to verify that the person providing the information has the necessary authority and knowledge to do so, and that your firm has taken appropriate measures to identify and verify that individual. This information should also be readily available for review if requested by ICPAC or other competent authority.

15. **Q.: If the Ultimate Beneficial Owner (UBO) is different from the shareholder, and this information is known, documented, and recorded in the UBO register, have we as auditors committed an offence under the Anti-Money Laundering (AML) legislation?**
A.: Under the AML Law (Article 61A), there is a clear obligation to record the beneficial owner of each entity in the UBO Register. Beneficial Owners are defined in **Article 2** of the AML Law. According to **Article 61(1)(b)** of the AML Law, obliged entities must identify and verify the beneficial owner of their clients. In situations where the legal shareholder differs from the actual beneficial owner, the obliged entity must take appropriate measures to obtain and retain supporting documentation, such as a Declaration of Trust or other relevant evidence, to substantiate the ownership structure. Furthermore, in accordance with **Article 61A(5)(b)**, obliged entities are required to report to the Registrar of Companies any discrepancies identified between the information recorded in the Beneficial Owners Register and the information held in their own records.

16. **Q.: If a client structure is large and complex, are we required to obtain information on all group companies, including their sources of funds and activities?**
A.: Under Article 61(1)(b) of the *Prevention and Suppression of Money Laundering and Terrorist Financing Law (188(I)/2007)*, obliged entities must take reasonable measures to verify the identity of the beneficial owner **and to understand the ownership and control structure of the client**.
In addition, Article 61(1)(c) requires obliged entities to obtain information on the purpose and intended nature of the business relationship, while Article 61(1)(d) obliges them to conduct ongoing monitoring and, where necessary, to establish the source of funds.
Therefore, where a client belongs to a large or complex group, the obliged entity must gather sufficient information to understand:
    - The ownership and control structure of the group;
    - The purpose and intended nature of the business relationship; and
    - The source of funds relevant to the client relationship.

    As clarified in Article 61(2), the extent of due diligence measures should be determined on a ***risk-sensitive basis***. This means that the depth of information collected should be proportionate to the assessed level of money laundering or terrorist financing risk.

    In summary, it may not be required to obtain **detailed** information on every entity within the group, but the obliged entity must be able to demonstrate a clear understanding of the group's structure and the flow of funds relevant to the client, consistent with its AML/CFT obligations.

17. **Q.: In the case of non–face-to-face clients, must we always consider these clients as high risk and perform Enhanced Due Diligence (EDD)?**
A.: Non–face-to-face relationships do not automatically constitute a high-risk situation. However, under Article 61(1)(a) of the Prevention and Suppression of Money Laundering and Terrorist Financing Law (188(I)/2007), obliged entities must verify a client's identity

using reliable and independent sources, including secure electronic identification methods (please revert to FAQ 9).
According to Article 61(2) of the same Law, the extent of due diligence measures should be determined on a ***risk-sensitive basis***. This means that where non–face-to-face onboarding presents a higher risk of impersonation, fraud, or anonymity, the obliged entity must apply *enhanced due diligence (EDD)* measures to mitigate those risks.
Enhanced measures may include:

- Obtaining additional identification documents or information;
- Using secure electronic identification systems regulated under the EU eIDAS Regulation (EU) 910/2014;
- Performing additional verification checks or independent confirmation of documents.
- Furthermore, paragraph 5.4 of the ICPAC AML Directive provides that non–face-to-face business relationships should be assessed carefully and appropriate measures must be taken to compensate for the higher risk of impersonation or identity fraud.
- In summary, non–face-to-face clients are not automatically high risk, but such relationships require a thorough risk assessment. If higher risk factors are identified, the firm must apply Enhanced Due Diligence to ensure compliance with both the AML Law and ICPAC's AML Directive.

18. Q.: If we consider a third party's AML procedures insufficient, must we request to bypass them and communicate directly with the client?

Concerning the first part of the question regarding the insufficient AML procedures, as per section 5.10.2 of ICPACs AML Directive, reliance for CDD purposes may only be placed on a credit institution, a financial institution, an auditor, an external accountant, a tax advisor, a trust and company service provider or an independent legal professional that operates in a country of the European Economic Area or in a third country and fulfils the following conditions:

a. It applies CDD and record keeping measures which are consistent with the measures pursuant to the EU Directive and
b. It is subject to supervision which is consistent with the requirements of the EU Directive.

According to 5.10.3- Before accepting the information and documentation by the said third party, the firm should apply the following additional measures/procedures:

a. Assess the systems and procedures applied by the third party for the prevention of money laundering and terrorist financing
b. Satisfy itself based on the assessment of point (a) that the third party implements client identification and due diligence systems and procedures which are in line with the requirements of the Law and this Directive
c. Maintain a separate file for every such third party, where it stores the assessment report relating to point (a) and other relevant information
d. Take steps to ensure that the third party to be relied upon will provide copies of the original documentation immediately
e. The commencement of the cooperation with the third party and the acceptance of client identification data verified by the third party is subject to approval by the Compliance Officer.

Therefore, if the firm's assessment of the third party's AML framework produces unsatisfactory results, the **Compliance Officer should not approve the cooperation**.
Furthermore, reliance on a third party is permitted **only at the outset** of the business relationship. Firms that initially rely on a third party must conduct all ongoing monitoring directly with the client.
Finally, it should be noted that, under **Section 5.10.1 of the Directive**, the firm **remains fully liable** for any compliance failure, notwithstanding its reliance on a third party.
In conclusion, the firm must complete the assessment of the third party prior to accepting any new clients introduced by that party, while all ongoing monitoring obligations remain the firm's direct responsibility and must be carried out through direct contact with the client.

19. **Q.:If an audit firm does not provide administrative services to its clients, is it required to perform transaction monitoring in the same way as an Administrative Service Provider (ASP)?**
A.: Audit firms are not expected to perform transaction monitoring in the same way as Administrative Service Providers (ASPs), since the nature, scope, and timing of their professional engagement/service are fundamentally different.

Auditors and ASPs both have obligations under the AML/CFT Law (188(I)/2007) and ICPAC's AML Directive, but their monitoring responsibilities differ in practice:

- Auditors are *not involved in real-time transaction processing*. Their work is retrospective, focusing on the review of financial statements and historical data. As such, their responsibility lies in considering compliance with laws and regulations related to money laundering, terrorist financing, and sanctions, as prescribed in ISA 250 (Revised).
    - Auditors must remain alert for indications of non-compliance during the audit, such as unusual payments, transactions with tax havens, or unexplained related-party dealings.
    - When such indicators arise, the auditor must assess whether these constitute a reportable suspicion under Articles 69 and 27 of the AML Law and report to MOKAS if necessary.

- Administrative Service Providers (ASPs), on the other hand, are actively involved in real-time transaction execution—for example, managing bank accounts, authorising payments, or providing directorship services. Consequently, they are required to implement continuous, proactive, and detailed transaction monitoring on an ongoing basis.

In essence, while both auditors and ASPs are obliged to comply with AML/CFT and sanctions monitoring requirements, the extent and frequency of monitoring must be risk-based and proportionate to the nature of the service provided:

- Auditors apply monitoring through audit procedures and professional scepticism, mainly post-transaction.

- ASPs apply continuous transaction scrutiny before and during transaction execution. Therefore, an audit firm that does not provide administrative services should still perform ongoing monitoring in line with its AML/CFT obligations — but this monitoring is limited to the review and scrutiny of transactions and information encountered during the audit process, not the same operational or real-time level required of ASPs.
  (More information can be found in "Guidance to ICPAC members on transaction monitoring".

20. Q.: How should we handle clients who do not fully cooperate during the information collection and refuse to provide sufficient evidence?

A.: A client's refusal or persistent reluctance to provide information is itself considered a red flag and may indicate a potential money laundering or terrorist financing risk.
Suggested steps for a firm to follow:

1. **Explain the legal requirement and the firms internal policies**
   Inform the client that providing CDD information is not optional — it is a legal obligation that applies to all obliged entities, including auditors and accountants.
2. **Make a formal request**
   Document all requests and communications, including reminders, deadlines, and the client's responses or lack thereof.
3. **Assess the behaviour as a risk indicator**
   Client resistance, avoidance, or repeated delays are recognised red flags under AML framework and may warrant applying Enhanced Due Diligence (EDD) or escalating the matter to the Compliance Officer.
4. **Do not proceed with the engagement**
   If the required information cannot be obtained, the firm *must not establish or must terminate the business relationship*. Continuing without appropriate CDD is prohibited.
5. **Consider submitting a suspicious activity report (SAR)**
   Where the refusal to cooperate is unusual, unjustified, or suggests concealment, the matter must be evaluated by the Compliance Officer and may need to be reported to MOKAS in accordance with Article 69 of the AML Law.
6. **Avoid tipping-off**
   When considering or submitting a report to MOKAS, ensure that the client is not informed in a way that violates the tipping-off prohibition under Article 48 of the AML Law.

21. Q.: How are obliged entities expected to perform due diligence on minority shareholders who have contributed significant funds to the entity, when AML legislation requires identification and verification only of UBOs holding 25% or more ownership? Clients frequently refuse to provide information for shareholders below the 25% threshold and challenge the legal basis for requesting KYC on such minority shareholders. How should this situation be handled?

A.: The definition of a Ultimate Beneficial Owner (UBO) is not limited to ownership of 25% + 1 share. Under AML legislation and ICPAC's Directive, a UBO also includes any natural person who exerts control through other means, such as:

- voting rights or shareholder agreements,

- the ability to appoint or remove directors or senior officers,
- significant financial influence or decision-making power,
- or any other arrangement that gives effective control over the entity

In this case, although the individual is a minority shareholder by percentage, they have **introduced a significant amount of funds** and therefore may exercise **material influence or control**. This may place them **within the scope of due-diligence requirements**, even if they do not meet the 25% ownership threshold.
If the client refuses to provide the required information, this constitutes a red flag and the obliged entity must assess whether such refusal is unusual or suspicious in light of the circumstances. Where concerns persist, the matter may need to be escalated to the MLRO for further evaluation and, if appropriate, consideration of submitting an internal or external suspicious activity report.

22. Q.: Where the service provided is a company secretary, to what extent do we apply CDD and transaction monitoring?

Even when the engagement is limited to providing company secretarial services, the firm is still an obliged entity and must apply full CDD commensurate to the risk level.
Regarding transaction monitoring, the approach must be **risk-sensitive and proportionate** to the nature and type of services provided. A company secretary is not involved and does not have the authority to access and/or approve transactions. Typically, such services involve very restricted and low-volume transactional activity, such as:

- filing documents,
- signing or sealing resolutions,
- administrative actions carried out under mandate or agreement.
  In such cases, monitoring should focus on ensuring that any transaction or corporate action:
- is consistent with the economic profile of the client,
- matches the expected scope of the secretarial engagement, and
- does not present red flags based on the client's risk classification.
  If a transaction or requested action appears inconsistent or unusual for the client's economic profile or business structure, enhanced checks may be required.

Miscellaneous

1. **Q.: Where can I access ICPAC's published materials on AML/CFT and sanctions compliance?**
   A.: All materials related to AML/CFT and sanctions compliance published by ICPAC can be found under the **"Monitoring & Compliance"** tab on ICPAC's official website. This section includes guides, directives, and updates to assist with compliance requirements.

2. **Q.: Does ICPAC offer free seminars for its members or other educational material?**
   A.: ICPAC, in collaboration with VinciWorks, an online compliance training provider, offers its members free e-learning modules on compliance-related topics. The e-learning platform provides access to a variety of subjects, including Money Laundering, Client Due

Diligence, Identifying and Dealing with Suspicions, Sanctions, Bribery and Corruption, Fraud, and Market Abuse, among others.

ICPAC Members can access the platform here
Furthermore, the educational initiative "ComplianceBriefs" has been developed to enhance understanding and awareness of AML/CFT and sanctions-related topics. The ComplianceBriefs series is available on the ICPAC website here. Please note that viewing this training material qualifies as non-verifiable CPD units for compliance purposes.

3. **Q.: When is the Consolidated AML/CFT & Sanctions Questionnaire released for completion?**
A.: The submission of the Consolidated AML/CFT & Sanctions Questionnaire to ICPAC is an annual obligation. It is usually circulated to all firms and Compliance Officers at the end of May each year and aims at collecting information for the previous calendar year.

The submission deadline for the Questionnaire is the 30th of June every year.

To facilitate the preparation process, a template has been developed, highlighting key statistical data that firms should maintain to ensure readiness for the Questionnaire's release. The template can be accessed here under the name *«Annual AML-CFT Questionnaire - Template (statistics)»*. Please check the link regularly for any updates or revisions.

4. **Q.: Where can I find the required forms and templates for reporting information to ICPAC?**
A.: All required forms are available on the ICPAC website here. These forms cover various reporting requirements, including the following:

Forms:

a) **Trust Registration or Information Update:** To notify ICPAC about the registration of a trust in the trust registry or to update trust information, access the relevant form here. For any inquiries, contact trusts@icpac.org.cy
b) **Notification of Natural Persons Employed by an ASP**: The relevant form can be accessed here. For any questions, contact info@icpac.org.cy
c) **Notification of Subsidiary Companies of an ASP:** The relevant form is available here. For inquiries, contact info@icpac.org.cy
d) **Amendments to Firm Details:** To update firm details (e.g., name, addresses, compliance officer, director, shareholder, contact information, etc.), complete the Amendment of Firm's Details form, available here. For any questions, contact info@icpac.org.cy

Additionally, the ICPAC website offers compliance-related templates, which can be accessed here. These include:

Compliance Templates:

a) ICPAC AML Monitoring Visits – PVQ
b) ICPAC AML Monitoring Visits – AML Client List – PVQ

c) Reporting Template for Sectoral Sanctions
d) Template for True Matches Based on the Sanctions Directive
e) Sample Third-Party Reliance Questionnaire
f) Annual AML/CFT Questionnaire – Template (Statistics)

5. **Q.: What penalties can be automatically imposed for late submissions?**
A.: While penalties may be imposed for various infringements, in accordance with the ICPAC Regulation for Administrative Procedures and the Process of Imposing Administrative Sanctions, below are answers to some of the most frequently asked questions regarding penalty enforcement:

a) Failure to notify ICPAC within 7 days of any changes to the **Compliance Officer's** details incurs a predefined penalty of €500.
b) Failure to notify ICPAC within 15 days of the registration of a new **trust** or any changes to an existing trust incurs a predefined penalty of €100.
c) Failure to submit the annual **AML/CFT Questionnaire** within the set deadline incurs a predefined penalty of €500.
d) Failure to provide notification within 7 days of any changes to the Firm's **shareholding structure and directors** incurs a predefined penalty of €1000.