UNITED ARAB EMIRATES
MINISTRY OF ECONOMY & TOURISM

الإمارات العربية المتحدة
وزارة الاقتصاد والسياحة

Countering Money Laundering, Terrorism Financing and Proliferation Financing

Guidelines for Designated Non-Financial Businesses and Professions

Supplemental Guidance for Independent Accountants & Auditors (IAA)

المستشار / سالم أحمد الطنيجي

مدير إدارة مواجهة غسل الأموال وتمويل الإرهاب

Counselor / Salem Ahmed AlTeneiji

Director of the Anti-Money Laundering & Terrorist Financing Department

April 2026

Table of Contents

1. Introduction

Pursuant to the *Federal Decree-Law No. (10) of 2025* and its Executive Regulations, *Cabinet Resolution No. (134) of 2025*, Independent Accountants fall under the Designated Non-Financial Businesses and Professions (DNFBP) category. In the context of the United Arabi Emirates (UAE), professional licenses issued to entities operating within the accounting profession include both accounting and auditing services. *Federal Law No. (12) of 2014* on the Regulation of the Auditing Profession recognizes auditors registered with the Ministry of Economy & Tourism (MoET) as authorised to *audit and prepare reports on the financial statements and budgets of companies of all types, institutions, public and private establishments, and prepare reports on the periodic and annual accounts of the establishments and companies audited*. In practice, entities operating under the Accounting and Auditing license often engage in the provision of a broader range of professional accounting, financial reporting, assurance, advisory and related services that fall within the scope of activities for Independent Accountants as defined under the AML/CFT/CPF framework of the UAE.

Independent Accountants and Auditors (IAA) play a pivotal role in upholding integrity, transparency and accountability across financial and commercial activities within the UAE economy. The financial governance and corporate compliance across a wide range of industries is strengthened through the significant contribution of the professional services provided by IAA. At the same time, the nature of services provided may expose the sector to potential misuse by criminals who seek to obscure the ownership and control of assets or disguise and legitimise the proceeds of crime.

Given the broad scope of professional activities, IAAs are uniquely placed at the core of an establishment's financial reporting and governance processes allowing for the identification of potential Anti-Money Laundering, Combatting Financing of Terrorism, Countering Proliferation Financing (AML/CFT/CPF) weaknesses and Money Laundering (ML), Terrorism Financing (TF), Proliferation Financing (PF) vulnerabilities, as well as the detection of potentially suspicious activities. Thus, it is of critical importance that IAAs are equipped to identify ML, TF, PF risks, various typologies and effectively implement AML/CFT/CPF measures that are aligned with mandates of the UAE's AML/CFT/CPF legislative and regulatory framework.

In developing this Supplemental Guidance for the sector, findings of the 2024 UAE National Risk Assessment (NRA) as well as MoET's 2024 Sectoral Risk Assessment (SRA) have been considered. Both assessments indicate that while the IAA sector has not been widely associated with systemic abuse for terrorist financing, there are sectoral vulnerabilities in relation to potential misuse of professional services to facilitate money laundering through the layering of illicit funds, concealment of beneficial ownership and use of complex cross-border corporate structures. The sector is categorized as presenting a medium level of inherent ML risk with a Medium-Low residual risk owing to vulnerabilities related to the sector's gatekeeping role as well as the generally strong regulatory and professional standards governing the sector. Nonetheless, the strong presence of corporate customers with complex ownership structure, cross-border transactions and diverse geographic exposure continue to remain risk factors that may increase the risk of exploitation of professional services by criminals seeking to integrate illicit proceeds into the legitimate economic and financial systems.

In view of the risk environment of the sector, this Supplementary Guidance complements the *Guidelines for Designated Non-Financial Businesses and Professions* issued by MoET by providing practical sector-specific guidance on the understanding and identification of ML, TF and PF risks and their mitigation measures, in line with the legal obligations set forth through the UAE's regulatory framework which are aligned with the Financial Action Task Force (FATF) standards.

This document must be read and implemented with a risk-based perspective; requirements indicated by "shall/must" are compulsory and "should" signifies recommended practice unless a recorded, risk-based justification supports an alternative that provides equal or greater control. In cases of any discrepancies, the Federal Decree Law, Cabinet Resolutions, and directives from the Competent Authority take precedence. Sector entities should maintain records, document decision-making processes, and regularly evaluate compliance programs to address emerging risks (such as virtual-asset exposures), supervisory input, and modifications in their business model.

Professional accountants should also consider their ethical obligations as set out under the Code of Ethics issued by the International Federation of Accountants (IFAC) where relevant[1].

[1] Handbook of the International Code of Ethics for Professional Accountants issued in 2022.

1.1. Purpose and Scope

The purpose of this Supplemental Guidance is to provide guidance and assistance to regulated entities that fall under the IAA sector, in order to provide better understanding and effective implementation of applicable statutory obligations under the legal and regulatory framework in force in the UAE.

This Supplemental Guidance has been prepared by MoET and sets out minimum expectations regarding the factors that should be taken into consideration by each supervised IAA, when identifying, assessing and mitigating the risks of money laundering, terrorism financing and proliferation financing. These expectations align with, and are intended to complement, the existing legal and regulatory framework in force.

This Supplemental Guidance is not intended to limit, replace or otherwise affect the applicability of additional circulars, notifications, memoranda, communications, or other forms of guidance or feedback (whether direct or indirect) that may be published periodically by any relevant authority in relation to regulated entities within the respective jurisdictions, or to any specific regulated entity.

IAAs must refer to and comply with the comprehensive guidelines on AML/CFT/CPF issued by MoET. This Supplemental Guidance does not duplicate provisions in the comprehensive guidelines, rather it provides sector-specific expectations, risk factors and practical considerations relevant to the unique characteristics of the sector. The general requirements therein are to be applied together with the additional sector-specific guidance outlined here, using a risk-based approach proportionate to the business activity.

It should be noted that, while this document provides high-level guidance on TFS and CPF obligations, all operational, procedural and implementation requirements remain governed by the applicable Executive Office for Control and Non-Proliferation (EOCN) guidelines.

Independent Accountants & Auditors should refer to the full TFS guidelines issued by the Executive Office for Control and Non-Proliferation (EOCN), which detail their obligations under *Cabinet Decision No. (74) of 2020*, including requirements for screening, freezing, and reporting in relation to designated persons or entities.

Additionally, entities within the IAA sector should also refer to the *Guidance on Counter Proliferation Financing Institutions (FIs), Designated Non-financial Businesses and Professions (DNFBPs) and Virtual Assets Services Providers (VASPs)* and the *Guidance on Proliferation Financing Institutional Risk Assessment* issued by EOCN to gain understanding of obligations pertinent to CPF measures and to incorporate PF risk in their Business Risk Assessment (BRA).

It should be noted that the scope of this guidance is intended to cover professionals within the IAA sector acting independently, whether as sole practitioners or as members or employees of firms or companies engaged primarily in the provision of audit and accounting-related services.

1.2. Applicability

Unless otherwise noted, this Supplemental Guidance apply to all regulated entities within the IAA sector, and the members of their boards of directors, management and employees, established and/or operating in the territory of the UAE and Commercial Free Zones, whether they establish or maintain a Business Relationship with a Customer, or engage in any of the professional activities outlined in Articles (2) and (3) of *Cabinet Decision No. (134) of 2025 Concerning the Executive Regulations of Federal Decree-Law No. (10) of 2025 Concerning Combating Money Laundering, Terrorist Financing, and the Financing of the Proliferation of Weapons*.

1.3. Legal Status

This Supplementary Guidance serves as a practical tool to assist regulated entities in effectively implementing the relevant crime-combatting measures and are intended to be read in conjunction with the relevant laws, cabinet decisions, regulations and regulatory rulings which are currently in force in the UAE. However, it does not constitute additional legislation or regulation, and is not intended to set legal, regulatory, or judicial precedent. Regulated entities are reminded that the Supplemental Guidance does not replace or supersede any legal or regulatory requirements or statutory obligations. In the event of a discrepancy between this Guidance and the legal or regulatory frameworks currently in force, the latter will prevail. Specifically, nothing in this Supplemental Guidance should be interpreted as providing any explicit or implicit guarantee or assurance that the Supervisory or other Competent Authorities would defer, waive, or refrain from exercising their enforcement, judicial, or punitive powers in the event of a breach of the prevailing laws, regulations, or regulatory rulings.

This Supplemental Guidance, and any lists and/or examples provided in it, are not exhaustive and do not set limitations on the measures to be taken by regulated entities to meet statutory obligations under the legal and regulatory framework currently in force. As such, this Supplemental Guidance should not be construed as legal advice or legal interpretation. Regulated entities should perform their own assessments of the manner in which they should meet statutory obligations and should seek legal or other professional advice if they are unsure of the application of the legal or regulatory frameworks to circumstances.

1.4. Summary of AML/CFT/CPF Obligations

Pursuant to *Federal Decree Law No. (10) of 2025* and *Cabinet Resolution (134) of 2025*, entities within the IAA sector must fulfil AML/CFT/CPF obligations set forth, that collectively form the basis of an effective risk-based AML/CFT/CPF programme. These obligations are designed to prevent sector misuse for ML, TF or PF purposes. Consistent with the findings of the NRA and SRA, the IAA sector exhibits a medium level of inherent risk at an aggregate sector level, with elevated inherent risk arising from the specific services provider, customer types and cross-border exposure, underscoring the importance of well-implemented mitigating measures.

In line with the associated risk scoring, entities are required to fulfil the following obligations:

- *Compliance Administration* – Entities must put in place an adequate AML/CFT/CPF governance framework which consists of the appointment of a qualified Compliance Officer (CO) / Money Laundering Reporting Officer (MLRO), staff training and screening mandates, subjecting the AML/CFT/CPF framework to independent audit and overall oversight by senior management, assuming responsibility for AML/CFT/CPF compliance, in line with *Section 7* of the *Guidelines for Designated Non-Financial Businesses and Professions*. Where IAAs are part of a group, they shall implement group-wide AML/CFT/CPF programmes (policies, consolidated risk assessment, intra-group information-sharing and controls).
- *Risk Identification & Assessment* – Exposure to ML, TF and PF risks is to be identified, assessed and documented in line with *Section 8* of the *Guidelines for Designated Non-Financial Businesses and Professions*. This entails undertaking a BRA that is proportionate to the nature, size and complexity of the entity's activities as well as the risk landscape of the activities and the sector in which it operates.
- *Policies, Procedures and Internal Controls* – On the basis of the risk assessment outcome, the entity must establish, document, implement and regularly update AML/CFT/CPF policies and procedures tailored to the entity's specific business model and risk exposure with explicit measures to mitigate identified risks, in line with *Section 9* of the *Guidelines for Designated Non-Financial Businesses and Professions*.
- *Customer Due Diligence (CDD) and Ongoing Monitoring* – Entities must maintain adequate risk-based customer due diligence and ongoing monitoring procedures, in line with *Section 9* of the *Guidelines for Designated Non-Financial Businesses and Professions*. These procedures must address key areas such as the identification and verification of customers and beneficial owners, intended nature / purpose of business transactions and business relationships, creation and maintenance of customer risk profiles and application of Enhanced Due Diligence (EDD) measures where higher risks are identified. It is imperative that entities apply a risk-driven CDD and EDD measure as opposed to a threshold-driven measure so that reliance on transaction value alone does not result in the overlooking of material risk indicators. Additionally, entities must adopt an approach for dealing with Politically Exposed Persons (PEPs), cognizant that foreign corruption is identified as one of the key ML threats in the 2024 NRA.
- *Sanctions Compliance* – Entities must comply with the directives issued by Competent Authorities of the UAE in relation to the United Nations Security Council Resolutions (UNSCR), inclusive of obligations relating to terrorism lists, targeted financial sanctions (TFS) and proliferation financing controls.
- *Suspicious Activity / Transaction Reporting (SAR/STR)* – Entities must identify and promptly report any suspicion that arises in relation to transactions and/or business relationships, in line with *Section 10* of the *Guidelines for Designated Non-Financial Businesses and Professions*. The timeliness of SAR/STR reporting and quality of these reports continue to be key supervisory focus areas for the IAA sector.
- *Record-Keeping* - Entities must establish and maintain comprehensive records covering all transactions, CDD documentation, business correspondence, and outcomes of any analysis performed. Records must also encompass documentation generated as part of the entity's ML/TF/PF risk assessment and mitigation processes, in accordance with the requirements set out under the Executive Regulations. As outlined in *Section 11* of the *Guidelines for Designated Non-Financial Businesses and Professions,* records are to be retained for at least five (5) years from the latest of the following events:

- The termination of a business relationship or closure of a customer account.
- Completion of an occasional transaction where no business relationship exists.
- The issuance of a final judgment by a competent judicial authority.
- Dissolution, liquidation, or termination of a legal person or arrangement.

Records must be retained in an orderly manner that allows for effective analysis and the tracing of financial activities. They must be sufficient to reconstruct transactions in a manner that, if required, can support investigations or be used as evidence in legal proceedings. All CDD and transactional records must be readily available to Competent Authorities upon request and without undue delay.

2. Sector & Risk Context

2.1. Risk Identification & Assessment

The Executive Regulations requires regulated entities to identify, understand, manage and assess ML/TF/PF risks *in a manner proportionate to the nature and size of their business, taking into account the risk-based approach and the results of the National Risk Assessment [and Sectoral Risk Assessment]*. As part of this process, certain risk factors are specified, which should be taken into consideration when identifying and assessing ML/TF/PF risks at both the business and customer levels. General guidance on these risk factors is provided in *Section 8* of the *Guidelines for Designated Non-Financial Businesses and Professions*.

Independent Auditors and Accountants are in a unique position of approaching the statutory risk identification and assessment requirements from two complementary perspectives. The first is centred around the identification and assessment of ML/TF/PF risks arising from the professional activities undertaken and the entity's overall business operations. The second relates to risks associated to the customers serviced by the entity which include situations where professional services may be misused by those customers to facilitate money laundering, terrorist financing or proliferation financing.

As noted in the NRA and SRA, professional accountants have a gatekeeping role through the provision of services that support financial reporting, corporate structuring and financial advisory activities which may be abused by criminals. More specifically the roles or functions performed by Independent Accountants & Auditors relating to their activities include:

- Financial audits related to a customer's books, records, and annual and periodic accounts; operational audits related to a customer's internal controls, governance structures, and risk management processes and procedures.
- Compliance audits related to a customer's adherence to legal and regulatory requirements.

Based on the FATF Guidance for a Risk-Based Approach for the Accounting Profession[2] there are a wide range of services in the profession. The actual services delivered by accountants may vary between jurisdictions and the examples provided here may not be applicable in every jurisdiction. Services may include[3]:

- Audit and assurance services (including reporting accountant work in initial public offerings)
- Book-keeping and the preparation of annual and periodic accounts
- Tax compliance work
- Tax advice
- Trust and company services
- Internal audit (as a professional service), and advice on internal control and risk management
- Regulatory and compliance services, including outsourced regulatory examinations and remediation services
- Company liquidation/insolvency/receiver-managers/bankruptcy related services
- Advice on the structuring of transactions, corporate structuring, cross-border arrangements and ownership structures
- Due diligence in relation to mergers and acquisitions
- Succession advice
- Advice on investments and custody of customer money
- Forensic accounting

[2] FATF Guidance for a Risk-Based Approach for the Accounting Profession issued in 2019.

[3] The services listed are referenced for the purpose of identifying potential ML/TF/PF exposure points. Inclusion of a service in this list does not imply that all such services fall within the IAA sector.

Independent Accountants and Auditors acting in any of the roles mentioned above, whether singly or in combination, may be involved in examining and opining on a range of financial transactions or operations that could expose them to ML/TF/PF risks. For example, their work may involve the valuation of certain types of assets or liabilities, the review or reporting on changes in a company's capital structure or the payment of dividends; due diligence in relation to mergers or acquisitions; the assessment of the write-off of uncollected debts or the use of reserve accounts; or other similar corporate actions.

Furthermore, Independent Accountants and Auditors receive professional fees from their customers, which could potentially represent the proceeds of crime. In this regard, when performing their own risk identification and assessment, they must carefully consider factors such as the customer risk, geographic risk, channel risk, and product and services risk (refer to *Section 8 of the Guidelines for Designated Non-Financial Businesses and Professions*). In particular, consideration should be given to such factors as:

- Customer type, size, complexity and transparency (e.g. whether the customer is a single legal entity or is part of a larger, more complex group).
- Country of origin of persons associated with the customer, including beneficial owners, senior managers, legal representatives or signatories, etc. (i.e. whether a UAE national or a foreign customer, and in the case of the latter, whether the person is associated with a high-risk country).
- Industry/sector of the customer (i.e. whether it is associated with a higher risk of ML/TF/PF, taking into consideration the results of the NRA and other relevant sectoral risk assessments).
- Channel by which the customer is introduced and communicates (e.g. referral versus walk-in, in-person meeting versus remote communication via the internet or other media).
- Type, size, complexity, transparency, and geographic origins of financial arrangements associated with the customer.
- Novelty or unusual nature of the financial arrangements, structures, or circumstances associated with the customer, particularly compared with what is normal practice in the local market.

Thus, for example, an individual customer that is a mainland UAE entity involved in producing goods for domestic consumption may have a very different ML/TF/PF risk profile from that of a limited liability company in a Free Zone, engaged in international trade in electronics, and whose ownership or control structure involve persons or entities from a high-risk jurisdiction. The types of risk profiles identified and assessed, and the resultant risk ratings applied to the customers, should be used in determining the efficient risk-based allocation of the Independent Accountants and Auditors' AML/CFT/CPF resources, as well as the appropriate application of reasonable and proportionate risk-mitigation measures, including customer due-diligence measures.

2.1.1. Sector-Specific Vulnerabilities

The Sectoral Risk Assessment (SRA) has identified several key inherent and emerging vulnerabilities of the IAA sector that require careful consideration when assessing the sector's exposure to ML, TF and PF risks. The following key drivers highlight the primary areas where sectoral vulnerabilities may be heightened and should therefore be prioritised in risk assessments and mitigation frameworks:

- Complex Ownership Structures – the IAA sector services a predominantly corporate customer based thereby inherently increasing ownership complexity and transparency. Corporate often operate through offshore entities, nominees, holding companies and trusts, all of which can obscure the ultimate beneficial owner. This aspect also brings forth challenges in the verification of BO information, particularly where there is foreign jurisdiction associated – one that had weak AML/CFT/CPF controls or limited public registries. Furthermore, exposure to a foreign customer base increase the sector's exposure to foreign predicate offences that would have taken place in jurisdictions with opaque regulatory environments.
- Exposure to High-Risk Jurisdictions and Provision of Professional Services – the IAA sector may inadvertently authenticate financial statements used to disguise illicit funds, support the incorporation of entities or assist with documentation used for international ML networks and/or for sanctions and tax evasion thereby increasing the potential of cross-border misuse of professional services.

2.1.2. Customer ML/TF/PF Risk Identification & Assessment

When performing services that involve the review, assessment or testing of a customer's internal control framework, risk management of AML/CFT/CPF programme (such as internal audit, advisory or assurance engagements, Independent Accountants and Auditors should evaluate the adequacy

and effectiveness of a customer's risk identification and assessment framework. In doing so, careful consideration should be given to the following:

- Consideration of appropriate risk factors
- Effective application of a risk-based approach, including the differentiation of customers and transactions based on risk
- Formulation, documentation, and consistent application of an appropriate risk assessment methodology
- Involvement of appropriate internal stakeholders, including the AML/CFT/CPF compliance officer, senior management, risk managers, or others as appropriate to the nature and size of the customer's business
- Existence of processes for periodic review/update of both the risk assessment and its methodology

It is imperative that Independent Auditors and Accountants recognize that deficiencies in a customer's risk assessment framework elevates potential for business misuse for ML/TF/PF purposes.

2.1.3. Key Risk Factors

When undertaking an ML/TF/PF risk assessment, Accounting and Audit professionals should note that a range of methodologies may be utilized, both by the IAA entity and its customers, which is dependent on the size, nature and complexity of activities involved. This may entail the use of sophisticated models with weighted risk factors and calculation of aggregate risk scores, or the use of relatively simpler models based on indicative risk profiles of customers, aligned to the business model and market practices.

Irrespective of which methodology is adopted, it should be proportionate and should allow for the identification of higher-risk scenarios. Furthermore, the methodology should be clearly documented, justified, approved by senior management and consistently applied across relevant business activities.

A combination of the following risk factors should be taken into account, noting that the list below is not exhaustive and additional factors may be relevant depending on the circumstances.

Customer Risk

- The firm's customer base includes industries or sectors where opportunities for ML/TF are particularly prevalent.
- The firm's customers include PEPs or persons closely associated with or related to PEPs, who are considered as higher risk customers (refer to the FATF Guidance (2013) on Politically Exposed Persons for further guidance on how to identify PEPs).
- Customers where the structure or nature of the entity or relationship makes it difficult to identify in a timely manner the true beneficial owner or controlling interests or customers attempting to obscure understanding of their business, ownership or the nature of their transactions, such as:
    - Unexplained use of shell and/or shelf companies, front company, legal entities with ownership through nominee shares or bearer shares, control through nominee and corporate directors, legal persons or legal arrangements, splitting company incorporation and asset administration over different countries, all without any apparent legal or legitimate tax, business, economic or other reason.
    - Unexplained use of informal arrangements such as family or close associates acting as nominee shareholders or directors.
    - Unusual complexity in control or ownership structures without a clear explanation, where certain circumstances, structures, geographical locations, international activities or other factors are not consistent with the accountants' understanding of the customer's business and economic purpose
- Customers who appear to be acting on somebody else's instructions without disclosure.
- Customers with previous convictions for crimes that generated proceeds, who instruct accountants (who in turn have knowledge of such convictions) to undertake specified activities on their behalf.
- Customers who have no address, or multiple addresses without legitimate reasons.
- Customers who have funds that are obviously and inexplicably disproportionate to their circumstances (e.g. their age, income, occupation or wealth).
- Reason for customer choosing the accountant is unclear, given the firm's size, location or specialization.

- Frequent or unexplained change of customer's professional adviser(s) or members of management.
- Customer is reluctant to provide all the relevant information or accountants have reasonable grounds to suspect that the information provided is incorrect or insufficient.
- Customers with complex, opaque or unusual ownership or control structures, including multi-layered legal entities, offshore arrangements, nominee shareholders/directors without a clear economic rationale.
- Customers where beneficial ownership cannot be readily identified or verified, or where there are attempts to obscure ownership, control or the nature of business activities.
- Customers acting on behalf of undisclosed third parties or whose instructions appear inconsistent with their profile.
- Customers including politically exposed persons (PEPs), or persons associated with PEPs.
- Customers reluctant to provide information, or where information provided appears inconsistent, insufficient or unreliable.

Geographic Risk

- Customers, beneficial owners, or transactions linked to jurisdictions identified as higher risk, including those subject to sanctions, or with weak AML/CFT controls.
- Customers operating across multiple jurisdictions without a clear economic or commercial rationale.
- Transfer of corporate structures or activities to jurisdictions without genuine business activity.

Business and Industry Risk

- Customers operating in sectors identified as higher risk in the UAE NRA or other risk assessments.
- Cash-intensive businesses or businesses dealing in cash equivalents.
- Customers involved in emerging or high-growth sectors where regulatory oversight may be evolving (including virtual asset-related activities);
- Non-profit or charitable organisations where transactions lack clear economic purpose or alignment with stated activities.

Transaction and Behavioural Risk

- Transactions or arrangements that are inconsistent with the customer's known business profile or economic purpose.
- Unusual or unexplained complexity in financial arrangements, structures or transactions.
- Sudden changes in transaction patterns, including activity from dormant entities.
- Last-minute or unexplained changes in transaction instructions, payment methods or counterparties.
- Use of third-party payments or complex payment chains without clear justification.
- Use of virtual assets or other methods intended to obscure the origin of funds.

Control and Governance Risk

- Weaknesses in the customer's AML/CFT/CPF framework, including lack of oversight, inadequate policies or ineffective implementation.
- Insufficient involvement of senior management or compliance functions in risk management processes.
- Indicators of falsification or manipulation of financial records, including false invoices, fictitious loans or misleading accounting entries.

Additional Indicators

- Customers with assets or transaction volumes disproportionate to their known profile.
- Frequent or unexplained changes in professional advisers, management or ownership structures.
- Customers requesting unusually expedited services without reasonable justification.
- Customers offering unusually high fees without clear commercial rationale.
- Indicators that the customer is attempting to avoid regulatory approvals or reporting requirements.

3. Due Diligence and Ongoing Monitoring

3.1. Due Diligence

Together with the accurate identification and assessment of ML/TF/PF risks and the ongoing monitoring of customer relationships and transactions, the implementation of reasonable and proportionate customer due-diligence measures is one of the key components of an effective risk-based AML/CFT/CPF programme. The *Guidelines for Designated Non-Financial Businesses and Professions*, of which this supplemental guidance is a part, discusses customer due diligence (including enhanced and simplified customer due diligence measures) in detail, and DNFBPs should refer to the related sections of the Guidelines carefully and comply in full with CDD/EDD, monitoring, sanctions screening and record-keeping requirements. Nevertheless, there are some additional points that are of particular relevance to IAA. These additional points highlight typologies and risk indicators specific to the IAA sector which are intended to support entities in implementing measures in a manner that is risk-based, proportionate and effective.

Independent Accountants and Auditors should ensure that appropriate processes for screening customer, prospective customers (including beneficial owners and persons exercising management control) against applicable sanctions lists and adverse media are in place. Such processes need to be ongoing and risk-based and should include the detection of possible links to financial crime, politically exposed persons (PEPs), or other indicators of higher risk. Screening requirements must be implemented on a continuous, risk-based and proportionate basis at onboarding, during material changes and periodically consistent with the nature of the engagement and access to information , particularly concerning proliferation financing and targeted financial sanctions.

Independent Accountants and Auditors should become familiar with the various tools available for these purposes, including but not limited to publicly accessible government and intergovernmental Sanctions Lists; commercially available or subscription-based customer intelligence databases and due-diligence investigation services; and the use of internet search techniques. It must be noted that IAA are expected to ensure that the depth and frequency of screening is commensurate with the associated risks.

Independent Auditors and Accountants need to recognize that a frequent tactic employed in ML/FT/PF typologies includes hiding beneficial ownership using third-party intermediaries, proxies, or intricate legal frameworks and arrangements. These may consist of relatives, business partners, legal advisors, or additional third parties. In this context, Independent Auditors and Accountants must utilize a risk-based method for identifying and confirming the actual beneficial owner of their customers. When applicable to the engagement's nature, they should also assess how effective their customers' customer due diligence measures are concerning important business relationships or counterparties. Although Independent Auditors and Accountants are not required to independently examine all customer counterparties during standard audit procedures, they should, when relevant, evaluate if the customer’s due diligence processes are sufficient and properly executed

Typically, the starting point in determining beneficial ownership of a legal entity or legal arrangement is to ask pertinent questions and to obtain information directly from the business relationship or customer. The information thus obtained should be analysed for reasonableness and consistency and should be appropriately confirmed or corroborated with reference to reliable independent sources whenever possible, using a risk-based approach (for example, when higher risk situations are identified). Thus, sole reliance on representations provided by customers where the overall risk profile warrants enhanced scrutiny. This verification process may raise additional questions that require further scrutiny by the IAA and clarifying explanations from the business relationship or customer, with the goal of ensuring reasonable satisfaction that the IAA knows the identity of the true beneficial owners and believes their source of funds to be legitimate.

Generally, in the context of this corroboration process, reliable independent sources may include (but are not limited to) bank references or bank account information provided by financial institutions or commercial credit reporting agencies/services; the use of public registries and/or tax information, such as commercial registries or federal/national tax identification numbers to verify the ownership of legal entities. In cases where such sources are unavailable, IAAs should consider reliable alternatives as means of corroboration, ones that are appropriate to the level of risk identified. When required to conduct customer due diligence, IAA should be alert to situations in which existing or prospective business partners or customers appear unable or unwilling to divulge relevant ownership information or to grant any required permissions to third parties to divulge such information about them for corroboration or verification purposes. Heightened risk could be indicated through such circumstances which are contextual.

They should also be alert to customer due-diligence factors such as:

- Compatibility of the customer's profile (including their economic or financial resources, and their personal or professional circumstances) with the specifics (including nature, size, frequency) of the transaction or activities involved.
- Utilisation of complex or opaque legal structures or arrangements (such as trusts, foundations, personal investment companies, investment funds, or offshore companies), which may tend to conceal the identity of the true beneficial owner or source of funds
- Possible association with politically exposed persons (PEPs), especially in regard to foreign customers.
- Possible prior association between the parties to a transaction (buyer and seller), or other indications that the transaction is not being conducted on an arm's length basis
- Attempts to influence (including through bribery or other means of coercion) the transparency or accuracy with which IAAs carry out their duties.

The aforementioned factors should be taken into account at the time of establishing a business relationship as well as during the course of the relationship (on an ongoing basis). The application of due diligence measures should be informed by the risk assessment undertaken, including the intensity of ongoing monitoring. IAA must refuse or exit relationships where beneficial ownership or source of funds/origin cannot be reasonably verified or where sanctions/PF risks cannot be mitigated.

Another technique often employed in various ML/TF/PF typologies is the use of fraudulent and/or forged documents. In cases in which Independent Accountants and Auditors act in a capacity related to the approval or opinion with regard to an acquisition, disposition, transfer, or financing of legal entities or legal arrangements, they should pay particular attention to the authenticity of documents or financial instruments (including securities, bonds, title deeds, loan or mortgage documents, promissory notes, or other documents and information) involved.

3.2. Ongoing Monitoring

Depending on the nature of the accounting and audit activities and the frequency and type of services provided, it may not always be possible for Independent Accountants and Auditors to perform detailed ongoing monitoring of the entirety of their customer's activity in the same manner as Licensed Financial Institutions (for example, when auditing a specific aspect of a customer's internal controls or AML/CFT/CPF programme). Nevertheless, it is important that Independent Accountants and Accountants take reasonable steps to protect themselves and their customers from misuse by criminals. This includes taking steps to ensure they do not become unwitting accomplices to ML/TF/PF via the sources and methods by which they are compensated for the services they provide, to the extent that such sources and methods are visible to the IAA through fee arrangements, engagement documentation or information obtained in the normal course of providing professional services.

In this regard, Independent Accountants and Auditors should make reasonable efforts to examine the nature, size, frequency, and consistency of the transactions in which the customer is involved, with particular regard to the customer's expected activities and with what is considered normal for organisations in similar circumstances. Some examples of ways in which they may do so include, but are not limited to:

- Examining information contained in commercial registries or held by registered agents, to detect any unexpected changes, amendments, or transfers.
- Monitoring changes in ownership, dividend payments, additional capital contributions, lending and borrowing activity, powers-of-attorney, and similar indicators of true beneficial ownership and/or control, to detect any inconsistencies, unusual patterns or unexpected changes.
- Monitoring, through the review of accounting records, audit evidence or information provided during engagements, the frequency and size of transactions or funds transfers as reflected in the customer's financial records to identify inconsistencies with the expected business profile.
- When collecting fees for services, or when being reimbursed for out-of-pocket expenses: ensuring where fees or reimbursements are received, that funds received come from known sources on which Independent Accountants and Auditors have performed CDD, and not from third-parties, foreign accounts, or other unknown sources; and also ensuring that the methods of payment and/or the financial instruments used are consistent with the customer's profile, and are not methods which could disguise the origin of the funds (such as cash, cashier's cheques, postal money orders, prepaid cards, third-party endorsed cheques, cryptocurrencies, or other difficult-to-trace payment methods).

3.3. Reporting Obligations

IAAs are subject to reporting obligations under the UAE's AML/CFT/CPF framework, which form a critical component of the national system for the detection, analysis, and mitigation of money laundering, terrorist financing, and proliferation financing risks. These obligations apply irrespective of whether a transaction or activity is completed, attempted, or discontinued, and must be fulfilled in a timely, accurate, and confidential manner.

In line with the risk-based approach, reporting obligations within the IAA sector are primarily driven by the identification of suspicious activity, relationships, or structures. Accordingly, IAAs are required to submit Suspicious Transaction Reports (STRs) or Suspicious Activity Reports (SARs) and any other types of reports, were applicable to the Financial Intelligence Unit (FIU) where there are reasonable grounds to suspect that funds, transactions, or related activities are linked to ML/TF/PF, or to the proceeds of crime. This obligation applies regardless of the value of the transaction where reasonable grounds for suspicion arise based on the information available to the IAA in the course of providing its services and extends to attempted activities, including situations where an IAA declines to establish or continue a business relationship due to concerns identified during customer due diligence or ongoing monitoring.

The obligation to report is not dependent on certainty or proof of illicit activity. Rather, it is triggered by reasonable suspicion formed on the basis of available information, professional judgement, and the assessment of risk indicators. IAAs should therefore ensure that internal processes enable the timely identification, escalation, and assessment of such suspicions.

In addition to suspicion-based reporting, IAAs must ensure that reporting obligations are fully integrated into their operational and governance frameworks. This includes establishing clear internal escalation procedures, ensuring that relevant staff are aware of their responsibilities to report concerns to the Compliance Officer / Money Laundering Reporting Officer, and maintaining appropriate documentation to support the decision-making process.

Where a suspicion is identified, the IAA must promptly submit an STR or SAR to the FIU in accordance with applicable requirements and timelines. Reports should be comprehensive, accurate, and supported by sufficient detail to enable the FIU to understand the nature of the suspicion, the parties involved, and the underlying activity.

In all cases, the focus should be on clearly articulating the basis for suspicion, rather than providing definitive conclusions. Supporting documentation, transaction details, and relevant background information should be included where available.

Following the submission of an STR/SAR, IAAs must comply with any instructions issued by the FIU and ensure that appropriate measures are taken in relation to the business relationship. This may include enhanced monitoring, restrictions on certain activities, or, where appropriate and in the absence of contrary instructions, consideration of terminating the relationship.

IAAs are strictly prohibited from disclosing, directly or indirectly, to the customer or any third party, the fact that an STR or SAR or any other types of reports has been submitted to the Financial Intelligence Unit, is intended to be submitted, or that an investigation is being or may be conducted. This prohibition extends to any information that could reasonably lead to the customer becoming aware of such reporting.

Maintaining confidentiality is essential to preserving the integrity of investigations and protecting the effectiveness of the UAE's AML/CFT/CPF framework. Breaches of tipping-off provisions may result in legal and administrative sanctions.

It should be noted that taking steps to decline a transaction, delay the provision of services, or request additional information for legitimate compliance purposes does not constitute tipping-off, provided that such actions are conducted in a manner that does not reveal the existence of a report or suspicion.

It is important to note that IAAs are required to refer to the *Guidelines for Designated Non-Financial Businesses and Professions* issued by the Ministry of Economy and Tourism for comprehensive requirements and additional guidance on reporting obligations. They remain subject to all post-reporting requirements, including record-keeping, confidentiality, and cooperation with competent authorities, as set out in the applicable legal and regulatory framework.

4. Common Sectoral Challenges & Best Practices

4.1. Sectoral Challenges

- The IAA sector acts as a gatekeeper and assurance provider, which is fundamentally different from sectors that handle cash or high-value goods. The primary challenge is therefore not the actual transfer of value, but the potential for professional services to be exploited to create an appearance of legitimacy for financial matters, corporate structures, ownership arrangements, or transactions. In practice, accountants and auditors may be involved at stages where they have access to beneficial ownership details, financial documentation, tax standings, internal controls, cross-border arrangements, and financial transactions. When those services are exploited, they can enable the layering of illegal profits, the hiding of ownership or control, or the obscuring of irregular transactions within otherwise lawful business operations.
- The prevalence of corporate customers, such as those with complex legal structures, nominee setups, foreign ownership, and cross-border operational models, poses difficulties in accurately identifying and verifying the actual beneficial owner and understanding who ultimately controls the customer or benefits from the engagement. The lack of transparency in ownership and control can be heightened when structures span across multiple jurisdictions, where group entities carry out different roles in various countries, or when accounting records do not adequately align with the stated business model. This is especially relevant in the UAE context, where the broader DNFBP landscape encompasses international business, interaction with foreign customers, and activities in free zones.
- The sector's exposure engagement with foreign customers and cross-border operations poses additional difficulties regarding due diligence, transparency, sanctions checks, and the uniformity of documentation. Variations in legal frameworks, access to reliable registries, the quality of foreign corporate records, and the use of offshore or intermediate holding entities might complicate IAA firms' ability to verify ownership, source of funds, or economic justification with the same level of assurance as for domestic customers. In practice, this can elevate the likelihood of misuse of professional services to support structures or transactions that do not align with the customer's legitimate business or financial activities.
- Another challenge comes from the tension between professional independence, commercial pressures and customer influence. Where a business engagement is commercially important, or where the customer is well-connected or insistent on speed, there may be explicit or implicit to regard gaps in documentation, opacity in ownership or unusual transaction features as routine. This issue is particularly acute where customers require immediate work on restructurings, acquisitions, tax plans, liquidation processes, financial statement approvals or other engagements that may create pressure to proceed adequately addressing risks. FATF's guidance for accountants emphasizes the significance of professional judgement and risk-based measures in precisely these situations.
- MoET's SRA has noted uneven compliance maturity across firms, especially smaller practices where limited dedicated compliance resources, gaps in escalation to senior management, insufficient tailored AML/CFT/CPF training, and over-reliance on manual processes yield inconsistent risk assessments, weak documentation of decisions, and under-identification of suspicious activity. Such weaknesses in control have been noted as requiring improvement in order to mitigate ML/TF/PF risks effectively.

4.2. Best Practices

- IAA should demonstrate national, sectoral and business level risk awareness and implement a documented and proportionate risk-based approach to mitigating ML/TF/PF risks. The risk-based approach deployed must guide all aspects of compliance from customer onboarding to monitoring and escalation. This should include periodic business-wide risk assessments that consider customer profile, ownership opacity, geographic exposure, service type, delivery channel, fee/payment arrangements and sanctions/PF exposure. Structured methodologies should guide risk scoring, weights of risk factors and qualitative assessment, consistent with the scale and complexity of activities. Senior management approval and involvement in the risk-based approach process remain pivotal. Risk assessment must be subject to routine updates, especially where significant changes occur in business, risk or regulatory environments.
- Entities must establish a strong governance framework appropriate to the size of their business and risk exposure. A qualified AML/CFT/CPF Compliance Officer / Money Laundering Reporting Officer (CO/MLRO) with sector-specific knowledge and sound understanding of regulatory obligations must be appointed. There should be written policies and procedures aligned with regulatory mandates and best practices. All employees must undergo regular AML/CFT/CPF training, including front-line staff and senior management. Entities must

ensure group-wide AML/CFT/CPF frameworks where there are multiple branches or affiliates. Given that the SRA identifies incomplete senior reporting and inadequate training as sector vulnerabilities, entities should ensure that AML/CFT/CPF issues are escalated to senior management regularly and that decisions relating to higher-risk customers or engagements are documented and reviewed.

- Due diligence remains critical to preventing sector misuse for ML/TF/PF. Entities must understand who they are dealing with, understand beneficial ownership, controla and economic rationale. Best practices include the verification of identity through reliable and independent sources, understanding the purpose and intended nature of the engagement and assessing whether the control structure is in alignment with the customer's declared business profile. Where there is association with high-risk jurisdictions, politically exposed persons and close associates, non-resident customers or intermediaries where the role is unclear and there is no economic rationale should warrant for enhanced due diligence. Furthermore, entities must implement ongoing monitoring that is proportionate to the customer risk.
- Entities should take a service-based approach to risk identification and mitigation. Services associated with higher risk should be identified and be subject to heightened controls from engagement acceptance and throughout service delivery. In practical terms, engagements involving company structuring, complex cross-border arrangements, liquidation or insolvency work linked to unexplained wealth, or non-routine financial transactions should receive enhanced scrutiny and management oversight. In doing so, the calibration of controls not restricted to the customer being serviced but to the type of service the entity is asked to provide.
- Entities should ensure that screening and adverse media checks are undertaken on a risk-based and ongoing basis for customers, beneficial owners, controlling persons and associated counterparties, where appropriate. Sanctions screening should be conducted against UAE and UN sanctions lists.
- Entities should ensure an appropriate level of scrutiny applied to documents, justification and transaction narrative provided by the customer, particularly in instances where the the service involves financial reporting, handling ownership records, tax information, or customer-supplied corporate records. Best practice includes ensuring the consistency of documents across different sources, verifying the reconciliation of figures, dates, counterparties and ownership information, and escalating where records appear backdated, fabricated, commercially inconsistent or unsupported by the entity's understanding of the customer's business.
- Clear and documented internal escalation procedures must be put in place and employees must be trained to identify red flags pertinent to the accounting profession, including ownership opacity, cross-border structures that are not justified, false invoicing, false loans, abuse of corporate vehicles, sanctions evasion indicators and attempts to pressure the entity to reduce scrutiny process and ignore gaps that may arise.

5. Typologies

As stated in the Guidelines, the techniques used by offenders for money laundering, terrorism financing, and proliferation financing are perpetually advancing and becoming increasingly complex. Consequently, it is not feasible to present a comprehensive list of ML/TF/PF typologies pertinent to Independent Accountants and Auditors, since new techniques and variations keep appearing. However, there are studies, case analyses, and FATF recommendations that suggest that several common typologies that pertain specifically to the accounting field and Independent Accountants and Auditors might discover these while delivering services to customers.

These typologies generally align with the classic goals of money laundering and associated financial crimes, which include:

- Concealing or disguising the identity of the true beneficial owner or controlling person.
- Concealing or disguising the illicit origin of the funds involved.
- Transferring or extracting value or utility from the assets involved for the benefit of the criminal perpetrators.

Independent Accountants and Auditors should recognise that, in practice, multiple typologies and techniques are often used together in a single arrangement, transaction or series of related transactions. They should therefore remain alert to indicators of suspicious activity across the full range of services they provide. Furthermore, the regular review of ML/TF/PF trends and typologies should be incorporated into employment screening, staff training and risk assessment processes.

The following are among the more common typologies relevant to the Independent Accountants and Auditors sector:

Use of Corporate Vehicles and Complex Legal Structures

Formation and/or use of corporate vehicles, companies (including shell companies), and complex legal structures or arrangements (such as trusts). While there are numerous legitimate reasons for legal entities to create other legal entities or legal arrangements (such as trusts or foundations, special-purpose vehicles, and even shell companies under certain circumstances), these structures may also be exploited by criminals for the purpose of ML/TF/PF.

Examples of some of the ways in which this may be done include but are not limited to:

- Use of companies, trusts and/or bearer shares to obscure beneficial ownership
- Use of shell companies* for the placement and/or layering of the proceeds of crime
- Use of professional intermediaries, trustees or nominee shareholders in order to provide the appearance of legitimacy and/or to obscure beneficial ownership.

This typology is particularly relevant to Independent Accountants and Auditors wherein engagement entails financial reporting, tax advisory or other services that provide visibility into ownership and control structures.

Misuse of Professional Services to Create Appearance of Legitimacy

The professional services provided by Independent Accountants and Auditors may be misused, whether knowingly or unknowingly, to provide an appearance of legitimacy to financial affairs, accounting records, corporate structures, tax arrangements or transactions.

Examples include:

- preparation or presentation of financial statements that obscure the true source or nature of funds
- creation or support of accounting entries, intercompany transactions, loans, royalty arrangements or consultancy fees lacking genuine economic substance
- use of tax, restructuring or corporate advisory work to support transactions or structures that conceal the origin, destination or ownership of assets
- use of audit, assurance or accounting outputs to create comfort for counterparties, financial institutions or other professional service providers in circumstances where the underlying activity is suspicious

Real Estate – Related Laundering Through Corporate or Financial Structures

Real estate continues to be a commonly used vehicle for the laundering of illicit proceeds. The intersection with Independent Accountants and Auditors lies in the type of engagement either through accounting, tax structuring, etc.

Some examples include but are not limited to:

- Use of corporate vehicles to acquire or hold property
- Use of complex lending or mortgage arrangements
- Manipulation of the appraisal or valuation of a property
- Use of properties to conceal money generated by illegal activities

Trade Based Money Laundering and Misuse of Commercial Documentation

Transactions involving domestic or international trade are a known typology for money laundering and the financing of terrorism and proliferation. From an accounting, audit, advisory or forensic review perspective, some of the most common methods used in this regard, which Independent Accountants and Auditors should be aware of, include but are not limited to:

- Manipulation of invoices (over-, under-, or fictitious invoicing)
- Fraudulent shipments (misrepresented goods, false shipments)
- Customs, excise or value-added tax fraud

Sanctions Evasion and PF-Related Obscuration

Independent Accountants and Auditors should recognize that their professional services may be misused to support sanctions evasions attempts or proliferation financing related activities which primarily involve the obscurement of beneficial ownership, disguising counterparties or structuring transactions to avoid detection.

Some examples include but are not limited to:

- Use of front companies or affiliated entities to disguise links to sanctioned persons or jurisdictions
- Use of complex ownership or payment chains to obscure the end-user, end-destination or true beneficiary
- Manipulation of accounting or commercial records to conceal the nature of goods, services or counterparties
- Use of professional services to support apparently legitimate structures that in reality facilitate sanctions evasion or PF-related trade

Misuse of Customer or Third-Party Accounts, Payment Flows and Settlement Arrangements

In limited circumstances, engagements that entail services wherein Independent Accountants and Auditors are exposed to payment instructions, customer money, or third-party settlements (insolvency, liquidation, restructuring support or advisory engagements involving settlement visibility) or closely related financial flows, those arrangements may be exploited to facilitate ML/FT/PF.

Examples include:

Transfers to or from third parties unrelated to the underlying business purpose
Cancellation of transactions followed by instructions to return funds to a different party
Unexplained changes in payment methods, settlement instructions or counterparties
Use of loans, advances, reimbursements or professional fee arrangements to disguise the movement of value

While this typology is more commonly associated with the provision of services by legal professionals or TSPs, it remains relevant to the IAA profession particularly in situations where accountants are involved in restructuring support, insolvency work, customer money arrangements, or advisory services linked to payment flows.

Other Related Typologies

Examples of other methods used by criminals for the purpose of ML/TF/PF, often related to tax evasion, but also to other predicate offences, include but are not limited to:

- Transactions related to licence or royalty payments
- Private loan/credit agreements
- Use of fraudulent consultancy agreements
- Use of fraudulent investment agreements
- Misuse of charities or non-profit entities through poor transparency or weak financial oversight

6. Red Flag Indicators

The following list of red-flag indicators for potentially suspicious activity / transactions is not exhaustive. It is important to note that the presence of one or more of these indicators does not automatically imply that a transaction involves a crime. Rather, it serves as an indication that enhanced due diligence, or further investigation may be warranted. The appointed Compliance Officer of the entity should carefully assess the circumstances to determine whether the activity / transaction is indeed suspicious.

6.1.1. Customer Behaviour - Individual

Concealing or Disguising Identity of the UBO

- Use of companies, trusts, and / or bearer shares to obscure beneficial ownership.
- Use of shell companies for the placement and / or layering of the proceeds of crime.
- Use of professional intermediaries, trustees or nominee shareholders in order to provide the appearance of legitimacy and / or to obscure beneficial ownership.
- Creation or use of multi-jurisdictional structures of legal entities and legal arrangements to disguise beneficial ownership, or to facilitate a predicate offence related to ML/TF.
- The entity is owned by or affiliated with a legal entity incorporated/established in a jurisdiction that does not require companies to report beneficial owners to a central registry.
- Changing the ownership without notifying the accountant on the changes made.
- Acquires or uses shelf companies, or pre-constituted shell companies, in jurisdictions that allow their use but do not require updating of ownership information.
- When questioned about the source of funds, tax history, beneficial ownership or cross-border transactions, the individual becomes defensive, evasive or hostile.

Suspicious Behaviour or Lack of Transparency

- Customer is reluctant or refuses to provide personal information, or the accountant has reasonable doubt that the provided information is correct or sufficient.
- Refuses to co-operate or provide information, data, and documents usually required to facilitate an audit, or is unfamiliar with the details of the company's business.
- The customer is unable or refuses to explain:
  - The business activity and corporate history.
  - The identity of the beneficial owners.
  - The source of the wealth and funds.
  - The nature of their business dealings mainly with parties located in foreign jurisdictions.
  - The reason behind conducting their activities in a certain manner.
- Customer actively avoids personal contact without sufficient justification.
- Does not maintain contact or communication after initial appointment of the accountant, when this would normally be expected.
- Customer is the signatory to multiple company accounts (especially unrelated companies) without sufficient explanation.
- Makes unusual requests (including those related to secrecy) of the accountant or its employees.
- Appears very concerned about or asks detailed questions about compliance-related matters, such as customer due-diligence or transaction reporting requirements.
- Individual claims to be self-employed, operates cash-based businesses, or operates within an informal sector abroad, but fails to provide verifiable tax filings, audited financial statements, or reliable third-party verification.
- The individual is either unable or unwilling to provide tax returns from their home-country, tax residency certificates, proof of tax payments on reported income.
- There are frequent assertions of being "tax exempt" or "not required to file" without credible legal or jurisdictional justification.
- The individual requests the accountant or auditor to "simplify" explanations, accept management representations without evidence, exclude certain accounts, transactions, or jurisdictions from scope.

Unusual Customers and High-Risk or Criminal Associations

- Customer is under investigation, has known connections with criminals, has a history of criminal indictments or convictions, or is the subject of adverse information in reliable publicly available information sources.
- Customer is a politically exposed person or has familial or professional associations with a person who is politically exposed.
- Attempts to improperly conceal beneficial ownership from competent authorities.
- Has previously been prohibited from holding a directorship role in a company.
- When the entity or any of the UBO's are on any Sanctions lists or international lists.
- Funds originate from or transit through jurisdictions characterized by high tax secrecy, known for aggressive tax avoidance schemes, exhibiting weak tax enforcement or transparency.

Unusual Timing or Patterns in Transactions

- Conduct and unusual number or frequency of transactions in a relatively short time period.
- Disposes of assets under conditions which are unusual, or which involve unnecessary expense or losses, without a logical explanation.
- Makes deposits or other payments from multiple accounts or sources.

6.1.2. Customer Behaviour - Entity

- Cannot demonstrate a history or provide evidence of real activity.
- Suddenly becomes active after a long period of dormancy, without a logical explanation.
- Cannot be found on the internet, social business network platforms, or public domain.
- Is registered at an address that does not match the profile of the company, or that cannot be located on internet mapping services (such as Google Maps).
- Is registered at an address that is also listed against numerous other companies or legal arrangements, indicating the use of a mailbox service.
- Has directors or controlling shareholder(s) who cannot be located or contacted, or who do not appear to have an active role in the company, or where there is no evidence that they have authorised transactions.

- Has directors or controlling shareholder(s) and/or beneficial owner(s) who are also found to be representatives of other legal persons or arrangements, indicating the possible use of professional nominees.
- Has an unusually large number of beneficiaries and other controlling interests or has authorised numerous signatories for the transaction without sufficient explanation or business justification.
- Is not normally a cash intensive business but appears to have substantial amounts of unexplained cash.
- Provides falsified records or counterfeit documentation.
- Is owned by or affiliated with a legal entity incorporated or established in a jurisdiction with weak or absent AML/CFT laws.
- Transfers its registration or domicile from another jurisdiction without any evidence of genuine economic activity in the country of origin.
- The customer requests that shortcuts be taken, or that the work is completed in an unreasonably short time period and is prepared to pay substantially higher fees than usual in exchange.
- The customer's requested or preferred means of payment is unusual (e.g. precious metals or stones, virtual currencies, or other unconventional payment methods).
- Individuals manage multiple entities that transfer funds among themselves without corresponding commercial activity.

6.1.3. Transaction Behaviour

Concealing the Source of Funds

- Involve unexplained last-minute changes involving the identity of the parties (e.g. it is begun in one individual's name and completed in another's without a logical explanation for the name change) and/or the details of the transaction (such as the amount or terms) and/or the details of the financing or the payment instrument/procedures (e.g. a mortgage is arranged for a property purchase, but cash is substituted as the final payment method).
- Involves cash or negotiable instruments which do not state the true payer. Especially where the amount of such instruments is significant in relation to the total value of the transaction.
- Individual describes funds as originating from "family", "friends", or "community networks" without formal documentation.

Suspicious Use of Investment Schemes or Financial Instruments

- Transactions are financed by a non-financial institution third party, whether a natural or a legal person, with no logical explanation or commercial justification.
- Transactions involving loans or other financing from private third parties without adequate supporting agreements, collateral, or regular interest payments or principal repayments.
- Involve assets purchased with cash, which are then used as collateral for a loan within a short period of time.
- Involves third-party funding (either for the transaction or for fees) with no apparent connection or legitimate explanation.
- The individual injects substantial amounts into UAE entities as shareholder loans, capital contributions, advances or related-party funding lacking clear loan agreements, repayment terms, or economic justification.

Unusual Transaction Frequency or Structure

- Funds that are sent to, or received from, a foreign country when there is no apparent connection between the country and the customer, and/or which are sent to, or received from, high-risk jurisdictions.
- Involve several transactions which appear to be linked, or which involve the same parties or those persons who may have links to one another (for example, family ties, business ties, persons of the same nationality, persons sharing an address or having the same representatives or attorneys, etc.).
- A significant increase in capital, or successive capital contributions over a short period of time, for a recently incorporated company with no logical explanation.
- Personal funds are funnelled through corporate accounts, followed by personal expenditures or asset acquisitions.

Suspicious Relationships and Pressures

- Transactions involving family members of one or more of the parties without a legitimate business rationale.

- Transactions appear to involve parties with a questionable connection or generates doubts that cannot be sufficiently explained by the customer.
- Involving frequent or high-value transactions between a small number of related natural or legal persons.
- Transactions involving requests for payments to / from third parties without a substantiating reason or corresponding transaction.
- The unexplained use of powers-of-attorney or other delegation processes.
- Transactions appear to be directed by someone (other than a formal legal representative) who is not a formal party to the transaction.
- Income, occupation or business activities in an individual's home country do not align with the level of assets or capital investments observed in the UAE.
- Individual frequently utilized relatives, employees, business partners, offshore contacts to execute payments or hold assets on their behalf.
- Individual avoids appearing as the direct counterparty in transactions despite exercising actual control.

Irregularities in Contracts or Agreements

- Involving multiple appearances of the same parties in different transactions over a short period of time or involves transactions or financial transfers (e.g. disbursements or repayments) between the parties over an unusually long contractual period.
- Including contractual agreements with terms that are unusual or that do not make business sense for the parties involved.
- Unreasonable choice of accountant without a clear explanation, given the size, location or specialisation of the accountant.
- When the customer has changed the accountant a number of times in a short space of time without legitimate reason.

Transactions That Do Not Make Economic Sense

- Appointing a counterparty acting in the capacity of the director, signatory, or other authorised representative of the entity, who does not appear to have the required competency or suitability.
- There is rapid buying and selling of assets without commercial rationale (potential layering).

Other Transaction Pattern Red Flags

- Transactions executed from a business account but appears to involve personal purchases or sales, or public finances.
- Involve complicated transaction routings or multi-jurisdictional corporate structures without sufficient explanation or trade records.
- Involving foundations, cultural or leisure associations, or non-profit-making organizations, when the characteristics of the transaction do not match the goals of the entity.
- Explanations provided regarding the commercial purpose of foreign transactions are inconsistent.
- Customer claims to export technical equipment without any manufacturing capacity.
- Financial statements reflect payments to unknow suppliers in high-risk jurisdictions.
- Customer refuses to provide end-use / end-user information, customs documentation, supply chain partners.

7. Case Studies

The following case studies are illustrative typologies intended to highlight risks that may be identified through professional judgement, document review, audit evidence or advisory engagements and do not imply that IAAs perform transactional execution, fund handling or account-level controls.

Case Study 1: <u>Concealment of Corruption Proceeds by a Politically Exposed Person through Corporate and Trust Structures</u>

Synopsis

A politically exposed person (PEP) was found to have utilized a group of corporate companies, trust arrangements, intermediaries and professional service providers across various jurisdictions for the concealment the ownership of assets acquired with the proceeds of corruption. High-value properties and other assets were acquired despite inconsistencies noted between the individual's declared income and the value of the assets. Furthermore, it was found that the assets purchased were held through previously incorporated entities and structures that obscured the true beneficial owner. The transfer of funds occurred through multiple corporate and bank accounts, including entities owned by the PEP but controlled through associates or intermediaries. In support of these arrangements, forged company accounts, false incorporation documents and misleading ownership records were produced to create an appearance of legitimacy. The identity of the true beneficial owner was obscured through the companies, trust accounts and intermediary-controlled accounts that enabled the movement of value across jurisdictions. From the perspective of Independent Accountants and Auditors, this case showcases how corporate structures, financial records, ownership documentation and professional services may be misused to conceal beneficial ownership, legitimise illicit wealth and deter due diligence efforts where risk-based verification is weak.

Key Red Flags

Particular indicators (as listed below, but not limited to), especially when occurring in combination, should serve as alerts:

- *The customer's declared income, assets, or visible economic profile does not align with the value, scale, or geographical distribution of the assets owned or obtained.*
- *Utilization of previously established corporations, offshore organizations, trusts, or comparable setups lacking a transparent commercial or economic justification.*
- *Ownership and control of businesses seem to be carried out via associates, family, intermediaries, or representatives instead of the actual customer.*
- *Corporate, financial, or incorporation papers seem inconsistent, incomplete, unusually timed, backdated, or otherwise dubious.*
- *The customer depends on documentation from overseas jurisdictions that is challenging to confirm independently, especially when these documents are essential for proving ownership or legitimacy.*
- *Funds circulate through various legal entities or accounts across different jurisdictions lacking a distinct business justification.*
- *The beneficial owner cannot be reliably and promptly identified, or various documents show conflicting ownership or control positions.*
- *Transactions or arrangements seem intended to establish legitimacy for wealth or assets that are excessive compared to the customer's recognized circumstances.*

Supervisory Expectations

- *Apply increased scrutiny when complex corporate frameworks, international legal setups, middlemen, or unclear ownership links are employed without a transparent and valid justification.*
- *Evaluate if the customer's declared wealth, funding sources, and ownership details align with the assets, frameworks, and financial transactions noted.*
- *Verify beneficial ownership details through trustworthy and independent resources, especially when the structure extends across various jurisdictions or includes proxies, trusts, or offshore entities.*
- *Apply professional scepticism to company accounts, incorporation records, trust documents, and additional supporting materials, particularly when they are vital for verifying legitimacy.*
- *When there are valid reasons for suspicion, determine if a report for suspicious transactions/activities needs to be submitted.*

- *Keep adequate records to show the investigations conducted, the discrepancies noted, the reasons for conclusions drawn, and the implementation of a risk-based strategy*

Case Study 2: <u>Use of Shell Companies and Procurement Manipulation to Launder Proceeds of Corruption</u>

Synopsis

An extensive infrastructure project that included building an international airport underwent a competitive public procurement process designed to guarantee transparency and equitable pricing. The designated project manager, in conspiracy with specific contractors, rigged the bidding process to guarantee that chosen companies received contracts at exaggerated amounts.

To aid the plan, a web of shell corporations was created in various jurisdictions. These entities collaborated to submit bids in a coordinated manner, fostering a deceptive illusion of competition while guaranteeing that contracts were granted to organizations managed by the corrupt network. After contracts were finalized, excessive payments were issued to these firms, creating unlawful profits. These funds were thereafter channelled through a number of dealings involving affiliated parties, consulting contracts, and subcontracting deals. Payments were validated by accompanying documents like invoices, contracts, and financial records, which seemed authentic but did not indicate true economic activity. At times, money was sent to offshore organizations or passed through middlemen prior to being utilized for asset purchases or subsequently distributed to the participants. From the viewpoint of Independent Accountants and Auditors, the scheme depended significantly on the improper use of corporate frameworks, financial records, and accompanying documents to hide the actual nature of transactions, obscure beneficial ownership, and create an appearance of legitimacy for illegal financial activities.

Key Red Flags

Particular indicators (as listed below, but not limited to), especially when occurring in combination, should serve as alerts:
- Multiple companies participating in a bidding process appear to have overlapping ownership, management, contact details or financial arrangements
- Unusual patterns in procurement documentation suggesting lack of genuine competition (e.g. similar pricing structures, coordinated submissions, or repeated involvement of the same entities)
- Use of shell or recently incorporated companies with no clear operational history participating in large-value contracts.
- Payments supported by consultancy, subcontracting or service agreements that lack clear economic substance or deliverables
- Invoices or financial records that appear standardised, repetitive or inconsistent with the scale and nature of the services claimed
- Funds flowing through multiple entities in quick succession without a clear business rationale
- Cross-border transfers to entities in jurisdictions unrelated to the project or underlying business activity
- Discrepancies between the financial records and the actual progress or substance of the project.

Supervisory Expectations

- Assess whether transactions, contracts and financial arrangements reflect genuine economic activity and are consistent with the customer's business profile
- Apply enhanced scrutiny to customers involved in public procurement, large infrastructure projects or high-value contracts, particularly where multiple related entities are involved
- Examine the ownership and control structure of entities participating in transactions to identify potential links, common control or undisclosed relationships
- Exercise professional scepticism when reviewing invoices, consultancy agreements and subcontracting arrangements, especially where these are used to justify large payments
- Evaluate whether financial flows, including cross-border transfers, are consistent with the underlying business purpose and contractual arrangements
- Where reasonable grounds for suspicion arise, assess whether to file a suspicious transaction / activity report
- Maintain sufficient documentation evidencing the review performed, inconsistencies identified, and conclusions reached in line with a risk-based approach

Case Study 3: <u>Use of Front Companies and Structured Real Estate Transactions to Launder Illicit Proceeds</u>

Synopsis

A person using a fake identity formed a company and set up a bank account to receive funds from overseas, including instructions from third parties. The funds were utilized by the company to acquire a property. Soon after, the business underwent voluntary liquidation, and the person reacquired the asset at an increased price. This allowed the person to funnel illegal money into the financial system and create an appearance of a legitimate capital gain by using a front company in a structured real estate deal.

Key Red Flags

Particular indicators (as listed below, but not limited to), especially when occurring in combination, should serve as alerts:

- *Utilization of a newly formed business with undefined commercial operations to carry out significant transactions.*
- *Monies obtained from various international entities or external directives lacking explicit rationale.*
- *Acquisition and quick reselling or transferring of assets involving connected parties.*
- *Inflated property value without appropriate market rationale.*
- *Liquidation of the company soon after finalizing a significant deal.*
- *Ambiguous or inconsistent advantageous ownership of the entity engaged.*
- *Utilization of corporate frameworks that do not correspond with the individual's evident profile or business objective*

Supervisory Expectations

- *Evaluate if the arrangement and order of transactions have a distinct economic justification and align with the customer's characteristics.*
- *Confirm the rightful ownership and authenticity of funds, especially in international situations.*
- *Implement increased examination of transactions involving newly established entities and property acquisitions.*
- *Recognize trends of rapid asset relocation, liquidation, or value enhancement as possible signs of layering.*
- *When there are valid reasons for suspicion, evaluate the need to file a suspicious transaction / activity report.*
- *Keep records that show the recognition and evaluation of risk indicators in line with a risk-based methodology.*

Case Study 4: <u>Misuse of Professional Customer Account and Corporate Structure for Real Estate Laundering</u>

Synopsis

A firm employed a notary's customer account to buy property, with money being transferred through a chain of cheques and transfers that seemed to align with professional dealings. Nevertheless, the framework facilitated the hiding of the connection between the person and the organization. The scheme was utilized to clean dirty money via property investments, and it was subsequently disclosed that the company's only shareholder was an identified drug dealer.

Key Red Flags

Particular indicators (as listed below, but not limited to), especially when occurring in combination, should serve as alerts:

- *Utilization of customer accounts for routing funds not associated with core professional services.*
- *Transactions organized via intermediaries (e.g. notary accounts) that conceal the actual source or recipient of funds.*
- *Regular cheque transactions and transfers that seem excessive or inconsistent with typical professional practices.*
- *Use of a firm with ambiguous ownership or lacking transparency regarding significant transactions.*
- *Obscurity or ambiguity concerning the connection between the person and the company.*
- *Real estate deals carried out via layered or indirect financing methods.*

Supervisory Expectations

- *Assess if the utilization of professional or customer accounts aligns with valid business objectives.*
- *Verify beneficial ownership of corporate entities engaged in transactions, especially when intermediaries are involved.*
- *Apply increased scrutiny for transactions in which funding pathways are indirect or channelled through intermediaries.*
- *Evaluate if transaction patterns correspond with the anticipated behaviour of the professional account in question.*
- *When there are justifiable reasons for suspicion, evaluate the need to file a suspicious transaction / activity report.*
- *Keep sufficient documentation showing how risks were recognized and evaluated according to a risk-based method.*

Case Study 5: <u>Use of Front Company and Structuring to Launder Proceeds of Tax Fraud</u>

Synopsis

A criminal group produced illegal profits via tax evasion and diverted these funds into a business overseen by the primary perpetrator. The firm, lacking real business operations or staff, was utilized to obtain assets like properties and vehicles to conceal the source of funds. Cash proceeds were organized via several individuals, deposited in smaller sums into bank accounts, and subsequently sent to the company. The firm boosted its facade of legitimacy by asserting VAT refunds associated with property deals, thus generating apparently legal sources of income

Key Red Flags

Particular indicators (as listed below, but not limited to), especially when occurring in combination, should serve as alerts:

- *Utilization of various people to deposit cash in smaller increments (structuring) prior to pooling into a business account.*
- *Cash deposits made, subsequently transferred into a company without a distinct economic justification.*
- *Acquisition of properties or assets that do not align with the company's declared business objectives.*
- *Unjustified or disproportionate VAT refund requests linked to transactions.*
- *Revenue sources that seem to be artificially created or lack genuine business backing*
- *Links between people and businesses that are not explicitly revealed or recorded*

Supervisory Expectations

- *Evaluate if the company's financial actions are consistent with its business model, operational presence, and workforce.*
- *Recognize trends in structured cash deposits and assess their alignment with the customer's profile.*
- *Verify the authenticity of income sources, such as tax returns and revenue from transactions.*
- *Apply enhanced scrutiny when firms are utilized to obtain assets lacking obvious income-generating functions.*
- *Where reasonable grounds for suspicion arise, determine whether to file a suspicious transaction / activity report.*
- *Keep records demonstrating the evaluation of financial transactions, ownership frameworks, and the implementation of a risk-based strategy.*

Case Study 6: <u>Use of multi-jurisdictional companies and charities to launder the proceeds of official corruption</u>

Synopsis

An international company used a network of shell companies, proxy shareholders, and overseas bank accounts to hide corrupt payments made to a public official. Money was sent via subsidiaries and organizations in various jurisdictions before arriving in accounts associated with the beneficial owner. In certain cases, kickbacks were also funnelled through charities linked to government officials. To hide the payments, fake invoices were entered into the accounting books, giving the illusion of valid business dealings.

Key Red Flags

Particular indicators (as listed below, but not limited to), especially when occurring in combination, should serve as alerts:

- *Use of shell companies with proxy shareholders and directors lacking a distinct business purpose.*
- *Cross-border funds movements that pass through various jurisdictions and organizations prior to arriving at the final beneficiary.*
- *Beneficial ownership linked to government employees, public officials, or affiliated individuals.*
- *Donations to charitable organizations or non-profit groups associated with politically exposed individuals or government officials.*
- *Utilization of deceptive, unclear, or unverified invoices to validate payments.*
- *Accounting entries indicating transactions that do not possess real economic significance.*
- *Business structures and payment paths that seem overly complicated for the declared business operations*

Supervisory Expectations

- *Assess whether corporate structures, ownership arrangements and payment flows are commercially justified and transparent*
- *Apply enhanced scrutiny where nominee arrangements, offshore entities or multiple transit jurisdictions are involved*
- *Verify beneficial ownership and identify any links to government employees, PEPs or associated charities*
- *Exercise professional scepticism when reviewing invoices, accounting entries and supporting documentation used to justify payments*
- *Where reasonable grounds for suspicion arise, assess whether to file a suspicious transaction / activity report*
- *Maintain sufficient documentation evidencing ownership verification, transaction review and the application of a risk-based approach*

Case Study 7: <u>Use of Trust Structures and Underlying Companies to Channel Corruption Proceeds</u>

An individual established a trust and an underlying company in an offshore jurisdiction, using a professional service provider as trustee and registered office. Over time, the trust and company received multiple transfers of funds and assets from sources later linked to a corruption and kickback scheme involving government officials. Funds were subsequently distributed to individuals associated with the scheme. The structure enabled the concealment of the origin, ownership and movement of illicit funds through layered legal arrangements and cross-border transactions.

Key Red Flags

Particular indicators (as listed below, but not limited to), especially when occurring in combination, should serve as alerts:

- *Use of trusts and underlying companies without a clear or proportionate commercial rationale*
- *Funds and assets received from multiple or unclear sources into trust or corporate structures*
- *Links between the customer and adverse media, corruption allegations or government officials*
- *Transfers from the structure to individuals associated with high-risk or politically exposed environments*
- *Timing of fund inflows aligning with known or suspected illicit activity*
- *Complex legal arrangements that obscure beneficial ownership and control*
- *Reliance on offshore structures that limit transparency and independent verification*

Supervisory Expectations

- *Apply enhanced scrutiny to customers using trusts, offshore entities or layered legal arrangements, particularly where there is cross-border exposure*
- *Assess whether the structure and flow of funds are consistent with the customer's known profile and stated purpose*
- *Verify the source of funds and source of wealth, especially where funds originate from multiple or unclear sources*
- *Where reasonable grounds for suspicion arise, assess whether to file a suspicious transaction / activity report*
- *Maintain documentation evidencing the timeline analysis, risk assessment and application of a risk-based approach*

8. Glossary of Terms

Term	Definition
Bearer Negotiable Instruments / Cash Equivalents	Monetary instruments that function like cash and allow value transfer without normal banking traceability including cashier's cheques, money orders, postal orders, treasury bills, bearer bonds, bearer negotiable instruments, promissory notes, or similar instruments that can be transferred without identifying the underlying owner. Cash equivalents count toward the AED 55,000 threshold for covered transactions.
Beneficial Owner	The natural person who owns or exercises ultimate effective control over the customer, or the natural person on whose behalf the transactions are conducted; including any person who exercises ultimate effective control over a legal person or legal arrangement, whether directly or through a chain of ownership, control, or other indirect means, and who is identified, whether one or more, in accordance with the Executive Regulations of AML/CFT/CPF Law.
Business Relationship	Any ongoing commercial or financial relationship established between Financial Institutions, Designated Non-Financial Businesses and Professions, and their customers in relation to activities or services provided by them.
Committee	National Committee for Combating Money Laundering and the Financing of Terrorism and Illegal Organisations.
Concerned Authorities	The governmental entities concerned with the implementation of any provision of this Decree by Law within the UAE.
Crime	The crime of Money Laundering and the predicate offences related thereto, or the financing of terrorism, or the proliferation financing.
Customer Due Diligence (CDD)	The process of identifying and verifying the information of a Customer or Beneficial Owner, whether a natural or legal person or a legal arrangement, as well as identifying the nature of their business, the purpose of the business relationship, and the ownership structure and control thereover, including ongoing monitoring procedures.
Customer	Any natural or legal person, or legal arrangement, who establishes or seeks to establish a business relationship with Financial Institutions, any of the Designated Non-Financial Businesses and Professions, or Virtual Asset Service Providers.
Designated Non-Financial Businesses and Professions (DNFBPs)	Any person engaged in one or more of the commercial or professional activities or businesses, as specified in the Executive Regulations of AML/CFT/CPF Law.
Egmont Group	The Egmont Group is an intergovernmental body of 159 Financial Intelligence Units (FIUs), which provides a platform for the secure exchange of expertise and financial intelligence to combat money laundering and the financing of terrorism (ML/TF).
Executive Office	The Executive Office for Control and Non-Proliferation, concerned with the implementation of targeted financial sanctions within the UAE.
Executive Regulations or AML/CFT/CPF Resolutions	Cabinet Resolution No. (134) of 2025 Regarding the Executive Regulations of Federal Decree by Law No. (10) of 2025 Regarding Anti-Money Laundering, and Combating the Financing of Terrorism and Proliferation Financing

Term	Definition
FATF	The Financial Action Task Force is an inter-governmental body that sets international standards and promotes effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system.
Freezing	The taking of an action without prior notice or involvement of the owner, Customer, or the affected Party.
FSRBs	FATF-Style Regional Bodies are regional intergovernmental organisations which promote and assess the implementation of internationally accepted AML/CFT policies and regulations.
Financial Group	A group of financial institutions that consists of holding companies or other legal persons exercising the control over the rest of the group and coordinating functions for the application of supervision on the group, branch, and subsidiary level, in accordance with the international core principles for financial supervision, and AML/CFT policies and procedures.
Financial Institution	Any person engaged in one or more financial activities or operations determined by the Executive Regulations of the AML/CFT/CPF Law, on behalf of or for the benefit of a customer.
Financing of Terrorism	Any of the acts defined in Clause (1) of Article (3) of the AML/CFT/CPF Law.
FIU	Financial Intelligence Unit
Funds	Assets or properties, however acquired, of any type or form, tangible or intangible, movable or immovable, electronic, digital, or cryptographic, including national and foreign currencies, legal documents, and instruments of whatever form, including electronic or digital forms, evidencing the ownership of such assets or properties, or shares or rights therein; as well as economic resources deemed as assets of any kind, including oil and other natural resources and all rights pertaining thereto, whatever their value or means of acquisition; together with bank credits, cheques, payment orders, shares, securities, bonds, bills of exchange, letters of credit, and any proceeds, profits, or other income derived or resulting therefrom, which may be used to obtain any financing, goods, or services.
High Risk Customer	A customer who represents a risk either in person, activity, Business Relationship, nature or geographical area, such as a customer from a high-risk country or non-resident in a country that does not hold an identity card, or a costumer having a complex structure, performing complex operations or having unclear economic objective, or who conducts cash-intensive operations, or operations with an unknown third party, or operations without directly confronting any other high risk operations identified by Financial Institutions, or Designated Non-Financial Businesses and Professions, or the Supervisory Authority.
Illegal Organisations	Organisations whose establishment is criminalised or which exercise a criminalised activity.
Intermediary Account	Corresponding account used directly by a third party to conduct a transaction on its own behalf.
Intermediary / Third-Party Payer or Recipient	A person or entity (other than the customer or supplier) used to make or receive payments, collect goods, or execute parts of a transaction. Use of intermediaries without clear commercial rationale is a red-flag indicator of ML/TF/PF risk.

Term	Definition
Law (or "AML/CFT/CPF Law")	Federal Decree by Law No. (10) of 2025 Regarding Anti-Money Laundering, and Combating the Financing of Terrorism and Proliferation Financing
Law Enforcement Authorities	The federal and local authorities entrusted, pursuant to the provisions of AML/CFT/CPF Law and their applicable legislation, with combating, investigating, detecting, and gathering evidence in respect of the offenses, including Money Laundering, Predicate Offences, the Financing of Terrorism, and the Proliferation Financing.
Legal Arrangement	Trusts or other similar arrangements.
MENAFATF	MENAFATF is a FATF-Style Regional Body (FSRB), for the purpose of fostering co-operation and co-ordination between the countries of the MENA region in establishing an effective system of compliance with international AML/CFT standards. The UAE is one of the founding members of MENAFATF.
Means	Any means used or intended to be used for the commitment of an offence or felony.
Money Laundering	Any of the acts defined in Clause (1) of Article (2) of the AML/CFT/CPF Law, including its commission through digital systems, Virtual Assets, or cryptographic technologies.
Non-Profit Organisations (NPOs)	Any organized group of a continuing nature for a definite or indefinite duration, consisting of natural or legal persons or a legal arrangement, not aimed at profit, which collects, receives, or disburses funds for charitable, religious, cultural, educational, social, solidarity, or other purposes that fall within the scope of benevolent acts.
Politically Exposed Persons (PEPs)	Natural persons who are or have been entrusted with prominent public functions in the UAE or any other foreign country such as Heads of States or Governments, senior politicians, senior government officials, judicial or military officials, senior executive managers of state-owned corporations, and senior officials of political parties and persons who are, or have previously been, entrusted with the management of an international organisation or any prominent function within such an organisation; and the definition also includes the following: 1. Direct family members (Of the PEP, who are spouses, children, spouses of children, parents). 2. Associates known to be close to the PEP, which include: a- Individuals having joint ownership rights in a legal person or arrangement or any other close Business Relationship with the PEP. b- Individuals having individual ownership rights in a legal person or arrangement established in favour of the PEP.
Predicate Offense	Any act constituting a felony or misdemeanour, including the financing of terrorism, the proliferation financing, and evasion of direct and indirect taxes, in accordance with the applicable legislation of the UAE, whether committed within or outside the UAE, provided that such an act is punishable in both countries.
Proceeds	Funds derived, directly or indirectly, from the commission of any felony or misdemeanour, including profits, privileges, economic interests, and other benefits derived therefrom, and any equivalent Funds that have been converted, in whole or in part, into other Funds.

Term	Definition
Proliferation	The illicit and unauthorized trade, as regulated under the applicable legislation in the UAE, in materials, systems, equipment, components, programs, or technology contributing to the production or development of Weapons of Mass Destruction, related technology, or their delivery means, including any act stipulated in Clause (3) of Article (3) of this Decree by Law.
RBA	A Risk-Based Approach is a method for allocating resources to the management and mitigation of ML/TF/PF risk in accordance with the nature and degree of the risk.
Registrar	The competent authority responsible for supervising the economic or trade register of the various types of establishments registered in the UAE, as regulated by the legislation in force in the UAE.
Sanctions Committee	The UN Security Council Committee established as per resolution numbers 1988 (2011), 1267 (1999), 1989 (2011), 2253 (2015), 1718 (2006) and all other related resolutions.
Sanctions List	A list wherein individuals and terrorist organisations, which are subject to the Sanctions imposed as per the Security Council Sanctions Committee are listed, along with their personal data and the reasons for Listing.
Settlor	A natural or legal person who transfers the management of their own Funds to a Trustee pursuant to a Trust Instrument.
Shell Bank	Bank that has no physical presence in the country in which it is incorporated and licensed and is unaffiliated with a regulated financial group that is subject to effective consolidated supervision.
Supervisory Authority	The federal and local authorities entrusted under the legislation with the supervision of the financial institutions, designated non-financial businesses and professions, virtual asset service providers, and non-profit organizations (NPOs); or the competent authorities responsible for granting approval to engage in an activity or profession, where no specific supervisory authority is designated by the legislation.
Suspicious Transactions	Transactions involving funds for which there are reasonable grounds to suspect that they constitute Proceeds of any felony or misdemeanour, or are related to Money Laundering, Financing of Terrorism, or Proliferation Financing, whether such transactions were executed or merely attempted.
Terrorist	Any natural person, whether within or outside the UAE, who intentionally commits any of the following acts: 1. Commits or attempts to commit a Terrorist Act by any means, whether directly or indirectly. 2. Participates as an accomplice in a Terrorist Act. 3. Organizes a Terrorist Act or incites others to commit it. 4. Participates with a group of persons acting with a common intent to commit a Terrorist Act for the purpose of expanding terrorist activity or to commit such act, knowing the group's intention.
Terrorist Organization	A group of two or more persons, whether within or outside the UAE, that has committed a terrorist act, directly or indirectly, or has threatened to commit it, aims, plans, or seeks to commit it, or promotes or participates in its commission, whether directly or indirectly, regardless of its name, form, place of establishment, location, activity, or the nationality or residence of its members; including any organization recognized as a Terrorist Organization under any other law.

Term	Definition
Targeted Financial Sanctions (TFS)	The freezing of funds and the prohibition of making them available, directly or indirectly, for the benefit of any natural or legal person or organization designated by resolutions issued by the Cabinet regarding Terrorist Lists, or by the United Nations Security Council under Chapter VII of the Charter of the United Nations concerning the prevention and suppression of terrorism and its financing, as well as the prevention, suppression, and halting of proliferation and its financing.
Trade-Based Money Laundering (TBML)	The process of disguising the proceeds of crime and moving value through trade based transactions, including under/over invoicing, misrepresentation of quality, false documentation, layering through involvement of multiple intermediaries.
Transaction	Any disposal or utilization involving Funds or Proceeds, including, inter alia, deposit, withdrawal, transfer, sale, purchase, lending, exchange, mortgage, or donation.
Trust	A legal relationship whereby the Settlor places Funds under the control of a Trustee for the benefit of a Beneficiary or for a specific purpose, and such Funds are deemed separate from the Trustee's own property, while the title thereto remains in the name of the Settlor or another person on behalf of the Settlor.
Trustee	A natural or legal person vested with the rights and powers granted thereto by the Settlor or by the Trust, authorized thereby to manage, utilize, and dispose of the Settlor's Funds in accordance with the conditions imposed by either of them.
Virtual Assets	Digital representation of value that may be digitally traded or transferred and may be used for payment or investment purposes, excluding digital representations of fiat currencies, securities, or other Funds.
Weapons of Mass Destruction	Weapons capable of inflicting harm on a large number of persons and posing a threat to human life and the natural environment through their catastrophic effects, such as nuclear, biological, chemical, or radiological weapons.
Without Prior Notice	The taking of an action without prior notice or involvement of the owner, Customer, or the affected Party.
Virtual Asset Service Providers (VASPs)	Any natural or legal person who, as a commercial activity, conducts one or more of the virtual asset activities specified in the Executive Regulations of this Decree by Law or conducts transactions related thereto, on behalf of or for the benefit of another natural or legal person.
Wire Transfer	Financial transaction conducted by a Financial Institution or through an intermediary institution on behalf of a transferor whose funds are received by a beneficiary in another financial institution, whether or not the transferor and the beneficiary are the same person.